KOMPONENTOWA BUDOWA SYSTEMÓW INFORMACYJNYCH 2022/V

Założenia elastycznej i bezpiecznej budowy komponentowej systemów informacyjnych

pawel.walczak@microsoft.com

Warszawa, 2022

SPIS TREŚCI

Informacje zawarte w niniejszym dokumencie przedstawiają aktualną ocenę przedstawianych zagadnień w dacie sporządzenia tego dokumentu i mogą one ulec zmianie w każdym czasie, bez zawiadamiania Państwa. Niniejszy dokument oraz informacje w nim zawarte są przekazywane w STANIE, w JAKIM SIĘ ZNAJDUJĄ i wyłącza się odpowiedzialność z tytułu jakiejkolwiek rękojmi, gwarancji czy zapewnień. Niniejszy dokument nie stanowi i nie powinien być interpretowany, jako oferta ani jako zaciągnięcie jakiegokolwiek zobowiązania. Ponadto, nie gwarantuje się, że przedstawione w nim informacje są dokładne. AUTOR NIE SKŁADA w NINIEJSZYM DOKUMENCIE ŻADNYCH ZAPEWNIEŃ ANI NIE UDZIELA ŻADNYCH GWARANCJI, ZARÓWNO WYRAŹNYCH JAK i DOMNIEMANYCH.

Opisy produktów osób trzecich zawarte w niniejszym dokumencie są przekazywane wyłącznie dla Państwa wygody. Ponadto, opisy mają na celu przedstawienie ogólnych informacji, które mają raczej ułatwić orientację, niż przekazać pełną informację.

W celu uzyskania wiążących opisów takich produktów należy skontaktować się z ich producentami.

Niniejsze materiały są przekazywane w STANIE, w JAKIM SIĘ ZNAJDUJĄ i AUTOR WYŁĄCZA ODPOWIEDZIALNOŚĆ z TYTUŁU JAKIEJKOLWIEK RĘKOJMI, GWARANCJI CZY ZAPEWNIEŃ.

Wszystkie znaki towarowe stanowią własność właściwych podmiotów.

Zezwala się na rozpowszechnianie i cytowanie całości i fragmentów niniejszego dokumentu pod warunkiem podania źródła cytatów.

Microsoft oraz nazwy produktów Microsoft są zarejestrowanymi znakami towarowymi lub znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Nazwy istniejących spółek i produktów przywołane w niniejszym dokumencie mogą być znakami towarowymi należącymi do ich odpowiednich właścicieli.

1. WSTĘP

Wobec ciągłych zmian w technologiach teleinformatycznych i zmianie modelu dostarczania usług większości producentów oprogramowania standardowego i usług standardowych (Dostawców[1]) powstaje konieczność zastosowania nowego podejścia do budowy rozwiązań wspierających działalność podmiotów, zgodnego z wymogami prawa, efektywnego i odpowiadającego na potrzeby użytkowników. Niniejsze opracowanie jest podsumowaniem kluczowych zaleceń i dobrych praktyk w zakresie budowy systemów otwartych, tanich w budowie i utrzymaniu oraz umożliwiających rozbudowę i zmiany przy rozsądnych kosztach.

W opracowaniu przyjęto następujące kryteria tworzenia założeń dla komponentowego systemu:

- Sprawne i skuteczne funkcjonowanie, przyczyniające się w znaczący sposób do wysokiego poziomu zadowolenia obywateli, przedsiębiorców i użytkowników wewnętrznych i zewnętrznych.
- Przyjazność i łatwość obsługi systemu dla użytkowników.
- Możliwość szerokiej i elastycznej konfiguracji systemu bez konieczności ingerencji Wykonawcy[2] czy Dostawcy.
- Zachowanie niskich kosztów wytworzenia systemu, a przede wszystkim zapewnienie niskich i przewidywalnych kosztów późniejszej eksploatacji.
- Zapewnienie bezpieczeństwa systemu, zarówno w zakresie jego dostępności, jak i bezpieczeństwa danych i zarządzania uprawnieniami użytkowników.
- Zapewnienie mechanizmów integracji z systemami zewnętrznymi,
- Zachowanie pełnej zgodności z wymaganiami prawa.
- Wykorzystanie w maksymalnym stopniu wdrożonych już komponentów teleinformatycznych.

[1] Dostawca – producent oprogramowania standardowego i pakietów usług standardowych powszechnie dostępnych na rynku – Produktów
[2] Wykonawca – podmiot realizujący przedmiot zamówienia publicznego - kontrahent Zamawiającego.

- Oparcie się na standardowych komponentach (*COTS*[3]) ograniczających czas i ryzyko wdrożenia oraz koszt utrzymania systemu.
- Uniezależnienie się od konkretnego wykonawcy w przypadku dalszych modyfikacji czy rozwoju systemu poprzez zastosowanie powszechnie dostępnych rozwiązań.

Niezwykle istotnym założeniem jest budowa systemu w postaci funkcjonalności szkieletowych, które mogłyby być uzupełniane poprzez specjalizowane aplikacje dziedzinowe różnych dostawców.

W pierwszej części opracowania poruszone zostaną założenia funkcjonalne, a w drugiej założenia komponentów architektury systemów, które te założenia pozwolą zrealizować.

Jednocześnie opracowanie bierze pod uwagę zalecenia Komisji Europejskiej w zakresie tworzenia jednolitego rynku cyfrowego. Należy też zauważyć wiele zbieżności z promowaną przez Ministra Cyfryzacji koncepcją Wspólnej Infrastruktury Informatycznej Państwa (WIIP[4]).

Szanowni Państwo,

W związku z tym, że w tekście opracowania znajduje się wiele przypisów w postaci hiper-linków zaleca się korzystanie z wersji elektronicznej dokumentu.

3 Commercial Off the Shelf –Produkt standardowy „z półki"
4 https://www.gov.pl/web/cyfryzacja/wspolna-infrastruktura-panstwa-wip-20

2. ZAŁOŻENIA FUNKCJONALNE

Założeniem niniejszego dokumentu jest przedstawienie wizji szkieletowego, komponentowego systemu (dalej nazywanego Platformą) realizującego podstawowe, powszechnie wymagane funkcjonalności, w którym mogą być osadzane aplikacje dziedzinowe, niezależnie od ich poziomu komplikacji czy użytej technologii. Takie założenie wymaga spełnienia kilku warunków poprzez te osadzane czy integrowane aplikacje. Muszą one posługiwać się uznanymi, powszechnymi i otwartymi standardami komunikacji oraz muszą pozwalać na wykorzystanie spójnych dla całego systemu mechanizmów definiowania i udostępniania profili użytkowników, ich uprawnień oraz sposobu uwierzytelniania. Niezależnie od posiadanych obecnie rozwiązań, konieczne jest zaplanowanie i wytworzenie obrazu docelowej architektury, który (konsekwentnie realizowany) pozwoli na potraktowanie całości posiadanych zasobów IT, jako jednego, spójnego, rozliczalnego, zarządzalnego i bezpiecznego systemu.

2.1. CO TO JEST ARCHITEKTURA KOMPONENTOWA?

Zwykle pojęcie architektury komponentowej (*Component Architecture*) stosowane jest w kontekście programowania obiektowego, w którym program jest zestawem generycznych komponentów o określonej funkcjonalności i interfejsach.

W niniejszym opracowaniu poszerzamy zakres tej definicji rozszerzając ją na warstwę sprzętową, procesową i usługową.

Za architekturę komponentową systemu informacyjnego uważamy oparcie się o generyczne komponenty sprzętowe, programowe, procesowe i usługowe o dobrze zdefiniowanej funkcjonalności i interfejsach, które pozwalają budować rozwiązania złożone poprzez wielokrotne użycie komponentów w ramach różnych scenariuszy funkcjonalnych.

Jak widać definicja ta najlepiej pasuje do modelu opartego o Produkty, a więc komponenty standardowe.

Dlaczego takie podejście wydaje się kluczowym dla planowania budowy czy rozbudowy systemów informacyjnych?

Historia znanych, dużych projektów teleinformatycznych, których założeniem było zbudowanie skomplikowanych, dedykowanych rozwiązań wskazuje, że były one kosztowne we wdrożeniu, czas ich wdrożenia był bardzo długi i zwykle przekraczał założone terminy. Takie systemy są też zwykle kosztowne w eksploatacji i często wymagają interakcji z ich wykonawcą w przypadku jakichkolwiek problemów czy konieczności modyfikacji.

Architektura komponentowa pozwala na znaczne ograniczenie ryzyka i czasu wdrożenia poprzez wykorzystanie standardowych, sprawdzonych rozwiązań, które są dobrze udokumentowane i znane szerokiemu gronu potencjalnych wykonawców. Dobrym porównaniem może być budowa sprzętu komputerowego – na przykład serwerów. Nikt nie ryzykuje projektów samodzielnej budowy serwera pod potrzeby konkretnego projektu. Oczywistym jest, że byłby to pomysł kosztowny, czasochłonny i ryzykowny, choć na końcu mógłby dostarczyć wymarzoną funkcjonalność sprzętową, idealnie pasującą do założonych celów. Dodatkowym efektem takiego dedykowanego projektu byłoby całkowite uzależnienie od jego wykonawcy i brak możliwości zastąpienia go jakimkolwiek standardowym komponentem.

Dla warstwy sprzętowej, są to stwierdzenia oczywiste. Dlaczego więc nie zastosować ich dla całości systemu informacyjnego?

Model komponentowy odnosi się nie tylko do warstw sprzętu i oprogramowania. z powodzeniem stosowany jest również w przypadku usług czy strukturalnie opisanej informacji. Dobrym przykładem może być podejście związane z architekturą SOA (*Service Oriented Architecture*), gdzie w praktyce okazało się, że nie da się stworzyć dedykowanych usług dla każdego procesu. Natomiast możliwe jest stworzenie zbioru prostych, reużywalnych usług atomowych, na bazie których budowane są usługi złożone.

Podobne założenia zostały zrealizowane przez firmę ResultMaker dla celów zarządzania wzorami dokumentów elektronicznych (schematów XML) w skali całego państwa[5]. Tworzenie wzorów dokumentów (szablonów) na bazie atomowych schematów XML, utrzymywanych przez różnych dostawców, okazało się jedynym rozwiązaniem zarządzalnym od strony organizacyjnej i technicznej.

[5] http://english.virk.dk/home.html

Następnym przykładem koncepcji komponentowej jest architektura trójwarstwowa z jasno i precyzyjnie wyodrębnionymi warstwami prezentacji, logiki i danych.

Zastosowanie koncepcji architektury komponentowej niesie jednak za sobą pewne ograniczenia.

- Po pierwsze, nie zawsze funkcjonalność pokrywa 100% naszych oczekiwań - jak zwykle w przypadku rozwiązań generycznych. Natomiast bilans kosztów i efektu wskazuje na słuszność takiego podejścia.
- Po drugie, przyjęcie założeń architektury komponentowej wymaga konsekwencji w dłuższym czasie. Nie opłaca się budować jednej części systemu w oparciu o standardowe komponenty, a innej jako tzw. dedykowany system zintegrowany. w takim przypadku trudno nawet będzie zaobserwować ogólny skutek finansowy czy funkcjonalny.

3. ZAŁOŻENIA ARCHITEKTURY

Każdy z opisanych komponentów zawiera propozycję realizacji zdefiniowanych uprzednio założeń w postaci konkretnych rozwiązań komponentowych w oparciu o technologię Microsoft. Zaproponowane zostały produkty, które w pełni realizują postulaty architektury korporacyjnej oraz minimalizacji ryzyk projektowych. Uzyskanie założonych funkcji jest w większości przypadków możliwe raczej poprzez konfigurację oprogramowania niż dokonywanie skomplikowanych, czasochłonnych i ryzykownych projektowo prac programistycznych.

Zakłada się, że do realizacji systemu komponentowego niezbędne będą następujące elementy składowe wspomagające:

- standaryzacja interfejsu użytkowników,
- wspomaganie pracy grupowej,
- metodyki i oprogramowanie wspomagające zarządzanie projektami,
- metastandard dokumentów elektronicznych w tym danych przestrzennych i opisowych,
- wykorzystanie zasad interoperacyjności usług opartych na standardach przemysłowych,
- wprowadzenie mechanizmów i standaryzacja zasad bezpieczeństwa w systemach teleinformatycznych.

Wszystkie prace prowadzone w ramach projektowania systemów powinny zostać przeprowadzone z poszanowaniem minimalnych wymagań dla systemów informatycznych[6]. Wszystkie użyte narzędzia informatyczne muszą być zgodne z zapisami prawa polskiego i powszechnymi normami, na przykład ISO, WCAG czy W3C.

3.1. PODSTAWY ARCHITEKTURY

Architektura planowanego systemu teleinformatycznego powinna zapewnić:

- oparcie się o strategiczne założenia funkcjonalne, prawne i organizacyjne,

[6] *KRI - https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20170002247 https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160001744/O/D20161744.pdf*

- wprowadzenie priorytetu bezpieczeństwa i dostępności usług,
- zapewnienie wymaganego kształtowania procesów i obsługiwanych procedur,
- wykorzystanie zasad otwartej architektury zbudowanej na standardach przemysłowych umożliwiające swobodny przepływ informacji, interoperacyjność i elastyczną rozbudowę systemu,
- użycie rozpowszechnionych narzędzi (interfejsów) w celu przyspieszenia cyklu szkoleń,
- zachowanie rozsądnych i przewidywalnych kosztów budowy systemu, a przede wszystkim – jego utrzymania i rozbudowy,
- uzyskanie szybkiego efektu ekonomicznego i społecznego,
- zachowanie skalowalności rozwiązania – od jednej grupy usług do całościowego rozwiązania wdrażanego etapowo,
- zagwarantowanie możliwości wyboru spośród wielu Wykonawców posługujących się daną technologią.

Technicznie projekt powinien zakładać:

- fizyczną realizację założeń interoperacyjności i architektury korporacyjnej,
- modularną budowę systemu,
- oparcie się o standardowe, gotowe komponenty w tym: bazy i hurtownie danych, portale wewnętrzne i zewnętrzne oraz odpowiednią infrastrukturę telekomunikacyjną.

W zakresie wymiany danych pomiędzy systemami teleinformatycznymi zaplanowane powinno być wykorzystanie plików i usług sieciowych wykorzystujących język XML. Dane publikowane w Internecie powinny być sformatowane przy pomocy języka HTML. Dokumenty elektroniczne zostaną zdefiniowane na podstawie schematów plików XML, oparte na strukturach XML i zrenderowane za pomocą plików XSLT do postaci HTML.

Dodatkowym wymogiem jest wykorzystanie istniejących, zgodnych z w sposobie działania z istniejącym prawem (w tym z rozp. eIDAS), komponentów umożliwiających:

- złożenie i weryfikację podpisu elektronicznego w oparciu o certyfikaty gwarantujące zgodnie z prawem niezaprzeczalność treści i działań,
- wykorzystanie standardowych pakietów biurowych jako interfejsów do współpracy z systemami obiegu informacji w zakresie wypełniania formularzy czy standardowych dokumentów opartych na przygotowanych szablonach z wewnętrznych repozytoriów.

Niezwykle ważnym założeniem jest zbudowanie i konsekwentne wykorzystanie w całym systemie ogólnie dostępnych modeli i standardów interoperacyjności zapewniających bezproblemowy przepływ informacji. Dlatego też przyjęto model wykorzystania wbudowanych w produkty Microsoft narzędzi zapewniających komunikację poprzez otwarte standardy oraz wykorzystanie założeń interoperacyjności zgodnych z założeniami EIF[7] oraz założeniach ISA[8].

Takie podejście umożliwia budowę i rozwój systemu w oderwaniu od konkretnych technologii oraz zachowanie konsekwentnie zasad architektury korporacyjnej. z uwagi na szeroki zakres i różnorodność wdrożeń, nie jest możliwe na przeprowadzenie pełnej analizy dotyczącej szczegółowego projektu technicznego na poziomie studium wykonalności.

Szczegółowe założenia dotyczące struktury komponentów systemu, przepływów danych, konfiguracji interfejsów komunikacyjnych oraz analizy danych i raportowania powinny być opracowane i przedstawione przez wykonawcę do akceptacji w pierwszej fazie wdrożenia systemu.

3.2. INFRASTRUKTURA WŁASNA I Z CHMURY

Rozwiązania z chmury, często zawierające się w określeniu „*Cloud*" stają się coraz częściej najbardziej oczekiwaną drogą uzyskania wspomagania działań statutowych poprzez technologię IT.

[7] *European Interoperability Framework - https://ec.europa.eu/isa2/eif_en*
[8] *Interoperability solutions for public administrations, businesses and citizens - Homepage | ISA² (europa.eu)*

Dla uporządkowania pojęć proponujemy definicję przetwarzania w chmurze (*Cloud computing*) zdefiniowaną w ISO/IEC DIS 17788[9].

Jest to udostępnianie sieciowego dostępu do skalowalnego, elastycznego i współdzielonego zasobu fizycznego lub wirtualnego umożliwiające samoobsługę i wsparcie administracyjne.

Inną definicję podaje National Institute of Standards and Technology[10].

W opracowaniu przyjęto definicje opublikowane w Uchwale Rady Ministrów z dania 11 września 2019 w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”[11].

Korzystanie z usług w chmurze staje się coraz bardziej popularne z kilku powodów:

- Uniezależniamy się od miejsca dostępu. Zwykle usługi takie osiągalne są za pomocą dostępu zdalnego przez intranet lub via Internet. Pozwala nam to dostarczyć usługę niezależnie od lokalizacji użytkownika.
- Zwykle, tego typu rozwiązania udostępniają na żądania mechanizmy typu samoobsługowego.
- Znacznie redukujemy czas, koszt i ryzyko wdrożenia usługi.
- Rozwiązania bazujące na usługach chmury są zwykle bardzo elastyczne i skalowalne, umożliwiając obsługę w momentach zwiększonego zapotrzebowania na moc obliczeniową.
- Użycie usług z chmury jest mierzalne i pozwala w łatwy sposób przewidzieć koszt wykorzystania takiego środowiska.
- Oprócz oczywistych aspektów, w modelu takim możemy uzyskać parametry, na które w modelu klasycznym nie wystarczyłoby budżetu i innych zasobów, takie jak:

  wysoka dostępność usług,

  · wysoko kwalifikowany personel pracujący w trybie 24/7,

  · bardzo wysoki poziom bezpieczeństwa,

[9] *ISO/IEC DIS 17788 | Resolution ITU-T X.ccdef - ISO - ISO/IEC 17788:2014 - Information technology — Cloud computing — Overview and vocabulary*
[10] *http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*
[11] *http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190000862*

- zaawansowane i konfigurowalne plany zachowania ciągłości biznesowej,
- stały rozwój technologiczny systemu pozwalający na minimalizację tzw. długu technologicznego, często występującego we własnych rozwiązaniach na skutek nieodnawiania na czas posiadanej technologii.

W przypadku decyzji o wykorzystaniu komponentów z chmury mamy obecnie kilka różnych modeli pozyskania usług.

Są to usługi pochodzące z chmury publicznej, chmury prywatnej lub rozwiązań hybrydowych.

Poniżej zamieszczamy definicję tych pojęć[12]:

Chmura publiczna –usługi dostępne poprzez Internet, dostarczane z centrum przetwarzania danych dla dowolnych użytkowników, oferująca usługi standardowe o precyzyjnie określonym zakresie funkcjonalności i sposobie działania.

Chmura prywatna –usługi dostępne poprzez sieć, dostarczane z centrum przetwarzania danych przedsiębiorstwa lub instytucji dla własnych pracowników i wybranych podmiotów, oferująca dowolne usługi platformowe, standardowe i dedykowane (wytwarzane na zamówienie).

Rozwiązanie hybrydowe – usługi oferowane na bazie współpracujących systemów z chmury i infrastruktury własnej (*on-premise*).

W przypadku chmury publicznej, oferowanej przez podmioty komercyjne, możemy zwykle wybierać z dwóch podstawowych typów takich usług:

- usług platformowych,
- usług standardowych.

Usługi platformowe mogą być świadczone na bazie platformy systemowej, z możliwością osadzania własnych maszyn wirtualnych czy aplikacji użytkowników w gotowym, bezpiecznym i wydajnym środowisku serwerowym. Taka usługa zapewnia podstawową platformę systemową dla osadzania dowolnych aplikacji klientów, zarówno istniejących jak i nowych, powstających na skutek realizacji projektów lokalnych.

[12] *Model usług z chmur prywatnych jako nowe podejście do informatyzacji, Paweł Walczak 2012.*

Usługi standardowe pozwalają na dostarczenie ich jako dobrze zdefiniowanego, gotowego i przewidywalnego w koszcie rozwiązania, o następujących właściwościach:

- precyzyjne określenie końcowej funkcjonalności,
- obniżenie ryzyka projektowego,
- redukcja czasu i kosztu wdrożenia,
- mierzalny i przewidywalny koszt,
- konkretne metryki w zakresie wydajności i bezpieczeństwa,
- wykorzystanie zaawansowanych standardów przy rozsądnym koszcie.

Trzeba jednak pamiętać o tym, że usługi standardowe mają swoje ograniczenia:

- trudno jest negocjować jakiekolwiek zmiany w ich działaniu,
- należy czasem zrezygnować z części założeń lub je zmodyfikować mając na uwadze wymienione wyżej korzyści.

Usługi dedykowane - budowane są dla konkretnego użytkownika z wykorzystaniem wspólnej infrastruktury techniczno-organizacyjnej i są ściśle dopasowane do jego wymagań. Mogą one zaadresować całość naszych wymagań, ale za to są:

- bardziej czasochłonne i kosztowne na etapie wdrożenia,
- zwykle droższe w utrzymaniu,
- niosą za sobą większe (choć zwykle mniejsze niż w implementacji klasycznej) ryzyko projektowe.

Alternatywnym dla chmury publicznej podejściem jest budowa tzw. chmury prywatnej. Polega ono na stworzeniu przez wybraną organizację (rządową lub komercyjną) ośrodków przetwarzania i składowania danych udostępnianych innym jednostkom. w ramach takiego rozwiązania można zdefiniować usługi platformowe, standardowe oraz dedykowane.

Wykorzystanie modelu chmury prywatnej jest celowe, gdy:

- dane nie mogą być przetwarzane i przechowywane poza strukturami np. rządowych jednostek (dane niejawne),

- istnieje potencjalnie duża grupa odbiorców usług chmury prywatnej o podobnych, nietypowych i nieosiągalnych w chmurze publicznej potrzebach.

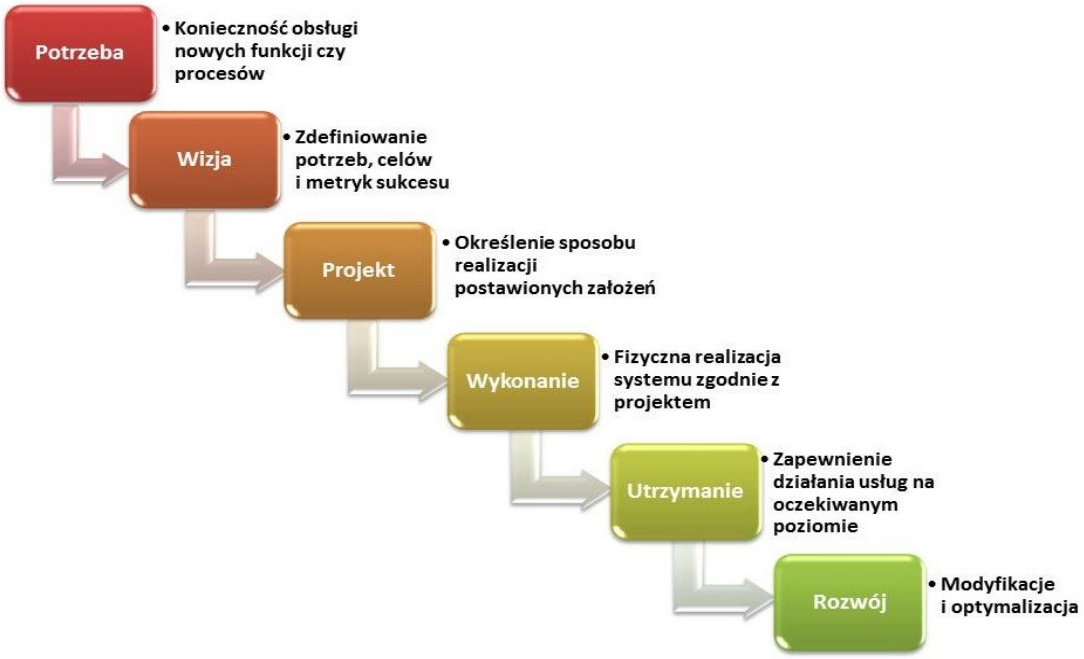
3.2.1. WYBÓR SPOSOBU REALIZACJI ZAŁOŻEŃ

Wybór sposobu realizacji systemów wspomagających działanie danej jednostki każdorazowo należy poprzedzić analizą, w trakcie której trzeba ustalić:

- precyzyjny zakres potrzeb i oczekiwanych funkcjonalności,
- cel wprowadzenia nowych rozwiązań,
- metryki sukcesu, które wykorzystane będą do oceny przydatności i efektywności nowych rozwiązań,
- zgodność z obowiązującym prawem w tym zasadami bezpieczeństwa,
- potencjalny zakres wykorzystania już działających systemów i procedur,
- wykonalność w określonym czasie i budżecie,
- potencjalny koszt utrzymania nowego rozwiązania.

Szczególnie ten ostatni punkt wymaga wielokrotnej analizy na różnych etapach wdrożenia, a bardzo często jest traktowany jako drugoplanowy lub wręcz pomijany. Prowadzić to może do sytuacji, w której nowy system zostanie oddany i uruchomiony w ramach istniejących i zatwierdzonych środków inwestycyjnych, natomiast jego utrzymanie może okazać się wielokrotnie droższe i nieuzasadnione z punktu widzenia efektów jego działania. Tutaj dużą przewagę mają systemy oparte na rozwiązaniach hostowanych (z chmury), pozwalające z dużym prawdopodobieństwem ocenić koszty ich utrzymania.

Typowy cykl budowy rozwiązań teleinformatycznych można przedstawić w uproszczeniu w następujący sposób.



Takie podejście jest typowe zarówno w odniesieniu do systemów budowanych w oparciu o własne zasoby i infrastrukturę jak i systemów czy ich komponentów pozyskiwanych jako usługa.

Pomiędzy modelem lokalnym i zdalnym wykorzystywania komponentów systemu istnieje kilka zasadniczych różnic odnoszących się do wszystkich, oprócz dwóch pierwszych, etapów powstawania systemu. Projekt jest decydującym etapem, na którego poziomie trzeba podjąć decyzje dotyczące możliwości skorzystania z komponentów hostowanych, współistniejących z własnymi rozwiązaniami lub też zamówienia całej funkcjonalności - jako usługi. Proces decyzyjny powinien brać pod uwagę zaadresowanie i ocenę w zakresie wszystkich etapów projektu (od wizji do rozwoju) oraz uwzględniać analizy ekonomiczne, osadzenia projektu w konkretnym budżecie i czasie, spełnienia założeń funkcjonalnych i maksymalnego ograniczenia ryzyka.

Wybór usługi hostowanej powinien jednak uwzględniać:

- gwarancje Dostawcy w zakresie bezpieczeństwa danych i dostępności systemu potwierdzone niezależnymi certyfikatami i audytami,
- możliwość integracji z własnymi systemami,
- doświadczenie usługodawcy w świadczeniu tego typu usług.

3.2.2. USŁUGI Z CHMURY

W wielu organizacja udało się wytworzyć w ostatnich latach nowoczesne, a jednocześnie wymagające stosunkowo niskich nakładów usługi teleinformatyczne, oparte o klasyczną technologię Microsoft wdrożoną we własnych centrach przetwarzania (DC).

Obserwując trendy rynkowe, przykłady wdrożeń oraz wytyczne rządowe i unijne w zakresie sposobu realizacji wdrożeń systemów teleinformatycznych rysuje się koncepcje dalszej rozbudowy usług w oparciu o tzw. chmurę hybrydową – a więc rozszerzenie dotychczasowej platformy o usługi hostowane.

Szczególnie przydatną do realizacji takiego założenia okazała się hostowana usługa platformowa firmy Microsoft – Azure[13], która spełnia wszystkie wymienione w opracowaniu warunki.

Usługa Azure pozwala na uruchamianie nowych rozwiązań standardowych i dedykowanych – dostarczanych przez różnych wykonawców po znacznie niższych kosztach w stosunku do modelu klasycznego, wymagającego projektów technicznych infrastruktury, jej budowy, dostaw sprzętu i oprogramowania, kosztownego utrzymania wymagającego znacznego zwiększenia liczby etatów administratorów, rozszerzenia pomieszczeń serwerowni i wymiany całości infrastruktury w kilkuletnim cyklu. Dodatkowo budując własne usługi trzeba skalować je zgodnie z potencjalnym najwyższym obciążeniem, co powoduje, że przez pewne okresy są one słabo wykorzystana, a co za tym idzie kosztowne.

Platforma Azure jest subskrypcją o stałej cenie pewnej puli jej zasobów. Zużycie tej puli zależne jest od poziomu ich wykorzystania. Uprawniony użytkownik może decydować o sposobie i zakresie wykorzystania tej puli - w przypadku zwiększenia zapotrzebowania może przydzielić systemowi więcej zasobów lub ograniczyć je w przypadku spadku zapotrzebowania.

Niezwykle istotnym jest założenie takiej budowy systemów, aby nie następowało uzależnienie ich działania i rozwoju od jednego Wykonawcy czy Dostawcy. Takie podejście jest realizowane przez różne podmioty od wielu lat i opiera się na dwóch zasadniczych elementach:

[13] https://azure.microsoft.com/pl-pl/

- Pierwszą cechą Azure jest to, że posiada narzędzia wspomagające migrację aplikacji i danych zarówno ze środowisk własnych do Azure, jak i z Azure na dowolną inną platformę opartą o standard serwerów X64, a więc pozwala na przeniesienie usług w przypadku podjęcia takiej decyzji. Typowym przykładem roboczego zastosowania tych mechanizmów jest budowa środowisk testowo-rozwojowych na platformie Azure, a po wykonaniu testów – przenoszenie gotowych aplikacji na środowiska własne.
- Drugim jest stosowanie powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy.

Dostępność usług hostowanych Microsoft oraz ich bezpieczeństwo oferują najwyższy dostępny poziom, który byłby niezwykle kosztownych i trudny do uzyskania w środowiskach własnych.

Oferowany jest poziom dostępności na poziomie 99,9% (lub wyższy) oraz stale modyfikowane i rozszerzane procedury bezpieczeństwa, poddawane corocznie audytom kilkunastu uznanych niezależnych firm.

3.2.3. CHMURA HYBRYDOWA – NAJCZĘŚCIEJ STOSOWANY MODEL

Rozpatrując wszelkie dostępne modele budowy systemów informacyjnych, należy stwierdzić, że optymalną i coraz popularniejszą[14] wydaje się koncepcja chmury hybrydowej, w skład której wchodzi odpowiednio przygotowana infrastruktura własna oraz usługi z chmury.

Takie rozwiązanie łączy w sobie wiele zalet. z jednej strony pozwala na pełną kontrolę nad własną, dostosowaną do unikalnych potrzeb infrastrukturą, w tym nad usługą katalogową oraz przetwarzaniem wrażliwych i niejawnych danych, z drugiej strony pozwala uzyskać efekt szybkiej i bezpiecznej rozbudowy funkcji systemów bez dodatkowych inwestycji i z przewidywalnymi kosztami utrzymania.

Dodatkową zaletą rozwiązania hybrydowego jest to, że przy prawidłowym jego zaprojektowaniu bardzo proste staje się przenoszenie komponentów systemu z własnych środowisk do chmury i odwrotnie. Podkreślić należy, że nie każde rozwiązanie hybrydowe

[14] https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-hybrid-cloud-computing/

możemy nazwać chmurą hybrydową. Dostosowanie własnej infrastruktury tak aby stała się chmurą prywatna wymaga zwykle przebudowy systemów własnych.

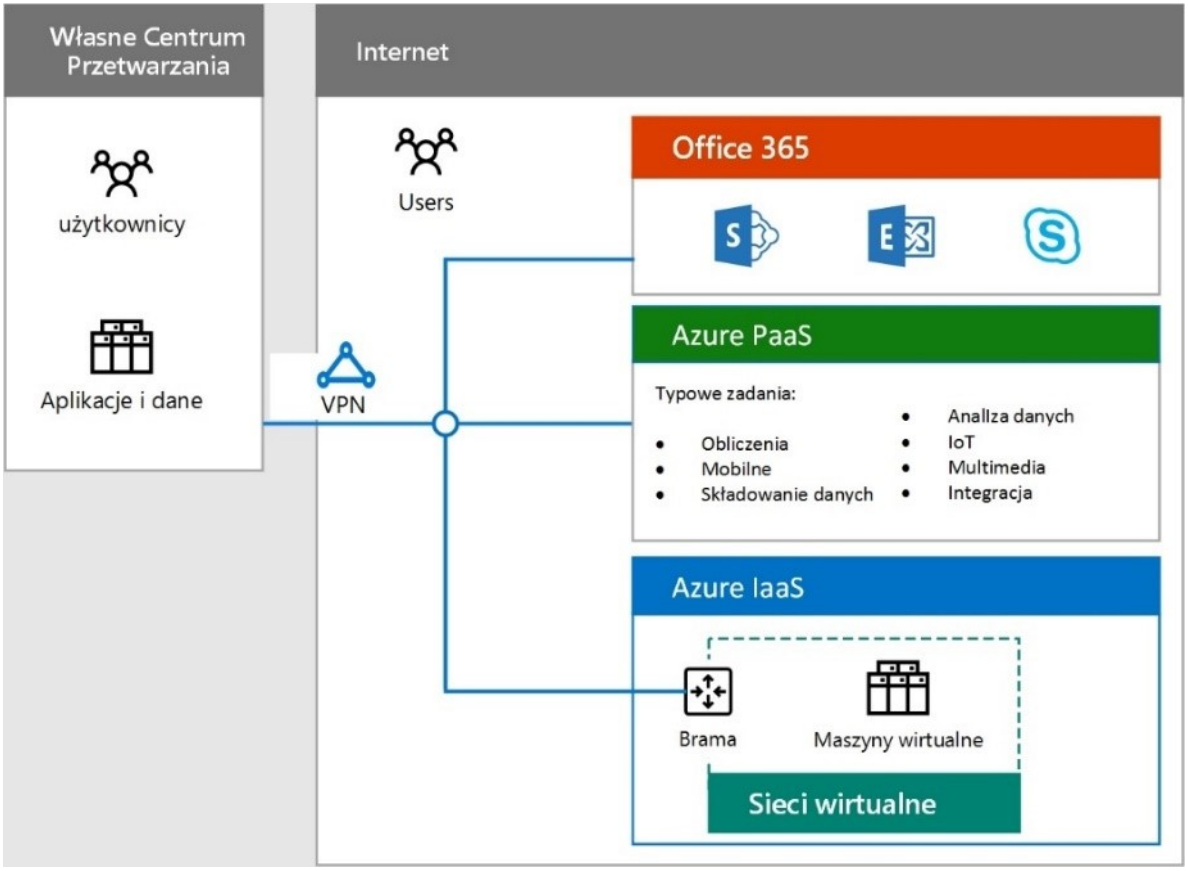
Ważnym aspektem dotyczącym łatwości zarządzania hybrydowym środowiskiem złożonym z Azure oraz własnej infrastruktury zbudowanej zgodnie z zaleceniami Microsoft w oparciu o Windows Server, wirtualizację Hyper-v, Azure Stack HCI[15] i zarządzania danymi przez Purview[16], jest spójny sposób zarządzania tymi środowiskami.

Rozwiązanie hybrydowe proponowane przez Microsoft[17], oprócz wymienionych już zalet, pozwala w prosty i tani sposób realizować następujące scenariusze:

- Przygotowanie środowisk testowych w postaci maszyn wirtualnych na platformie Azure z możliwością przenoszenia ich do środowisk własnych.
- Konfiguracja całości środowiska zapasowego w Azure – scenariusz niezwykle efektywny kosztowo z uwagi na minimalne opłaty za „zamrożone" środowiska.
- pPrzeniesienie na Azure całego środowiska dostępowego dla użytkowników zewnętrznych, co rozwiązuje problemy:
    - dużej i nieprzewidywalnej liczby użytkowników i związanych z tym problemów skalowania rozwiązania i pików przetwarzania,
    - gotowego mechanizmu niezaprzeczalnego uwierzytelniania,
    - stabilności i gwarantowanej dostępności.
- Uruchomienie w Azure gotowych i skonfigurowanych narzędzi analizy danych i raportowania, korzystających z lokalnych zasobów danych, z granulacją praw dostępu do poszczególnych zakresów danych i analiz.
- Uruchomienie w Azure zewnętrznych stron internetowych – informacyjno-usługowych.
- Uruchomienie w Azure interfejsu zasilającego danymi z innych systemów z mechanizmami czyszczenia i integracji danych.

[15] https://docs.microsoft.com/en-us/azure-stack/hci/overview
[16] https://docs.microsoft.com/en-us/purview/purview
[17] https://docs.microsoft.com/pl-pl/hybrid/

Dodatkową korzyścią ze stosowania architektury hybrydowej opartej na usługach hostowanych Microsoft jest łatwa integracja z własną infrastrukturą oraz wykorzystanie gotowych mechanizmów wysokiej dostępności i ochrony przed atakami.

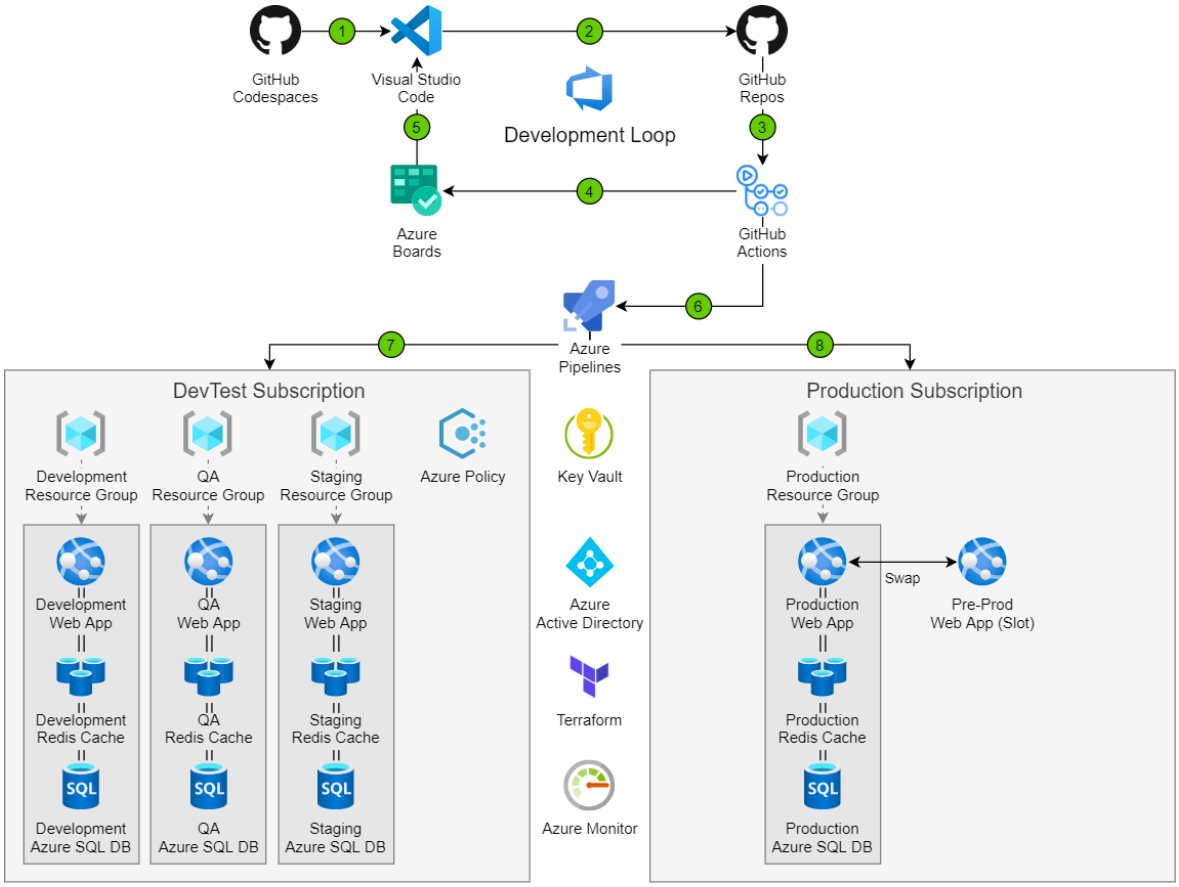


Jednym z oczywistych przykładów wykorzystania modelu hybrydowego jest stworzenie w usłudze Azure środowisk testowo-rozwojowych, które po zakończeniu fazy testów podlegają wdrożeniu w postaci gotowych maszyn wirtualnych w środowiskach własnych lub usłudze Azure[18].

Dodatkową zaletą takiego rozwiązania jest możliwość „zamrożenia” w Azure maszyn wirtualnych czy całych komponentów systemu do czasu, gdy trzeba będzie dokonać modernizacji systemu, a więc wykonać następną serię testów.

Przykład schematu takiej struktury przedstawia poniższy rysunek.

[18] https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/dev-test-paas



Dalszym rozwinięciem koncepcji spójnej i zarządzalnej platformy hybrydowej jest Azure Stack opisany w dalszej części opracowania.

4. KOMPONENTY TECHNICZNE

Pierwszą funkcją opisywanych standardowych komponentów technicznych jest zagwarantowanie budowy stabilnego, bezpiecznego i zarządzalnego środowiska platformowego dla wszelkich aplikacji i usług, czyli elastycznej, łatwo rozwijalnej infrastruktury, która jednocześnie ma zagwarantować realizację założeń interoperacyjności. Takie środowisko będziemy w dalszej części opracowania nazywać Platformą.

W zakresie budowy wydajnej i bezpiecznej infrastruktury Platforma powinna zapewniać określony zakres usług obejmujący:

- zarządzanie użytkownikami oraz zasobami,
- uwierzytelnianie użytkowników wewnętrznych i zewnętrznych,
- zapewnienie bezpieczeństwa,
- zapewnienie ciągłości usług na bazie gwarantowanego SLA.

Dodatkowo system powinien zapewniać wszystkim użytkownikom systemu teleinformatycznego usługi wspierające ich codzienną pracę w zakresie:

- bezpiecznego dostępu do sieci Internet,
- dostępności informacji, plików i urządzeń peryferyjnych
- dostępności z różnego rodzaju urządzeń (w tym mobilnych) opartych o różne systemy operacyjne.

Druga funkcja komponentów standardowych związana jest z dostarczeniem podstawowych rozwiązania, które są zwykle niezbędne niezależnie od rodzaju aplikacji dziedzinowych. Mogą one być wdrażane w dużej części metodą konfiguracji natywnych (wbudowanych) cech produktów (zbliżonych w działaniu do modelu SaaS), co pozwala na:

- szybkie uzyskanie założonych efektów przy obniżeniu ryzyka projektu,
- ograniczenie kosztów związanych z wdrożeniem,
- możliwość rekonfiguracji i zmian przez użytkownika lub dowolnego wykonawcę,
- wielokrotne obniżenie kosztów opieki serwisowej i kosztów eksploatacyjnych.

Przykładami takich funkcjonalności są:

- sprawna poczta e-mail zintegrowana z usługami informacyjnymi,
- zarządzanie kalendarzami, czasem i zasobami,
- udostepnienie narzędzi kolekcjonowania, porządkowania, publikowania i wymiany informacji,
- analiza posiadanych danych,
- integracja systemów wewnętrznych i zewnętrznych.

Podstawowymi komponentami funkcjonalnymi, którymi zajmiemy się w opracowaniu są:

- usługi katalogowe,
- zarządzanie tożsamością,
- infrastruktura klucza publicznego (PKI),
- zarządzanie bezpieczeństwem,
- zarządzanie środowiskiem IT i zasobami, w tym danymi,
- platforma współpracy i zarządzania informacją,
- bazy danych, analiza danych i raportowanie,
- poczta elektroniczna,
- zunifikowana komunikacja,
- integracja,
- zarządzanie dowolnymi obiektami biznesowymi,
- aplikacje dedykowane.

Przedstawione poniżej produkty (komponenty techniczne) odpowiadają uprzednio sprecyzowanym założeniom funkcjonalnym i wskazują na potencjalny sposób realizacji postawionych systemowi założeń.

Proponowane rozwiązania będą oparte na następujących produktach Microsoft:

- Pakiety usług hostowanych (Microsoft 365, Azure, Dynamics 365, Defender, EMS).
- Zawartych w platformie Azure maszynach wirtualnych z systemami Windows Server, dystrybucjami Linux, czy kontenerami.
- Usługach Azure z zakresu bezpieczeństwa systemów.
- Usługach Azure w zakresie baz danych, pobierania, składowania, przetwarzania i analizy danych.
- Windows.
- SharePoint Online.
- Teams.
- Exchange Online.
- narzędziach programistycznych Visual Studio i PowerApps.

Dlaczego proponujemy oparcie się na produktach Microsoft? Jesteśmy przekonani, że klienci, którzy wybrali technologie Microsoft, budują na niej rozwiązania, które:

- Zapewniają niskie całkowite koszty użytkowania – łączna cena zakupu, rozwoju, utrzymania i opieki serwisowej jest jedną z najniższych dostępnych na rynku.
- Są wyposażone w otwarte i ogólnie uznane interfejsy komunikacyjne pozwalające na wymianę informacji z dowolnymi systemami opierając się na standardach przemysłowych.
- Są oparte na standardowych, konfigurowalnych, dostępnych dla wszystkich i dobrze udokumentowanych komponentach, pozwalających na modularną budowę systemów i jej kontynuację przez dowolnego wykonawcę.
- Są przewidywalne – ścieżka rozwojowa produktów MS jest sygnalizowana na wczesnych etapach, co pozwala bez ryzyka budować systemy i planować ich rozwój.
- Zapewniają dostęp do szerokich zasobów szkoleniowych.
- Ich bezpieczeństwo potwierdzone jest umowami *Government Security Program*, dzięki którym administracja publiczna ma dostęp do:

- kodów źródłowych produktów Microsoft,
- wczesnego ostrzegania o zagrożeniach,
- pomocy przy rozwiązywaniu problemów z bezpieczeństwem.

4.1. INFRASTRUKTURA BEZPIECZEŃSTWA

Infrastruktura bezpieczeństwa to szerokie pojęcie zawierające w sobie wiele elementów, takich jak ogóle założenia architektury systemu, budowa aplikacji dziedzinowych oraz komponenty bezpieczeństwa, ochrona antywirusowa, silne uwierzytelnianie, detekcja zagrożeń czy polityki bezpieczeństwa.

Założeniem koncepcji systemu komponentowego jest budowa bezpiecznej i odpornej na ataki architektury, który to temat jest uwzględniany w całym prezentowanym modelu zgodnie z zasadą triady, na którą składają się **poufność, integralność i dostępność** informacji. Jednocześnie założeniem jest realizacja zasady **rozliczalności** działań w systemach, czyli możliwości potwierdzenia kto i kiedy dokonał jakich zmian w systemie lub przetwarzanych danych.

Podejście do minimalizacji ryzyka związanego z cyberatakami czy dostępnością systemów okazuje się niezwykle skomplikowanym i kosztownym w realizacji zagadnieniem – między innymi dlatego, że musi to być podejście kompleksowe, biorące pod uwagę wszelkie możliwe zagrożenia. Przykładem takiego holistycznego podejścia jest referencyjna architektura bezpieczeństwa Microsoft[19]. Wprowadzanie zasad bezpieczeństwa przy posiadani odpowiednich narzędzi jest dużym wyzwaniem. Pomocne w takim działaniu mogą być przewodniki Microsoft[20].

[19] https://github.com/MicrosoftDocs/security/blob/main/Downloads/microsoft-cybersecurity-reference-architectures.pptx?raw=true
[20] https://docs.microsoft.com/pl-pl/azure/cloud-adoption-framework/get-started/security

Analizując problem zgodności oprogramowania i budowanych usług z obowiązującym prawem, należy poczynić zastrzeżenie, że rozpatrywane czynniki bezpieczeństwa wynikają z techniczno-organizacyjnych cech samych usług, a nie z tego jak są one wykorzystywane i jakie procedury i polityki bezpieczeństwa zostały wdrożone przez podmiot wykorzystujący usługi. w poniższej analizie przedstawione zostaną wyłącznie aspekty bezpieczeństwa technicznego, pozwalające na budowę pozostałych warstw modelu bezpieczeństwa teleinformatycznego.

4.1.1. ROZPORZĄDZENIE KRI

Komponenty techniczno-organizacyjne będące składowymi warstwy bezpieczeństwa muszą spełniać wiele wymagań.

Od strony wymogów prawnych w 2012 roku nastąpił przełom, dzięki wprowadzeniu ROZPORZĄDZENIA RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI).

Rozporządzenie to po raz pierwszy w spójny sposób określa zalecenia i wymagania minimalne dla systemów teleinformatycznych. w zasadzie, można stwierdzić, że rozporządzenie to wskazuje na elementy zawarte w niniejszym rozdziale, między innymi:

- specyfikację formatów danych oraz protokołów komunikacyjnych i szyfrujących, które mają być stosowane w oprogramowaniu interfejsowym,
- sposoby zapewnienia bezpieczeństwa przy wymianie informacji,
- standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej,
- sposoby zapewnienia dostępu do zasobów informacji podmiotów publicznych dla osób niepełnosprawnych.

Co może być skutkiem wprowadzenia KRI? Między innymi konieczność wprowadzenia zmian technicznych, logicznych i organizacyjnych, takich jak:

- implementacja właściwej infrastruktury,

- modyfikacje architektury systemów,
- standaryzacja, w tym m.in. standardów związanych z przystosowaniem systemów dla osób niepełnosprawnych
- wdrożenie zarządzania systemami,
- wdrożenie zarządzania tożsamością,
- wdrożenie (a nie tylko posiadanie) polityk bezpieczeństwa,
- eliminacja duplikacji danych,
- przygotowanie wymagań dla nowych systemów,
- szkolenia.

4.1.2. INNE REGULACJE DOTYCZĄCE CYBERBEZPIECZEŃSTWA

Następne elementy określające obowiązujące zasady bezpieczeństwa pojawiły się w kilku aktach prawnych Parlamentu Europejskiego i Rzeczypospolitej Polskiej w ostatnich latach. Są to przede wszystkim:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych (RODO).
- Dyrektywa NIS i bazująca na niej ustawa o cyberbezpieczeństwie[21] wraz z umocowanymi w niej rozporządzeniami[22].
- Wymagania dotyczące bezpieczeństwa zawarte w Rozporządzeniu eIDAS.

Niezwykle istotnym jest to, że wymagania dotyczące bezpieczeństwa warstwy technicznej są wspólne i tożsame dla wszystkich wymienionych regulacji i wymagają wprowadzenia zasad:

- bezpieczeństwa danych i systemów,
- dostępności,
- niezaprzeczalności,
- rozliczalności.

[21] http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/O/D20181560.pdf
[22] https://www.gov.pl/web/cyfryzacja/finalizacja-prac-nad-tworzeniem-krajowego-systemu-cyberbezpieczenstwa

Jeszcze jednym ważnym elementem szeroko pojętego bezpieczeństwa jest stosowanie odpowiednich metodyk projektowych, uwzględniających analizę ryzyk oraz gwarantujących wdrożenie wszystkich założonych zasad i realizację metryk sukcesu. Temat ten będzie omówiony w dalszej części opracowania.

Należy pamiętać, że bezpieczeństwo to temat daleko szerszy niż sama infrastruktura. Ciekawym materiałem na ten temat jest opracowanie OECD (*Organisation for Economic Co-operation and Development*) *Digital Security Risk Management for Economic and Social Prosperity*[23].

Niezależnie od wymogów prawnych **każda organizacja powinna zdefiniować własne minimalne standardy**. Postawa ryzyka i kolejna tolerancja dla tego ryzyka może się znacznie różnić w zależności od branży, kultury i innych czynników. Na przykład bank może nie tolerować żadnych potencjalnych szkód dla jego reputacji nawet z drobnego ataku na system testowy. Niektóre organizacje chętnie zaakceptują to samo ryzyko, jeśli przyspieszy realizację kluczowych zadań.

4.1.3. USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa powstała na bazie europejskiej dyrektywy NIS - *The Directive on security of network and information systems*[24].

Rozwija ona wymagania w zakresie realizacji mechanizmów organizacyjno-technicznych postawione w innych aktach prawnych, takich jak KRI, GDPR czy eIDAS.

Ustawa Definiuje krajowe organy do spraw cyberbezpieczeństwa i ich obowiązki, definiuje usługi kluczowe, definiuje operatorów usług kluczowych oraz dostawców usług cyfrowych i ich obowiązki oraz określa jakie są kary związane z jej nieprzestrzeganiem i kiedy mogą być nałożone.

Jakie obowiązki techniczno-organizacyjne wynikają z ustawy?

Aby wypełnić wszystkie wymagania dotyczące nadzoru nad systemem teleinformatycznym z punktu widzenia niezbędnych środków techniczno-organizacyjnych należy między innymi:

[23] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
[24] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

a) prowadzić analizy ryzyka dla powstających i eksploatowanych systemów,

b) zachować zasadę monitorowania – monitorować i raportować wszystkie incydenty oraz zdarzenia z nimi związane,

c) zachować zasadę rozliczalności – dokumentować kto dokonywał akcji (i jakich) w systemie teleinformatycznym,

d) zbierać informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego,

e) zarządzać incydentami,

f) posiadać systemy i procedury raportujące incydenty do odpowiednich organów.

Ustawa odnosi się przede wszystkim do podmiotów świadczących usługi kluczowe (usług, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych) oraz dostawców usług cyfrowych.

Zgodnie z ustawą operator usługi kluczowej stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego:

1) dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami,

2) ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności,

3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.

Ponadto operator usługi kluczowej:

1) zapewnia obsługę incydentu,

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań,

3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny,

4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV,

5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe,

6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

Jakie obowiązki techniczno-organizacyjne wynikają z ustawy?

Aby wypełnić wszystkie wymagania dotyczące nadzoru nad systemem teleinformatycznym z punktu widzenia niezbędnych środków techniczno-organizacyjnych należy między innymi:

a) zachować zasadę monitorowania – monitorować i raportować wszystkie incydenty oraz zdarzenia z nimi związane,

b) zachować zasadę rozliczalności – dokumentować kto dokonywał akcji (i jakich) w systemie teleinformatycznym,

c) zbierać informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego,

d) zarządzać incydentami,

e) posiadać systemy i procedury raportujące incydenty do odpowiednich organów.

4.1.4. POLITYKI BEZPIECZEŃSTWA

Podstawą do budowy założeń bezpiecznego systemu jest opracowanie polityk bezpieczeństwa, czyli zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa, wraz z ich planem wdrożenia i egzekwowania.

Polityka bezpieczeństwa jest dokumentem o znaczeniu strategicznym, który warunkuje możliwość efektywnego i całościowego zarządzania bezpieczeństwem informacji w organizacji.

Dwa kluczowe pytania, na które odpowiadają polityki bezpieczeństwa to:

- co chronimy (informację, dane, sprzęt),
- w jaki sposób chronimy.

Typowymi elementami polityki bezpieczeństwa są:

- model bezpieczeństwa,
- mechanizmy kontroli dostępu,
- poziomy uprawnień (jakie poziomy uprawnień istnieją i jakie są zasady ich przyznawania),
- mechanizmy identyfikacji i zapewnienie autentyczności (na poziomie fizycznym i systemów),
- śledzenie zdarzeń w systemie (jakie mechanizmy/programy/procedury stosowane są do śledzenia zmian w systemach).

Dla podmiotów świadczących usługi publiczne obowiązujące jest rozporządzenie KRI (o którym była mowa wcześniej), nakładające obowiązek opracowania i posiadania formalnej instrukcji polityki bezpieczeństwa.

Z punktu widzenia normatywów w Polsce obowiązuje norma PN-ISO/IEC 27001:2013 polskie tłumaczenie normy ISO/IEC 27001 - normy międzynarodowej standaryzującej systemy zarządzania bezpieczeństwem informacji. Norma ta określa następujące obszary:

- polityki bezpieczeństwa;
- organizację bezpieczeństwa informacji;
- zarządzanie aktywami;
- bezpieczeństwo zasobów ludzkich;
- bezpieczeństwo fizyczne i środowiskowe;
- zarządzanie systemami i sieciami;
- kontrolę dostępu;
- zarządzanie ciągłością działania;
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych;

- zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- zgodność z wymaganiami prawnymi i własnymi standardami.

Szczegółowy opis zasad budowy polityk bezpieczeństwa można znaleźć na stronach NASK[25].

4.1.5. PODSTAWOWE REKOMENDACJE BEZPIECZEŃSTWA

Podejmując prace związane z budową, rozbudową lub modyfikacjami systemów teleinformatycznych warto przyjąć poniższe techniczne rekomendacje bezpieczeństwa.

Realizacja wymagań prawnych w zakresie bezpieczeństwa, w tym uwierzytelniania, niezaprzeczalności działań oraz monitorowania następuje poprzez:

1. Przyjęcie jako priorytetu ochrony tożsamości cyfrowej administratorów i użytkowników systemów.
2. Wdrożenie i pielęgnację usług katalogowych lub mechanizmów zarządzania tożsamością obejmujących wszystkich użytkowników systemów danego podmiotu. Zaleca się wykorzystanie, niezależnej od wewnętrznej, usługi katalogowej dla użytkowników zewnętrznych.
3. Tam, gdzie jest to możliwe, korzystanie usługi katalogowej jako podstawy uwierzytelnienia i nadawania uprawnień do wszystkich systemów teleinformatycznych danego podmiotu z wprowadzeniem mechanizmu pojedynczego logowania (single sign-on).
4. Tam, gdzie nie jest możliwa realizacja globalnego mechanizmu single sign-on, należy objąć bazy tożsamości użytkowników w poszczególnych systemach jednym wspólnym systemem zarządzania tożsamością.
5. Nadawanie uprawnień dostępu do danych i usług ról i grup ról, a nie dla użytkowników i ich grup.
6. Wykorzystanie uwierzytelnienia wieloskładnikowego dla dostępu do danych wrażliwych oraz w przypadku uwierzytelniania spoza chronionych sieci wewnętrznych.

[25] https://www.nask.pl/pl/aktualnosci/oferta/oferta-telekomunikacyjn/bezpieczenstwo/2666,Polityka-Bezpieczenstwa-Informacji.html

7. W każdym przypadku rozdzielenie funkcji kont administratorskich i kont użytkownika systemów oraz izolacja tych typów kont.
8. Wdrożenie mechanizmów wymuszających zmianę haseł użytkowników lub odnawiania certyfikatów w zgodzie z zapisami polityk bezpieczeństwa.
9. Wdrożenie mechanizmów samoobsługi użytkownika w przypadku konieczności zmiany lub utraty poświadczeń do systemu.
10. Przygotowanie bezpiecznych środowisk klienckich poprzez przygotowywanie sprawdzonych, testowanych i monitorowanych „obrazów" oprogramowania, zawierających system operacyjny wraz z kompletem aplikacji niezbędnych dla danej grupy użytkowników, systemy firewall i antywirusowy, oraz narzędzia pozwalające na:
    I. monitorowanie stanu sprzętu i jego inwentaryzację,
    II. monitorowanie działania oprogramowania i jego inwentaryzację,
    III. zarządzanie konfiguracją środowisk klienckich,
    IV. udostępnienie możliwości instalacji przez użytkownika tylko wybranych aplikacji pozwalających na realizację jego zadań.
11. Przygotowanie schematów implementacji środowisk serwerowych pozwalających na ich monitorowanie i zarządzanie.
12. Wprowadzenie spójnych mechanizmów klasyfikacji informacji i danych.
13. Wprowadzenie mechanizmów wymuszających szyfrowanie plików zawierających informację wrażliwą wraz z mechanizmami gwarantującymi niezaprzeczalność dostępu do nich.
14. Wprowadzenie mechanizmów wymuszających szyfrowanie zasobów dyskowych i nośników zawierających informację wrażliwą, które mogą być wynoszone poza teren danego podmiotu wraz z mechanizmami gwarantującymi niezaprzeczalność dostępu do nich.
15. Przeprowadzanie regularnych (przynajmniej raz do roku) audytów, lub oparcie się o audyty niezależnych, uznanych firm – w przypadku wykorzystywania usług hostowanych.

Bezpieczeństwo w systemach teleinformatycznych należy traktować zawsze jako ciągły proces uzupełniony odpowiednimi narzędziami, procedurami i kompetencjami. Przy podejściu procesowym należy opisać wszystkie kluczowe procesy, wdrożyć je, poddawać audytom i okresowym działaniom dostosowawczym.

Uproszczony schemat reagowania na incydent naruszający bezpieczeństwo przedstawia poniższy rysunek:

4.1.6. ZASADA „ZERO ZAUFANIA”

Zerowe zaufanie (Zero Trust) to proaktywne, zintegrowane podejście do bezpieczeństwa na wszystkich warstwach zasobów cyfrowych, które stale weryfikuje każde działanie, redukuje uprawnienia do niezbędnych i opiera się na zaawansowanej analizie, wykrywaniu i reagowaniu w czasie rzeczywistym na zagrożenia.

Dlaczego Microsoft stosuje zasadę Zero Trust?

Głównie dlatego, że:

1. Bezpieczeństwo IT jest złożone - wiele urządzeń, użytkowników, procesów i połączeń – każdy z tych elementów jest potencjalnym przedmiotem ataku.
2. Stosowana uprzednio strategia bezpieczeństwa "Zaufana sieć" była adekwatna do typowych ataków skupionych na sieci. Prosta i ekonomiczna ochrona przed nimi okazała się zawodna wobec obecnie stosowanych wektorów ataku.

3. Zasoby coraz częściej opuszczają sieć, zgodnie z zasadami mobilności BYOD (*Bring your own Device*), WFH (*work from home*) i stosowania rozwiązań z chmury.
4. Atakujący przeszli na ataki tożsamości oparte o wyłudzanie informacji i kradzież danych uwierzytelniających.
5. Mnogość istniejących wektorów ataku powoduje, że praktycznie każdy element techniczny, organizacyjny czy ludzki jest zagrożony.
6. Zespoły ds. bezpieczeństwa są często przeciążone i nieskuteczne.

Strategia zwiększania bezpieczeństwa obowiązuje dla wszystkich użytkowników, zasobów i aplikacji - wszędzie, w tym w własnych, sieciach publicznych i niezaufanych.

Podstawowe podejście do stosowania zasady Zero Trust pokazane są na poniższym diagramie:

Niezaprzeczalna weryfikacja	**Dostępu z najmniejszymi uprawnieniami**	**Założenie, że naruszenia wystąpią**
Zawsze sprawdzaj poprawność wszystkich punktów dostępu do danych, w tym • Tożsamość i lokalizację użytkownika • Kondycję urządzeń • Kontekst usługi lub obciążenia • Klasyfikację danych • Anomalie	Aby zabezpieczyć zarówno dane, jak i produktywność, ogranicz dostęp użytkowników za pomocą • Dostępu w ograniczonym czasie • Dostępu w potrzebnym zakresie • Adaptacyjnych polityk opartych na ryzyku • Ochrona danych przed wektorami pozapasmowymi •	Zminimalizuj zakres problemu w przypadku naruszeń poprzez • Segmentacje dostępu według sieci, użytkowników, urządzeń i aplikacji. • Szyfrowanie wszystkich sesji od końca do końca. • Korzystanie z analityki do wykrywania zagrożeń i wyboru najlepszych scenariuszy działania

Szczegółowe rekomendacje w tym zakresie udostępnia firma Microsoft na stronie [Zero Trust Guidance Center | Microsoft Docs]

4.1.7. ZABEZPIECZENIA WYCIEKU INFORMACJI NA POZIOMIE UŻYTKOWNIKA

Użytkownik systemu jest zwykle najsłabszym ogniwem w systemie cyberbezpieczeństwa. Konieczne jest wprowadzenie wszystkich wymienionych procedur i mechanizmów ochrony jego tożsamości i środowiska pracy. Kluczowym elementem tych działań są okresowe

szkolenia użytkowników, aktualizujące wiedzę o potencjalnych zagrożeniach, wdrożonych politykach bezpieczeństwa i wymaganych scenariuszach zachowań.

Dużym problemem jest wyciek czy nieuprawniony dostęp do informacji w wypadku kradzieży komputerów z dyskami zawierającymi dane lub wynoszenia czy zgubienia pamięci przenośnych, na przykład kluczy USB.

W tych przypadkach standardowym działaniem powinno być szyfrowanie danych na dyskach i nośnikach danych. Mechanizm taki powinien umożliwiać centralnie zarządzanie zgodnie z ustalonymi politykami bezpieczeństwa poprzez *Group Policy* przez jednoznaczne określenie i wymuszenie konieczności szyfrowania informacji pod rygorem odcięcia dostępu do danych.

4.1.8. ZABEZPIECZENIE DANYCH, NIE TYLKO DOSTĘPU DO MIEJSCA ICH SKŁADOWANIA

Przez długi czas zabezpieczano dokumenty poprzez składowaniu ich w repozytoriach o ograniczonym uprawnieniami użytkowników dostępie. Scenariusz ten nie zabezpieczał jednak przed beztroską lub celową działalnością pracowników wynoszących lub udostępniających dane, do których mają dostęp. Obecnie, coraz częściej stosowaną i znacznie efektywniejszą techniką jest zabezpieczanie samych danych niezależnie od miejsca ich przechowywania. Mechanizmy takie, określane jako *Rights Management*, czyli zarządzanie prawami dostępu do informacji, są już powszechnie dostępne i często stanowią usługę typowych systemów operacyjnych czy narzędzi biurowych.

Pozwalają na centralizację polityk bezpieczeństwa w tym zakresie i zabezpieczenie informacji tak by była dostępna dla innych użytkowników tylko w określonym zakresie – od pełnych praw, zakazu wydruku, wykonania funkcji *print screen* do całkowitego braku uprawnień do odczytu.

Umożliwiają też określenie, czy dane mogą zostać odczytane na komputerze, który nie pracuje w domenie organizacji.

Oczywiście ma to sens wtedy, gdy wprowadzimy odpowiednie mechanizmy ochrony cyfrowej tożsamości użytkownika, która jest podstawą przydzielania uprawnień dostępowych.

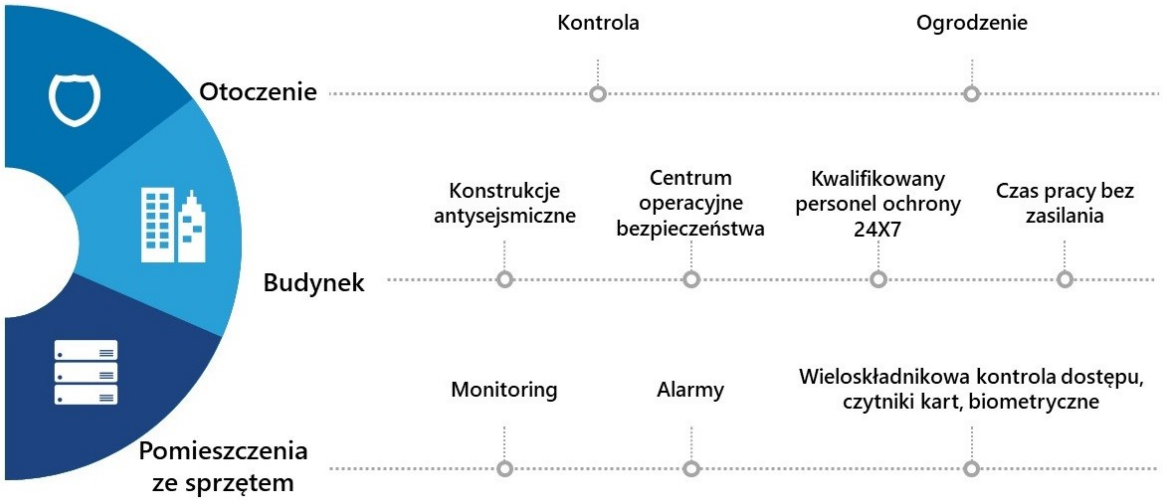
4.1.9. BEZPIECZEŃSTWO CENTRUM PRZETWARZANIA

Centrum przetwarzania (CP) jest miejscem, w którym nie tylko przetwarza się i składuje dane, ale też miejscem wyposażonym w narzędzia administratorskie pozwalające na zarządzanie infrastrukturą, usługami i danymi. Konieczne jest więc wprowadzenie mechanizmów zabezpieczających centrum na poziomie fizycznym, logicznym i operacyjnym.

Zabezpieczenia muszą być wbudowane w kompleksowy projekt CP zgodnie z zasadą *Security by design* oraz zasadą *Zero Zaufania*. Innymi słowy, architekturę i procedury zabezpieczeń należy zaprojektować wraz z całym CP, gdyż po jego uruchomieniu może to być zwyczajnie niemożliwe lub bardzo kosztowne.

Najbardziej efektywną formą zachowania bezpieczeństwa CP jest prewencja, a więc taki projekt zabezpieczeń, które przewidują wszelkiego rodzaju znane ataki czy zdarzenia, ale też przewidują ich rozwój z zmiany.

W praktyce najprostsza okazuje się realizacja warstwy zabezpieczeń fizycznych. Bywa ona bardzo kosztowna, tym niemniej dosyć łatwo jest ją zaprojektować. Uproszczony schemat zabezpieczeń fizycznych CP przedstawia poniższy rysunek.



W dużych CP świadczących usługi wielu klientom z różnych organizacji należy zapewnić niezawodną separację danych. Separacja taka polegająca na logicznej izolacji danych poszczególnych użytkowników musi być zagwarantowana mechanizmem niezaprzeczalnego uwierzytelnienia i autoryzacji dostępu do danych. Wdrożenie odpowiednich mechanizmów dostępu do danych powinno łączyć się z ich klasyfikacją i zastosowaniem dla poszczególnych klas danych odpowiednich procedur dostępu. Na przykład, dla danych osobowych,

wrażliwych czy objętych tajemnicą przedsiębiorstwa powinien być zastosowany mechanizm uwierzytelnienia wieloskładnikowego.

W stosunku do danych składowanych w CP należy zapewnić możliwość szyfrowania danych, przestrzeni dyskowych czy też maszyn wirtualnych.

Uzupełnieniem takiego modelu ochrony danych musi być możliwość szyfrowania ich w trakcie przesyłu – zarówno do i z CP, jak i wewnątrz CP.

Niezwykle istotnym mechanizmem zabezpieczającym przed utratą danych w CP jest nadmiarowość (redundancja) danych. w tym zakresie zalecane jest tworzenie 2-3 kopii danych w jednym CP i tzw. georedundancja pozwalająca na tworzenie kopii zapasowych danych (lub całych systemów) w drugim CP oddalonym o kilkadziesiąt do kilkuset kilometrów.

Następnym, koniecznym do wdrożenia w CP procesem jest trwałe usuwanie danych użytkowników po zakończeniu przez nich korzystania z usługi CP, z zaplanowaniem uzgodnionego z użytkownikiem okresu karencji, w czasie którego dane są nadal dla niego dostępne przed ostatecznym ich usunięciem.

Bardzo ważną częścią obszaru bezpieczeństwa są procedury upoważnionego dostępu do danych dla pracowników CP. Założeniem podstawowym jest zasada, że administratorzy CP **nie mają** dostępu do danych użytkowników usług CP. w przypadku, gdy wystąpi konieczność takiego dostępu musi być ona obwarowana szczegółowymi procedurami, wymagającymi sprawnej, wieloetapowej ścieżki akceptacyjnej, zgody uprawnionego reprezentanta użytkownika oraz jasnych zasad – komu, w jakim celu i na jaki okres takie uprawnienia zostały udzielone. Wymagane jest też monitorowanie i dokumentowanie wszystkich działań związanych z dostępem do danych.

Takie oraz wiele innych zasad zostało określonych w normach, takich jak ISO 27018[26] czy ISO 27017[27]. Potwierdzone audytem stosowanie tego typu norm w zasadniczy sposób ogranicza typowe ryzyka związane z przetwarzaniem danych i pozwala na zaufanie dla usług świadczonych przez CP.

[26] http://iso27001security.com/html/27018.html
[27] http://iso27001security.com/html/27017.html

Dobrym przykładem fizycznego zastosowania opisywanych, kompleksowych zabezpieczeń są centra przetwarzania firmy Microsoft oferujące tysiące usług na całym świecie, w tym usługi Office 365, Azure, Dynamics 365 i wiele innych.

4.1.10. KRYPTOGRAFIA

Z uwagi na prace Komisji Europejskiej, zapisy nowego rozporządzenia eIDAS[28] i zgodnie z zaleceniami związanymi z coraz częstszymi próbami przełamania zabezpieczeń w szyfrowaniu, systemy, szczególnie te przetwarzające dane wrażliwe lub objęte klauzulą, powinny być migrowane do nowych narzędzi kryptograficznych wykorzystujących nieskompromitowane i silne szyfrowanie.

W większości przypadków, systemy wykorzystują stare algorytmy i metody kryptograficzne, których przełamanie przy użyciu narzędzi znalezionych w Internecie nie stanowi większego problemu.

Od kilku lat Microsoft oferuje w systemach operacyjnych (od Windows i Windows Server) moduł CNG[29] (*Cryptography Next Generation*), która zastąpiła CAPI[30]. Interfejs CNG udostępnia elastyczną platformę projektowania kryptograficznego, która umożliwia informatykom tworzenie, aktualizowanie i używanie niestandardowych algorytmów kryptograficznych w aplikacjach powiązanych z kryptografią, takich jak usługi centrum certyfikatów w Active Directory (AD CS), protokół SSL (*Secure Sockets Layer*) i protokół IPsec (*Internet Protocol security*). Interfejs CNG służy do implementowania algorytmów kryptograficznych Suite B rządu USA, obejmujących algorytmy szyfrowania, podpisów cyfrowych, wymiany kluczy i wyznaczania wartości skrótu.

Interfejs CNG udostępnia zestaw interfejsów API, które służą do następujących celów:

- wykonywanie podstawowych operacji kryptograficznych, takich jak tworzenie wartości skrótów i szyfrowanie oraz odszyfrowywanie danych,
- tworzenie, przechowywanie i pobieranie kluczy kryptograficznych,
- instalowanie i używanie dodatkowych dostawców usług kryptograficznych.

[28] https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32014R0910&from=EN
[29] https://docs.microsoft.com/en-us/windows/win32/seccng/cng-portal
[30] http://msdn.microsoft.com/en-us/library/windows/desktop/aa380255(v=vs.85).aspx

W ramach narzędzi CNG dostępne są:

- interfejsy *Credential Service Provider*, które zastąpiły bibliotekę GINA,
- interfejs użytkownika logowania mogący oddziaływać z wieloma wtyczkami *Credential Providers*,
- bezpośrednia obsługa uwierzytelniania wieloczynnikowego: karty inteligentne i tokeny, biometria itp.
- interfejs plug-and-play dla kart inteligentnych,
- moduły komunikacyjne kart,
- propagacja certyfikatu głównego,
- zintegrowane odblokowywanie kart inteligentnych.

Wraz z najnowszymi systemami dostępne są algorytmy szyfrujące, tzw. Suite B[31] - spełniające typowe wymogi naszych klientów. Między innymi w tramach tej technologii oferowane są: szyfrowanie: AES FIPS 197 (z kluczami o długości 128 oraz 256 bitów), podpis cyfrowy: EC-DSA FIPS 186-2 (korzystający z krzywych z 256- i 384-bitowymi współczynnikami pierwszymi), wymiana kluczy: *Elliptic Curve Diffie-Hellman* lub *Elliptic Curve MQV Draft NIST Special Publication 800-56* (korzystający z krzywych z 256- i 384-bitowymi współczynnikami pierwszymi) oraz mieszanie: *Secure Hash Algorithm* (SHA-2) FIPS 180-2 (korzystający z SHA-256 oraz SHA-384). Udostępnione są też narzędzia umożliwiające kontenerowanie własnych algorytmów szyfrujących.

Aby używanie nowych algorytmów kryptograficznych było możliwe, zarówno urząd certyfikacji użytkownika, jak i aplikacje użytkownika powinny obsługiwać kryptografię ECC (*Elliptic-curve Cryptography*) lub dowolny inny algorytm implementowany w ramach interfejsu CNG. Urząd certyfikacji musi wystawić certyfikaty nowego typu i zarządzać nimi, natomiast aplikacje muszą obsługiwać sprawdzanie poprawności łańcucha certyfikatów i używać kluczy wygenerowanych przez algorytmy Suite B.

Algorytmy Suite B, takie jak algorytmy kryptografii ECC, są obsługiwane tylko przez systemy operacyjne Windows Vista i nowsze wersje Windows oraz Windows Server 2008 i nowsze

[31] http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

wersje. Oznacza to, że certyfikatów tych nie można używać w starszych wersjach systemów operacyjnych, np. Windows XP lub Windows Server 2003. Można jednak używać klasycznych algorytmów, takich jak klucz RSA (*Rivest-Shamir-Adleman*), nawet jeśli zostały wygenerowane przy użyciu dostawcy klucza CNG.

Wszystkie te narzędzia są dostępne w ramach licencji aktualnych systemów operacyjnych Microsoft, a narzędzia programistyczne z gotowymi bibliotekami w ramach pakietu Visual Studio.

4.1.11. USŁUGI DOSTĘPU DO SIECI WEWNĘTRZNYCH I ZEWNĘTRZNYCH

W celu zrealizowania zadań postawionych w projekcie systemu, konieczna jest realizacja podsystemu bezpiecznego dostępu do usług wewnętrznych i zewnętrznych.

System dostępowy ma zapewnić łatwość obsługi, zaawansowaną ochronę oraz szybki i bezpieczny dostęp do wszystkich typów sieci.

W skład podsystemu musi wejść rozbudowana zapora filtrująca ruch do warstwy aplikacji włącznie. Zapewni ona jednostkom objętym projektem podstawową ochronę przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. Proponowane rozwiązanie ma integrować funkcje zapory z architekturą VPN (*virtual private network*). Wirtualne sieci prywatne to sieć dwukierunkowych kanałów do transmisji danych, tworzona w oparciu o sieć publiczną (Internet). Wirtualne kanały VPN są ustalane wyłącznie na czas transmisji między węzłami sieci stanowiącymi rutery, przez które informacja z sieci prywatnych jest przesyłana w zaszyfrowanej postaci. Współczesne rozwiązania VPN są ukierunkowane na budowanie wirtualnych sieci w oparciu o protokół IP. Umożliwiające kontrolę i filtrowanie z pamięcią stanu całego ruchu w kanałach VPN, a także, poprzez współpracę z usługami katalogowymi, kontrolę dostępu klientów VPN przez mechanizm kwarantanny pozwalające na zabezpieczenie sieci przed atakami zewnętrznymi przeprowadzanymi przez połączenia VPN.

Rozwiązanie ma zapewnić również możliwość pracy w trybie „*web cache*" buforując strony internetowe i dostarczając je użytkownikom z kopii lokalnej.

Całość podsystemu ma dostarczyć następujące usługi:

- zabezpieczenie i publikacja usług sieci urzędu dostępnych od strony sieci zewnętrznych,
- zapewnienie kontroli nad dostępem użytkowników do sieci Intranet i Internet,
- zapewnienie wydajnego dostępu do zasobów sieci Intranet i Internet.

4.1.11.1. PUBLIKOWANIE USŁUG

Podsystem dostępu ma pozwolić na ochronę sieci oraz publikowanie usług wewnętrznych do sieci Internet poprzez możliwość filtrowania ruchu sieciowego na poziomie połączeń sieciowych i protokołów aplikacyjnych:

- Filtrowanie pakietów z pamięcią stanu określa, które pakiety mogą być transmitowane przez zabezpieczone połączenie i usługę proxy w warstwie aplikacji. Filtrowanie to dynamicznie otwiera porty tylko wtedy, gdy jest to niezbędne, a po zakończeniu komunikacji natychmiast je zamyka.
- Filtrowanie połączeń pozwala na stworzenie przezroczystych dla aplikacji bramek, umożliwiając dostęp z różnych platform do usług internetowych, takich jak na przykład Telnet, RealAudio, technologie Windows Media, IRC, a w szczególności usług hostowanych, takich jak Azure czy Office 365.
- filtrowanie w warstwie aplikacji i kontrola z pamięcią stanu potrafi zrozumieć polecenia w protokołach aplikacyjnych stosowanych przez aplikacje działające na komputerze klienckim (np. HTTP, FTP, Gopher). Firewall działa w tym wypadku w roli komputera klienckiego, ukrywając topologię sieci i adresy internetowe IP przed siecią zewnętrzną.

Podsystem musi wspierać bezpieczne publikowanie serwerów usług, takich jak serwerów Web lub serwerów poczty elektronicznej pozwalające na wprowadzenie dodatkowej ochrony tych usług przed atakami z zewnątrz. Należy wykorzystać reguły publikowania serwerów, które chronią wewnętrzne serwery przed nieuprawnionym dostępem użytkowników zewnętrznych. Dodatkowo filtrowanie w warstwie aplikacji zabezpieczy wszystkie opublikowane serwery przed atakami z zewnątrz. w ramach całości rozwiązania podsystem

dostępu w bramce internetowej będzie pełnił rolę ochronną poprzez publikacje usług serwerów (np. serwerów front-end) i filtrowanie ruchu związanego z tymi usługami.

4.1.11.2. OPTYMALIZACJA RUCHU – WEB PROXY

Podsystem musi umożliwiać pracę w trybie buforowania odwołań do zasobów sieci Internet, przyspieszając pracę użytkowników z zasobami serwerów WWW i optymalizując wykorzystanie pasma w ramach sieci urzędu.

4.1.11.3. KONTROLA DOSTĘPU

System dostępowy musi być zintegrowany z usługą katalogową (UK) pozwalając na określenie uprawnień dostępu użytkowników do zasobów sieci Internet na podstawie informacji o koncie użytkownika domeny UK. Uprawnienia dostępu do poszczególnych usług mogą być przyznawane i odbierane pojedynczym użytkownikom lub grupom zdefiniowanym w ramach usługi katalogowej.

Mechanizm ten powinien zostać wykorzystany w ramach usług systemu informatycznego do zapewnienia możliwości kontroli nad dostępem użytkowników do zasobów sieci Internet.

Standardowo już architektura systemów przewiduje stosowanie mechanizmów typu firewall, coraz częściej w postaci software, z uwagi na częstotliwość aktualizacji definicji. Zwykle niezbędna jest rozbudowana zapora filtrująca ruch do warstwy aplikacji włącznie. Dobrym rozwiązaniem jest integracja mechanizmów zapory z architekturą VPN, co umożliwia kontrolę i filtrowanie z pamięcią stanu całego ruchu w kanałach VPN, a także kontrolę dostępu klientów VPN przez mechanizm kwarantanny. Pozwala to na zabezpieczenie sieci przed atakami zewnętrznymi przeprowadzanymi przez połączenia VPN.

Ponadto warto przewidzieć w zakresie komponentu dostępowego następujące funkcjonalności:

- zapewnienie wydajnego i bezpiecznego dostępu do zasobów sieci Intranet i Internet,
- zabezpieczenie i publikacja usług sieci dostępnych od strony sieci zewnętrznych,
- zapewnienie kontroli nad dostępem użytkowników do sieci Internet,
- możliwość pracy w trybie „*web cache*" buforując strony internetowe i dostarczając je użytkownikom z kopii lokalnej,

- optymalizacja ruchu Web proxy,
- kontrola dostępu do usług na bazie uprawnień opartych na definicji użytkowników i ich grup w usługach katalogowych.

4.1.12. BEZPIECZEŃSTWO STACJI ROBOCZYCH

Oddzielnym problemem jest zdefiniowanie i wdrożenie bezpieczeństwa stacji roboczej, co w szerokim zakresie zostało przedyskutowane w opracowaniu „Komputer Przyszłości”[32].

Wychodząc od postulatu zabezpieczenia informacji, autorzy twierdzą, że zapewnienie bezpieczeństwa komputera wymaga uwzględnienia kilku obszarów:

- Informacje zawsze bezpieczne – zaszyfrowane, niedostępne dla osób niepowołanych, zabezpieczone przed dostępem po kradzieży lub zgubieniu, przesyłane bezpiecznymi kanałami komunikacji poprzez:
    - szyfrowania danych na każdym poziomie - dysku twardego, plików, dokumentów, kanałów komunikacji,
    - uniemożliwienie kopiowania informacji na zewnątrz za pomocą nośników zewnętrznych lub poprzez witryny internetowe,
    - przechowywane danych na serwerach – dane nigdy nie znajdują się na stacjach roboczych Pracowników,
    - zabezpieczenie, zaszyfrowanie i archiwizację danych.
- Kontrola platformy – system i aplikacje – znana, zdefiniowana i kontrolowana platforma systemu operacyjnego, ochrona przed niepowołanym dostępem, ochrona przed kradzieżą, odpowiednio dobrane i skonfigurowane aplikacje, stała kontrola i zarządzanie stacją niezależnie od tego, czy znajduje się ona wewnątrz lub zewnątrz sieci, gwarancja bezpieczeństwa danych przy złomowaniu, jak też dopuszczanie do komunikacji w środowisku tylko tych stacji, które spełniają wymogi bezpieczeństwa w konfiguracji.

[32] *Adam Dzwonkowski, Microsoft 2009*

- Kontrola uprawnień i aktywności użytkownika – użytkownik ma odgórnie zdefiniowane uprawnienia, jego aktywność jest kontrolowana i audytowana w czasie rzeczywistym.
- Kontrola środowiska – obszar ten obejmuje kontrolę notebooka poza siecią firmy, wykorzystanie „komputera w sejfie" dostępnego tylko zdalnie przez bezpieczne kanały komunikacji, rozdzielenie komputera do pracy biurowej z komputerem do pracy z informacjami niejawnymi, jak także możliwość wykorzystania bezpiecznego korzystania z komputera z kafejki internetowej, w dowolnej lokalizacji na świecie.

Dodatkowe problemy związane z bezpieczeństwem systemów i informacji poruszone zostały w rozdziale „Założenia interoperacyjności". Szersze opracowanie tego problemu można znaleźć w opracowaniu RISA[33] – Ramy Interoperacyjności Systemów Administracji.

4.1.12.1. STANDARYZACJA STACJI ROBOCZYCH

Wprowadzenie sprawnych mechanizmów zarządzania i monitorowania stacji roboczych nie jest warunkiem dostatecznym osiągnięcia stanu kontroli nad zasobami systemowymi na poziomie stanowiska pracy. Bardzo ważnym elementem, związanym tez z bezpieczeństwem i wdrożeniem odpowiednich polityk, jest standaryzacja konfiguracji stacji roboczej. Dotyczy ona takich obszarów standaryzacji jak:

- konfiguracja systemu operacyjnego,
- właściwy zestaw aplikacji i uprawnionych usług na danym stanowisku,
- właściwa konfiguracja pod kątem współpracy z siecią organizacji oraz systemami zarządzania i monitorowania,
- legalność zestawu zainstalowanego oprogramowania,
- bezpieczeństwo.

Standaryzacja pozwala na zdefiniowanie i utrzymywanie wielu zasad pozwalających na bezpieczeństwo systemu i danych, podniesienie dostępności usług systemu i znaczne obniżenie kosztów jego eksploatacji.

[33] https://bfcoea.bn1304.livefilestore.com/y3mgu-nB-Q5L36HYpHUG1H2Xk2Xd6cfvi9lrfzprtRK85J1CLLBRIKnfYaslpdh-sbLEN7GV1p_ia7yTtZQBCEzux4i3A3cusk-QjrLHYAkn9KcYrs4BKkrtfmuNAqqIWCnJpv7pGIaOUuMRgSQHgFzIg/RISA_PL_V4.pdf?psid=1

Aby zapewnić bezpieczeństwo i zarządzalność stacji roboczej autorzy opracowania „Komputer Przyszłości”[34] proponują ustalenie i egzekwowanie następujących zasad:

- Pracownik jest przypisany do określonej roli i na tej podstawie posiada odpowiednią konfigurację swojej stacji roboczej, dostępnych aplikacji i zestawu uprawnień.
- Przygotowanie lub odbudowanie stacji dla pracownika odbywa się automatycznie lub półautomatycznie.
- Konfiguracja stacji roboczej Pracownika jest zawsze taka sama, zdefiniowana, znana, kontrolowana.
- Możliwa jest automatyzacja procesu instalacji stacji roboczej od zera, jak i procesu podniesienia wersji systemu operacyjnego na już istniejących stacjach roboczych.
- Pracownicy mają zestaw aplikacji im przypisanych, które wędrują za użytkownikiem i są dostępne do użycia niezależnie od stacji roboczej, lub laptopa, z którego korzysta pracownik, jak też niezależnie od lokalizacji – wewnątrz organizacji, lub na zewnątrz.
- Wędrujące aplikacje pojawiają się „w locie”, zaraz po zalogowaniu się pracownika na swoje konto na dowolnej stacji roboczej lub laptopie, w postaci skrótów na pulpicie i w menu.
- Pracownicy nie mogą uruchamiać i korzystać z aplikacji innych, niż im przypisane.
- Dane generowane na dowolnych stacjach roboczych przez aplikacje są zawsze dostępne dla użytkownika, ponieważ nie są one zlokalizowane na aktualnie wykorzystywanej maszynie.
- Aplikacje Pracownika są dostępne do użycia przez określony okres, po którym mogą wygasać i wymagać ponownej aktywacji przez administratora danej aplikacji i upewnienia się, że Pracownik wciąż potrzebuje danego oprogramowania, lub że aplikacja wciąż posiada ważną i aktywną licencję.
- Pracownicy mobilni muszą podłączyć się do sieci i uwierzytelnić w celu aktywacji wygaszonych aplikacji.

[34] *Adam Dzwonkowski, Microsoft 2009*

- Aplikacje nie są zainstalowane na stacji roboczej Pracownika, czyli nie robią żadnych zmian w konfiguracji plików, rejestrze systemu, skojarzeniach rozszerzeń plików, ale pomimo to działają wykorzystując możliwości obliczeniowe stacji Pracownika, a nie serwerów.
- Dzięki temu, że aplikacja nie jest zainstalowana, szybkie i bezpieczne dla konfiguracji stacji jest jej usunięcie, bez pozostawienia jakichkolwiek danych – śmieci.
- Konfiguracja systemów operacyjnych jest kontrolowana w porównaniu z określonym wzorcem (np. konfiguracją bazową). Odstępstwa od standardowych konfiguracji mogą być powodem awarii i przestoju w działaniu aplikacji, lub świadczyć o zagrożeniu pod kątem bezpieczeństwa środowiska. Kontrola konfiguracji może być wykonana w zakresie parametrów w rejestrze, wpisów w plikach konfiguracyjnych, uprawnieniach.

Ważnym elementem bezpieczeństwa – często pomijanym – jest konieczność kontroli nad obrazem oprogramowania stacji roboczej, czy urządzenia przenośnego. Często wybierany jest model dostawy urządzeń klienckich z zainstalowanych systemem operacyjnym i zakupionym jednocześnie oprogramowaniem standardowym. Szansa na pełną kontrolę CO i JAK zostało zainstalowane przez dostawcę w takim scenariuszu - jest znikoma.

Tak więc jedynym prawidłowym rozwiązaniem jest przygotowanie obrazów zawierających zestaw oprogramowania i konfigurację, odpowiadających potrzebom wyodrębnionych grup użytkowników, przetestowanie ich, wgranie na urządzenia, a następnie stała ich pielęgnacja i monitoring.

4.1.12.2. OCENA BEZPIECZEŃSTWA STACJI ROBOCZYCH

W przypadku gdy nie stosujemy standardowych, sprawdzonych i pielęgnowanych obrazów stacji roboczych, dosyć trudne jest dokonanie oceny stanu ich zabezpieczenia. w takich przypadkach można zastosować narzędzia, które w przybliżony sposób ocenią stan bezpieczeństwa urządzeń klienckich.

Takim narzędziem jest Secure Score zawarte w pakiecie Microsoft Defender for Endpoint[35]. Mechanizm ten pozwala ocenić, czy podstawowe elementy ochrony urządzenia są zaimplementowane i działają poprawnie, dając w skali punktowej wynik dla każdej z zdefiniowanych metryk.

Jednocześnie rekomendowane są podstawowe działania podwyższające wynik dla urządzenia, takie jak:

- zainstalowane aktualne poprawki bezpieczeństwa dla systemu operacyjnego – do 72 pkt;
- włączone mechanizmy Exploit Guard – do 33 pkt;
- zdefiniowane foldery dla działania Exploit Guard – do 32 pkt;
- skonfigurowane raporty i akcje systemu antywirusowego – do 19 pkt;
- włączony Credential Guard – do 17 pkt;
- włączona ochrona BitLocker – do 17 pkt;
- szyfrowanie dysków – do 8 pkt;
- skonfigurowany mechanizm Windows Hello – do 7 pkt.

Należy pamiętać, że bezpieczeństwo jest procesem dynamicznym, a więc jednokrotne dokonanie oceny nie daje nam właściwej oceny bezpieczeństwo. Dużo lepszym rozwiązaniem jest okresowe (np. codzienne) badanie statusu bezpieczeństwa i przygotowanie automatycznie dostarczanych raportów o spadku sumarycznej liczby punktów poniżej zdefiniowanego progu.

4.1.12.3. KLASYFIKACJA BEZPIECZEŃSTWA STACJI ROBOCZYCH

Ochrona dużej liczby urządzeń klienckich w organizacji na najwyższym możliwym poziomie jest droga i angażująca zasoby. Dlatego też firma Microsoft proponuje klasyfikację grup stacji roboczych w zależności od sposobu ich wykorzystania, a co za tym idzie – oczekiwanego poziomu bezpieczeństwa[36] nazywanego dalej indeksem bezpieczeństwa.

[35] https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-microsoft-secure-score-devices?view=o365-worldwide
[36] https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md

Proponowany podział na grupy bezpieczeństwa urządzeń końcowych wygląda następująco:

Dla typowych stacji roboczych

- Poziom 5 – poziom podstawowy – określony jako minimalne wymagania bezpieczeństwa dla wszystkich urządzeń.
- Poziom 4 – poziom podstawowy podwyższony – dla stacji roboczych których użytkownicy mają dostęp do danych wrażliwych.
- Poziom 3 – poziom wysoki – dla urządzeń wykorzystywanych przez użytkowników mających dostęp do danych mających krytyczny wpływ na działanie organizacji, na przykład objętych tajemnicą przedsiębiorstwa.

Dla stacji z uprzywilejowanym dostępem

- Poziom 2- poziom uprzywilejowany podstawowy – dla urządzeń wykorzystywanych przez programistów czy testerów stanowiących atrakcyjny cel ataków.
- Poziom 1 – poziom uprzywilejowany wysoki – dla urządzeń wykorzystywanych przez administratorów systemów, w szczególności, gdy ich uprawnienia nie mają ograniczeń czasowych i zakresu uprawnionych działań.

4.1.13. OCHRONA ANTYWIRUSOWA

Z uwagi na to, że każdego dnia pojawiają się nowego typu zagrożenia bezpieczeństwa systemów teleinformatycznych – wirusy, robaki, trojany, rootkity, ataki typu phishing czy exploity zero-day, wymaganym składnikiem systemu jest komponent bezpieczeństwa, który ma zminimalizować ryzyko infekcji systemu. Tego typu ataki związane z ochroną na zbyt niskim poziomie, są ciągle największą przyczyną strat danych lub nieupoważnionego dostępu do nich.

Założeniem jest budowa jednolitego systemu ochrony przed wirusami i oprogramowaniem szpiegowskim, przeznaczonego do zastosowania na komputerach stacjonarnych, laptopach i serwerach, łatwy w zarządzaniu i kontroli. Zapewniając prostą administrację możliwą dzięki centralnemu zarządzaniu oraz wykrywanie zarówno zagrożeń, jak i słabości systemu, system antywirusowy ma wspomagać wydajną i skuteczną obronie sieci.

Projektowane rozwiązanie składa się z dwóch elementów: pierwszym jest agent zabezpieczeń, instalowany na komputerach stacjonarnych, laptopach i serwerach, pozwalający zarówno na monitorowanie w czasie rzeczywistym, jak i planowane skanowanie w poszukiwaniu wirusów, oprogramowania szpiegowskiego i innych zagrożeń. Drugi element to centralny system zarządzania, pozwalający administratorom w prosty sposób zarządzać agentami zabezpieczeń, aktualizować je instalując najnowsze sygnatury, a także generować raporty i alerty dotyczące stanu zabezpieczeń.

4.1.14. BEZPIECZEŃSTWO W CHMURZE

W odróżnieniu od kosztownego i czasochłonnego procesu budowy własnych narzędzi bezpieczeństwa, korzystając z usług właściwie zaprojektowanej chmury, otrzymujemy je jako immanentny składnik usług. Nie oznacza to, że automatycznie zapewniamy swoim systemom opartym na chmurze bezpieczeństwo – mamy tylko taką możliwość. Należy świadomie zaprojektować zasady bezpieczeństwa, skonfigurować i użyć tych narzędzi.

Platforma Azure to platforma usługi w chmurze publicznej obsługująca szeroki zakres systemów operacyjnych, języków programowania, struktur, narzędzi, baz danych i urządzeń.

Usługi chmury publicznej platformy Azure obsługują technologie wytworzone i przetestowane przez wielu dostawców.

Infrastruktura platformy Azure została zaprojektowana dla obsługi setek milionów klientów, udostępniając szeroki zakres konfigurowalnych opcji zabezpieczeń oraz możliwość sterowania nimi, dzięki czemu można było dostosować zabezpieczenia, aby spełniały specyficzne wymagania wdrożenia w organizacji.

4.2. NARZĘDZIA CYBERSECURITY

Problem bezpieczeństwa w systemach informacyjnych występuje praktycznie w każdej fazie planowania, budowy i utrzymania. Pojawiał się też wielokrotnie w niniejszym dokumencie w kontekście założeń do różnych komponentów. Aby nie powtarzać już opisanych zagadnień wskażemy tylko kilka dodatkowych możliwości wynikających wprost z zastosowania rozwiązań Microsoft.

Oprócz mechanizmów bezpieczeństwa wbudowywanych we własną infrastrukturę, coraz częstszym przypadkiem jest korzystanie z gotowych usług bezpieczeństwa z „chmury”. Jest

to rozwiązanie wielokrotnie tańsze, bezpieczniejsze i bardziej efektywne od budowy, utrzymania i rozwoju własnych rozwiązań w tym zakresie. Przykładem mogą być opisane poniżej usługi bezpieczeństwa Microsoft, zgodnie z raportami firmy Gartner - lidera w tym zakresie[37].

Spoób licencjonowania tych usług można znaleźć pod adresem - Microsoft 365 guidance for security & compliance - Service Descriptions | Microsoft Docs

4.2.1. AZURE MONITOR

Azure Monitor to zespół usług pomagających zmaksymalizować dostępność i wydajność aplikacji i usług w chmurze hybrydowej. Zapewnia kompleksowe rozwiązanie do zbierania, analizowania i działania na podstawie telemetrii ze środowisk chmurowych i lokalnych. Te informacje pomagają proaktywnie identyfikować problemy, które mają wpływ na aplikacje oraz zasoby, od których są zależne.

W ramach Azure Monitor można wyróżnić następujące usługi:

- Wykrywanie i diagnozowanie problemów w aplikacjach i zależnościach za pomocą Application Insights.
- Korelację problemów z infrastrukturą przy pomocy VM insights i Container insights.
- Szczegółową analizę danych monitorowania za pomocą Log Analytics w celu rozwiązywania problemów i szczegółowej diagnostyki.
- Wspieranie skalowania systemów za pomocą automated actions.
- Tworzenie wizualizacji działania platformy Azure za pomocą dashboards i workbooks.
- Zbieranie danych z monitorowanych zasobów[38] za pomocą Azure Monitor Metrics.
- Badanie zmian w danych w celu rutynowego monitorowania lub klasyfikacji incydentów za pomocą Change Analysis.

[37] *https://www.microsoft.com/pl-pl/security/business/security-leaders-gartner-magic-quadrant*
https://www.gartner.com/doc/reprints?id=1-27UADDR3&ct=211102&st=sb
[38] *https://docs.microsoft.com/en-us/azure/azure-monitor/monitor-reference*

Wynikiem działania Azure Monitor jest zaadresowanie niezwykle ważnego obszaru bezpieczeństwa, jakim jest realizacja postulatów monitorowania i rozliczalności w systemach.

Jej działanie polega na zbieraniu danych z systemów, zarówno tych osadzonych we własnej infrastrukturze jak i w infrastrukturze– np. na platformie Azure.

Analizie podlegają dane powstające na skutek aktywności zasobów systemów – zarówno użytkowników jak i zasobów sprzętowo-programowych. Wyniki takich analiz, zawierających dane syntetyczne, korelacje i trendy, są przedstawiane w postaci raportów oraz wizualizowane w kokpitach zarządczych.

W poniższym scenariuszu przedstawiony jest schemat działania usługi.

1. Użytkownik korzysta z zasobów Azure.
2. Strona na Azure korzysta z zasobów danych strukturalnych w Azure SQL Database.
3. Strona internetowa Azure generuje dane o aktywności użytkownika.
4. Akcje użytkowników systemów hostowanych i własnych są zapisywane w dziennikach zdarzeń.
5. Powstające dane niestrukturalne i semistrukturalne są przechowywane w magazynie Blob udostępniane pozostałym komponentom.
6. HDInsight przetwarza dane z magazynu blob wykorzystując narzędzia technologii Hadoop takie jak Hive, Pig i Mahout. Może też orkiestrować przemieszczanie danych wykorzystując Sqoop i Oozie. Dla zadań czasu rzeczywistego wykorzystuje Storm i HBase.
7. HDInsight wspiera PowerShell dla automatyzacji zadań takich jak tworzenie i usuwanie klastrów danych, uruchamianie programów MapReduce, Realizacja komend Hive i wiele innych.
8. SQOOP współdziała z danymi strukturalnymi, na przykład z bazy danych SQL w Azure w celu importu i eksportu danych z klastrów danych HDInsight (Hadoop).
9. Dane przetwarzane w HDInsight zasilają istniejące hurtownie poprzez narzędzia ETL.

10. Azure Machine Learning (ML) wykorzystuje dane w tabelach Hive wykrywając i przewidując przyszłe trendy lub wspomagając analizy dostępności i bezpieczeństwa.
11. ML zasila hurtownie informacją predykcyjną.
12. ML dostarcza też informację predykcyjną poprzez stronę internetową Azure.
13. Hurtownia danych zasila systemy analizy danych takich jak Power BI, SQL Server Analysis Services czy własne aplikacje tworzące modele danych.
14. HDInsight przesyła przetworzoną i wyselekcjonowaną informację od komponentu BI.
15. Komponent BI publikuje modele danych dla kokpitów informacyjnych i raportów wykorzystujących Power View, Power Map, SQL Server Reporting Services i SharePoint BI.

4.2.2. AZURE ACTIVE DIRECTORY IDENTITY PROTECTION

Ponieważ tożsamość cyfrowa jest kluczowym elementem ochrony informacji, usług i systemów, więc bezpieczeństwo jest krytycznie ważne. Należy też pamiętać, że AAD jest „nośnikiem" tożsamości cyfrowej użytkowników dla wszystkich usług z chmury Microsoft.

Usługa AADIP umożliwia organizacjom osiągnąć następujące cele:

- Automatyzację wykrywanie i korygowanie zagrożeń związanych z tożsamością.
- Badanie zagrożeń za pomocą danych w portalu.
- Eksportowanie danych wykrywania ryzyka do innych narzędzi.

Sygnały generowane przez ochronę tożsamości mogą być dalej przekazywane do narzędzi takich jak:

- Dostęp warunkowy - w celu podejmowania decyzji dotyczących dostępu.
- SIEM w celu dalszego zbadania.

Usługa AADIP umożliwia dla systemów bazujących na Azure Active Directory:

- Ochronę tożsamości, niezależnie od ich poziomu uprawnień.
- Proaktywne zabezpieczanie użycia skompromitowanych tożsamości.

AADIP oferuje następujące funkcje ochrony tożsamości:

- Udostępnia pulpit nawigacyjny ochrony tożsamości.
- Wykrywa luki w zabezpieczeniach i wskazuje konta wysokiego ryzyka.
- Generuje niestandardowe zalecenia, aby poprawić ogólny stan zabezpieczeń przez wyróżnianie luk w zabezpieczeniach.
- Oblicza poziom ryzyka logowania.
- Oblicza wskaźniki ryzyka dla użytkownika.
- Bada zdarzenia o podwyższonym ryzyku.
- Bada i wysyła powiadomienia dla zdarzeń o podwyższonym ryzyku.
- Zapewnia mechanizmy przepływu pracy wspomagające śledzenie naruszenia bezpieczeństwa tożsamości.
- Zapewnia łatwy dostęp do krytycznych akcji, takich jak resetowanie haseł.
- Wprowadza zasady dostępu warunkowego dla kont uprzywilejowanych na podstawie szacunku ryzyka.

4.2.3. DDOS PROTECTION

Ataki typu „rozproszona odmowa usługi" (*Distributed Denial of Service*, DDoS) należą do największych obaw związanych z dostępnością i zabezpieczeniami wśród klientów, którzy udostępniają swoje zasoby i usługi w sieci internet.[39] Atak DDoS polega na próbie wyczerpania zasobów aplikacji, przez co aplikacja staje się niedostępna dla zwykłych użytkowników. Celem ataku DDoS może być dowolny punkt końcowy publicznie dostępny za pośrednictwem Internetu.

Usługa *Azure DDoS Protection* zapewnia następujące rodzaje funkcji:

Podstawowe: Automatycznie włączone w ramach subskrypcji platformy Azure, zapewniające monitorowanie ruchu, a także ograniczenie w czasie rzeczywistym typowych ataków na poziomie sieci.

Standardowe: Udostępniające dodatkowe zabezpieczenia skierowane na ochronę zasobów usługi Azure Virtual Network. Usługi z tej grupy nie wymagają dodatkowej konfiguracji

[39] *Kumud Dwivedi, Microsoft 2018*

aplikacji. Za pomocą dedykowanego monitorowania i algorytmów uczenia maszynowego następuje dostosowanie zasad ochrony. Zasady są stosowane do publicznych adresów IP skojarzonych z zasobami wdrożonymi w sieciach wirtualnych, takich jak usługa Azure Load Balancer, Azure Application Gateway i usługi Azure Service Fabric. Ta ochrona nie ma zastosowania do środowiska usługi App Service. Telemetria usług, zarówno on-line jak i danych historycznych, jest dostępna dzięki Azure Monitor.

4.2.4. AZURE WEB APPLICATION FIREWALL

Azure Web Application Firewall to wbudowana w chmurę Microsoft usługa, która chroni aplikacje internetowe przed typowymi technikami hakowania sieci Web, takimi jak wstrzykiwanie kodu SQL, oraz lukami w zabezpieczeniach, takimi jak skrypty międzywitrynowe.

Podstawowymi funkcjami Azure WAF są:

- Kompleksowa ochrona dla określonych w Open Web Application Security Project (OWASP) dziesięciu najważniejszych zagrożeń bezpieczeństwa.
- Niestandardowe i zarządzane zestawy reguł zapobiegające złośliwym atakom na brzegu sieci.
- Wgląd w czasie rzeczywistym w środowisko i alerty bezpieczeństwa.
- Pełna obsługa interfejsu API REST w celu automatyzacji procesów DevOps.

4.2.5. AZURE FRONT DOOR

Azure Front Door to usługa sieciowa dostarczania zawartości z chmury (CDN), która zapewnia wysoką wydajność, skalowalność i bezpieczne środowisko użytkownika dla danych i aplikacji.

Oferuje ona następujące funkcje:

- Narzędzia i DevOps do automatyzacji i usprawnienia wdrożeń.
- W pełni konfigurowalny silnik reguł dla zaawansowanego routingu.
- Skalowalność dzięki globalnemu równoważeniu obciążenia HTTP i przełączaniu awaryjnemu.

- Dołączanie zapory aplikacji internetowych (WAF), ochronę DDoS i ochrona botów w zakresie ochrony aplikacji i treści.

4.2.6. ROLE BASED ACCESS CONTROL

Kontrola dostępu oparta na rolach (*Role Based Access Control* – RBAC) jest systemem pozwalającym precyzyjnie zarządzać uprawnieniami do danych i usług na platformie Azure na bazie uprawnień ról zdefiniowanych w systemie, także w kontekście przydziału zadań w zespołach. RBAC wykorzystuje usługę *Azure Resource Manager*[40] zapewniającą spójną warstwę zarządzania, umożliwiającą tworzenie, aktualizowanie i usuwanie zasobów w subskrypcji platformy Azure.

Przykładami użycia RBAC są:

- Zezwolenie jednemu użytkownikowi na zarządzanie maszynami wirtualnymi w ramach subskrypcji, a innemu na zarządzanie sieciami wirtualnymi.
- Zezwolenie grupie administratorów baz danych na zarządzanie bazami danych SQL w ramach subskrypcji.
- Zezwolenie użytkownikowi na zarządzanie wybranymi zasobami w grupie zasobów, w tym maszynami wirtualnymi, witrynami internetowymi i podsieciami.
- Zezwolenie aplikacji na dostęp do wybranych zasobów w grupie zasobów.

4.2.7. APPLICATION GATEWAY

Usługa Application Gateway (AG) pozwala na równoważenie obciążenia ruchu internetowego z zarządzaniem ruchu do konkretnej aplikacji internetowej w odróżnieniu od tradycyjnych rozwiązań działających w warstwie transportu na podstawie źródłowego adresu IP i portu do docelowego adresu IP i portu.

AG pozwala kierować ruch na podstawie przychodzącego adresu URL. Jeśli w przychodzącym adresie URL jest element /obrazy, można kierować ruch do określonego zestawu serwerów (nazywanego pulą) skonfigurowanego na potrzeby obrazów, a zawierające element /video kierowane są do innej puli, która jest zoptymalizowana pod kątem filmów wideo.

[40] https://docs.microsoft.com/pl-pl/azure/azure-resource-manager/resource-group-overview

Usługa automatycznie skaluje się w górę lub dół zależności od zmieniających się wzorców obciążenia ruchu.

4.2.8. VPN GATEWAY

Usługa VPN Gateway to specyficzny typ bramy sieci wirtualnej, która służy do wysyłania zaszyfrowanego ruchu sieciowego między siecią wirtualną platformy Azure, a siecią lokalną za pośrednictwem publicznego Internetu. Za pomocą bramy sieci VPN można także wysyłać zaszyfrowany ruch sieciowy między sieciami wirtualnymi platformy Azure za pośrednictwem sieci dedykowanej firmy Microsoft. Każda sieć wirtualna może mieć tylko jedną bramę sieci VPN. Można jednak utworzyć wiele połączeń do tej samej bramy sieci VPN. w przypadku utworzenia wielu połączeń do tej samej bramy sieci VPN wszystkie tunele VPN współdzielą dostępną przepustowość bramy.

4.2.9. MICROSOFT PURVIEW INFORMATION PROTECTION

Microsoft Purview Information Protection to zespół usług bezpieczeństwa w ramach usługi Purview opisanej dalej w tym opracowaniu.

Jest to kompleksowy zestaw rozwiązań firmy Microsoft, które ułatwiają zarządzanie całym zasobem danych, ich ochronę i zarządzanie nimi. Łącząc dawną platformę Azure Purview i dawne portfolio Microsoft 365 Compliance pod jedną nazwą[41]. Główne zadania nowej usługi[42] pozwalają na:

Rozpoznanie danych w organizacji

Nie jest możliwa ochrona danych organizacji bez ich rozpoznania. Aby zrozumieć strukturę danych, miejsce ich składowania, sposób użycia i zidentyfikować poufne dane w środowisku hybrydowym, można użyć następujących funkcji:

- Identyfikacji poufnych danych za pomocą wbudowanych lub niestandardowych wyrażeń regularnych albo funkcji.

[41] https://azure.microsoft.com/pl-pl/blog/azure-purview-is-now-microsoft-purview/
[42] https://docs.microsoft.com/en-us/azure/purview/overview

- Identyfikuje poufne dane, używając przykładów danych, które przeglądamy, zamiast identyfikować elementy poprzez dopasowywanie wzorców. Możliwe jest użycie wbudowanych klasyfikatorów lub budowa klasyfikatorów z własną zawartością.
- Graficznie identyfikuje zasoby w organizacji, które mają etykietę poufności, etykietę przechowywania lub zostały sklasyfikowane w inny sposób. Na podstawie tych informacji można uzyskać wgląd w działania podejmowane przez użytkowników na tych zasobach.

Ochrona danych

Aby zastosować działania chroniące dane (np. szyfrowanie, ograniczenia dostępu i oznaczenia wizualne, można użyć następujących funkcji:

- Spójnego etykietowania danych w aplikacjach, usługach i na urządzeniach w celu ochrony danych podczas ich przesyłania wewnątrz i na zewnątrz organizacji.
- Na urządzeniach z systemem Windows rozszerzenie zakresu etykietowania na Eksploratora plików i PowerShell, czy dodatkowych funkcji aplikacji pakietu Office.
- Przy odpowiednich uprawnieniach - odszyfrowania chronionej informacji lub ze względu na wymagania prawne przechowywania kluczy szyfrowania w określonej lokalizacji.
- Szyfrowania wiadomości e-mail i załączonych dokumentów, które są wysyłane do dowolnego użytkownika na dowolnym urządzeniu, dzięki czemu tylko uprawnieni odbiorcy mogą odczytywać informacje wysłane pocztą e-mail.
- Ochrona przed odczytem danych przez nieautoryzowane systemy lub personel.
- Ochrona list i bibliotek programu SharePoint, dzięki czemu, gdy użytkownik wyewidencjonuje dokument, pobrany plik jest chroniony, i tylko upoważnione osoby mogą odczytać plik i używać go zgodnie z zasadami określonymi w organizacji.
- Ochrona dla istniejących wdrożeń lokalnych korzystających z programu Exchange, SharePoint albo serwerów plików z systemem Windows Server i infrastrukturą klasyfikacji plików (FCI).

- Dzięki ujednoliconemu skanerowi etykiet usługi Information Protection odnajdowanie, etykietowanie i ochrona poufnych informacji znajdujących się w lokalnych zasobach danych.
- Dzięki usłudze Defender for Cloud Apps odnajdowanie, etykietowanie i ochrona poufnych informacji znajdujących się w chmurze.
- Identyfikacja poufnych danych i stosowania automatycznego etykietowania do zawartości w zasobach Microsoft Purview Data Map, w tym Azure Data Lake i Azure Files, oraz dane schematyzowane, takie jak kolumny w Azure SQL DB i Cosmos DB.
- Dzięki pakietowi Microsoft Information Protection SDK rozszerzanie zakresu etykietowania na wytwarzane aplikacje i usługi.

Zapobieganie wyciekowi danych

Aby zapobiec celowemu, przypadkowemu lub nadmiarowemu udostępnianiu poufnych informacji, można użyć następujących funkcji:

- Microsoft Purview Data Loss Prevention (DLP) - zapobiega nieuprawnionemu udostępnianiu poufnych zasobów.
- Endpoint data loss prevention - rozszerza zakres działania DLP na elementy, które są używane i udostępniane na komputerach z systemem Windows 10 i Windows 11.
- Microsoft Compliance Extension - rozszerza zakres działania DLP na przeglądarkę Chrome.
- Microsoft Purview data loss prevention on-premises scanner - rozszerza zakres monitoringu DLP na lokalne udziały plików oraz foldery i biblioteki dokumentów programu SharePoint.
- Rozszerza niektóre funkcje DLP na czaty i wiadomości kanałów Teams.

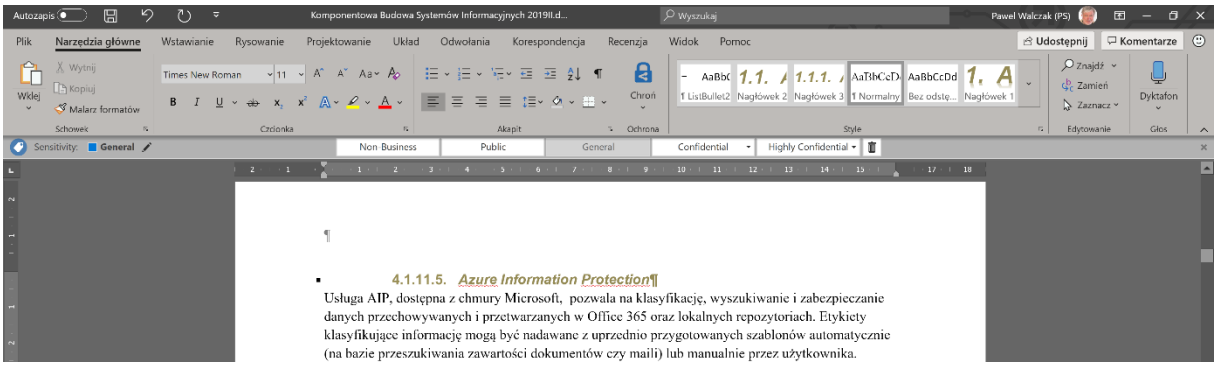
4.2.10. PODSTAWOWE KOMPONENTY PURVIEW INFORMATION PROTECTION

4.2.10.1. INFORMATION PROTECTION

Usługa Information Protection, dostępna z chmury Microsoft, pozwala na klasyfikację, wyszukiwanie i zabezpieczanie danych przechowywanych i przetwarzanych w Office 365 oraz lokalnych repozytoriach. Jest to kluczowy mechanizm dla ochrony informacji, gdyż musimy

wiedzieć CO chronimy a następnie dobrać odpowiednie metody zabezpieczeń. Jest też wstępem do opisanej uprzednio klasyfikacji stacji roboczej. Etykiety klasyfikujące informację mogą być nadawane z uprzednio przygotowanych szablonów automatycznie (na bazie przeszukiwania zawartości dokumentów czy maili) lub manualnie przez użytkownika. Dotyczy to zarówno już istniejącej, składowanej czy edytowanej informacji, jak i procesu opatrywania nowo tworzonych dokumentów/maili. Nadanie odpowiedniej klasyfikacji powoduje dodanie metadanych do dokumentu, które mogą być wykorzystywane przez różne aplikacje i systemy.

Obecnie wszystkie aplikacje klienckie w Office 365 wyposażone są w narzędzie wskazujące jak sklasyfikowana została informacja oraz umożliwiające (po podaniu powodu) zmienić tą klasyfikację.



Szablony etykiet mogą być (po zatwierdzeniu) przygotowane i dystrybuowane w całej organizacji.

Dodatkowo można zastosować mechanizm *Azure Rights Management*, co po wybraniu odpowiedniej etykiety (np. „dane osobowe”) spowoduje automatyczne zaszyfrowanie informacji z wybranymi uprawnieniami dostępu.

Ten sam mechanizm klasyfikacji danych jest też dostępny w usłudze Purview dla danych w środowiskach hybrydowych.

4.2.10.2. COMMUNICATION COMPLIANCE

Microsoft Purview Communication Compliance to rozwiązanie do analizy ryzyka wewnętrznego, które pomaga zminimalizować ryzyko związane z komunikacją, pomagając wykrywać, przechwytywać niezgodne z politykami wiadomości w organizacji i reagować na nie.

Zasady uprawnionego przekazywania informacji komunikacji w organizacji pomagają przezwyciężyć wiele wyzwań związanych ze zgodnością oraz komunikacją wewnętrzną i zewnętrzną, w tym:

- coraz większej liczby typów kanałów komunikacji,
- rosnącej liczby danych wiadomościach,
- egzekwowania przepisów,
- ryzyka kar.

Zalecany jest rozdział obowiązków między administratorami IT a zespołem zarządzania zgodnością. Zgodność komunikacji ułatwia oddzielenie konfiguracji zasad od badania i przeglądania komunikatów. Na przykład grupa IT w organizacji może być odpowiedzialna za konfigurowanie uprawnień, grup i zasad roli zgodności z komunikacją, a badacze i recenzenci mogą być odpowiedzialni za klasyfikację wiadomości, przegląd i działania ograniczające zagrożenie.

Propozycje dotyczące planowania rozwiązania problemu zgodności i ryzykownych działań w organizacji opisane są w dokumencie Uruchamianie programu zarządzania ryzykiem wewnętrznym.

Najnowsze prezentacje dotyczące zgodności komunikacji można znaleźć w następujących filmach:

- Wspieranie kultury bezpieczeństwa i integracji dzięki zgodności z komunikacją
- Zmniejszanie ryzyka związanego z komunikacją w organizacji
- Wymagania zgodności z przepisami w zakresie komunikacji
- Zintegrowane funkcje Teams w zakresie zgodności komunikacji

4.2.10.3. COMPLIANCE MANAGER

- Pozwala spełnić wymagania dotyczące zasad zgodności z globalnymi, przemysłowymi lub lokalnymi przepisami i standardami w środowiskach hybrydowych.
- Oferuje kompleksowe funkcje zarządzania zgodnością, takie jak zarządzanie przepływem pracy, wdrażanie kontroli i katalogowanie dowodów.

- Umożliwia korzystanie z gotowych, konfigurowalnych i wielochmurowych szablonów oceny regulacyjnej.
- Zmniejsza ryzyko braku zgodności dzięki funkcjom, takim jak ocena zgodności, mapowanie kontroli, wersjonowanie i raporty kontroli.
- Dostarcza ponad 300 gotowych do użycia i konfigurowalnych szablonów oceny zgodności stosowanych usług z regulacjami.

4.2.10.4. DATA LIFECYCLE MANAGEMENT

- Klasyfikuje i zarządza danymi na dużą skalę, w celu uzyskania zgodności z prawem, politykami prywatności i regulacyjne obowiązki dotyczące treści.
- Klasyfikuje, przegląda i usuwa dane na platformie Microsoft 365.
- Korzysta z inteligentnych funkcji uczenia maszynowego, aby klasyfikować zawartość i automatycznie stosować odpowiednie zasady.
- Dostarcza informacji o działaniach na danych, dowody usunięcia i udokumentowane ścieżki audytu z zarządzaniem informacjami.

4.2.10.5. DATA LOSS PREVENTION

Automatycznie chroni poufne informacje przed nieautoryzowanym i nieuprawnionym dostępem do aplikacji, usług, punktów końcowych i plików.

Organizacje mają pod swoją kontrolą poufne informacje, takie jak dane finansowe, dane zastrzeżone, numery kart kredytowych, dane osobowe czy medyczne. Aby chronić te poufne dane i zmniejszyć ryzyko ich wycieku, trzeba zapobiegać niewłaściwemu udostępnianiu ich przez użytkowników nieuprawnionym osobom lub organizacjom. Ta praktyka nazywa się zapobieganiem wyciekom danych (DLP) - tych umyślnych jak i przypadkowych.

Dzięki DLP możliwe jest wprowadzenie skutecznych zabezpieczeń przed wyciekiem informacji i dostosowaniem (w tym zakresie) do obowiązującego prawa, regulaminów i polityk bezpieczeństwa.

Po ustaleniu w organizacji zasad DLP można identyfikować, monitorować i automatycznie chronić poufne elementy w następujących systemach:

- Microsoft 365 (Teams, Exchange, SharePoint i OneDrive),
- aplikacje Office (Word, Excel i PowerPoint),
- Windows 10, Windows 11, MacOS (Catalina 10.15 i wyższe),
- wybrane usługi SaaS,
- lokalne zasoby plików i lokalne zasoby SharePoint.

Funkcja DLP wykrywa poufne elementy danych za pomocą analizy treści, a nie tylko prostego skanowania tekstu. Zawartość jest analizowana pod kątem dopasowania danych podstawowych do słów kluczowych, oceny wyrażeń regularnych, sprawdzania poprawności funkcji wewnętrznych oraz dopasowania danych pomocniczych, związanych z danymi podstawowymi. DLP wykorzystuje również algorytmy uczenia maszynowego i inne metody do wykrywania zawartości określonej w zasadach DLP.

W zależności od konfiguracji usługa może zablokować dostęp do informacji osobom nieuprawnionym lub zaszyfrować tą informację. DLP generuje też podpowiedzi dla użytkowników sugerując im odpowiednie działania w zakresie klasyfikacji i ochrony informacji.

Administratorzy bezpieczeństwa mają do dyspozycji kokpit pozwalający na tworzenie polityk ochrony informacji, zarządzanie nimi i raportowanie zgodności ochrony informacji z założeniami.

4.2.10.6. EDISCOVERY

Purview eDiscovery (Premium) opiera się na istniejących funkcjach zbierania elektronicznych materiałów dowodowych i analiz firmy Microsoft. Zbieranie elektronicznych materiałów dowodowych jest wspierane przez kompleksowy przepływ pracy służący do zachowywania, gromadzenia, analizowania, przeglądania i eksportowania zawartości, która wspomaga wewnętrzne i zewnętrzne dochodzenia w organizacji. Umożliwia zespołom prawnym zarządzanie całym przepływem pracy w celu komunikowania się z osobami zaangażowanymi w sprawę[43].

[43] *Omówienie rozwiązania zbierania elektronicznych materiałów dowodowych (Premium) w Microsoft Purview - Microsoft Purview (zgodność) | Dokumenty firmy Microsoft*

Przepływami pracy związanymi ze zbieraniem elektronicznych materiałów dowodowych można zarządzać, identyfikując badane w procesie osoby i wykorzystywane przez nie źródła danych. Umożliwia stosowanie blokad w celu zabezpieczenia danych, a następnie zarządzanie procesem komunikacji z zespołem prawnym. Funkcje uczenia maszynowego, wykorzystujące zaawansowane indeksowanie i wyszukiwanie, pomagają również zredukować duże ilości danych do analizy.

4.2.10.7. INSIDER RISK MANAGEMENT

Zarządzanie i minimalizowanie ryzyka w organizacji zaczyna się od zrozumienia rodzajów ryzyka występujących w miejscu pracy. Niektóre ryzyka są powodowane przez zdarzenia zewnętrzne i czynniki, na które nie mamy wpływu. Inne zagrożenia są wynikiem wewnętrznych incydentów i działań użytkowników, których można uniknąć lub ograniczyć ich występowanie. Często ryzyko związane jest z nielegalnymi, nieodpowiednimi, nieautoryzowanymi lub nieetycznymi zachowaniami i działaniami użytkowników w organizacji, takimi jak:

- wycieki danych, w tym danych poufnych,
- kradzież własności intelektualnej (IP),
- oszustwa poprzez nieuprawnioną zmianę danych,
- wykorzystywanie poufnych danych do celów prywatnych i niezgodnych z prawem,
- naruszenia przepisów.

Użytkownicy w miejscu pracy mają dostęp do tworzenia, zarządzania i udostępniania danych w szerokim spektrum platform i usług. w większości przypadków organizacje mają ograniczone zasoby i narzędzia do identyfikowania i ograniczania ryzyka w całej organizacji, a jednocześnie muszą spełniać standardy prywatności użytkowników.

Zarządzanie ryzykiem wewnętrznym wykorzystuje pełen zakres usług i uznane wskaźniki firm trzecich, aby pomóc identyfikować, klasyfikować i działać na podstawie ryzyka. Korzystając z dzienników z platformy Microsoft 365 i programu Microsoft Graph, zarządzanie ryzykiem wewnętrznym umożliwia definiowanie określonych zasad w celu identyfikowania wskaźników ryzyka. Zasady te pozwalają identyfikować ryzykowne działania i działać w celu ograniczenia tego ryzyka.

Zarządzanie ryzykiem wewnętrznym koncentruje się wokół następujących zasad:

- transparentności,
- prawa do prywatności,
- dostosowania do zasad opartych na grupach branżowych, geograficznych i sektorowych,
- Adekwatności - zapewnienia właściwych informacji umożliwiających powiadamianie audytorów, badanie danych i badanie zachowań użytkowników.

Microsoft Purview Insider Risk Management to rozwiązanie do zapewniania zgodności, które pomaga zminimalizować ryzyko wewnętrzne, umożliwiając wykrywanie, badanie i działanie na złośliwe i nieumyślne działania w organizacji. Zasady dotyczące ryzyka niejawnego dostępu do informacji umożliwiają zdefiniowanie typów zagrożeń do zidentyfikowania i wykrycia w organizacji, w tym podejmowanie działań w przypadku spraw i eskalowanie spraw do eDiscovery. Analitycy ryzyka w organizacji mogą szybko podjąć odpowiednie działania, aby upewnić się, że użytkownicy są zgodni ze standardami organizacji.

Insider Risk Management

- Wykrywa, bada i umożliwia podejmowanie działań w związku z krytycznymi zagrożeniami w organizacji, w tym kradzieżą danych, wyciekami danych i naruszeniami zasad zabezpieczeń.
- Zarządza ryzykiem związanym z danymi dzięki użyciu pseudonimizacji i kontrolom.
- Identyfikuje ukryte zagrożenia za pomocą konfigurowalnych szablonów uczenia maszynowego, które nie wymagają agentów w punktach końcowych.
- Wspomaga zespoły zajmujące się bezpieczeństwem, zasobami ludzkimi i prawem dzięki zintegrowanym przepływom pracy w dochodzeniach.

4.2.11. MICROSOFT 365 DEFENDER

Microsoft 365 Defender to ujednolicony pakiet ochrony organizacji przed i po naruszeniu bezpieczeństwa, który pozwala koordynować wykrywanie, zapobieganie, badanie i reagowanie w punktach końcowych, tożsamościach, poczcie e-mail i aplikacjach, zapewniając zintegrowaną ochronę przed zaawansowanymi atakami.

Dzięki zintegrowanemu rozwiązaniu Microsoft 365 Defender specjaliści ds. cyberbezpieczeństwa mogą łączyć sygnały o zagrożeniach odbierane przez każdy z tych produktów oraz określać pełny zakres i wpływ zagrożenia. w jaki sposób wszedł do środowiska, na co ma wpływ i jak obecnie wpływa na organizację. Właściwie skonfigurowana usługa Microsoft 365 Defender podejmuje automatyczne działania w celu zapobieżenia atakowi lub jego zatrzymania oraz samoleczenia skrzynek pocztowych, punktów końcowych i tożsamości użytkowników, których dotyczy problem.

Microsoft 365 Defender zawiera wiele znanych już usług.

4.2.11.1. DEFENDER FOR ENDPOINT

Defender for Endpoint zarządza zasadami ochrony przed złośliwym kodem i zabezpieczeniami zapory systemu Windows dla komputerów klienckich.[44] Jest korporacyjną platformą bezpieczeństwa punktów końcowych zaprojektowaną, aby wspomagać działania w obszarze zapobiegania, wykrywania, badania i reagowania na zaawansowane zagrożenia.

Usługa korzysta z mechanizmów Windows i usług chmury Microsoft, takich jak:

- Czujniki behawioralne punktów końcowych: Czujniki te, osadzone w systemie Windows 11 i Windows 11, zbierają i przetwarzają sygnały behawioralne z systemu operacyjnego i wysyłają te dane z czujników do prywatnej, izolowanej usługi Microsoft Defender for Endpoint.
- Analiza bezpieczeństwa w chmurze: Wykorzystując duże zbiory danych, mechanizmy uczenia się urządzeń, produkty z chmury (takie jak Office 365) i zasoby online, sygnały behawioralne są tłumaczone na szczegółowe informacje, pozwalające wykryć i zalecić reakcje na zaawansowane zagrożenia.
- Analiza zagrożeń: Generowana przez mechanizmy wyszukiwania firmy Microsoft, zespoły ds. zabezpieczeń i wzbogacona o informacje o zagrożeniach dostarczane przez partnerów, analiza zagrożeń umożliwia usłudze Defender for Endpoint identyfikowanie narzędzi, technik i wektorów ataku oraz generowanie alertów.

[44] https://docs.microsoft.com/pl-PL/mem/configmgr/protect/deploy-use/endpoint-protection

4.2.11.2. DEFENDER FOR OFFICE 365

Usługa Microsoft Defender for 0ffice 365[45] chroni organizację przed złośliwymi zagrożeniami stwarzanymi przez wiadomości e-mail, łącza (adresy URL) i narzędzia do współpracy. Usługa Defender dla usługi Office 365 zawiera:

- **Zasady ochrony przed** zagrożeniami: Pozwala zdefiniować zasady ochrony przed zagrożeniami, aby wprowadzić odpowiedni poziom ochrony dla swojej organizacji.
- **Raporty**: Udostępnia raporty w celu monitorowania wydajności usługi Defender for Office 365.
- **Funkcje badania zagrożeń i reagowania na nie**: Udostępnia narzędzia do badania, poznania, symulowania i zapobiegania zagrożeniom.
- **Zautomatyzowane funkcje dochodzenia i reagowania**: Automated investigation and response (AIR) wspomaga działania zespołu SOC w zakresie funkcji dochodzenia i reagowania. Gdy pojawiają sie alerty są, do zespołu ds. operacji bezpieczeństwa należy przeglądanie tych alertów, ustalanie priorytetów i reagowanie na nie. Środowisko AIR umożliwia wydajne i skuteczne działanie. Funkcje środowiska AIR obejmują zautomatyzowane procesy dochodzeniowe w odpowiedzi na dobrze znane zagrożenia. Odpowiednie działania naprawcze wymagają zatwierdzenia, umożliwiając zespołowi operacji bezpieczeństwa skuteczne reagowanie na wykryte zagrożenia. Dzięki środowisku AIR można skupić się na zadaniach o wyższym priorytecie, nie tracąc z oczu ważnych alertów.

4.2.11.3. DEFENDER VULNERABILITY MANAGEMENT

Wbudowane podstawowe funkcje zarządzania lukami w zabezpieczeniach wykorzystują nowoczesne, oparte na ryzyku podejście do wykrywania, oceny, ustalania priorytetów i korygowania luk w zabezpieczeniach punktów końcowych i błędnych konfiguracji.

4.2.11.4. REDUKCJA POWIERZCHNI ATAKU

Zestaw możliwości redukcji powierzchni ataku zapewnia pierwszą linię obrony. Upewniając się, że ustawienia konfiguracji są prawidłowe i stosowane są techniki ograniczania

[45] *https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description*

możliwości ataku. Ten zestaw funkcji obejmuje również ochronę sieci, blokując dostęp do złośliwych adresów IP, domen i adresów URL.

4.2.11.5. NEXT-GENERATION PROTECTION

Aby jeszcze bardziej wzmocnić obwód zabezpieczeń sieci, usługa *Microsoft Defender for Endpoint* korzysta z ochrony nowej generacji zaprojektowanej do wykrywania wszystkich typów pojawiających się zagrożeń wykorzystując:

- Ochronę antywirusową opartą na zachowaniu, heurystyce i czasie rzeczywistym, która obejmuje ciągłe skanowanie przy użyciu monitorowania zachowania plików i procesów oraz innych heurystyk (znanych również jako ochrona w czasie rzeczywistym). Obejmuje to również wykrywanie i blokowanie aplikacji, które są uważane za niebezpieczne, ale mogą nie zostać wykryte jako złośliwe oprogramowanie.
- Ochronę jako serwis, która obejmuje niemal natychmiastowe wykrywanie i blokowanie nowych i pojawiających się zagrożeń.
- Dedykowaną ochronę i aktualizację produktów, które obejmują aktualizacje związane z Microsoft Defender.

4.2.11.6. ENDPOINT DETECTION AND RESPONSE EDR

Funkcje wykrywania i reagowania na zagrożenia w punktach końcowych są wprowadzane w celu wykrywania, badania i reagowania na zaawansowane zagrożenia, które mogły przekroczyć pierwsze dwa filary bezpieczeństwa. Zaawansowane wyszukiwanie zapewnia oparte na zapytaniach narzędzie do wyszukiwania zagrożeń, które pozwala znajdować naruszenia i wykrywać niestandardowe ataki.

Po wykryciu zagrożenia w systemie tworzone są alerty, które analityk może zbadać. Alerty z tymi samymi technikami ataku lub przypisane do tej samej osoby atakującej są agregowane w jednostkę zwaną incydentem. Agregowanie alertów w ten sposób ułatwia analitykom wspólne badanie zagrożeń i reagowanie na nie.

Zgodnie z zasadą Zero Zaufania *Defender for Endpoint* stale zbiera behawioralną telemetrię cybernetyczną. Obejmuje to informacje o procesach, działaniach w sieci, procesy w jądrze systemu i menedżerze pamięci, działania związane z logowaniem użytkowników, zmiany

w rejestrze i systemie plików oraz inne. Informacje są przechowywane przez sześć miesięcy, co umożliwia analitykowi cofnięcie się w czasie do początku ataku. Analityk może wykorzystywać różne widoki i podchodzić do badania za pomocą wielu wektorów.

4.2.11.7. ZAUTOMATYZOWANE DOCHODZENIE I NAPRAWA

W połączeniu z możliwością szybkiego reagowania na zaawansowane ataki usługa *Microsoft Defender for Endpoint* oferuje funkcje automatycznego badania i korygowania, które pomagają zmniejszyć liczbę sygnalizowanych alarmów.

4.2.11.8. MICROSOFT SECURE SCORE FOR DEVICES

Usługa Defender for Endpoint zawiera mechanizm Microsoft Secure Score for Devices, który ułatwia dynamiczną ocenę stanu zabezpieczeń sieci, identyfikowanie niechronionych systemów i podejmowanie zalecanych działań w celu poprawy ogólnego bezpieczeństwa organizacji.

4.2.11.9. APPLICATION GUARD

Microsoft Defender Application Guard jest usługą izolującą użytkowników od stron internetowych, usług typu chmurowego i sieci zdefiniowanych jako niezaufane. Umożliwia definiowanie listy zasobów zaufanych, do których użytkownicy mają pełny dostęp.
w przypadku, gdy użytkownik chce skorzystać z zasobu nie będącego na takiej liście, jest on otwierany w izolowanym kontenerze, odseparowanym od środowiska systemu operacyjnego. Taki kontener jest anonimowy, a więc atakujący nie tylko nie jest w stanie dostać się do środowisk produkcyjnych, ale też nie może przechwycić tożsamości użytkownika.

4.2.11.10. EXPLOIT GUARD

Windows Defender Exploit Guard jest usługą chroniącą użytkowników systemu operacyjnego Windows w następujących obszarach:

- chroni aplikacje o znanych podatnościach,
- zmniejsza powierzchnię ataków na aplikacje,
- chroni urządzenia klienckie przed zagrożeniami w ruchu sieciowym,
- chroni pliki w katalogach systemowych.

Zaletami tej usługi są skuteczność, małe obciążenie systemu klienckiego i przezroczystość dla użytkownika.

4.2.12. MICROSOFT DEFENDER ANTIVIRUS

Ważnym składnikiem usług ochrony urządzeń klienckich i serwerów jest Defender Antivirus (dawniej Windows Defender). Począwszy od systemu Windows 10 i serwerów z systemem Windows Server 2022, usługa Defender Antivirus jest instalowana wraz z systemem operacyjnym.

Program antywirusowy Microsoft Defender jest głównym składnikiem ochrony w usłudze Microsoft Defender for Endpoint. Ta ochrona łączy uczenie maszynowe, analizę dużych zbiorów danych, dogłębne badania odporności na zagrożenia oraz infrastrukturę chmury firmy Microsoft w celu ochrony urządzeń (lub punktów końcowych) w organizacji. Program antywirusowy Microsoft Defender jest wbudowany w system Windows i współpracuje z usługą Microsoft Defender for Endpoint, aby zapewnić ochronę na urządzeniu i w chmurze.

Oprogramowanie antywirusowe i anty-malware może być implementowane na poziomie serwerów i na poziomie stacji klienckich. Usługa Defender Antivirus ma następujące możliwości:

- wykrywanie złośliwego oprogramowania i programów szpiegujących oraz wykonywanie działań korygujących,
- możliwość aktualizacji oraz wdrożenia klienta poprzez infrastrukturę WSUS (klient oraz definicje),
- możliwość aktualizacji/wdrożenia klienta poprzez system dystrybucji oprogramowania (np. System Center),
- możliwość konfigurowania zasad bezpieczeństwa za pomocą polityk,
- możliwość generowania raportów, alertów pozwalających na pełną kontrolę nad zagrożeniami, stanem komputerów, aktualizacjami,
- możliwość wykrywania błędów w konfiguracji systemów operacyjnych, braku krytycznych uaktualnień,
- wsparcie instalacji serwerowej dla maszyn wirtualnych,

- generowanie szczegółowych raportów do poziomu pojedynczego komputera,
- wykorzystanie wbudowanych w systemy operacyjne Windows mechanizmów monitorujących (Windows Filter Manager),
- wykrywanie programów typu rootkit i wykonywanie działań korygujących,
- ocena krytycznych luk w zabezpieczeniach i automatyczne aktualizowanie definicji oraz oprogramowania antymalware,
- wykrywanie luk w zabezpieczeniach sieci przy użyciu systemu Network Inspection System,
- integracja z usługą Cloud Protection w celu zgłaszania złośliwego oprogramowania do firmy Microsoft. Po dołączeniu do tej usługi klient Endpoint Protection lub usługa Windows Defender pobiera najnowsze definicje z Centrum ochrony przed złośliwym oprogramowaniem w przypadku wykrycia niezidentyfikowanego złośliwego oprogramowania na komputerze,
- zarządzanie ustawieniami zapory systemu Windows.

Zapewniona jest ochrona w czasie rzeczywistym przed wirusami i oprogramowaniem szpiegowskim dla środowisk systemów operacyjnych 32- i 64-bitowych.

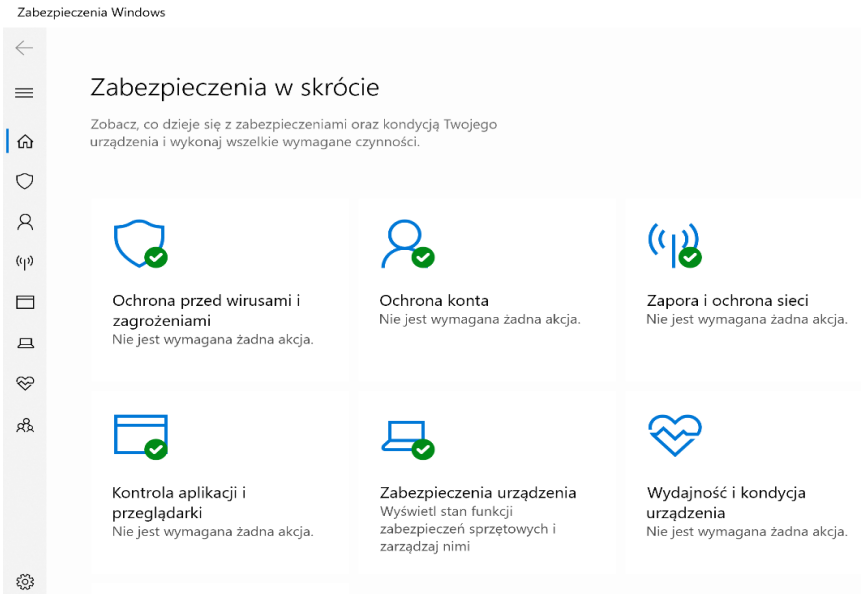
Serwer zarządzania jest obsługiwany przy użyciu centralnej konsoli. Umożliwia ona wybór ustawień prekonfigurowanych i zmianę ustawień klienckich w celu dostosowania do specyficznych warunków danego środowiska. Ustawienia dotyczą harmonogramu skanowania, aktywacji i dezaktywacji ochrony w czasie rzeczywistym, działań podejmowanych domyślnie w razie wykrycia różnych rodzajów zagrożeń oraz sposobu powiadamiania i raportowania. Aby uprościć dystrybucję ustawień na komputerach klienckich Defender został przystosowany do użycia Zasad Grupy (Group Policy) usługi Active Directory. Klienci mogą również zdecydować się na korzystanie z istniejącego systemu dystrybucji oprogramowania.

Aktualizacje definicji złośliwego oprogramowania są dostarczane z Microsoft Update. Defender upraszcza dystrybucję aktualizacji definicji na komputerach klienckich dzięki zastosowaniu usług Microsoft Windows Server Update Services (WSUS). Pozwalają one administratorom ustawić automatyczne zatwierdzanie pobierania najnowszych sygnatur lub

testować i zatwierdzać poszczególne aktualizacje. Klienci mogą również skorzystać z dowolnego systemu dystrybucji oprogramowania, używanego w danym środowisku. Konta użytkowników zdalnych mogą pobierać aktualizacje sygnatur z witryny Microsoft Update.

Ponadto Defender posiada następujące certyfikaty:

- Certyfikat vb100
- Certyfikat CESG Claims Tested Mark (CCTM) w kategorii Integrity Protection
- Certyfikat ICSA Labs w kategoriach:
  - Anti-Virus Detection
  - Anti-Virus Cleaning
- Certyfikat West Coast Labs' Checkmark w kategoriach:
  - Anti-Malware
  - Anti-Spyware Desktop
  - Anti-Trojan
  - Anti-Virus Desktop
  - Anti-Virus Disinfection
  - Anti-Virus Server
  - CCTM - Checkmark Anti-Spyware Desktop
  - CCTM - Checkmark Anti-Trojan
  - CCTM - Checkmark Anti-Virus Desktop
  - CCTM - Checkmark Anti-Virus Disinfection.



4.2.13. MICROSOFT DEFENDER FOR CLOUD

Usługa Microsoft Defender for Cloud umożliwia ujednolicone zarządzanie zabezpieczeniami i zaawansowaną ochronę przed zagrożeniami usług z chmury hybrydowej.

Jest to platforma zarządzania stanem zabezpieczeń w chmurze (CSPM) i platforma ochrony obciążeń w chmurze (CWPP) dla wszystkich zasobów platformy Azure, lokalnych i wielochmurowych (Amazon AWS i Google GCP). Defender dla chmury realizuje trzy istotne funkcje:

- Wskaźnika bezpieczeństwa - stale oceniającego stan zabezpieczeń, śledzącego nowe możliwości zabezpieczeń i raportującego postęp działań związanych z zabezpieczeniami.
- Kreowania zaleceń w zakresie akcji chroniących usługi przed znanymi zagrożeniami.
- Dostarczania alertów w czasie rzeczywistym, dzięki czemu można natychmiast reagować i zapobiegać incydentom.
- Przy współdziałaniu z innymi usługami bezpieczeństwa pozwala stosować zasady zabezpieczeń do różnych obciążeń, ograniczać podatność na zagrożenia i wykrywać ataki oraz reagować na nie.
- Ocenia środowisko i pozwala poznać stan zasobów i określić, czy są one bezpieczne.
- Umożliwia ocenę obciążeń i generuje zalecenia dotyczące zapobiegania zagrożeniom oraz alerty związane z wykryciem zagrożeń.

- Zapewnia wytyczne do automatycznego skalowania i ochronę w ramach usług platformy Azure.

Utrzymywanie bezpieczeństwa zasobów to wspólna odpowiedzialność dostawcy usług w chmurze i zarządzającego zasobami lokalnymi. Podczas przechodzenia do chmury trzeba upewnić się, że obciążenia będą bezpieczne w kontekście dostępności systemu. Przejście na model IaaS (infrastruktura jako usługa) to większa odpowiedzialność po stronie klienta niż w przypadku korzystania z modeli PaaS (platforma jako usługa) i SaaS (oprogramowanie jako usługa). Usługa Azure Security Center zapewnia narzędzia potrzebne do zwiększenia bezpieczeństwa sieci, zabezpieczenia usług i zapewnienia maksymalnego poziomu bezpieczeństwa przy utrzymaniu założonej dostępności.

Plany usługi Microsoft Defender for Cloud oferują kompleksową ochronę w następujących obszarach:

- Microsoft Defender for Servers
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Containers
- Microsoft Defender for App Service
- Microsoft Defender for Key Vault
- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS
- Microsoft Defender for open-source relational databases
- Microsoft Defender for Azure Cosmos DB

4.2.14. MICROSOFT DEFENDER FOR IDENTITY

Microsoft Defender for Identity (dawniej Azure Advanced Threat Protection, znana również jako Azure ATP) to oparte na chmurze rozwiązanie zabezpieczeń, które wykorzystuje sygnały lokalna usługa Active Directory do identyfikowania, wykrywania i badania zaawansowanych zagrożeń, tożsamości, naruszonych zabezpieczeń i złośliwych akcji wewnętrznych skierowanych na tożsamość cyfrową użytkownika.

Usługa Defender for Identity umożliwia analitykom i specjalistom ds. zabezpieczeń na wykrywanie zaawansowanych ataków w środowiskach hybrydowych pozwalając na:

- Monitorowanie użytkowników, ich zachowań i działań przy użyciu analizy opartej na uczeniu maszynowym, a w następstwie wyszukiwania nietypowych zachowań czy działań.
- Ochrona tożsamości użytkowników i poświadczeń przechowywanych w usłudze Active Directory.
- Identyfikowanie i badanie podejrzanych działań użytkowników oraz zaawansowanych ataków.
- raportowanie informacji o zdarzeniach na osi czasu na potrzeby szybkiej klasyfikacji.

4.2.14.1. MICROSOFT THREAT EXPERTS

Usługa ta udostępnia narzędzia dla Centrum Operacyjne Bezpieczeństwa (SOC) zarządzającego rozwiązywaniem problemów z bezpieczeństwem na poziomach technicznym i organizacyjnym.

Usługa dostarcza między innymi:

- Informacje o atakach, ich celu, użytych metodach, harmonogramie ataku, zasięgu i skutkach. Mechanizmy oparte są na monitorowaniu zagrożeń i ich analizie w skali globalnej, uczeniu maszynowym analizującym występowanie znanych i nieznanych zagrożeń, korelacji informacji identyfikacji ryzyk oraz symulacji potencjalnego rozwoju ataku i jego skutków.
- Konsultacji zespołu ekspertów dostępnej na żądanie.

4.2.14.2. ADVANCED THREAT ANALYTICS

Jednym z głównych problemów w walce z zagrożeniami jest wykrycie tych zagrożeń oraz zaistniałej penetracji systemów. Ocenia się, że średni czas upływający od udanego ataku do jego wykrycia wynosi około 180 dni, a w około 80% przypadków atak w ogóle nie zostaje wykryty. w tym czasie atakujący jest w stanie zapoznać się z mechanizmami obronnymi, sposobem ich obejścia, przejęciem uprawnień użytkowników a czasem administratorów – czyli przygotować właściwą destrukcyjną fazę działania. Istotną rolę z zespole narzędzi i procedur chroniących systemy teleinformatyczne są więc narzędzia wykrywania zagrożeń.

Przykładem takiego narzędzia jest *Advanced Threat Analytics (ATA)*[46], będące między innymi składową pakietu licencji dostępowych Enterprise CAL oraz pakiecie Enterprise Mobility Suite.

Jest to oprogramowanie pozwalające analizować, poznawać i identyfikować typowe i nietypowe zachowania użytkowników, urządzeń, aplikacji i wszelkich zasobów.

Dzięki wbudowanej bazie wzorców jest w stanie wykryć typowe efekty ataku na system, a jednocześnie dzięki mechanizmom uczenia się – rozpoznawać nietypowe zachowania i zdarzenia będące odstępstwami od normalnego działania systemów. Najczęściej wykorzystywanym źródłem informacyjnym zasilającym usługę ATA jest System Center Operation Manager – przekazujące dane do Security Information and Event Management (SIEM) – na przykład Microsoft Sentinel[47].

Poniżej przedstawiono główne etapy działania usługi ATA:

Między innymi wykrywane i raportowane są:

- nietypowe zmiany w DNS,
- masowe zmiany w prawach dostępu,

[46] https://docs.microsoft.com/pl-pl/advanced-threat-analytics/what-is-ata
[47] Co to jest usługa Microsoft Sentinel? | Microsoft Docs

- nieoczekiwane zmiany na poziomie usługi LDAP,
- dostęp do zasobów bez posiadania uprawnień,
- posługiwanie tymi samymi uprawnieniami przez wielu użytkowników,
- wielokrotne nieudane próby dostępu,
- aktywności na poziomie mechanizmów *Honeypot* i *Honeytoken*,
- nietypowe zachowania użytkowników,
- masowe kasowanie obiektów czy informacji.

Ponadto wykrywane są typowe niedociągnięcia w konfiguracji czy procedurach, takie jak brak szyfrowania, przechowywanie haseł w postaci tekstu i tym podobne.

4.2.15. DEFENDER FOR CLOUD APPS

Microsoft Defender for Cloud Apps[48] to broker zabezpieczeń dostępu do chmury (CASB), który obsługuje różne tryby pracy, w tym zbieranie dzienników, łączniki interfejsu API i zwrotny serwer proxy. Zapewnia widoczność i kontrolę przepływu danych oraz zaawansowaną analitykę w celu identyfikowania i zwalczania cyberzagrożeń we wszystkich usługach w chmurze firmy Microsoft i innych firm.

Usługa Microsoft Defender for Cloud Apps integruje się z rozwiązaniami firmy Microsoft i została zaprojektowana z myślą o wsparciu administratorów bezpieczeństwa. Zapewnia scentralizowane zarządzanie i szerokie możliwości automatyzacji.

4.2.16. MICROSOFT SENTINEL

Usługa Sentinel bazująca na usługach platformy Azure pozwala na wykonywanie analiz zabezpieczeń systemów teleinformatycznych dla całej jednostki. Można ją określić jako usługę SIEM nowej generacji. Jest to usługa skalowalna, w której praktycznie nie ma limitów liczby zapytań, korzystająca z zaawansowanych mechanizmów uczenia maszynowego oraz innych usług bezpieczeństwa dostępnych w chmurze Microsoft. Dodatkowo posiada lub pozwala tworzyć konektory do większości dostępnych źródeł danych. Między innymi można wykorzystać wbudowany interfejs REST API.

[48] https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Podstawowymi funkcjami Sentinel są:

1. Zbieranie i agregowanie danych i informacji z całego ekosystemu lokalnego i chmury – użytkowników (i ich zachowań), urządzeń, aplikacji i infrastruktury. Dodatkowym narzędziem ułatwiającym pracę analityków zabezpieczeń są pulpity nawigacyjne pozwalające na obserwację i analizę tego co dzieje się w trakcie ataku.
2. Wykrywanie standardowych oraz nowych, nietypowych zagrożeń dzięki analizie danych i zdarzeń w systemie z wizualizacją rozwoju ataków, przy jednoczesnej minimalizacji ryzyka pojawienia się fałszywych alarmów. Jest to możliwe dzięki wykorzystaniu uczenia maszynowego pozwalającego na analizę i korelację milionów danych oraz porównywanie ich z typowymi schematami zachowań użytkowników i usług.
3. Badanie zagrożeń, ich przyczyn i potencjalnych skutków oraz tworzenie modeli skutecznego reagowania.
4. Reagowanie na wykryte zagrożenia. Reagowanie to odbywa się na bazie tzw. Playbook – kolekcji procedur reagowania na wykryte zagrożenie. Procedury te mogą być przygotowywane i testowane, a następnie uruchamiane ręcznie lub automatycznie.

Usługa Sentinel jest stale doskonalona poprzez udoskonalanie modeli wykrywania i reagowania na bazie milionów zdarzeń z całego świata i wymiany doświadczeń użytkowników.

4.3. USŁUGI KATALOGOWE

W przypadku budowania rozwiązań własnych (*On premise*) usługi katalogowe należą do klasy rozwiązań, bez których nie da się zbudować strukturalnego, komponentowego i bezpiecznego środowiska IT, ale są jednocześnie „mało medialne”. Same w sobie nie pozwalają na spektakularne nagłośnienie projektu. Dodatkowo należy zauważyć, że nie da

się zrealizować wymogów bezpieczeństwa i niezaprzeczalności nakładanych przez rozporządzenie KRI bez wdrożenia jednolitej dla wszystkich elementów systemów usługi katalogowej.

Usługa katalogowa to system pozwalający opisać, przechowywać i wykorzystywać informacje o zasobach w systemie, użytkownikach i ich grupach oraz relacjach między nimi.

Praktycznie w każdej jednostce organizacyjnej występuje wiele systemów teleinformatycznych realizujących różne usługi dla wielu użytkowników. Aby udostępnić te usługi i dane uprawnionym użytkownikom lub grupom użytkowników niezbędny jest system, który pozwala opisać, przechowywać i wykorzystywać informacje o użytkownikach, ich grupach i zasobach w systemie oraz administrować nimi. Tym właśnie zadaniom służą usługi katalogowe, pozwalające na zorganizowanie informacji o uczestnikach systemu w ujednolicony sposób. Usługi katalogowe (UK) pozwalają też na budowę mechanizmów uzyskiwania uprawnionego dostępu do zasobów sieci za pomocą pojedynczego uwierzytelnienia. Ta procedura nosi nazwę pojedynczego logowania (*single sign-on*). w oparciu o konta i grupy UK możliwe będzie kontrolowanie dostępu do zasobów i usług.

Usługi katalogowe są specyficzną bazą danych zawierającą definicje i opisy zasobów sieciowych i użytkowników o strukturze pozwalającej na sortowanie ich typów i właściwości.

Usługi katalogowe są specyficzną bazą danych zawierająca opisy obiektów i użytkowników w sieci. Często stosowanym przykładem takiego obiektu może być drukarka sieciowa, przyporządkowana to typu obiektu: drukarki, wraz informacjami o nazwie, lokalizacji, wydajności i innych parametrach. Przykładem opisu użytkownika w ramach obiektu: użytkownik, jest jego imię i nazwisko, adres e-mail, stanowisko, przynależność do działu, adres, telefon, miejsce pracy.

Katalogi umożliwiają użytkownikom i aplikacjom wyszukanie zasobów o określonych właściwościach. Można na przykład przeszukiwać spis użytkowników według adresów poczty elektronicznej lub numerów telefonu, lub znając te dane szukać miejsca jego pracy w jednostce. w innym katalogu można wyszukiwać informacje o najbliższym dostępnym urządzeniu wielofunkcyjnym.

Ważną funkcjonalnością UK jest udostępnianie informacji o obiektach innym współpracującym aplikacją, dzięki czemu możemy na przykład udostępniać te informacje

uprawnionym osobom przez klienta poczty elektronicznej (w postaci książki adresowej) lub na portalu.

Standaryzacja sposobu działania usług katalogowych stał się opis katalogu X.500, zalecanego przez międzynarodową unię telekomunikacyjną (*International Telecommunication Union)* ITU[49].

Założeniem X.500 jest stworzenie globalnego, rozproszonego katalogu, z dostępnego z dowolnego miejsca. Ma on strukturę drzewa, u podstawy którego znajduje się obiekt główny (*root*). Udostępniane przez katalog dane noszą nazwę *Directory Information Base* (DIB), zaś drzewo - *Directory Information Tree* (DIT).

Dla poszczególnych wpisów w katalogu zdefiniowano klasy obiektów, przy czym każdy wpis musi należeć przynajmniej do jednej z klas. w każdej klasie obiektów musi być przynajmniej jeden atrybut. w ten sposób każdy wpis w katalogu X.500 należy do jednej lub wielu klas obiektów oraz zawiera jedną lub wiele wartości poszczególnych typów atrybutów. Szczególnym rodzajem wpisów są aliasy, umożliwiające umieszczenie takiego samego wpisu w różnych miejscach drzewa. Dzięki takiemu rozwiązaniu zmiana dokonana w jednym wpisie powoduje odpowiednie zmiany we wszystkich aliasach.

Podstawowymi cechami zaawansowanych usług katalogowych są:

- Centralna administracja pozwalająca na zarządzanie zasobami i ich uprawnieniami w całej organizacji.
- Dostarczenie mechanizmów zasad grupowych (G*roup Policy*) pozwalającego na wymuszenie na stacjach roboczych i serwerach centralnie konfigurowanych ustawień systemu, uprawnień i środowiska użytkownika.
- Hierarchiczna budowa katalogu, zgodnie ze specyfikacją X.500.
- Przechodniość stosunków zaufania dzięki zastosowaniu protokołu bezpieczeństwa Kerberos. Zmniejsza to liczbę stosunków zaufania pomiędzy domenami. Stosunek przechodni oznacza, że gdy domena a ufa domenie B i domena C ufa domenie B, wówczas domena a ufa również domenie C.

[49] https://www.itu.int/rec/T-REC-X.500/e

- Wymuszenie w ramach całości systemu wspólnej polityki haseł określającej parametry i złożoność hasła, jak również warunki i długość blokady kont itp.
- Wspólne zasady i reguły dla całości usług katalogowych pozwalający na łatwe jego rozszerzanie i możliwość definiowania nowych obiektów i właściwości.
- UK pozwala również na delegację praw do zarządzania określoną grupą komputerów i użytkowników poprzez wbudowane mechanizmy delegacji uprawnień.
- Kontrola i definicja bezpieczeństwa oparta na listach *Access Control Lists* (ACL) pozwalająca na replikację dozwolonych odwołań w skali całej hierarchii, aż do poziomu obiektu.
- Szerokie możliwości formułowania zapytań i rozbudowany mechanizm zapytań sieciowych dzięki strukturze podobnej do indeksu obsługującego zapytania dotyczące każdego obiektu w katalogu.

Najważniejszą cechą usług katalogowych jest jednak możliwość stworzenia jednolitego systemu opisu użytkowników i zasobów dla wszystkich posiadanych aplikacji i centralnego uwierzytelnienia użytkowników w oparciu o wspólną bazę danych.

4.3.1. USŁUGI KATALOGOWE ACTIVE DIRECTORY

Usługi katalogowe Active Directory[50] (AD) są wbudowaną usługą Windows Server. Umożliwiają one opis obiektów, replikację i wyszukiwanie i działają zgodnie ze standardami internetowymi LDAP, DNS i DDNS (*Dynamic DNS*) oraz Kerberos v.5.

Podążając za koncepcją DNS, przestrzeń nazw Active Directory jest nazwą lub grupą nazw zdefiniowanych według pewnej konwencji. Internet posługuje się hierarchiczną przestrzenią adresową, która dzieli nazwy na domeny wysokiego poziomu, na przykład *.com* lub *.org*. Active Directory stosuje ten sam model hierarchiczny do budowy sieci.

Podczas instalacji Active Directory tworzy hierarchię, w której każda domena, każda jednostka organizacyjna i każdy zasób otrzymuje jednoznaczną nazwę w przestrzeni nazw.

[50] http://technet.microsoft.com/en-us/library/hh831669.aspx

Każdy obiekt w Active Directory jest naznaczony unikatową nazwą, zagnieżdżoną w hierarchicznej strukturze katalogu. Można też integrować inne usługi katalogowe z użyciem mechanizmu LDAP.

4.3.1.1. ELEMENTY LOGICZNE AD

W Active Directory są trzy różne elementy logiczne.

- Obiekty

Są to składniki mające wiele atrybutów. Przykładowe obiekty to użytkownicy lub drukarki. Obiekt może być również kontenerem dla innych obiektów.

- Atrybuty obiektu

Wszystkie obiekty w katalogu mają atrybuty lub właściwości. w Microsoft Active Directory oba pojęcia używane są zamiennie. Atrybut to pewna ilość informacji. Obiekty znajdujące się w tym samym kontenerze mają te same atrybuty.

- Klasy obiektów

Active Directory grupuje obiekty według ich atrybutów. Wszystkie obiekty są kategoryzowane właśnie w ten sposób, na przykład jako użytkownicy lub drukarki. Tego rodzaju grupowanie logiczne odpowiada za organizację zasobów w katalogu.

4.3.1.2. KOMPONENTY STRUKTURALNE

Oprócz obiektów typu liść w Active Directory są też komponenty strukturalne. Pomagają one w budowie hierarchii katalogu. Zaliczają się do nich kontenery, czyli pojemniki na inne obiekty w katalogu. Rozróżnia się dwie różne kategorie kontenerów:

- Domeny (*Domain*)

Domena zawiera obiekty odpowiadające zasobom sieciowym (komputery, użytkownicy, drukarki itd.), każda z domen przechowuje informacje tylko o obiektach do niej należących. Stanowią granicę bezpieczeństwa w pojedynczej sieci komputerowej. Active Directory składa się z jednej lub wielu domen. w samodzielnej stacji roboczej domeną jest sam komputer. Domena może być czymś więcej niż tylko fizyczną lokalizacją - każda dysponuje własnymi wytycznymi co do bezpieczeństwa w kontaktach z innymi domenami. Jeżeli kilka domen jest

połączonych stosunkami zaufania i wykorzystują wspólną konfigurację, mówimy o strukturze domen.

- Jednostki organizacyjne

Stanowią kolejny podział struktury katalogu. Możliwe są dowolne hierarchie w ramach jednej domeny.

Kolejne ważne jednostki podziału struktury określają relacje między domenami. Należą do nich:

- Drzewo (*Tree*)

Jest to zgrupowanie lub hierarchiczne ustawienie jednej lub wielu domen UK, które współdzielą wspólną przestrzeń nazw DNS.

Wiele organizacji utrzymuje kilka domen, choć nie jest to niezbędne z technicznego punktu widzenia. Zastosowanie wielu domen tworzy hierarchię, która ma współzależną przestrzeń nazw i określana jest mianem drzewa. Drzewo tworzy logiczną strukturę wysokiego poziomu, w której domeny są wzajemnie relacyjnie powiązane. w obrębie drzewa domeny są wzajemnie powiązane stosunkami zaufania.

- Las (*Forest*)

Zgrupowanie lub hierarchiczne ustawienie jednego lub wielu drzew domen UK, które tworzą wydzieloną przestrzeń nazw. Wszystkie drzewa w lesie współdzielą schemat katalogu. Microsoft opracował koncepcję "lasu", który umożliwia zachowanie struktur, którymi można nadal zarządzać dzięki współistnieniu dwóch różnych przestrzeni nazw.

- Katalog główny (Global Catalog Server)

Jest to centralny zasób informacyjny usługi katalogowej. Powstaje w wyniku replikacji usługi katalogowej i zawiera kopie wszystkich obiektów drzewa. Tak więc, jest czymś w rodzaju indeksu całej sieci zapisującego kopię każdego obiektu w katalogu.

Komponent usług katalogowych bazujący na Active Directory wraz mechanizmami zarządzania użytkownikami spełnia następujące wymagania:

a. Usługi katalogowe zgodne ze standardem LDAP v3 opisanym przez RFC 4510[51], który zawiera:

   - LDAP: The Protocol [RFC4511]
   - LDAP: Directory Information Models [RFC4512]
   - LDAP: Authentication Methods and Security Mechanisms [RFC4513]
   - LDAP: String Representation of Distinguished Names [RFC4514]
   - LDAP: String Representation of Search Filters [RFC4515]
   - LDAP: Uniform Resource Locator [RFC4516]
   - LDAP: Syntaxes and Matching Rules [RFC4517]
   - LDAP: Internationalized String Preparation [RFC4518]
   - LDAP: Schema for User Applications [RFC4519]

   Wspierając także następujący zestaw RFC:

   - RFC 2696 - LDAP Control Extension for Simple Paged Results Manipulation
   - RFC 2247 - Using Domains in LDAP/X.500 Distinguished Names
   - RFC 2589 - LDAP Protocol (v3): Extensions for Dynamic Directory Services
   - RFC 2798 - Definition of the inetOrgPerson LDAP Object Class
   - RFC 2831 - Using Digest Authentication as an SASL Mechanism
   - RFC 2891 - LDAP Control Extension for Server-Side Sorting of Search Results

b. AD udostępnia poniższe funkcje bez potrzeby instalowania dodatkowego oprogramowania („prosto z pudełka”):

   - zarządzanie środowiskiem użytkownika oraz konfiguracją stacji roboczych,
   - dystrybucja oprogramowania na stacje robocze,
   - uwierzytelnianie użytkowników i urządzeń za pomocą protokołu Kerberos.

[51] https://www.rfc-editor.org/info/rfc4510

c. Usługi katalogowe zapewniają replikację typu *multi-master* (katalog na serwerach przechowujących repliki zawsze do odczytu i zapisu)

d. Usługi katalogowe pozwalają na pracę w trybie aplikacyjnym wraz z możliwością instalacji wielu instancji na jednym serwerze.

e. Usługi katalogowe zapewniają możliwość komunikacji z innymi aplikacjami za pomocą języka XML.

f. Aplikacje posiadane (ew. planowane do wdrożenia) mogą integrować się z usługami katalogowymi.

4.3.1.3. USŁUGI KATALOGOWE W WINDOWS SERVER

W aktualnej wersji serwerowego systemu operacyjnego Windows Server wprowadzono wiele rozszerzeń i udoskonaleń w zakresie usług katalogowych.

Zajmiemy się krótko czterema głównymi usługami:

- usługą katalogową – Active Directory Domain Services (AD DS),
- usługą federacyjną – Active Directory Federation Services (AD FS),
- usługą centrum certyfikatów – Active Directory Certificate Services (AD CS),
- usługą zarządzania polityką dostępu do informacji w dokumentach – *Active Directory Rights Management Services (AD RMS)*.

4.3.1.3.1. USŁUGA AD DS

Wprowadzone już w Windows Server 2022 zmiany w znaczący sposób ułatwiają i przyspieszają wdrożenie kontrolerów domeny zarówno we własnej infrastrukturze (*on-premise*) jak i w modelu chmury (*Cloud*). Szczególnie przydatnym rozwiązaniem jest możliwość szybkiego uruchamiania nowych wirtualnych kontrolerów domeny poprzez klonowanie już istniejących.

Dodatkową pomocą jest nowy, rozbudowany kreator udostępniania kontrolerów domeny (*domain controller promotion wizard*) pozwalający na bezpieczne i szybkie przygotowanie lasu i domeny wraz z narzędziami zdalnej instalacji AD DS na docelowym serwerze.

Dostępny jest też mechanizm dynamicznej kontroli dostępu (*dynamic access control – DAC*) wykorzystujący uwierzytelnienie na bazie oświadczeń (*claims-based authorization*).

DAC zawierający centralne polityki dostępu, atrybuty katalogu oraz silnik klasyfikacji plików, pozwala na tworzenie złożonych tożsamości (*compound-identities*), łączących niezaprzeczalnie tożsamość użytkownika z tożsamością urządzenia w postaci jednego identyfikatora.

Ciekawą usługą AD DS jest Zarządzanie Uprzywilejowanym Dostępem (*Privileged Access Management – PAM*) wykorzystującą las (*bastion forest*) izolowany od standardowego lasu pozbawionego możliwości dostępu na prawach administratora. Obniża to ryzyka związane z technika mi kradzieży tożsamości w Active Directory takimi jak *pass-the-hash*, czy *spear phishing.*

Dużym ułatwieniem dla budowy rozwiązań hybrydowych wykorzystujących usługi online Microsoft jest mechanizm *Azure AD Join* dołączania użytkowników do Azure Active Directory, czyli usługi zarządzania tożsamością i dostępem w chmurze Microsoft. Obecnie nie jest wymagane już posiadanie konta Microsoft Account do wykorzystania tej usługi.

Nowością w zakresie uwierzytelniania jest standardowa usługa paszport Microsoft (*Microsoft Passport*). Jest to metoda uwierzytelniania bazująca na mechanizmach kluczy prywatnego/publicznego lub certyfikatu odporna na wiele form ataków na tożsamość użytkowników uwierzytelniających się w AD, Azure AD, Microsoft Account czy też w usługach wspierających tzw. Fast ID (FIDO). Po wstępnej dwustopniowej weryfikacji w procedurze wystawiania paszportu Microsoft, jest on konfigurowany na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu.

4.3.1.3.2. USŁUGA AD FS

Usługa ta zapewnia kontrolę nad realizacją uprawnień dostępu do systemów i informacji dla użytkowników oraz umożliwia wykorzystanie pojedynczego logowania (*single sign-on*) zasobów i usług.

AD FS generuje tokeny dla aplikacji klienckich w odpowiedzi na uprawnione żądanie dostępu, Przechowuje i przekazuje poświadczenia tożsamości użytkowników pochodzące z aplikacji sieciowej (*web application*).

Pozwala wykorzystać uwierzytelnienia oparte na oświadczeniach generowanych przez AD DS zawartych w biletach Kerberos po uwierzytelnieniu się do domeny.

4.3.1.3.3. USŁUGA AD CS[52]

Usługa ta umożliwia wydawanie cyfrowych certyfikatów oraz zarządzanie nimi w systemach wykorzystujących infrastrukturę klucza publicznego.

Certyfikaty wydane przez usługę AD CS mogą być wykorzystane do uwierzytelniania użytkowników i urządzeń, szyfrowania oraz podpisywania dokumentów i wiadomości poczty elektronicznej. Te dwie ostanie funkcje, oprócz niezaprzeczalnego potwierdzenia tożsamości podpisującego, dają możliwość monitorowania niezmienności dokumentu czy wiadomości, bo w przypadku zmiany podpisanej treści – podpis traci ważność.

Ciekawym rozwinięciem funkcji AD CS w najnowszej wersji jest możliwość rejestracji certyfikatów dla komputerów niepodłączonych do domeny lub nawet dla komputerów, które nie są członkami domeny.

4.3.1.3.4. USŁUGA AD RMS

Usługa AD RMS jest narzędziem pozwalającym na spójne wprowadzenie polityk ochrony informacji poprzez zabezpieczanie samej informacji, a nie miejsca przechowywania czy warstwy transportowej.

Zarządzanie polityką dostępu do informacji z wykorzystaniem AD RMS pozwala szyfrować dokumenty oraz wiadomości poczty elektronicznej wraz mechanizmami nadawania odpowiednich praw dostępu zarówno pojedynczym osobom jak i ich grupom. Zastosowanie tej usługi skutecznie chroni informację, nawet gdy zostanie ona przeniesiona w miejsce fizycznie dostępne nieuprawnionym osobom.

[52] *Dalsze informacje o centrum certyfikatów znajduje się w rozdziale „Infrastruktura klucza publicznego (PKI)”.*

4.4. ZARZĄDZANIE TOŻSAMOŚCIĄ

Tożsamość jest abstrakcyjną reprezentacją jednostki w systemie komputerowym. Filozofia definiuje ją jako „identyczność" dwóch rzeczy. Można powiedzieć, że tożsamość stwierdza, że jednostka jest definiowalna i rozpoznawalna.

W pierwszej części rozdziału zostaną opisane stare, dezaktualizujące się metody zarządzania tożsamością wykorzystywane w systemach on-premises, a w drugiej - nowe podejście oparte o usługi z chmury.

4.4.1. ZARZĄDZANIE TOŻSAMOŚCIĄ POZA CHMURĄ

Zarządzanie tożsamością to procedury, narzędzia i procesy pozwalające niezaprzeczalnie potwierdzić tożsamość użytkownika i zarządzać jej cyklem życia.

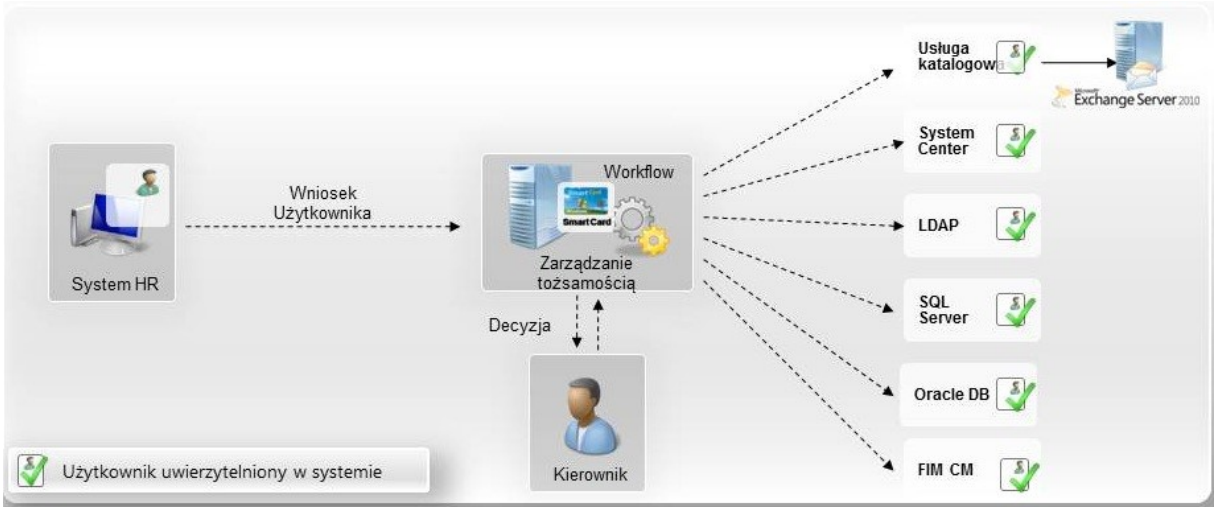
Jakie są obszary zarządzania tożsamością?

Niezwykle ważnym, acz często niedocenianym mechanizmem jest zarządzanie życiem tożsamości.

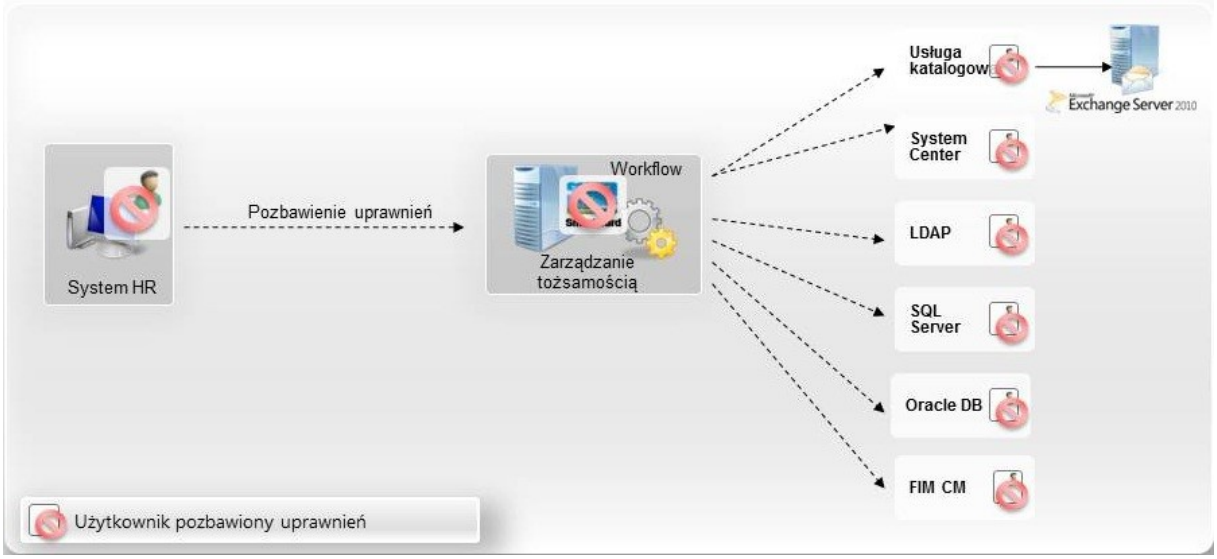
Przy rosnącej przyszłości liczbie użytkowników systemów oraz usług przez nich wykorzystywanych coraz większym wyzwaniem jest zarządzanie ich uprawnieniami. Administratorzy systemu nie mogą przy tym odpowiadać za procesy przyznawania uprawnień użytkownikom, gdyż wynikają one raczej ze struktury organizacyjnej i osadzenia pracowników w procesach realizowanych przez jednostkę organizacyjną. Tak więc, konieczne jest zapewnienie sprawnych i prostych w obsłudze mechanizmów umożliwiających uprawnionej kadrze kierowniczej nadawanie odpowiednich uprawnień bez konieczności posługiwania się skomplikowanymi narzędziami administracyjnymi. Ponadto konieczne jest umożliwienie osobom uprawnionym łatwe sprawdzenie przyznanych uprawnień oraz ich modyfikacji.

Równie ważnym jest problem nienadania przez przypadek uprawnień nie należnych danemu pracownikowi.

Proces nadawania uprawnień, w szczególności dla dostępu do różnych aplikacji dziedzinowych wymaga zwykle decyzji kilku osób oraz ostatecznej akceptacji (np. kierownika danego działu). Wygodnym rozwiązaniem jest stworzenie elektronicznej drogi akceptacji, które po dokonaniu decyzji na poszczególnych szczeblach wyzwoli mechanizmy założenia konta (login), konta w poczcie elektronicznej, nadania uprawnień, generowania certyfikatu itp. Ważnym krokiem w podniesieniu efektywności tego procesu jest Udostępnienie funkcjonalności wnioskowania przez zainteresowanego pracownika o nadanie specyficznych uprawnień z natychmiastowym przekazaniem do wyżej opisanej drogi akceptacji ich nadawania.



O ile pokazany powyżej proces nadawania uprawnień wymaga zwykle ścieżki akceptacyjnej (np. szefów poszczególnych działów) o tyle proces zablokowania uprawnień (np. w przypadku zwolnienia pracownika) powinien być możliwy do wykonania w jednym kroku, zwykle przez nadanie odpowiedniego statusu w systemie kadrowym, co powinno automatycznie generować odpowiednią akcję w systemie zarządzania tożsamością.

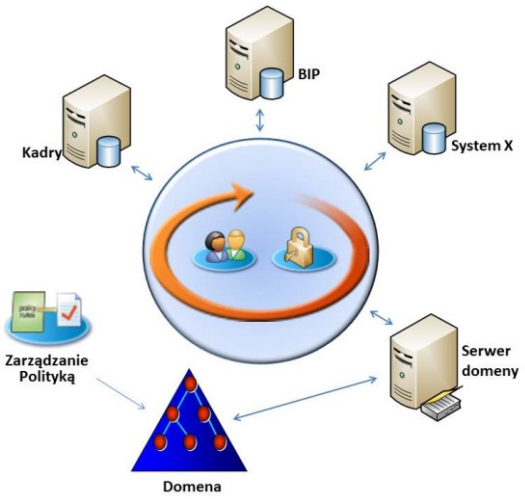


Dodatkową (i zwykle spotykaną) trudnością jest rozproszenie danych o użytkowniku w różnych systemach. Zwykle przechowywane one są w:

- bazie usług katalogowych,
- systemie kadrowo-płacowym,
- centrali telefonicznej,
- książce adresowej poczty elektronicznej,

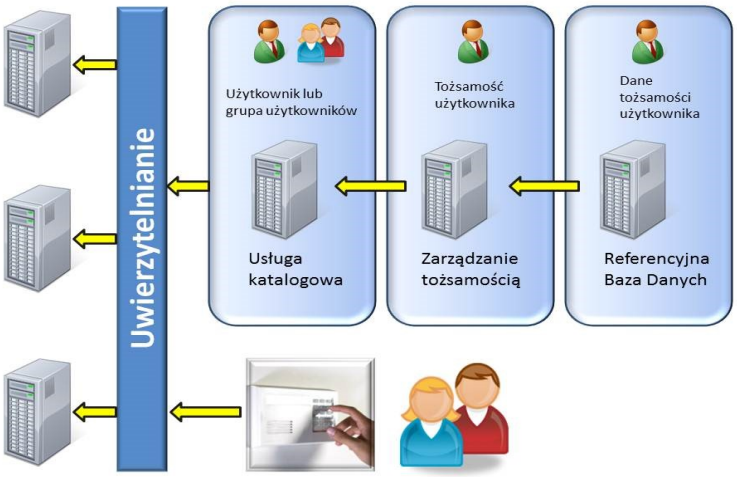
- BIP,
- innych natywnych bazach poszczególnych systemów.

Pierwszym krokiem do utworzenia spójnego systemu zarządzania tożsamością jest utworzenie spójnej bazy danych pracowników zasilanej z istniejących źródeł i stałej synchronizacji tej bazy ze źródłami w celu uzgadniania wszelkich zmian.



System zarządzania tożsamością może składać się z następujących elementów:

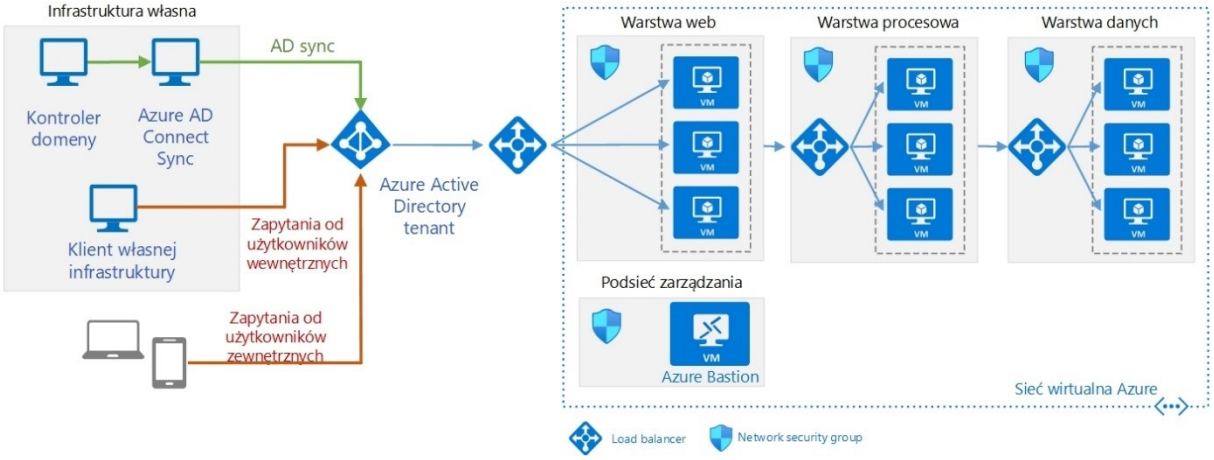
1. **Usługi katalogowe**, które są źródłem informacji o grupach użytkowników i wskazuje systemom, w obrębie której grupy zarządzamy członkostwem.
2. **Referencyjna baza informacyjna**, która będzie integrować i dostarczać pełne informacje o użytkownikach i grupach.
3. **System integrujący informację**, który zapewni łączność ze wszystkimi źródłami danych o użytkownikach w systemach dziedzinowych i zapewni logikę synchronizacji tej informacji.
4. **Portal**, zapewniający interfejs zarządzania nadawania uprawnień wraz z workflow akceptacyjnym oraz mechanizmem udostępniania formularzy poprzez przeglądarkę.



4.4.2. ZARZĄDZANIE TOŻSAMOŚCIĄ Z CHMURY (IDAAS)

Dobrym przykładem obecnego podejścia do zarządzania tożsamością cyfrową w systemach jest wykorzystanie Azure Active Directory w modelu IDaaS (tożsamość jako serwis).

Model ten może być z powodzeniem zastosowany zarówno dla systemów opartych o komponenty z chmury jak i rozwiązania hybrydowe oparte o komponenty własne organizacji i komponenty z chmury[53]. Ogólnym przykładem takiej architektury może być poniższy rysunek.



Oczywiście w podejściu obowiązuje zasada Zero Zaufania traktując wszystkie komponenty tak, jakby były otwarte na Internet i zakłada, że cała sieć jest potencjalnie zagrożona i wroga. Takie podejście koncentruje się na budowaniu silnego uwierzytelniania, autoryzacji i szyfrowania, zapewniając jednocześnie podzielony dostęp i elastyczność operacyjną.

[53] https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

Koncepcja wykorzystuje podejście Gartnera adaptacyjną architekturę zabezpieczeń, które zastępuje strategię opartą na reagowaniu na incydenty modelem *zapobiegania-wykrywania-reagowania-przewidywania*. Zabezpieczenia adaptacyjne łączą kontrolę dostępu, monitorowanie behawioralne, zarządzanie użyciem i wykrywanie z ciągłym monitorowaniem i analizą.

IDaaS wpisuje się w ogólną koncepcję Microsoft Cybersecurity Reference Architecture (MCRA), gdzie opisano mechanizmy cyberbezpieczeństwa firmy Microsoft oraz sposób ich integracji z istniejącymi architekturami zabezpieczeń, w tym środowiskami chmurowymi i hybrydowymi, które używają usługi Azure AD dla tożsamości jako usługi.

Poniżej przedstawiamy zarówno usługę AAD, jak i bazujący na niej model IDaaS.

4.4.2.1. ZAŁOŻENIA IDAAS

Większość architektur systemów informacyjnych udostępnia usługi współużytkowane, które są hostowane i dostępne w sieciach. Usługi te mają wspólną infrastrukturę, a użytkownicy muszą uzyskiwać dostęp do zasobów i danych z dowolnego miejsca. w przypadku takich architektur powszechnym sposobem zabezpieczania zasobów jest użycie kontroli sieci. To jednak nie wystarczy.

Konieczne jest zapewnienie bezpieczeństwa poprzez zarządzanie tożsamościami, procesami uwierzytelniania i autoryzacji. N proponowanym modelu usługi zarządzania tożsamościami umożliwiają uwierzytelnianie i udzielanie uprawnień użytkownikom, partnerom, klientom, aplikacjom, usługom i innym jednostkom.

Zarządzając tożsamością w naszych systemach musimy pamiętać o:

- Zdefiniowaniu jasnych reguł odpowiedzialności i podziału obowiązków dla każdej roli. Prowadzi to do przypisywania uprawnień jedynie w określonym zakresie i czasie, przy minimalnym, koniecznym do realizacji zadań poziome uprawnień.
- Przypisaniu uprawnień dla użytkowników, grup i aplikacji w określonym zakresie za pośrednictwem usługi Azure RBAC. Rekomendowane jest używanie wbudowanych ról.
- Zapobieganiu usuwania lub modyfikowania zasobu, grupy zasobów lub subskrypcji za pomocą blokad zarządzania.

- Użyciu wyłącznie tożsamości zarządzanych, aby uzyskać dostęp do zasobów na platformie Azure.
- Wykorzystaniu pojedynczego źródła tożsamości, w którym synchronizujemy tożsamości w chmurze i lokalnie, z wyjątkiem kont uprzywilejowanych.
- Konfiguracji dostępu warunkowego usługi Azure AD, egzekwującej i mierzącej kluczowe atrybuty zabezpieczeń podczas uwierzytelniania wszystkich użytkowników, zwłaszcza w przypadku kont uprzywilejowanych.
- Zapewnieniu oddzielnego źródła tożsamości dla użytkowników zewnętrznych, niebędących pracownikami naszej organizacji.
- Najlepiej używać metod bez haseł lub wybrać nowoczesne metody haseł.
- Blokuj starsze protokoły i metody uwierzytelniania.

4.4.2.2. PLATFORMA TOŻSAMOŚCI FIRMY MICROSOFT - AAD

Założenia funkcjonalne sprecyzowane we wcześniejszej części dokumentu wskazują jak istotnym dla prawidłowego działania całego systemu jest niezaprzeczalność tożsamości użytkownika systemu. Firma Microsoft oferowała dla celów zarządzania tożsamością oprogramowanie Microsoft Identity Manager[54] (MIM). Obecnie większość procesu zarządzanie tożsamością realizowane jest w oparciu o funkcje Azure Active Directory (AAD)[55].

AAD jest usługą z chmury publicznej Microsoft. Nie jest ograniczona do platformy Azure, ale jest podstawą nadawania, weryfikacji i wykorzystania tożsamości cyfrowej użytkowników we wszystkich usługach „chmurowych" Microsoft. i tak, rozpoczynając korzystanie z pakietu Office 365, Dynamics 365 czy Azure, musimy zdefiniować najpierw administratorów i użytkowników tych usług, ich cyfrowe poświadczenia (login, hasło, certyfikat, token) oraz nadać im odpowiednie uprawnienia personalne lub grupowe. Jeżeli zamierzamy korzystać z kilku różnych usług Microsoft – musimy pamiętać, aby zawsze korzystać z tej samej nazwy domenowej i tych samych definicji użytkowników, aby uzyskać jednolitą tożsamość użytkownika we wszystkich usługach.

[54] https://docs.microsoft.com/pl-pl/microsoft-identity-manager/
[55] https://docs.microsoft.com/pl-pl/security/compass/identity-capabilities

Istnieje wiele scenariuszy funkcjonalnych, dla których uzasadnione jest wykorzystanie usługi z przechowujące informacje o tożsamości użytkowników opartej o infrastrukturę wyniesioną do zewnętrznego centrum przetwarzania. Przykładami takich scenariuszy są:

1. Udostępnianie naszych usług i danych użytkownikom zewnętrznym, zwykle za pośrednictwem sieci Internet. w większości przypadków musimy zapewnić niezaprzeczalność i bezpieczeństwo takiego dostępu na bazie usługi katalogowej i zarządzania prawami dostępu użytkowników. Jednocześnie dobrą praktyką jest wyizolowanie takiej usługi katalogowej od usługi obsługującej użytkowników wewnętrznych. Oznacza to konieczność zbudowania własnej infrastruktury usługi zarządzania tożsamością i dostępem i utrzymanie jej lub skorzystanie z gotowego rozwiązania takiego jak Azure Active Directory (AAD).
2. Budowa systemu na bazie hostowanej usługi platformowej (np. Azure), gdzie najprościej jest wykorzystać usługę katalogową dostarczaną z platformą.
3. Izolacja użytkowników mobilnych dostających się do zasobów wewnętrznych poprzez Internet. Użycie usługi katalogowej z chmury daje możliwość niezaprzeczalnego dostępu do takich zasobów, weryfikowanego poza systemami wewnętrznymi.
4. Projekty krótkotrwałe, w których trzeba zapewnić niezaprzeczalność praw dostępu do danych i usług, a nie opłaca się na krótki okres budować specjalnej, wydzielonej infrastruktury.
5. Uwierzytelnianie użytkowników do zewnętrznej usługi lub pomiędzy różnymi systemami w modelu pojedynczego logowania (*single sign-on*).

Poza oczywistą korzyścią korzystania z gotowej, sprawdzonej i audytowanej usługi, AAD posiada wszystkie funkcje pozwalające na posługiwanie się tożsamością cyfrową. Co więcej możliwe jest bezpieczne tworzenie środowisk hybrydowych, w których bazując na uwierzytelnieniu użytkownika poprzez własną usługę katalogową, logujemy się do systemów bazujących na AAD zawierającego profil tego samego użytkownika. Można tu wykorzystać dwa scenariusze:

- stworzenie relacji wzajemnego zaufania pomiędzy AD i AAD,
- wykorzystanie mechanizmu bazującego skrócie skrótu tokenu generowanego przez AD i uwierzytelnianiu użytkownika na tej bazie w AAD.

Takie wykorzystanie AAD może też być przydatne, kiedy organizacja korzysta z jednego konta w dowolnej zewnętrznej usłudze (np. Twitter). Pozwala na zalogowanie się do niej każdego uprawnionego użytkownika poprzez własne, organizacyjne poświadczenia, które w AAD są mapowane na zdefiniowane uprzednio poświadczenia do zewnętrznej usługi, eliminując konieczność przekazywania użytkownikom tego samego loginu i hasła.

Dużym ułatwieniem dla administratorów jest to, że AAD zawiera mechanizmy samoobsługi użytkowników, np. zmiana hasła, reset hasła czy tworzenie grup użytkowników na bazie udzielonych uprawnień.

AAD posiada wbudowane, definiowalne mechanizmy uwierzytelniania wieloskładnikowego, co może być wykorzystane w dowolnych scenariuszu dla ochrony danych wrażliwych.

Mechanizmy zarządzania tożsamością w AAD można zastosować w połączeni z praktycznie dowolnymi środowiskami własnymi czy aplikacjami dzięki zastosowaniu standardowych protokołów takich jak SAML 2.0, WS-Federation, czy OpenID Connect. Poprzez wsparcie dla OAuth 2.0 możliwe jest pisanie własnych aplikacji i interfejsów komunikacyjnych wykorzystujących AAD.

Przydatnym rozwiązaniem jest to, że niekoniecznie musimy wykorzystywać certyfikaty do uwierzytelniania z CA będącego składową AAD. Możemy zastosować własne certyfikaty, z całą konsekwencją konieczności obsługi życia certyfikatu.

Dzięki wbudowanym mechanizmom, AAD pozwala (w zależności od nabytej wersji) na:

- utworzenie pojedynczego katalogu obiektów uwierzytelnianych jednostki w usłudze Azure AD,
- niezaprzeczalne uwierzytelnienie w AAD,
- uwierzytelnienie i autoryzację w usługach opartych o AAD,
- uwierzytelnienie wieloskładnikowe z wykorzystaniem telefonicznych komunikatów głosowych, sms lub aplikacji typu Authenticator[56],
- uwierzytelnianie bez haseł, w tym przy pomocy Windows Hello, aplikacji Microsoft Authenticator czy kluczy zabezpieczeń FIDO2[57],

[56] *Jak używać aplikacji Microsoft Authenticator*

- dostęp warunkowy, w którym Azure AD ocenia warunki logowania użytkownika i używa zasad dostępu warunkowego, które tworzy się w celu umożliwienia uprawnionego dostępu,
- samoobsługa w zakresie odnawiania poświadczeń, sposobu ich potwierdzania lub ich resetu dla uprawnionych użytkowników,
- synchronizację kont i uprawnień z lokalną usługą Active Directory,
- pojedyncze logowanie (single-sign on) do nieskończonej liczby systemów poprzez bezpieczne przechowywanie poświadczeń użytkownika i powiązanie ich z kontem w AAD,
- wykrywanie potencjalnych luk w zabezpieczeniach tożsamości organizacji i konfigurowanie zasad automatycznego rozwiązywania problemów ryzyka związanego z nieuprawnionym logowaniem,
- zarządzanie kontami, poświadczeniami użytkowników i urządzeń oraz ich grupami wraz z cyklem ich życia.

AAD umożliwia szerokie skalowanie, pozwalające na obsługę nawet setek milionów obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem, mając możliwość skalowania stanowisk wydających certyfikaty. Istnieje też możliwość zarządzania życiem certyfikatów w usługach katalogowych składających się z wielu lasów.

Poprzez zastosowanie rozpowszechnionych standardów i interfejsów AAD zapewnia możliwość wykorzystania dla wielu systemów w środowiskach heterogenicznych. Współpraca ta jest realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem. Zapewnia też możliwość realizacji dwukierunkowej wymiany informacji z połączonymi źródłami danych udostępniając standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Ponadto AAD zapewnia agregację i synchronizację danych poprzez:

[57] *FIDO2: Moving the World Beyond Passwords using WebAuthn & CTAP (fidoalliance.org)*

- Zapewnienie możliwości odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
- Zapewnienie możliwości integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:
    - pliki tekstowe CSV, AVP, LDIF,
    - relacyjne bazy danych,
    - usługi zarządzania tożsamością i dostępem Active Directory, Novell eDirectory, OpenLDAP.
- Zapewnienie komunikacji z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
- Umożliwienie tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
- Definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
- Definiowanie zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu.

4.4.2.3. NARZĘDZIA AAD W ZARZĄDZANIU TOŻSAMOŚCIĄ

Azure Active Directory oraz cała platforma Azure zawierają wiele usług wykorzystywanych przy zarządzaniu i posługiwaniu się tożsamością cyfrową.

Podstawowymi komponentami zarządzania tożsamością w AAD są:

4.4.2.3.1. ZARZĄDZANIE POŚWIADCZENIAMI

Zarządzanie poświadczeniami obejmuje usługi, zasady i praktyki, które umożliwiają, śledzą i aktualizują dostęp do zasobów lub usług. Zarządzanie poświadczeniami usługi Azure AD obejmuje następujące możliwości:

- Samoobsługowe resetowanie haseł (SSPR) umożliwia użytkownikom samodzielną obsługę i resetowanie własnych utraconych, zapomnianych lub naruszonych haseł. SSPR nie tylko zmniejsza liczbę interakcji ze wsparciem technicznym, ale zapewnia szybszą obsługę i bezpieczeństwo użytkownika.
- Zapisywanie zwrotne haseł synchronizuje hasła zmienione w chmurze z katalogami lokalnymi w czasie rzeczywistym.
- Blokada haseł analizuje dane telemetryczne wskazujące na często używane słabe lub naruszone hasła i blokuje ich użycie w całej usłudze Azure AD. Pozwala dostosować tę funkcję do swojego środowiska i dołączyć listę niestandardowych haseł do zablokowania we własnej organizacji.
- Inteligentna blokada porównuje uprawnione próby uwierzytelniania z próbami uzyskania nieautoryzowanego dostępu. Zgodnie z domyślnymi zasadami inteligentnej blokady konto jest blokowane na minutę po 10 nieudanych próbach logowania. Kiedy następne próby logowania nadal kończą się niepowodzeniem, czas blokady konta wzrasta. Za pomocą zasad można dostosować ustawienia w celu zapewnienia odpowiedniego zrównoważenia poziomu zabezpieczeń i użyteczności w organizacji.
- Uwierzytelnianie wieloskładnikowe (MFA) wymaga wielu form uwierzytelniania, gdy użytkownicy próbują uzyskać dostęp do wskazanych lub całości zasobów organizacji. Większość użytkowników jest zaznajomiona z używaniem czegoś, co znają - na przykład hasła, podczas uzyskiwania dostępu do zasobów. MFA prosi użytkowników o dodatkowego poświadczenia tożsamości, na przykład dostępu do zaufanego urządzenia lub identyfikatora biometrycznego. Usługa MFA może używać różnych rodzajów metod uwierzytelniania, takich jak połączenia telefoniczne, wiadomości tekstowe lub powiadomienia za pośrednictwem aplikacji uwierzytelniającej.
- Uwierzytelnianie bez hasła zastępuje hasło za pomocą uwierzytelniania tokenem smartfona lub sprzętu, identyfikatorem biometrycznym lub kodem PIN. Uwierzytelnianie bez hasła firmy Microsoft może współpracować z Windows Hello dla firm i aplikacją Microsoft Authenticator na urządzeniach przenośnych. Można również włączyć uwierzytelnianie bez hasła za pomocą kluczy zabezpieczeń zgodnych

z FIDO2, które używają WebAuthn i protokołu CTAP (Client-to-Authenticator) FIDO Alliance.

Komponenty te mogą być automatyzowane przez przepływy pracy, których głównymi funkcjami są:

- Zarządzanie poświadczeniami kontroluje uwierzytelnianie.
- Udostępnianie *(provisioning*) obsługi administracyjnej i zarządzanie uprawnieniami definiuje zasady dostępu, przypisuje użytkowników do zasobów i dostarcza dane do poświadczenia.
- Mechanizm autoryzacji ocenia zasady dostępu w celu określenia dostępu. Uwzględnia przy tym wykryte ryzyka, w tym dane analizy behawioralnej użytkowników/obiektów (UEBA - *user/entity behavioral analytics*), oraz sprawdza zgodność urządzeń z politykami dotyczącymi zarządzania punktami końcowymi.
- Po autoryzacji użytkownik lub urządzenie uzyskuje dostęp zgodnie z zasadami dostępu warunkowego.
- Jeśli autoryzacja nie powiedzie się, użytkownicy mogą wykonać weryfikację i dokonać wyboru właściwych poświadczeń w czasie rzeczywistym, aby ponownie przeprowadzić proces autoryzacji.
- Wszystkie dane sesji są rejestrowane dla celów analizy i raportowania.
- System zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) odbiera wszystkie dane dzienników zdarzeń, wykrytych ryzyk i dane UEBA dla tożsamości w chmurze i z systemów lokalnych.

4.5. INFRASTRUKTURA KLUCZA PUBLICZNEGO (PKI)

Uzyskiwanie dostępu do zasobów informacyjnych przez długi okres polegało na zaufaniu mechanizmom systemu operacyjnego, zwykle poprzez ograniczenie dostępu wymaganym hasłem dla danego użytkownika. Niestety, system ten polegał głównie na zaufaniu do

lojalności i zdrowego rozsądku pracowników, a złamanie zasad było stosunkowo proste i często niepozostawiające niezaprzeczalnych śladów.

Systemy klucza publicznego umożliwiają bezpieczną komunikację z daną organizacją wielu osobom - przy użyciu kluczy, które mogą być swobodnie rozpowszechniane i publikowane.

Standardem staje się wydawanie użytkownikom (a w niektórych systemach również urządzeniom) certyfikatów cyfrowych, wiążących klucze publiczne z osobą lub organizacją i potwierdzane podpisem zaufanych wydawców certyfikatów (CA - *Certification Authority*), a tym samym potwierdzające tożsamość tej osoby czy organizacji.[58]

Najważniejszymi powodami, dla których wdrażamy rozwiązania PKI są możliwości:

- Kontrola dostępu do zasobów sieciowych na bazie uwierzytelnienia 802.1x.
- Możliwość ograniczenia wykorzystania aplikacji do tych, których kod został podpisany przez zaufane źródło.
- Zabezpieczanie danych poprzez szyfrowanie plików.
- Wykorzystanie ochrony dostępu do sieci przez mechanizm IPSec.
- Ochrona zapytań do bazy LDAP.
- Stosowanie mechanizmów uwierzytelniania wieloskładnikowego.
- Szyfrowanie warstwy transportowej.
- Szyfrowanie wiadomości poczty elektronicznej.
- Zapewnienie integralności i nienaruszalności zawartości dokumentu poprzez jego podpisanie.
- Zapewnienie niezaprzeczalności autentyczności dokumentu poprzez jego podpisanie.

Głównym elementem struktury klucza publicznego jest cyfrowy dowód tożsamości, czyli certyfikat. Odgrywa rolę dowodu osobistego lub paszportu w świecie komunikacji elektronicznej. Zawiera informacje o posiadaczu i wystawcy certyfikatu oraz służy do przyporządkowania pary kluczy do osoby. Jako środek przekazu certyfikatów mogą służyć pliki chronione hasłem lub tokeny USB oraz karty chipowe *Smart Cards*. Zawierają one

[58] *Józef Muszyński, Infrastruktura klucza publicznego i podpisy elektroniczne.*

miniaturowy układ scalony, w którym zapisano algorytmy klucza publicznego i dane. Zaletą jest to, że szyfrowanie odbywa się na karcie, a więc klucz prywatny nie opuszcza karty.

Coraz częściej jednak wykorzystywane są systemy przechowywujące certyfikaty w chronionych repozytoriach sieciowych, co dopuszczane jest między innymi przez rozporządzenie eIDAS.

Jednym z ważniejszych elementów warunkujących potwierdzenie dokumentu elektronicznego z oryginałem zatwierdzonym przez autora jest jego podpis cyfrowy. Podpisy cyfrowe to nazwa technologii zapewniającej elektroniczny ekwiwalent tradycyjnego podpisu na papierze. Technologia ta zapewnia również niezaprzeczalność wystawienia takiego podpisu. To znaczy, że oprócz jednoznacznej identyfikacji źródła informacji zapewnia również możliwość kontroli jej nienaruszalności podczas przekazywania. Podpis cyfrowy jest mechanizmem pozwalającym na dodawania unikatowych danych do dokumentu w taki sposób, że generować je może jedynie właściciel klucza prywatnego, ale każdy, kto posiada odpowiedni klucz publiczny, może weryfikować autentyczność takiego podpisu. Podpisy cyfrowe umożliwiają ustanowienie prawnie uznawanej praktyki podpisywania dokumentów elektronicznych.

Zgodnie z przyjętymi w opracowaniu założeniami, system infrastruktury klucza publicznego (PKI) pozwalający na uwierzytelnianie pracowników oparty powinien być na certyfikatach z wewnętrznego CA (centrum certyfikacji) przechowywanych na kartach. Jednocześnie może być wykorzystywane zewnętrzne PKI (dostawcy zewnętrznej usługi) pozwalające na wykorzystanie certyfikatów kwalifikowanych służących do składania podpisu elektronicznego w procesie KPA. w wewnętrznym centrum certyfikacji wykorzystany zostanie mechanizm nadawania uprawnień zgodnie z rolą pełnioną w systemie. Uwierzytelnienie użytkowników zewnętrznych (np. interesantów) może opierać się na dwóch mechanizmach:

- Uprawnieniach dostępu na bazie profilu zaufanego[59].
- Uprawnieniach dostępu do danych klienta poprzez użycie certyfikatu z wewnętrznego CA. Po szerokim wprowadzeniu systemu PL ID ten mechanizm może zostać zastąpiony poprzez uwierzytelnianie za pomocą certyfikatu zawartego w dowodzie osobistym.

[59] https://www.gov.pl/web/cyfryzacja/profil-zaufany-ego-

Podstawą PKI jest centrum certyfikacji (CA), czyli mechanizm, który wydaje i unieważnia certyfikaty zgodnie z ustaloną przez siebie polityką (zasadami) wystawiania certyfikatów. Główne i podrzędne urzędy certyfikacji służą do wystawiania certyfikatów użytkownikom, urządzeniom i usługom oraz do zarządzania ważnością certyfikatów.

W obecnej erze globalnej ekonomii oszczędności kosztów stały się najważniejszym priorytetem dla wielu grup IT, a konsolidacja serwerów z pewnością może być jednym ze składników ogólnej strategii oszczędzania. Wprawdzie większość organizacji nie posiada dużej liczby urzędów certyfikacji, ale wiele firm używa większej liczby takich urzędów niż wynikałoby to wyłącznie z wymaganej przepustowości w wystawianiu nowych certyfikatów. Inaczej mówiąc, wiele firm posiada urzędy certyfikacji, które przeważnie nie są w pełni wykorzystane i ich możliwości zwyczajnie się marnują.

Istnieją dwie główne przyczyny takiego niepełnego wykorzystywania możliwości istniejących urzędów certyfikacji. Po pierwsze, niektóre organizacje mogą wymagać stosowania osobnych urzędów certyfikacji z przyczyn prawnych lub z powodu obranej polityki bezpieczeństwa. Część klientów decyduje się np. na wystawianie certyfikatów swoim zewnętrznym partnerom za pomocą urzędu certyfikacji, który jest całkowicie odseparowany od urzędów wystawiających certyfikaty dla użytkowników i komputerów wewnętrznych. w takich przypadkach wirtualizacja urzędu certyfikacji pozwala wyeliminować konieczność posiadania osobnego komputera dla tego urzędu, choć sam urząd certyfikacji nadal wymaga osobnego zarządzania pomimo tego, że działa jako maszyna wirtualna.

Drugą przyczyną był fakt, że automatyczne rejestrowanie certyfikatów obsługiwane było tylko dla scenariuszy ograniczających się do wewnętrznego lasu domen. w szczególności, urząd certyfikacji mógł automatycznie rejestrować certyfikaty tylko dla tych podmiotów, które są częścią tego samego lasu domen, do którego należy dany urząd certyfikacji. Nawet w przypadku, gdy na poziomie lasów domen istniało dwukierunkowa relacja zaufania, korzystanie z funkcji automatycznego rejestrowania certyfikatów wymagało użycia osobnych urzędów certyfikacji. w najnowszych wersjach usług katalogowych działa funkcja automatycznego rejestrowania certyfikatów pomiędzy różnymi lasami domen.

Mając na uwadze obowiązujące obecnie regulacje, ofertę rynkową oraz rachunek ekonomiczny, najbardziej efektywnym rozwiązaniem wydaje się zakup usługi dostarczania

certyfikatów wraz zarządzaniem ich życiem, a nie budowa własnej infrastruktury i procedur administracyjnych.

4.5.1. CENTRUM CERTYFIKACJI – CZYLI AD CS

Centrum certyfikacji jest wbudowaną usługą Windows Server.

Opcja *Active Directory Certificate Services* (AD CS) dostępna w kreatorze *Add Roles Wizard* pozwala zainstalować następujące komponenty AD CS:

- Urzędy certyfikacji (*Certification Authorities* – CA). Główne i podrzędne urzędy certyfikacji są wykorzystywane do wystawiania certyfikatów dla użytkowników, komputerów i usług oraz do zarządzania ich ważnością.
- Rejestrację w CA opartą o Web. Rejestracja oparta o Web pozwala użytkownikom na połączenie się z CA za pomocą przeglądarki Web w celu wykonania następujących działań:
    - utworzenia żądań certyfikatów i przejrzenia żądań,
    - pobrania list odwołań certyfikatów (*Certificate Revocation Lists* – CRL),
    - wykonania rejestracji certyfikatów kart inteligentnych,
    - usługę *Online Responder*. Usługa *Online Responder* implementuje *Online Certificate Status Protocol* (OCSP), pozwalający na dekodowanie żądań odwołania dla szczególnych certyfikatów, ocenę stanu tych certyfikatów i odsyłanie podpisanej odpowiedzi zawierającej informacje o statusie badanego certyfikatu.

Usługa Online Responder może zostać użyta jako alternatywa dla rozszerzeń list CRL w celu dostarczenia klientom informacji o odwołanych certyfikatach. Rozwiązanie *Microsoft Online Responder* jest oparte i zgodne z RFC 2560 opisującym OCSP. Pełny tekst RFC 2560 dostępny jest w witrynie *Internet Engineering Task Force* (http://www.ietf.org/rfc/rfc2560.txt).

Usługa rejestrowania urządzeń sieciowych. Usługa Network Device Enrollment Service pozwala routerom i innym urządzeniom sieciowym na uzyskiwanie certyfikatów opartych na mechanizmie *Simple Certificate Enrollment Protocol* (SCEP) opracowanym przez firmę Cisco Systems Inc.

Protokół SCEP został zaprojektowany w celu zapewnienia możliwości bezpiecznego i skalowalnego tworzenie certyfikatów dla urządzeń sieciowych przy użyciu urzędów certyfikacji. Protokół wspiera dystrybucję kluczy publicznych CA, rejestrowanie certyfikatów, odwoływanie certyfikatów oraz zapytania dotyczące certyfikatów.

Urzędy certyfikacji mogą zostać skonfigurowane na serwerach działających pod kontrolą różnych systemów operacyjnych, w tym wspieranych wersjach Windows Server. Jednak nie wszystkie systemy zapewniają wsparcie dla wszystkich funkcji lub wymagań projektowych, zatem utworzenie optymalnego rozwiązania wymaga starannego planowania i testów przed wdrożeniem AD CS w środowisku produkcyjnym. Jakkolwiek możliwe jest wdrożenie AD CS przy użyciu zaledwie pojedynczego serwera dla jednego CA, wiele rzeczywistych wdrożeń obejmuje kilka serwerów, skonfigurowanych jako urzędy główne, urzędy zasad i urzędy wystawiające oraz inne serwery skonfigurowane jako *Online Responder*.

4.6. ZARZĄDZANIE ŚRODOWISKIEM IT I ZASOBAMI

Zarządzanie środowiskiem IT i zasobami staje się kluczowym zadaniem w organizacjach, których działanie jest uzależnione od sprawnej pracy systemów teleinformatycznych. w przypadku współistnienia wielu systemów, bez mechanizmów monitorowania i zarządzania administrator nie jest w stanie zapanować nad wszystkimi zdarzeniami warunkującymi dostępność usług i zapewnić SLA swoim klientom.

Gdy aplikacja niezbędna dla działania konkretnego procesu napotyka na problem, przestaje działać w skomplikowanej, heterogenicznej i rozproszonej terytorialnie infrastrukturze, jej przywracanie może zająć działowi IT nawet cały dzień. w tym czasie pracownicy nie mogą realizować swoich zadań, co powoduje wymierne straty finansowe oraz drastyczne obniżenie zaufania klientów. Jedynym wyjściem jest zastosowanie proaktywnego podejścia, które pozwoli na wyeliminowanie komplikacji, zanim staną się one odczuwalne dla użytkowników. Doświadczenia firm komercyjnych wskazują, że inwestycja w oprogramowanie zarządzające i monitorujące może się zwrócić nawet w okresie kilku dni.

Podstawowe zadania takiego oprogramowania to:

- skalowalna platforma do monitorowania działania systemu na serwerach i stacjach roboczych,
- monitorowanie punktów końcowych np. magazynu czy łączności sieciowej,
- zarządzanie konfiguracjami,
- inwentaryzacja sprzętu i oprogramowania,
- skonsolidowane i konfigurowalne raportowanie,
- możliwość konfigurowania i filtrowania alertów i automatyzacja czynności przez nie generowanych,
- wsparcie i automatyzacja wdrożeń masowych i wdrażania poprawek,
- ujednolicona administracja maszynami wirtualnymi,
- tworzenie i przywracanie kopii zapasowych w skali całej organizacji.

4.6.1. PODSYSTEM MONITOROWANIA

Podsystem monitorowania pozwalałby w sieci wewnętrznej na monitorowanie:

- podstawowych funkcji systemów operacyjnych,
- usług UK,
- usług DFS (Distributed File System), FRS (File Replication Service),
- usług poczty elektronicznej,
- usług serwera zarządzania aplikacjami,
- usług sieciowych DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), WINS (Windows Internet Naming Service),
- usług wydruku,
- usług podsystemu dostępowego.

Podsystem monitorowania musi mieć również możliwość przechowywania danych historycznych i prezentowania raportów w oparciu o standardowe mechaniczny podsystemu raportowania.

W celu realizacji tego zadania w centralnej części systemu powinien być umiejscowiony serwer monitorujący wraz z bazą danych na potrzeby usług monitorowania. Na wszystkich serwerach pracujących w ramach sieci w organizacji zainstalowane i skonfigurowane zostałyby odpowiednie pakiety zarządzające.

Architektura usług takiego podsystemu składa się z następujących elementów:

- serwer zarządzający, odpowiedzialny za zbieranie informacji od agentów i przekazywanie ich do bazy danych,
- aplikacje zarządzające typu agent, pracujący na serwerach zarządzanych, odpowiedzialne za zbieranie danych i przekazywanie ich do serwera zarządzającego,
- bazy danych systemu monitorującego,
- interfejsu konsoli użytkownika / administratora,
- usług raportujących.

Elementy te oraz logiczne połączenie pomiędzy nimi tworzy grupę zarządzającą (*management group*).

W ramach usług podsystemu monitorującego dla całego systemu proponowane jest następujące rozwiązanie:

- utworzenie pojedynczej grupy zarządzającej,
- instalacje w centralnej części systemu serwera monitorującego wraz z serwerem bazy danych zbierającym dane oraz dostarczającym usług raportowania,
- instalacje na serwerach usług działających w ramach infrastruktury systemu agentów zarządzających.

4.6.2. PODSYSTEM ZARZĄDZANIA

W celu umożliwienia centralnego zarządzania środowiskiem pracy i usług użytkowników konieczne jest wdrożenie w ramach całości systemu usług opartych o komponent umożliwiający automatyzację instalacji oprogramowania i zarządzania nim.

Komponent ten ma umożliwiać zarządzanie poprzez klienta instalowanego na stacjach roboczych systemami operacyjnymi i aplikacjami.

Usługi systemu zarządzania oprogramowaniem mają pozwolić na:

- zarządzanie wdrażaniem aplikacji na stacjach roboczych klienta, poprzez wymuszaną instalację aplikacji,
- raportowanie zasobów, poprzez gromadzenie danych o zainstalowanych w systemach aplikacjach, zasobach sprzętowych stacji roboczych,
- zarządzanie poprawkami bezpieczeństwa, analizą systemów pod kątem aktualizacji bezpieczeństwa, odniesienie konfiguracji stacji roboczych do instalacji wzorcowej, dystrybucję i instalację poprawek,
- raportowanie stanu i zasobów stacji roboczych i serwerów.

Wdrożenie usług pozwoli na:

- przeprowadzenie inwentaryzacji oprogramowania,
- przeprowadzenie inwentaryzacji sprzętu,
- kontrolę uruchamianych aplikacji,
- dystrybucję oprogramowania,
- analizę danych w oparciu o predefiniowane raporty.

4.6.3. SYSTEM CENTER

Serwery z rodziny System Center tworzą pełen zestaw rozwiązań do zarządzania środowiskiem IT. Umożliwiają automatyzację kluczowych procesów w ramach działu IT i działów biznesowych, porządkują zasoby informatyczne przedsiębiorstwa oraz pozwalają na optymalizację kosztów związanych z ich utrzymaniem. Ponadto wraz z rozwiązaniami typu help-desk stanowią podstawę dla dostarczenia rzeczywistego SLA[60], będącego podstawą utrzymania wysokodostępnych i niezawodnych systemów.

Podstawowymi komponentami System Center są[61]:

- Operations Manager – służący do monitorowania zasobów.
- Configuration Manager – służący do zarządzania zasobami.

[60] *SLA (Service Level Agreement) – umowa pomiędzy klientem i dostawcą opisująca gwarantowane parametry dostarczanych usług*
[61] https://docs.microsoft.com/pl-pl/system-center/

- Virtual Machine Manager – służący do administracji maszynami wirtualnymi.
- Data Protection Manager – służący do zarządzania kopiami zapasowymi.
- Orchestrator (dawniej Opalis Integration Server) – służący do automatyzacji prac administracyjnych.
- Service Manager – służący do automatyzacji zarządzania zmianą i obsługi incydentów zgodnie z przyjętą metodyką (np. ITIL).
- App Controller – portal typu self-service służący do monitorowania i zarządzania maszynami wirtualnymi oraz aplikacjami na nich osadzonymi w środowiskach chmury prywatnej (własne zasoby) i chmury publicznej (Windows Azure).
- Unified Installer – narzędzie instalacji składników System Center na wielu serwerach.

Dla wygody użytkowników komponenty te zgrupowane są licencyjnie w tzw. suitach.

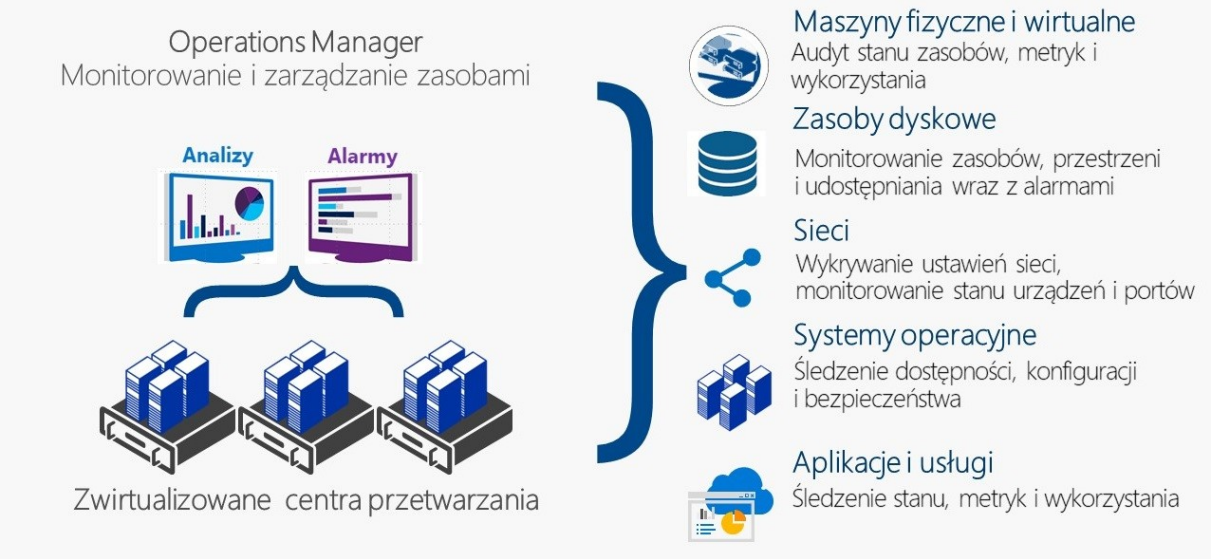
4.6.3.1. OPERATIONS MANAGER

System Center Operations Manager umożliwia monitorowanie usług, urządzeń i operacji na wielu komputerach z poziomu jednej konsoli. Operations Manager tworzy platformę do monitorowania działania systemu na serwerach i stacjach roboczych, jak również monitorowania innych punktów końcowych np. magazynu czy łączności sieciowej. Dodatkowo w najnowszych wersjach rozbudowano jego funkcje o monitorowanie warstwy wirtualnej. Infrastruktura Operations Manager może być zaprojektowana tak, aby mogła być skalowana w zależności od rozmiaru sieci, zachowując jednocześnie dużą elastyczność. w środowisku składającym się z kilkuset użytkowników oraz kilkudziesięciu serwerów instalacja Operations Manager na jednym serwerze spełnia wymagania dotyczące wydajności. Instancja SQL Server, służąca do przechowywania danych monitorujących Operations Manager, może być instalowana na tym samym lub innym serwerze.

Dużym ułatwieniem dla administratorów jest konsola (*Health Dashboard*) pozwalająca uzyskać syntetyczny obraz stanu monitorowanych systemów zarówno w kontekście całości chmury prywatnej, jak i jej komponentów.

Operations Manager wyróżnia się pośród pozostałych rozwiązań do monitorowania, które konsolidują i analizują dane z dziennika zdarzeń oraz wydajności w centralnej lokalizacji,

ponieważ wykorzystuje pakiety *Management Pack* (MP). Pakiety MP projektowane przez firmę Microsoft oraz innych dostawców sprzętu bądź oprogramowania stanowią w zasadzie zestaw reguł, które filtrują niepowstrzymaną falę danych, aby informować administratorów jedynie o potencjalnie interesujących spostrzeżeniach.



Katalog Microsoft MP, który zawiera szczegółowy opis możliwości monitorowania oferowanych przez poszczególne pakiety MP, jest dostępny w trybie online. Szeroki zakres różnego typu pakietów MP sprawia, że nawet organizacje o najbardziej zróżnicowanej infrastrukturze mogą odnaleźć mechanizmy integracji dostosowane do własnych potrzeb - także tych związanych z niestandardowymi technologiami, które są rzadko kojarzone z rozwiązaniami Microsoft. Wiele pakietów MP można pobrać nieodpłatnie, natomiast inne można zakupić u określonego dostawcy. Każdy z pakietów dostarcza do infrastruktury Operations Manager inny zestaw danych służący do aktywnego ostrzegania, gdy pojawią się problemy.

Jednym z kluczowych składników Operations Manager wspomagających monitorowanie aplikacji wykonanych w technologii .NET jest *Microsoft Monitoring Agent*, pozwalający na wyrywkowe lub ciągłe badanie stanu aplikacji. Ważnym rezultatem jego działania są logi zawierające szczegółową informację o błędach aplikacji lub ich problemach wydajnościowych. w nowych wersjach możliwe jest też monitorowanie stanu aplikacji napisanych w technologii Java poprzez wykorzystanie *Java Application Performance Monitoring* oraz monitorowanie systemów UNIX i Linux, takich jak Debian GNU i Linux 7.

4.6.3.2. CONFIGURATION MANAGER 

Samo monitorowanie środowiska nie wystarcza do osiągnięcia celu, jakim jest pełna kontrola nad zasobami IT. Druga kluczowa funkcja to możliwość wprowadzania zmian na serwerze oraz stacjach roboczych w powtarzalny, przewidywalny i dający się śledzić sposób. Organizacje, w których technicy są nadal wysyłani do biurek użytkowników, aby przeprowadzić instalację oprogramowania lub rozwiązać problem związany z działaniem aplikacji lub zarządzaniem poprawkami, mogą mieć spore trudności, gdy ich niewielka sieć zacznie się rozwijać. Takie rozwiązanie wymaga zbyt wielu realizowanych manualnie operacji, których powtarzanie na wielu maszynach byłoby zbyt czasochłonne. Dlatego potrzebne są scentralizowane narzędzia do instalowania oprogramowania, aktualizacji, a nawet całych systemów operacyjnych na wielu komputerach jednocześnie.

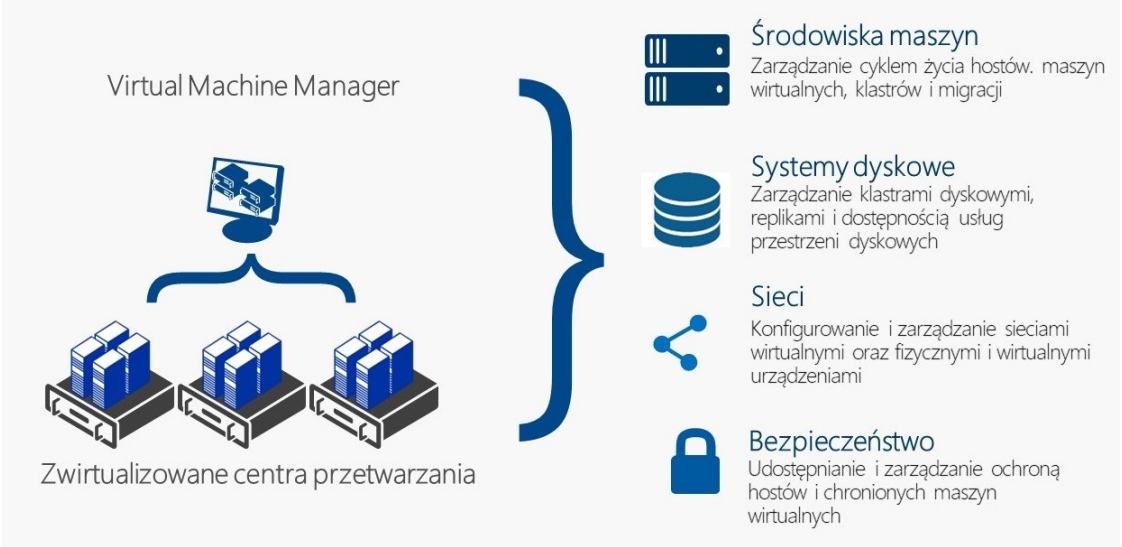
Rozwiązanie Configuration Manager do zarządzania zmianami można z łatwością skalować, dzięki czemu może być ono stosowane zarówno w małych środowiskach, jak i w dużych korporacjach obsługujących dziesiątki tysięcy użytkowników i setki lokacji. Niezależnie od rozmiaru infrastruktury do wdrażania zmian służą te same procesy i działania. Aby umieścić komponent lub cały system programistyczny na grupie komputerów, wystarczy stworzyć pakiet instalacyjny przy pomocy narzędzi wbudowanych lub niestandardowych, a następnie zastosować go w infrastrukturze Configuration Manager. Za pośrednictwem konsoli pakiet instalacyjny zostanie zintegrowany z anonsem (ang. *advertisement*) oraz kolekcją, co prowadzi do powstania zdarzenia zmiany. Kolekcja definiuje, na których komputerach ma zostać umieszczony pakiet, natomiast anons określa harmonogram wdrożenia. Przy użyciu anonsów i powiązanych z nimi okien obsługi w systemie Configuration Manager administrator może zaplanować proces instalacyjny tak, aby był on realizowany jedynie w czasie małej aktywności np. po godzinach urzędowania.

Aby skutecznie zarządzać oprogramowaniem po jego wdrożeniu, trzeba wiedzieć, gdzie się ono znajduje oraz czy działa prawidłowo. w firmach średniego rozmiaru inwentaryzacja stanu sprzętu oraz oprogramowania jest często dokonywana za pomocą długopisu i kartki papieru przy użyciu mało efektywnej metody prób i błędów. Funkcje spisywania (ang. *inventory*) dostępne w systemie Configuration Manager w połączeniu z funkcjami *Software Metering* oraz *Asset Intelligence* automatyzują prawie całą procedurę.

Wiele oferowanych na rynku narzędzi sprawdza obecność komponentów sprzętowych i programowych na serwerach oraz stacjach roboczych. Informacja ta jest przydatna, ale stanowi jedynie statyczną reprezentację. Funkcja *Software Metering* w systemie Configuration Manager dodaje możliwość identyfikowania, którzy użytkownicy oraz komputery korzystają z zainstalowanego oprogramowania. Dzięki tej funkcji organizacje IT mogą zlokalizować niewykorzystywane licencje oprogramowania i przekazać je innym osobom, zamiast kupować dodatkowe licencje. Integracja tej możliwości z wbudowaną bazą danych *Asset Intelligence* systemu Configuration Manager pozwala działowi IT dopasować cechy charakterystyczne zainstalowanego oprogramowania do określonych produktów, numerów wersji oraz edycji. w efekcie powstaje użyteczne rozwiązanie raportujące służące do identyfikowania, jaki dokładnie typ oprogramowania jest zainstalowany na analizowanych komputerach.

4.6.3.3. VIRTUAL MACHINE MANAGER

Operations Manager oraz Configuration Manager pomagają w obsłudze fizycznych serwerów, jednak obecnie wiele organizacji IT korzysta również z serwerów wirtualnych. Wirtualizacja wydaje się być w dzisiejszych czasach wszechobecna. Firmy niezależnie od rozmiaru masowo zastępują maszyny fizyczne wirtualnymi. Niegdyś możliwości wirtualizacji były ograniczone ze względu na wąski wybór platform wirtualnych, jednak wzrost zainteresowania wirtualizacją doprowadził do znacznego poszerzenia oferty. Obecnie o sukcesie decyduje przede wszystkim dostęp do narzędzi, które pomagają w zarządzaniu infrastrukturą wirtualną.



W związku z tym firma Microsoft zdecydowała się na zastosowanie podejścia wieloplatformowego w rozwiązaniu do zarządzania infrastrukturą wirtualną System Center Virtual Machine Manager (VMM). Możliwości systemu VMM nie ograniczają się do zarządzania maszynami wirtualnymi bazującymi na jednym typie Hypervisora. Administratorzy IT mogą przy pomocy tej samej konsoli zarządzać infrastrukturami wirtualnymi składającymi się zarówno z rozwiązań Microsoft Hyper-V, jak i produktów ESX oraz vCenter firmy VMware.

Aby móc rozmieszczać maszyny wirtualne (VM) w środowisku Microsoft, trzeba zainstalować Hypervisora Hyper-V, który domyślnie znajduje się w systemie operacyjnym Windows Server. Po zainstalowaniu roli Hyper-V w wystąpieniu Windows Server, serwer może obsługiwać tyle maszyn wirtualnych, na ile pozwolą mu zasoby, z dokładnością do ograniczeń licencyjnych.

Wbudowana funkcja *Windows Failover Clustering* pozwala dodatkowo uzyskać wysoką dostępność. Funkcja ta stanowi osobny komponent Hyper-V wykorzystywany przez pozostałe serwery wirtualne w danym klastrze. Klastry umożliwiają przenoszenie maszyn wirtualnych na inne hosty Hyper-V w przypadku awarii. Jest to doskonała okazja, aby poznać możliwości funkcji Windows Failover Clustering. Ulepszenia w zakresie instalacji oraz zarządzania ułatwiają konfigurację funkcji obsługi klastrów i czynią ją stałą częścią środowiska.

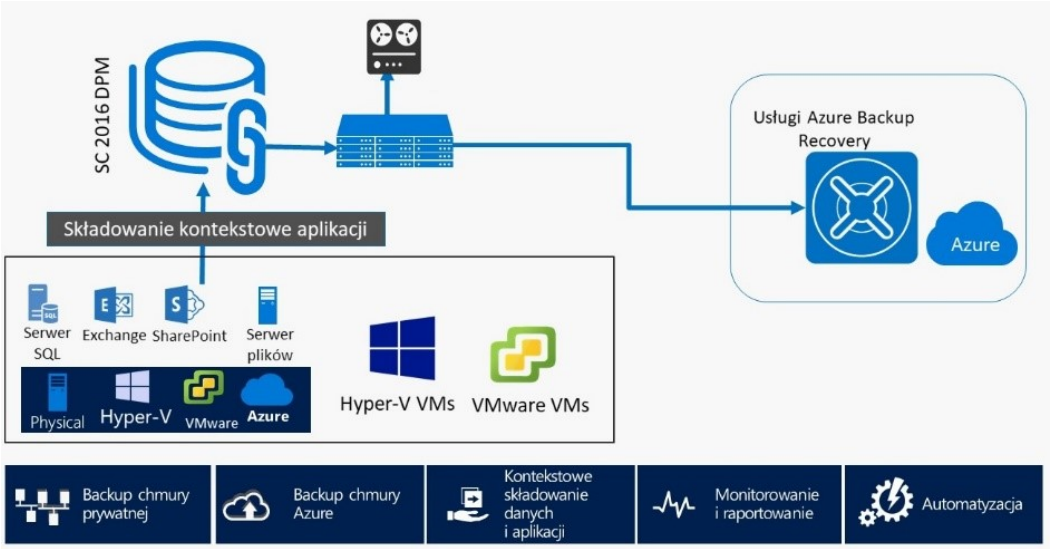
Ani funkcja Windows Failover Clustering ani system VMM nie są niezbędne do zarządzania maszynami wirtualnymi Hyper-V. Jednak ich obecność ogromnie ułatwia to zadanie, w szczególności w przypadku rosnącej liczby hostów Hyper-V. Przy użyciu systemu VMM można zarządzać hostami Hyper-V oraz maszynami wirtualnymi, realizując operacje na wybranych jednostkach lub na wszystkich naraz. w efekcie VMM pozwala na ten sam rodzaj automatyzacji w środowisku wirtualnym, jaki rozwiązania Configuration Manager oraz Operations Manager zapewniały na instancjach serwera.

4.6.3.4. DATA PROTECTION MANAGER

Czwarte rozwiązanie System Center, którego popularność gwałtownie rośnie w świecie IT, to Data Protection Manager (DPM). Ta dość nowa propozycja (publikacja kluczowej wersji R2 została ogłoszona ostatnio) oferuje platformę do tworzenia kopii zapasowych serwerów i komputerów w całym środowisku IT. DPM wyróżnia się spośród innych rozwiązań do

obsługi kopii zapasowych integracją z innymi produktami Microsoft oraz System Center, a także swobodą w zakresie zapisywanie kopii zapasowej danych serwera na dysku lub na taśmie.

DPM koncentruje się na tworzeniu kopii zapasowych z dysku na dysk, co jest szczególnie przydatne w mniejszych firmach, w których stosowanie zautomatyzowanych, korporacyjnych rozwiązań do obsługi taśm byłoby nie tylko zbyt kosztowne, ale i niepraktyczne. Ponieważ koszt napędów dyskowych stale maleje, tworzenie kopii zapasowej danych serwera na dysku zamiast na taśmie przynosi wiele korzyści m.in. możliwość szybkiego przywracania pojedynczych plików lub całych serwerów bezpośrednio z napędu dyskowego.



Integrując oferowaną przez DPM funkcję *Continuous Data Protection* z aplikacjami Microsoft (i nie tylko), takimi jak Exchange Server, SQL Server czy SharePoint Server, można chronić dane przed uszkodzeniem lub usunięciem niemal w czasie rzeczywistym. Menedżerowie IT mogą określić krótko- i długoterminowe cele ochrony danych, definiując wiele lokalizacji docelowych ochrony danych w zależności od potrzeb. Co więcej, ponieważ funkcja DPM należy do rodziny rozwiązań System Center, administratorzy mogą monitorować jej działanie za pośrednictwem konsoli Operations Manager.

Chociaż kopie zapasowe zapisywane na dysku pomagają w przeprowadzaniu szybkich operacji przywracania, większość organizacji archiwizuje dane w wydzielonym magazynie. Wymaganie to wiąże się zwykle z koniecznością przenoszenia taśm do odległej lokalizacji. DPM proponuje zmianę tego podejścia, umożliwiając przenoszenie kopii zapasowych z dysku na dysk, a następnie na nośnik taśmowy.

4.6.3.5. ORCHESTRATOR 

System Center Orchestrator (dawniej Opalis Integration Server) jest stosunkowo nowym produktem z rodziny System Center w ofercie Microsoft. Jest to bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk, pozwalające na definiowanie, testowanie i wielokrotne wykorzystanie prostych i złożonych zadań, procesów i procedur. Umożliwia testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie, wspomaga procesy zarządzania zmianami, planowanie wdrażania poprawek i zarządzanie życiem środowisk wirtualnych. Orchestrator wspomaga te obszary udostępniając mechanizmy workflow oraz integrację narzędzi System Center z rozwiązaniami firm trzecich do zarządzania oprogramowaniem i sprzętem.

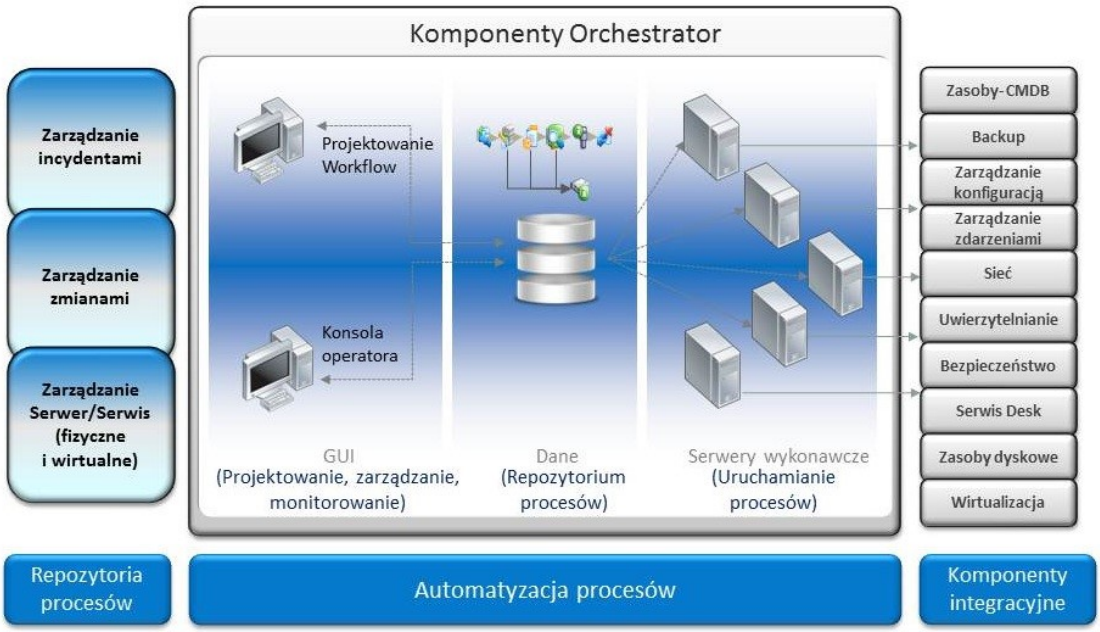
Typowe, dostępne „z pudełka” funkcje Orchestratora to:

- monitorowanie usług, zdarzeń, plików, folderów lub procesów,
- przenoszenie, kopiowanie lub edycja plików,
- wykonywanie zapytań SQL, skryptów PowerShell i VB, lub uruchamianie plików wykonywalnych,
- uruchamianie i zatrzymywanie serwerów lub usług.

Można też wykorzystywać predefiniowane i budowane samodzielnie przepływy pracy. Typowe (gotowe) przykłady workflow to:

- Active Directory Password Reset,
- Microsoft Cluster Patching,
- Microsoft SQL Server Cluster Patching,
- Microsoft SQL: Server Dump Copy Load,
- Operations Manager Event Remediation,
- Operations Manager Event Remediation and Enrichment,
- Operations Manager Service Alert Testing,
- VM Provisioning,
- Working with FTP,

- Operations Manager Tool Integration,
- Operations Manager: Manager of Managers,
- Operations Manager: Maintenance Windows,
- Active Directory: New Employee Onboarding,
- Operations Manager: Multi-Service Desk Integration.



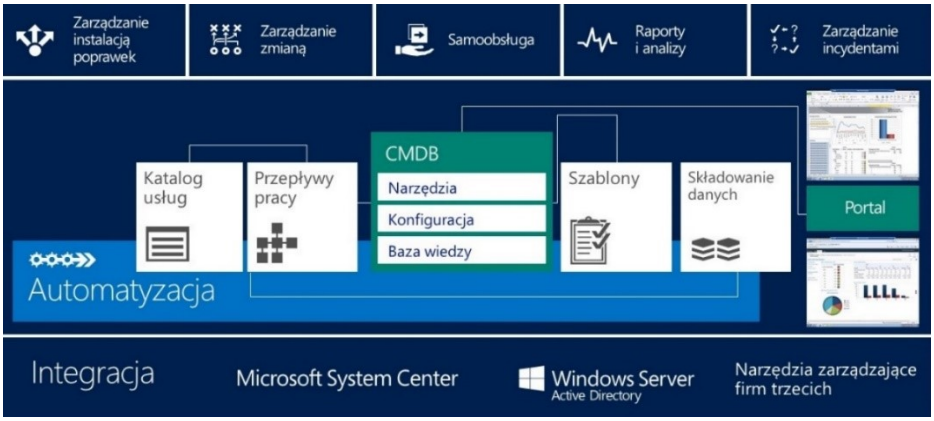
Dodatkowymi scenariuszami wykorzystania Orchestratora mogą być:

- Wdrożenie samoobsługi tworzenia maszyn wirtualnych i zarządzanie nimi,
- Wdrożenie samoobsługi w zakresie udostępniania użytkownikowi potrzebnych aplikacji,
- Wdrożenie samoobsługi w zakresie haseł i ich synchronizacji między różnymi platformami,
- Samoobsługa działań takich jak przypisanie uprawnień do plików lub dodanie użytkownika do grupy,
- Automatyzacja działań i scenariuszy naprawczych w przypadku wystąpienia znanych błędów.

Główną zaletą tego komponentu jest ograniczenie kosztów związanych z typowymi działaniami administracyjnymi w centrach przetwarzania (*DataCenter*) szczególnie w środowiskach heterogenicznych.

4.6.3.6. SERVICE MANAGER

System Center Service Manager jest zintegrowana platformą pozwalającą poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą. Centra przetwarzania danych, stanowiące platformę dla usług i systemów, wymagają narzędzi efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.



Poprzez integrację z innymi składnikami System Center, Service Manager zapewnia:

- Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką.
- Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia.
- Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu.
- Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania.
- Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów.

- Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej.
- Tworzenie baz wiedzy na temat rozwiązywania problemów.
- Automatyzację działań w przypadku znanych i opisanych problemów.
- Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

4.7. PLATFORMA ZARZĄDZANIA INFORMACJĄ

4.7.1. ZARZĄDZANIE INFORMACJĄ

Jednym z podstawowych elementów efektywnego systemu informacyjnego powinien być komponent umożliwiający tworzenie zestandaryzowanych centrów udostępniania informacji - portali dla całej organizacji i dla poszczególnych jednostek, przestrzeni roboczych (*workspace*) dla instytucji, zespołów i pracowników. Osoba posiadająca odpowiednie uprawnienia ma mieć w tym modelu możliwość tworzenia każdej z wymienionych typów przestrzeni roboczych i administrowania nimi.

Założeniem jest hierarchiczna struktura portalu pozwalająca tworzyć różnego typu struktury, przenosząc uprawnienia do nich z przestrzeni nadrzędnej lub nadając unikalne uprawnienia dla użytkowników wewnętrznych lub zewnętrznych. Ponadto niezbędny jest mechanizm określania na bazie uprawnień w użytkowników i ich grup w usługach katalogowych, które informacje są dostępne dla użytkowników lub ich grup, a które treści są dostępne dla wszystkich.

Aby zrealizować wymienione postulaty niezbędne jest wprowadzenie klasyfikacji informacji, który to temat poruszany był w rozdziale Infrastruktura bezpieczeństwa.

Budowa takiej struktury jest możliwa w oparciu o technologie Microsoft, tym niemniej przygotowanie jej złożeń wymaga dużych nakładów pracy. Dużo prostsze jest częściowo intuicyjne przygotowanie takiej struktury dzięki mechanizmom Microsoft Teams.

Zarządzanie dostępem do informacji wymaga wprowadzenia obowiązujących w całej organizacji mechanizmów klasyfikacji informacji – zarówno na etapie tworzenia dokumentów czy wiadomości poczty elektronicznej, jak i nadawania etykiet klasyfikujących składowanej informacji – zgodnie z ustalonymi regułami.

W celu uporządkowanego sposobu publikowania informacji oraz dostarczania poniżej opisanych narzędzi struktura portalu musi odzwierciedlać strukturę organizacyjną jednostki.

Portale wielofunkcyjne powinny być tworzone i zarządzane w zunifikowany sposób zgodnie z poniższymi zasadami.

- Tworzenie przestrzeni dla każdej jednostki czy zespołu musi odbywać się na bazie przygotowanych zasad, pozwalających na zachowanie tej samej struktury i narzędzi dostosowanych do potrzeb jednostki.
- Przewidziane powinno być ujednolicenie całej infrastruktury – na przykład poprzez wykorzystanie gotowego narzędzia z chmury.
- Zachowana powinna być hierarchiczność uprawnień i zarządzania treścią – dana jednostka (lub zespół) będzie zarządzać własnymi dokumentami i publikacjami.
- Każda przestrzeń powinna posiadać warstwę dostępną dla wszystkich użytkowników oraz część dostępną tylko dla uprawnionych.
- Każda przestrzeń powinna umożliwiać wyszukiwanie kontekstowe informacji, zarówno w witrynach danej jednostki, jak i w całym zespole portali. Wyszukiwanie będzie zwracało wyniki tylko z tym zakresem informacji, do których użytkownik ma uprawnienia.
- Nadawanie uprawnień do zawartości i narzędzi będzie następowało w danej jednostce poprzez „właściciela” odpowiedzialnego za witryny lub przestrzeni robocze lub poprzez ścieżkę akceptacyjną.

Warto przewidzieć mechanizm wymiany treści wspólnych oraz linków umożliwiających łatwy dostęp do informacji osobom uprawnionym.

W przyjętej konwencji, każda przestrzeń powinna zawierać:

1. nazwę jednostki organizacyjnej,
2. linki do portali innych jednostek,
3. linki do przestrzeni roboczych zespołów,
4. linki do ważnych instytucji współpracujących,
5. opis struktury organizacyjnej i pracowników,
6. mechanizm wyszukiwania,
7. część informacyjną zawierającą aktualne informacje i artykuły,
8. menu umożliwiające wejście do obszarów merytorycznych,
9. repozytorium wzorów (szablonów) dokumentów,
10. repozytoria dokumentów i archiwa,
11. przyciski otwierające predefiniowane formularze do tworzenia dokumentów, treści do witryn, ankiet, spotkań, ogłoszeń.

Optymalnym rozwiązaniem jest sytuacja, w której portal posiada wbudowane „gotowe" struktury, takie jak:

- podprzestrzenie o takiej samej funkcjonalności,
- biblioteki:
  - dokumentów z możliwością wersjonowania dokumentów,
  - formularzy pozwalających generować dokumenty XML,
  - stron Wiki,
  - zdjęć lub rysunków,
  - raportów.
- ogłoszenia stałe lub z zadanym okresem ważności (publikacji),
- kontakty, czyli bazy kontaktów,
- grupy dyskusyjne,
- linki do dokumentów oraz stron wewnętrznych i zewnętrznych,

- kalendarze prywatne i zespołowe,
- zadania dla użytkowników i zespołów z mechanizmami monitoringu ich wykonania, wykresami Gantta, i śledzeniem zadań,
- ankiety różnych typów z możliwością graficznej prezentacji ich rezultatów,
- definiowalne listy,
- tabele z możliwością definiowania kolumn (pól) i rekordów oraz wykonywania na nich różnych zdefiniowanych lub definiowalnych operacji wraz z generowaniem raportów,
- wskaźniki KPI monitorujące status procesów i zadań,
- tabele powstałe z importu arkuszy kalkulacyjnych.

Dodatkowo niezwykle użyteczną jest możliwość umieszczania w przestrzeniach roboczych okien różnego rodzaju aplikacji dziedzinowych.

Od strony funkcjonalnej zespół narzędzi stanowiący platformę współpracy i zarządzania informacją ma realizować następujące zadania w oparciu o konfigurację natywnych funkcjonalności oprogramowania, nie wymagając tworzenia nowych aplikacji:

- organizację pracy grupowej,
- wspólną, bezpieczną pracę nad dokumentami,
- publikację dokumentów,
- persjonowanie dokumentów (dla wersji roboczych),
- podpisywanie dokumentów,
- wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning).

Z uwagi na założenie polegające na daleko posuniętej standaryzacji, szczególnie w zakresie interakcji użytkownika z systemem, konieczne jest:

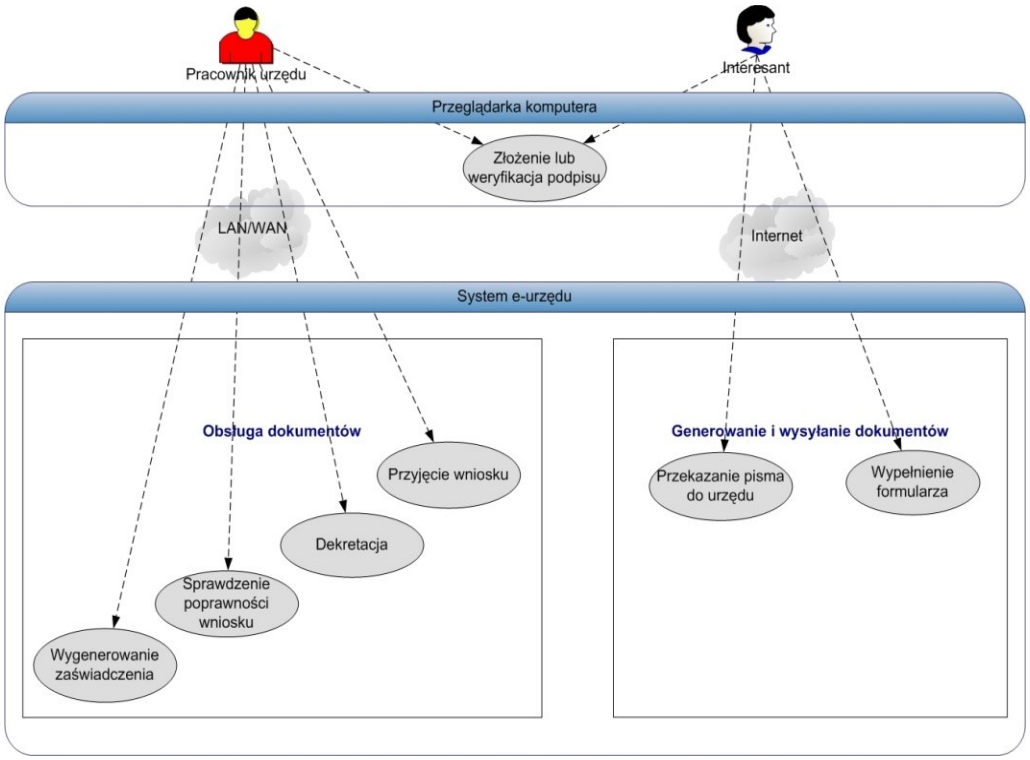
- oparcie się w maksymalnym stopniu o przeglądarkę jako interfejs użytkownika,
- wykorzystanie portalu jako standardowego interfejsu użytkownika dla wszystkich posiadanych aplikacji,
- zapewnienie wymiany danych z innymi systemami, w tym z centralnymi systemami.

Takie rozwiązanie umożliwia budowę portalu wielofunkcyjnego dla całej organizacji, umożliwiając wykorzystanie wszystkich opisanych funkcjonalności. Oczywiście z funkcjonalnego punktu widzenia, jedną fizyczną infrastrukturę portalu należy zaprojektować tak, by mogła stanowić zbiór WIELU niezależnych podportali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.

Za pomocą rozwiązania portalowego należy stworzyć mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

4.7.2. OBIEGI INFORMACJI I DOKUMENTÓW

Obieg dokumentów i spraw jest jednym z krytycznych narzędzi usprawniających działanie każdej organizacji, pod warunkiem przeprowadzenia przed jego wdrożeniem odpowiedniej analizy procesowej. z punktu widzenia komponentowej budowy systemu, traktujemy go jako usługę portalu wielofunkcyjnego, zrealizowaną w ramach jego architektury i zawartych w nim mechanizmów sterowanego obiegu informacji *workflow*.



Zakładana funkcjonalność ma umożliwiać przyjmowanie dokumentów elektronicznych od interesantów oraz tworzenie ich przez pracowników organizacji. Narzędzia systemu mają

umożliwiać budowanie schematów obiegu sprawy (*workflow*) dla każdego rodzaju sprawy i przyjmowanego dokumentu oraz budowania schematów wewnętrznego obiegu dokumentów.

Konfiguracja standardowego *workflow* to określenie:

- czy proces ma być wysyłany kolejno czy równolegle do wskazanych osób,
- czy istnieje możliwość przypisywania swoich zadań w danym workflow innym osobom,
- czy istnieje możliwość zmiany *workflow* ad-hoc,
- osób akceptujących oraz powiadamianych w danym procesie,
- ilości dni niezbędnych do wykonania zadania,
- zachowania po wykonaniu lub odrzuceniu zadania.

W zakładanym rozwiązaniu podstawowymi funkcjami udostępnianymi pracownikom urzędu są:

- przyjęcie wniosku,
- dekretacja dokumentu,
- akceptacja dekretacji,
- obsługa wniosku.

Podstawowymi elementami obiegu informacji i dokumentów są następujące, podstawowe struktury, opierające się na komponencie portalu wielofunkcyjnego:

- Repozytoria dokumentów i wzorów dokumentów elektronicznych.
- Repozytoria metadanych słownikowych i słów kluczowych.
- Środowisko definiowania i zarządzania metadanymi i ich zestawami.
- Środowisko definiujące zasady zarządzania dokumentami i cyklem ich życia.
- Silnik obiegu informacji (*Workflow*).
- Formularze elektroniczne (wzory dokumentów).
- Narzędzia wyszukiwania informacji i dokumentów.

4.7.2.1. REPOZYTORIA WZORÓW DOKUMENTÓW I DOKUMENTÓW

Pierwszym i kluczowym etapem budowy usług wewnętrznych dystrybucji informacji (czasem nazywany intranetem) jest utworzenie bezpiecznych i dostępnych dla uprawnionych osób repozytoriów dokumentów i repozytoriów wzorów dokumentów. Takie podejście jest możliwe jest możliwe poprzez wykorzystanie bibliotek dokumentów w portalu i rezygnację z modelu serwerów plików. Umożliwia między innymi oderwanie administracji uprawnieniami dostępu dla użytkowników od procesu zarządzania i administrowania infrastrukturą IT oraz wprowadzenia nowej kultury pracy z informacją.

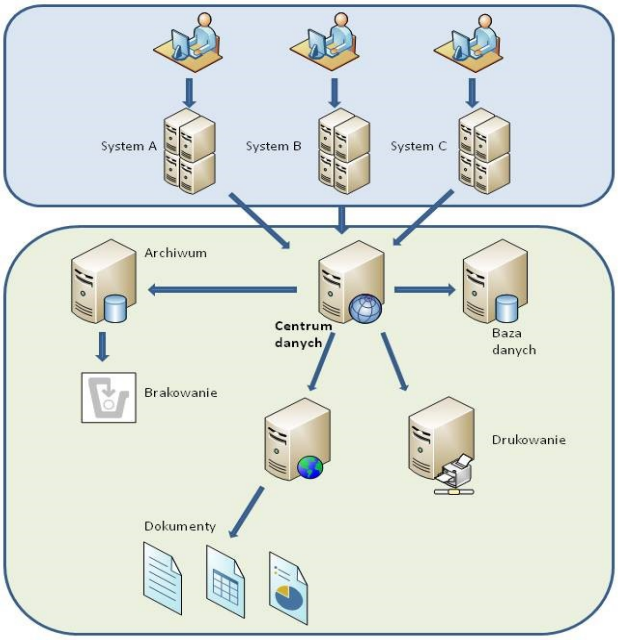
Zgodnie z dotychczasowymi założeniami, tworzenie nowych dokumentów (elektronicznych i papierowych) powinno odbywać się na bazie gotowych, zatwierdzonych i strukturalnie opisujących zawartą w nich informację szablonów (wzorów dokumentów).

Krytycznie ważne jest utworzenie repozytoriów szablonów dokumentów jak i samych dokumentów, czyli miejsc ich składowania zapewniających:

- bezpieczeństwo przechowywania,
- dostępność zgodnie z uprawnieniami użytkowników systemu,
- dostępność zgodnie z uprawnieniami dla systemów obiegów dokumentów.

Funkcjonalność tzw. Centrum danych umożliwia stworzenie centralnego repozytorium danych elektronicznych rekordów, dokumentów i szablonów. w proponowanym rozwiązaniu, administratorzy danych portalu wykorzystują centrum danych do określania typu oraz opisu metadanych dokumentów, które dzięki temu mogą być zarządzane jak typowe rekordy.

Centrum danych przedstawione na poniższym rysunku zawiera trzy repozytoria przygotowane do przechowywania projektów, raportów i umów kreowanych w postaci dokumentów XML poprzez odpowiednie departamenty czy biura. Przygotowywane są one w wyniku pracy zespołowej i mechanizmu workflow na wydzielonych przestrzeniach roboczych danego działu. Zaletą takiego rozwiązania jest automatyzacja segregowania dokumentów w skali organizacji, odpowiedni sposób ich procesowania i przechowywania (retencji) oraz wykorzystanie spójnego sytemu opisu metadanych dokumentu.



Centrum Danych przekierowuje odpowiednie dokumenty do odpowiadających ich typom repozytoriów, na przykład raporty finansowe przygotowane przez księgowość są przekierowywane do repozytorium danych finansowych. Osoba zarządzająca danymi może określić politykę unieważniania i usuwania dokumentów z repozytorium poprzez określenie czasu ich ważności oraz sposobu ich retencji. Na przykład dokumenty (lub ich typ opisany formularzem), będą w odpowiednim czasie archiwizowane, a te - których okres ważności został określony na (przykładowo) 10 lat – będą po tym czasie trwale usuwane.

4.7.2.2. REPOZYTORIA METADANYCH SŁOWNIKOWYCH I SŁÓW KLUCZOWYCH I ICH ZARZĄDZANIE

W systemie obiegu dokumentów musi być dostępne centralne repozytorium metadanych słownikowych[62]. w repozytorium tym należy tworzyć zestawy słownikowe, które mogą być centralnie tworzone, uzupełniane i zarządzane przez delegowane osoby.

Repozytorium to umożliwia tworzenie hierarchicznych słowników (np. kategorie spraw, rodzaje decyzji, struktura organizacyjna, typy dokumentów), które mogą być wykorzystane przy opisie dokumentów. Dodatkowo, mechanizm ten umożliwia wykorzystanie nawigacji według metadanych (*metadata navigation*) w bibliotekach dokumentów, który jest mechanizmem bardzo wydajnym i ułatwiającym zarządzanie treścią biblioteki. Uprawnione osoby mogą zarządzać poszczególnymi słownikami lub ich częściami.

[62] *Elektronizacja Informacji, Sławomir Bochowicz, Microsoft 2014*

Usługa zarządzania metadanymi i słownikami powinna być używana w następujących przypadkach:

1. definiowanie słowników hierarchicznych,
2. definiowanie słowników, które mogą być wykorzystane w wielu dokumentach i aplikacjach,
3. definiowane słowników dla celów wykorzystania nawigacji według metadanych (*Metadata Navigation*).

Stworzenie repozytorium metadanych słownikowych jest działaniem indywidualnym w ramach każdej organizacji. Usługa zarządzania metadanymi jest też repozytorium dla słów kluczowych (*Keywords*).

4.7.2.3. ŚRODOWISKO DEFINIUJĄCE ZASADY ZARZĄDZANIA DOKUMENTAMI I CYKLEM ICH ŻYCIA

Zgodnie z obowiązującymi procedurami i prawem, należy zdefiniować zasady zarządzania cyklem życia dokumentów (*Document Policies*).

Zasady zarządzania dokumentami pozwalają np. przenieść wybrane dokumenty pomiędzy bibliotekami ze względu na wybrane kryterium, np. wszystkie umowy starsze niż 5 lat powinny być przeniesione do biblioteki Archiwum.

W ramach systemu EOD dla niektórych typów dokumentów zostaną określone zasady zarządzania dokumentami. Zaletą tego mechanizmu jest fakt, że zasady mogą być tworzone zarówno poprzez interfejs użytkownika jak i za pomocą kodu i mogą być rozszerzane.

4.7.2.4. SILNIK OBIEGU INFORMACJI (WORKFLOW)

Typowy scenariusz zakłada, że interesant, który jest osobą fizyczną działającą w imieniu własnym lub w imieniu firmy wnosi sprawę składając odpowiednie dokumenty. w tym celu system wystawia formularz umożliwiający utworzenie dokumentu, złożenie pod nim podpisu elektronicznego oraz przekazanie przygotowanego dokumentu do urzędu.

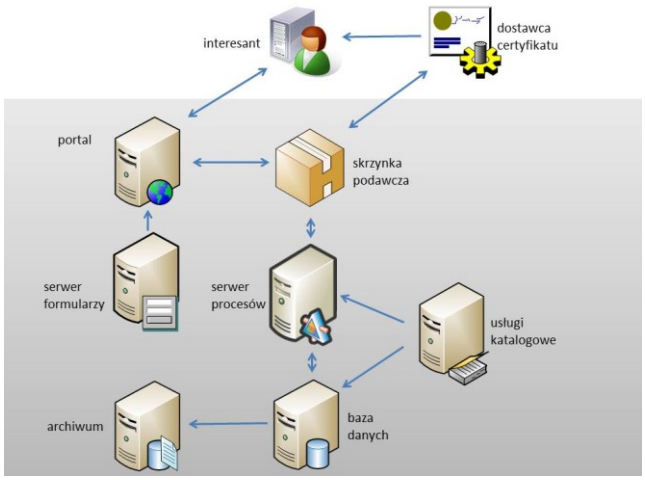
Pracownicy urzędu będą mieli możliwość realizowania różnych funkcji związanych z obsługą dokumentu i sprawy.

W niniejszym opracowaniu założono, że komponent portalu wielofunkcyjnego będzie mógł stanowić system obsługi spraw, który będzie się komunikował się z systemami zewnętrznymi (np. e-PUAP), przeznaczonymi do zarządzania obiegiem dokumentów i udostępniania usług dla systemów lokalnych. Dlatego poza funkcjonalnością przyjęcia dokumentu priorytetowym zadaniem jest Udostępnienie funkcji systemu w technologii *WebServices* oraz możliwość wykorzystywania zewnętrznych serwisów WS.

Realizacja powyższych funkcjonalności wymaga zastosowania architektury bazującej na udostępnianych serwisach poszczególnych komponentów. Takie przygotowanie systemu umożliwia optymalne wykorzystanie narzędzi, integrację z innymi systemami oraz rozszerzanie modelu o usługi udostępniane przez inne systemy.

System obiegu dokumentów spełniający wymogi prawa polskiego powinien uwzględniać następujące funkcjonalności:

- wystawianie Urzędowego Poświadczenia Odbioru (UPO) dla przyjmowanych dokumentów,
- doręczenie dokumentu elektronicznego (decyzji lub wezwania) obywatelowi lub firmie,
- wykonanie weryfikacji podpisów i zabezpieczenie ważności przez wykonanie paczki XAdES-A,
- przekazanie tzw. paczki archiwalnej do Archiwum Państwowego.



4.7.2.5. FORMULARZE ELEKTRONICZNE (WZORY DOKUMENTÓW)

Z uwagi na obowiązujące regulacje prawne obieg i archiwizacja informacji muszą opierać się na dokumentach elektronicznych w formacie XML tworzonych na bazie formularzy przechowywanych w repozytorium wzorów (szablonów) dokumentów elektronicznych.

Wymiana informacji pomiędzy systemami teleinformatycznymi, a także komunikacja pomiędzy organizacjami i osobami fizycznymi wymaga uzgodnienia standardów umożliwiających łatwe uzgodnienie interfejsów i jednolite rozumienie przekazywanych danych przez różne systemy teleinformatyczne. Jedną z podstawowych zasad dla ustalenia tych standardów jest przyjęcie języka komunikacji i standardu dla opisu struktur danych.

Możliwe są co najmniej dwie metody procesowania informacji w zgodzie z obowiązującymi regulacjami:

1. oparcie się całkowicie o dokument elektroniczny XML (od jego utworzenia do archiwizacji),
2. oparcie się o papierowy dokument źródłowy załączony do pliku XML zawierającego jego opis.

Dla realizacji wymaganego prawem obiegu dokumentów, niezbędne jest przygotowanie łatwych w użyciu i efektywnych narzędzi do tworzenia dokumentów XML, zarówno dla interesantów jak i dla urzędników.

Narzędzia tego typu powinny obsługiwać formularze elektroniczne (szablony dokumentów) i pozwalać na:

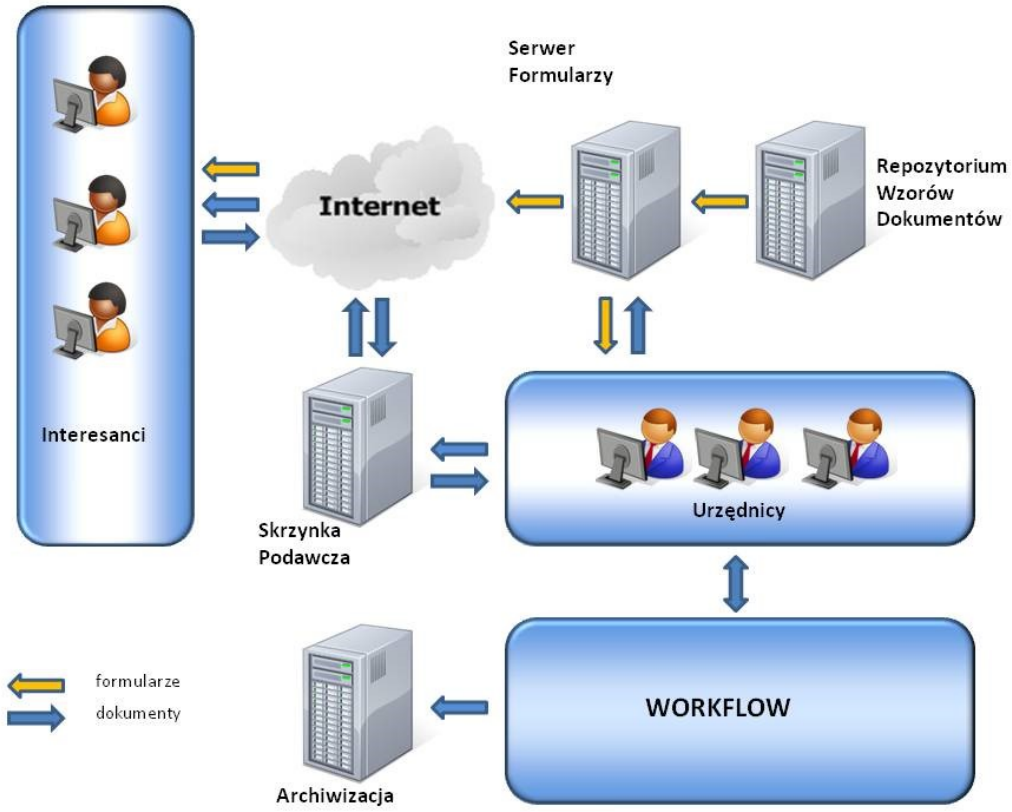
- wypełnienie formularza ze wspomaganiem walidacji poszczególnych pól (o ile to możliwe),
- zapisanie wypełnionego formularza w postaci dokumentu XML,
- wizualizację ostatecznej postaci dokumentu,
- podpisanie dokumentu podpisem elektronicznym.

Bardzo prostym, a zarazem skutecznym rozwiązaniem jest oparcie się o szablony edytora MS Word.

W ramach komponentowego systemu powinny być przygotowane następujące sposoby wprowadzania informacji na bazie formularzy, dostępne dla użytkowników wewnętrznych i zewnętrznych:

- Mechanizm on-line:
    - formularze dostępne poprzez przeglądarkę internetową z wykorzystaniem mechanizmów zawartych w komponencie portalu wielofunkcyjnego.
- Mechanizm off-line:
    - formularze bazujące na darmowym rozwiązaniu umożliwiającym użycie powszechnie wykorzystywanego edytora tekstów MS Word (formularz MSW),
    - formularze bazujące na bezpłatnej technologii Adobe Acrobat Reader (formularz AAR) wymagającej jednak opłaty licencyjnej za każdy utworzony formularz.

Ogólny mechanizm wykorzystania formularzy elektronicznych można przedstawić następująco:



4.7.2.6. NARZĘDZIA WYSZUKIWANIA INFORMACJI I DOKUMENTÓW

Oprócz standardowych przekierowań informacji w ramach zdefiniowanych procesów często trzeba wyszukać konkretną informację, dokument lub sprawę. Funkcjonalność wyszukiwania w ramach platformy obiegu dokumentów powinna dostarczać między innymi następujący zestaw funkcjonalności:

- wyszukiwanie dokumentów oraz informacji po metadanych,
- wyszukiwanie dokumentów oraz informacji po zawartości (*full text search*),
- definiowanie własnych zapytań do silnika wyszukującego,
- modyfikacja listy właściwości, po których można definiować wyszukiwanie,
- modyfikacja rankingu dla wyników danych,
- dostosowanie rankingu dla danych w zależności od profilu osoby z nich korzystającej.

4.7.3. PUBLIKOWANIE INFORMACJI

Publikowanie informacji na witrynach dla uprawnionych użytkowników jest jednym z najważniejszych sposobów jej udostępniania, zarówno na witrynach zewnętrznych (internet) jak i wewnętrznych (intranet).

4.7.3.1. WITRYNY ZEWNĘTRZNE I WEWNĘTRZNE

Korzystając z szablonów witryn i innych funkcji zawartych w standardowym portalu wielofunkcyjnym, można szybko i efektywnie tworzyć witryny odpowiadające potrzebom organizacji w zakresie publikowania określonej zawartości, zarządzania zawartością, zarządzania rekordami lub analiz biznesowych. Można na przykład tworzyć witryny na poziomie organizacji, takie jak witryny portali organizacyjnych lub urzędowe witryny sieci Web, albo witryny specjalistyczne, takie jak repozytoria zawartości lub obszary robocze spotkań. Witryny te umożliwią współpracę i udostępnianie informacji innym osobom, czy to wewnątrz, czy na zewnątrz organizacji. Konieczne jest też zaimplementowanie sprawnego mechanizmu wyszukiwania treści pozwalające skutecznie wyszukiwać osoby, dokumenty i dane, projektować procesy biznesowe sterowane formularzami i uczestniczyć w tych procesach, a także uzyskiwać dostęp do dużych ilości danych biznesowych i je analizować.

Podsystem portalu wewnętrznego (dla pracowników organizacji) i zewnętrznego (dla klientów) ma wspomagać działania takie jak:

- Efektywna współpraca z innymi osobami w organizacji. w kalendarzach można na przykład sprawdzać terminy wydarzeń dotyczących zespołu, a w bibliotekach dokumentów przechowywać dokumenty związane z zespołem, działem lub organizacją. Można również omawiać różne problemy za pomocą blogów lub rejestrować i przechowywać informacje na stronach typu wiki, które są bazami wiedzy zarządzanymi przez użytkowników.
- Tworzenie osobistych witryn, które umożliwiają zarządzanie informacjami i udostępnianie ich innym użytkownikom. Założeniem jest możliwość tworzenia portali i używania ich, jako centralnej lokalizacji do składowania i dostępu do wszystkich swoich dokumentów, zadań, łączy, kalendarza, współpracowników i innych osobistych informacji oraz do zarządzania całą tą zawartością.
- Znajdowanie osób, wiedzy i danych w aplikacjach biznesowych. Przeszukując na przykład witryny typu Moja witryna w intranecie, można znaleźć osobę o określonych umiejętnościach lub zainteresowaniach, nawet nie znając jej imienia i nazwiska. Dane można również znaleźć w firmowej bazie danych lub aplikacji biznesowej, na przykład w systemie zarządzania relacjami z klientami (CRM).
- Zarządzanie dokumentami, rekordami i zawartością sieci Web. Można na przykład opracować proces wycofywania dokumentów lub anulowania ich ważności po upływie określonego czasu zgodnie z obowiązującym prawem.
- Zarządzanie procesami za pomocą przepływów pracy (*workflow*), w łatwy sposób definiowalnego przez użytkowników.
- Obsługiwanie formularzy w formacie XML, które są składnikiem obiegu informacji i komunikacji z podmiotami zewnętrznymi. Można więc będzie opracowywać formularze wniosków (na bazie opublikowanych w repozytorium schematów XML), tak aby użytkownicy mogli wypełniać te formularze bezpośrednio w przeglądarce lub za pomocą dostępnych mechanizmów trybu off-line. Dane wprowadzone w formularzu mogą być przesyłane do bazy danych w sieci samorządu poprzez skrzynkę podawczą.

- Łatwe publikowanie raportów, list i kluczowych wskaźników wydajności (KPI) przez tworzenie łączy do aplikacji biznesowych, takich jak systemy ERP czy zasoby bazodanowe.

Ponadto mechanizm portalu ma zawierać mechanizm udostępniania dla użytkowników wewnętrznych i zewnętrznych formularzy opartych na schematach XML i umożliwiających podpisanie wynikowego dokumentu XML zgodnie z ustawodawstwem.

Tak więc budowa komponentu publikacji informacji i narzędzi wspomagających polegać będzie na tworzeniu portali o następujących własnościach:

- publikowanie informacji i multimediów,
- tworzenie portali wewnętrznych dla organizacji i portali zewnętrznych (internetowych),
- mechanizmy dostępu do publikowanej informacji na bazie uprawnień,
- mechanizmy ścieżki akceptacji w procesie publikacji,
- wsparcie i rozdzielenie procesu tworzenia treści i jej publikacji,
- sprawne, kontekstowe wyszukiwanie informacji,
- tworzenie hierarchicznych struktur wydzielonych podportali (dla jednostek lub zespołów) z delegacją uprawnień do ich zarządzania,
- wykorzystywanie wstępnie przygotowanych szablonów umożliwiających utworzenie podportalu w kilka minut,
- tworzenie i udostępnianie użytkownikom wewnętrznym i zewnętrznym baz wiedzy i słowników,
- udostępnienie warstwy informacyjnej i usługowej na podkładzie GIS,
- tworzenie forów, ankiet i komunikacji z jednostką.

4.7.3.2. ORGANIZACJA I PUBLIKACJA TREŚCI

W zakresie organizacji i publikacji treści komponent powinien spełniać następujące wymagania:

- Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści.
- Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu.
- Możliwość budowania hierarchicznej struktury stron portalu z prostym przenoszeniem stron i sekcji w ramach struktury nawigacji.
- Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię. Automatyczne generowanie mapy stron portalu.
- Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu.
- Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT.
- Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji.
- Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji.
- Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu.

4.7.4. PLATFORMA ZARZĄDZANIA INFORMACJĄ – CZYLI OFFICE 365

Microsoft Office 365 został zaprojektowany jako zbiór różnych usług zawierający między innymi SharePoint Online, czyli tzw. portal wielofunkcyjny, pozwalający zaadresować wiele scenariuszy użycia poprzez konfigurację wbudowanych własności, dostarczanych jako gotowe wprost po instalacji. Co więcej, dostępna jest detaliczna dokumentacja wspomagająca proces planowania, wdrożenia oraz jego utrzymania i audytu. Zapewnia ona ograniczenie ryzyk projektowych oraz gwarantuje stabilność i bezpieczeństwo systemu.

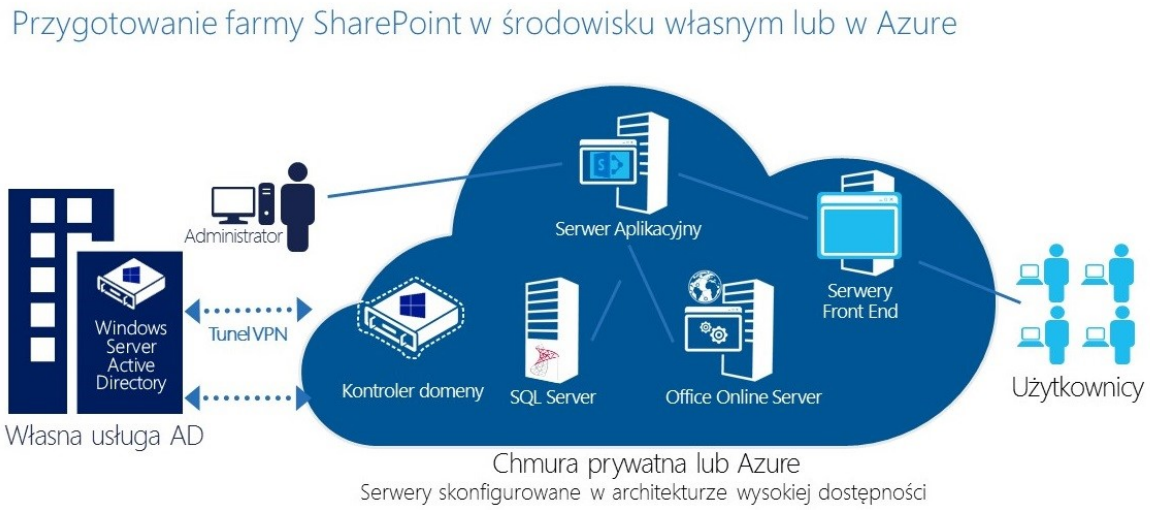
Office 365 łączy ludzi, procesy i informacje. Pozwala uzyskać poprawę udostępniania i wymiany informacji, kompleksowe zarządzanie zawartością i wyszukiwanie w jednostce, platformę i narzędzia potrzebne do administrowania serwerem oraz rozszerzalność i współdziałanie aplikacji.

Program oferuje:

- jednolity i przyjazny interfejs użytkownika,
- łatwość tworzenia narzędzi interakcji pracowników i dostępu do informacji,
- łatwość zarządzania i dostępność w skali całej organizacji lub wielu organizacji,
- wiele gotowych do użycia mechanizmów od nadawania uprawnień, publikacji treści po silnik workflow.

Ważną cechą nowych wersji jest też zrealizowanie w pełni koncepcji wykorzystania składników Office 365 takich jak SharePoint czy Exchange jako własnego rozwiązania (*on-premise*), jak i gotowych rozwiązań w chmurze. Istnieją również szczegółowo udokumentowane scenariusze i szablony instalacji farmy serwerów Office na platformie Microsoft Azure.

Przykładową architekturę portalu wielofunkcyjnego dla całej organizacji można przedstawić następująco:



Podkreślić należy, że ważnymi cechami SharePoint są:

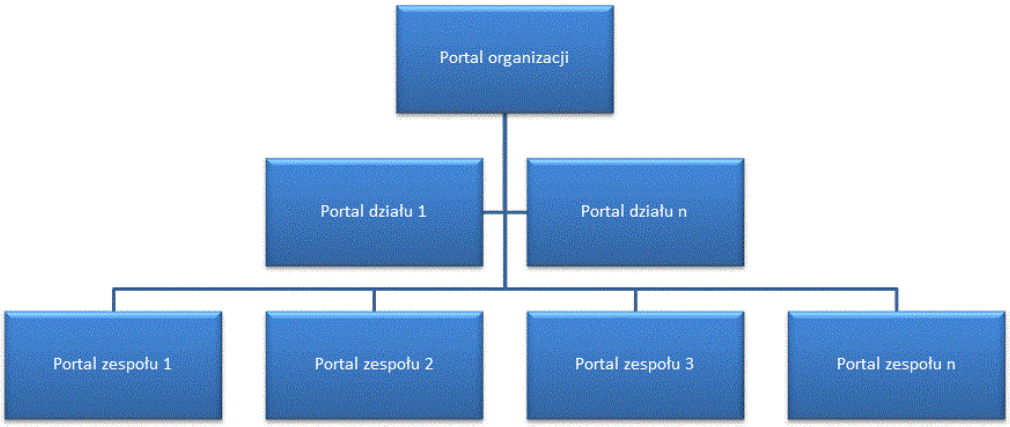
- pełne wykorzystanie usług katalogowych Active Directory lub Azure Active Directory (w chmurze),
- pełna integracja s systemami i usługami Exchange czy Teams,
- pełna integracja z pakietem Office.

Dużą zmianą wprowadzoną przez Microsoft jest rezygnacja z dwóch produktów SharePoint, tzn. portalu zewnętrznego (*internet*) i wewnętrznego (*intranet*), na rzecz jednego, pełniącego obydwie role.

Technologia SharePoint serwer wspiera architekturę warstwową tworzenia rozwiązań informatycznych. Istnieje wiele opisanych i dobrze udokumentowanych topologii wdrażania SharePoint w różnych scenariuszach użycia.

4.7.4.1. BUDOWA INTRANETU ORGANIZACJI

Jedna z bardzo ważnych cech SharePoint jest możliwość tworzenia dużych, wysoko dostępnych farm wielofunkcyjnych, na których wydzielane są „podportale” dla różnych jednostek czy użytkowników. Takie „podportale” mogą zarówno realizować różne funkcje, jak i być niezależnymi instancjami dla poszczególnych organizacji, czy grup użytkowników.



Przy hierarchicznej organizacji portali w jednostce zapewniamy dostęp do zawartości interesującej konkretnych użytkowników – od całej firmy do pojedynczego pracownika, korzystając jednocześnie ze spójnego modelu nadawania uprawnień – dziedziczonego w dół w całej strukturze lub kształtowanego zgodnie z politykami – niezależnie na każdym poziomie.

Jest to jeden z najbardziej efektywnych sposobów udostępnienia portali poprzez hostowanie z jednego centrum (własnego lub zewnętrznego), przy którym koszt wdrożenia i utrzymania na jednego użytkownika jest najniższy. Architektura taka jest niezwykle elastyczna i skalowalna, pozwalając na rozbudowę i rekonfigurację systemu w locie.

W celu polepszenia efektywności działania farm SharePoint stworzono trzy główne role:

- *User Role Server* – do która odpowiada bezpośrednio za obsługę działań użytkownika,
- Robot Server – odpowiadająca za wszystkie zadania nieinicjowane przez użytkownika,
- Caching Services – odpowiadająca za zarządzanie rozproszoną pamięcią buforującą.

4.7.4.2. BUDOWA ROZWIĄZAŃ W OPARCIU O SHAREPOINT

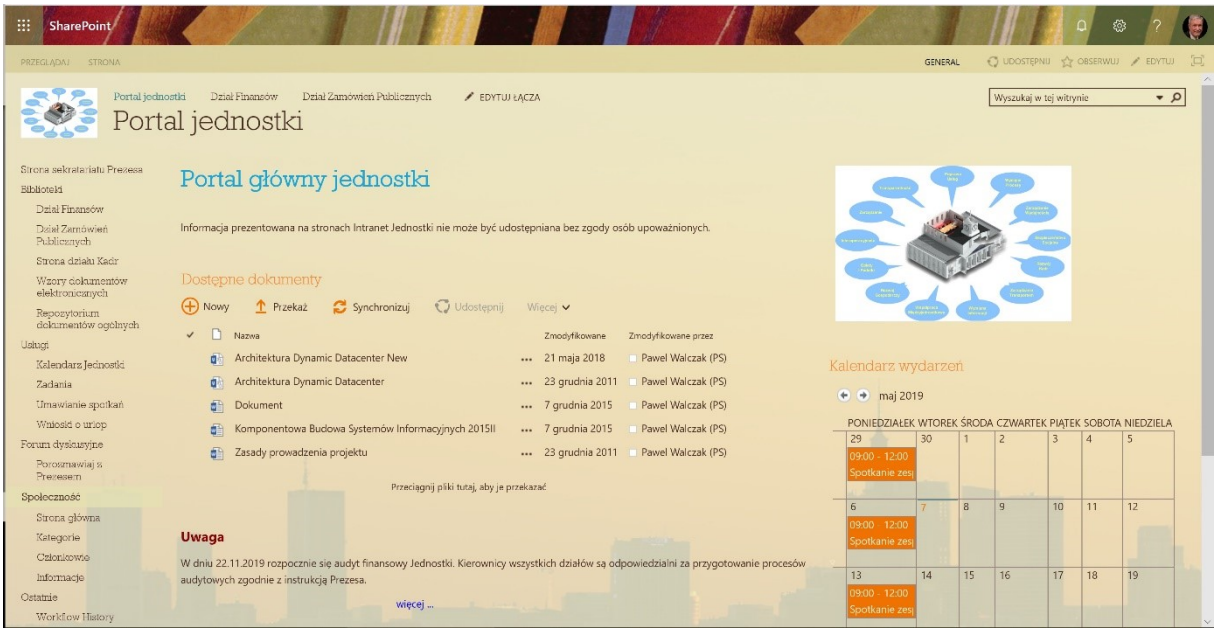
SharePoint udostępnia elementy konstrukcyjne, przy użyciu których można kompletować, łączyć i konfigurować rozwiązania współpracy. Wiele z zadań można wykonywać w oparciu o standardowe, wbudowane mechanizmy SharePoint. Jeżeli te standardowe funkcje są niewystarczające, można skorzystać z portalu jako platformy do osadzania własnych aplikacji, korzystających ze standardowych funkcji i interfejsu. Niestandardowe rozwiązania pozwalają reagować na nietypowe potrzeby lub zmiany w procesach czy prawie. SharePoint umożliwia każdemu uprawnionemu użytkownikowi łączenie gotowych elementów składowych w nowe,

potrzebne narzędzia bezpośrednio w przeglądarce. Użytkownicy zaawansowani technicznie mogą tworzyć bardziej rozbudowane rozwiązania SharePoint, korzystając z zaawansowanych narzędzi, a specjaliści IT mogą nadal kontrolować infrastrukturę, dane i aplikacje.

Różnorodne elementy składowe - od kalendarzy i zadań po dane biznesowe -umożliwiają szybkie tworzenie rozwiązań współpracy w przeglądarce.

4.7.4.3. SZABLONY WITRYN

Następną ważną cechą portalu SharePoint jest możliwość stworzenia szablonów stron dla poszczególnych poziomów organizacji. Przygotowany wstępnie szablon dla jednostki/działu/zespołu, z gotowym układem treści i wstępnie zdefiniowanymi usługami może być udostępniony konkretnej strukturze organizacyjnej w kilka minut.



4.7.4.4. WITRYNY INTRANETOWE I INTERNETOWE

Microsoft SharePoint to rozwiązanie spełniające większość oczekiwań związanych z witrynami intranetowymi i internetowymi. Udostępnia ono pełen zestaw narzędzi umożliwiających tworzenie witryn wszelkiego rodzaju oraz wspólną infrastrukturę, ułatwiającą zarządzanie witrynami. Wszystkie rodzaje informacji - od witryny zespołu, przez witrynę ekstranetową dla partnerów aż po witrynę w Internecie, przeznaczoną dla klientów – można udostępniać i publikować przy użyciu jednego, prostego w obsłudze i znajomego systemu.

Jeśli wdrożenie portalu SharePoint obejmowało przygotowanie standardowych szablonów stron (*template*), to tworzenie nowych witryn SharePoint jest proste i intuicyjne. Pełen zestaw funkcji dostępny w rozwiązaniu SharePoint pozwala każdemu użytkownikowi tworzyć witryny od początku do końca. Gotowe do użycia funkcje i szablony pomagają właścicielowi witryny w błyskawicznym utworzeniu pierwszej strony. Kolejne funkcje pozwalają bez trudu modyfikować strony, zmieniać zawartość, dodawać elementy interakcyjne lub stosować motywy graficzne. Niezależnie od poziomu zaawansowania, każdy może szybko utworzyć, dostosować i opublikować funkcjonalną witrynę, spełniającą określoną potrzebę organizacji.

4.7.4.5. PRZESTRZENIE ROBOCZE

Jedną z podstawowych funkcjonalności portalu SharePoint jest możliwość tworzenia przestrzeni roboczych (*workspace*) dla całej organizacji, zespołów i pracowników. Osoba posiadająca odpowiednie uprawnienia ma możliwość tworzenia każdej z wymienionych typów przestrzeni roboczych i administrowania nimi.

Założeniem jest hierarchiczna struktura portalu pozwalająca tworzyć różnego typu struktury przenosząc uprawnienia do nich z przestrzeni nadrzędnej lub nadając unikalne uprawnienia dla użytkowników wewnętrznych lub zewnętrznych. Ponadto dostępny jest mechanizm określania na bazie uprawnień w AD, które informacje są dostępne dla użytkowników lub ich grup, a które treści są dostępne dla wszystkich.

„Gotowe” struktury portalu SharePoint to:

- Podprzestrzenie o takiej samej funkcjonalności.
- Biblioteki:
  - dokumentów z możliwością wersjonowania dokumentów,
  - formularzy opartych o schematy XML,
  - stron Wiki,
  - zdjęć lub rysunków,
  - raportów,
- Ogłoszenia stałe lub z zadanym okresem ważności (publikacji).
- Kontakty, czyli bazy kontaktów.

- Grupy dyskusyjne.
- Linki do dokumentów oraz stron wewnętrznych i zewnętrznych.
- Kalendarze prywatne i zespołowe.
- Ankiety różnych typów z możliwością graficznej prezentacji ich rezultatów.
- Definiowalne listy.
- Tabele z możliwością definiowania kolumn (pól) i rekordów oraz wykonywania na nich różnych zdefiniowanych lub definiowalnych operacji wraz z generowaniem raportów.
- Wskaźniki KPI monitorujące status procesów i zadań.
- Tabele powstałe z importu arkuszy kalkulacyjnych.

Dodatkowo istnieje możliwość umieszczania w przestrzeniach roboczych okien różnego rodzaju aplikacji organizując tym samym standardowy interfejs dostępowy do wszystkich funkcji systemów potrzebnych użytkownikowi.

4.7.4.6. REPOZYTORIA DOKUMENTÓW I WZORÓW DOKUMENTÓW

SharePoint Server umożliwia budowanie repozytoriów dokumentów i wzorów dokumentów w oparciu o wbudowane mechanizmy. Utworzenie nowej biblioteki dokumentów polega na wyborze jej nazwy typu biblioteki oraz przydzieleniu odpowiednich uprawnień dla użytkowników czy ich grup. Mogą to być uprawnienia dziedziczone z portalu lub ustalane niezależnie przez osobę zakładającą nową bibliotekę. Proces trwa kilkadziesiąt sekund i nie wymaga wiedzy programistycznej. Dodatkowo można szybko wykreować dodatkowe mechanizmy wokół takiej biblioteki i jej zawartości, łącznie z:

- wymaganiem wersjonowania dokumentów,
- mechanizmami Workflow zależnymi od statusu dokumentu,
- mechanizmami ważności (brakowania) w założonym czasie.

Szeroki i elastyczny wybór widoków, umożliwia przedstawianie zawartości repozytorium w zależności od potrzeb, z uwzględnieniem wszelkich dostępnych metadanych.

Cały mechanizm posługiwania się repozytoriami pozwala na:

- Stworzenie repozytoriów szablonów dla konkretnych użytkowników i ich grup.
- Stworzenie repozytoriów dokumentów stosownie do ich klas i uprawnionego dostępu wraz z określeniem polityk bezpieczeństwa informacji.
- Monitorowanie zmian szablonów i dokumentów.
- Automatyzację procesów związanych z przekazywaniem, udostępnianiem, publikacją lub archiwizacją.
- Uprawnioną pracę nad konkretną wersją poprzez mechanizm wyewidencjonowania dla konkretnego użytkownika.

4.7.4.7. OBIEGI INFORMACJI I DOKUMENTÓW

Mając do dyspozycji bezpieczne, związane z rolą użytkownika repozytoria dokumentów można w łatwy sposób tworzyć obiegi dokumentów i teczek dokumentów. Możemy w nich skorzystać zarówno z gotowych dokumentów (plików), jak też tworzyć nowe z wykorzystaniem formularzy elektronicznych lub edytorów tekstu. Procesom przepływu (*workflow*) mogą podlegać w zasadzie dowolne pliki, tym niemniej zalecane jest wykorzystanie możliwości związanych z tagowaniem (opatrywaniem metadanymi) dokumentów.

Wbudowany silnik przepływów pracy pozwala tworzyć zadania, takie jak ścieżki akceptacyjne, obiegi dokumentów zatwierdzenia i przeglądy. w programie SharePoint Designer lub za pomocą projektanta przepływów pracy można tworzyć niestandardowe przepływy pracy, a następnie zarządzać uzyskanymi w ten sposób diagramami procesów biznesowych w centralnym repozytorium. Dodatkowo dostępna jest możliwość graficznego monitorowania przepływów i sprawdzania ich statusu w ujęciu przestrzennym.

Za pomocą funkcji zarządzania rekordami dostępnej w programie SharePoint organizacje mogą przechowywać i chronić rekordy biznesowe, umieszczając je razem z przetwarzanymi rekordami lub w centralnym repozytorium jako rekordy zablokowane. Do takich rekordów można stosować zasady utraty ważności, zapewniając w ten sposób zachowywanie tych rekordów przez odpowiedni czas, zgodny z wymaganiami prawnymi lub zasadami przyjętymi w firmie, co zmniejsza ryzyko prawne organizacji. Historie rekordów stanowią dowód dla

wewnętrznych i zewnętrznych audytorów, że rekordy zostały odpowiednio zachowane. Na określone rekordy będące dowodami prawnymi można nałożyć blokady, aby zapobiec ich zniszczeniu.

4.7.4.8. DYSK W CHMURZE, CZYLI ONEDRIVE

Od wersji 2013 SharePoint oraz SharePoint Online umożliwia konfigurację wirtualnego dysku użytkownika, przypisanego do jego konta – czyli *OneDrive*. Jest to dysk, który może być traktowany jako prywatny dysk użytkownika. Dostępny po odpowiedniej konfiguracji zawsze, gdy uprawniony użytkownik ma dostęp do sieci. Co więcej, instalowana na urządzeniu klienckim aplikacja *OneDrive* umożliwia synchronizację wskazanych katalogów na dysku urządzenia z przestrzenią *OneDrive*. Taka konfiguracja umożliwia pracę i zapisywanie jej wyników na dysku lokalnym nawet w przypadku braku połączenia z siecią, a zawartość katalogu (np. Moje Dokumenty) jest synchronizowana z *OneDrive* natychmiast po uzyskaniu połączenia. Tak więc użytkownik może pracować poza siecią oraz uzyskiwać dostęp do swoich plików z dowolnego urządzenia, na którym uwierzytelnił się do *OneDrive*.

W celu synchronizacji stosuje się szyfrowane połączenia, a uwierzytelnienie opiera się na poświadczeniach domenowych i może być wieloskładnikowe, co zapewnia bezpieczny, niezaprzeczalny i uprawniony dostęp do informacji.

W serwerze SharePoint ora jego repozytorium OneDrive zostały wbudowane narzędzia takie jak zabezpieczenie przed wyciekiem danych - *Data loss prevention* (DLP), rozróżnianie formatów danych wrażliwych (numery kart kredytowych, paszportów itp.) czy znajdowanie, raportowanie i usuwanie zastrzeżonych treści zgodnie z przyjętymi w organizacji zasadami i uprawnieniami.

Usługa *OneDrive* jest dostępna zarówno w przypadku posiadania własnej farmy opartej o SharePoint Server jak i subskrypcji Office 365 w modelu usługi hostowanej.

4.7.4.9. MECHANIZMY WYSZUKIWANIA

SharePoint Server udostępnia zaawansowaną usługę wyszukiwania (*Search Service*), która wspomaga inne funkcje takie jak zarządzanie zawartością w przedsiębiorstwie i współpraca. Pozwala szybciej wyszukiwać potrzebne informacje zarówno użytkownikom, jak też aplikacjom osadzonym na MSS.

Możliwe jest wyszukiwanie zarówno wyrażeń pełnotekstowych jak i (znacznie skuteczniejsze) oparte na metadanych opisujących wyszukiwany obiekt.

Wyszukiwanie uwzględnia informacje o użytkowniku, między innymi o jego uprawnieniach, tak aby w wynikach wyszukiwania pojawiały się wyłącznie treści do których ma prawo.

Search Service pozwala uściślać wyniki za pomocą interakcyjnych elementów nawigacyjnych, ułatwiając znalezienie potrzebnych informacji. Przykładem takich elementów są filtry, pozwalające ograniczyć zakres wyszukiwania w takim zakresie szczegółowości, na jaki pozwala struktura przeszukiwanych danych. Jeszcze raz należy więc podkreślić wagę przygotowania wszelkiej składowanej informacji poprzez opisanie jej spójnymi metadanymi. Jest to proces tak ważny, że warto rozpocząć implementację funkcji przechowywania i udostępniania informacji (w szczególności dokumentów) od wdrożenia prostych narzędzi pozwalających na opisanie metadanymi każdego nowego dokumentu (utworzenia jego metryki), który trafia do repozytoriów. Dzięki takiemu przygotowaniu można użyć mechanizmów filtrowania podając autora, datę utworzenia czy modyfikacji dokumentu, typu dokumentu, czy sprawy, której dotyczy. Oczywistym dla jednostek administracji publicznej jest opisywanie dokumentu numerem RWA.

Wyszukiwanie w programie SharePoint Server obejmuje wiele źródeł i typów zawartości, co pozwala korzystać ze wszystkich informacji w organizacji — włącznie z danymi w aplikacjach biznesowych takich jak systemy ERP, CRM i niestandardowe bazy danych — oraz udostępnić te informacje odpowiednim osobom.

Dostępne są standardowe mechanizmy takie jak tworzenie linków „sponsorowanych”, prezentowanych wysoko w wynikach wyszukiwania, podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu, wskazywanie w wynikach wyszukiwań duplikatów plików czy dostępność statystyk wyszukiwanych fraz.

4.7.4.10. DOSTĘP DO DANYCH Z INNYCH SYSTEMÓW

Dzięki gotowym, wbudowanym mechanizmom, możliwy jest prosty dostęp do danych pochodzących z dowolnych systemów wyposażonych w standardowe interfejsy komunikacyjne lub z baz danych obsługujących typowe zapytania SQL bez konieczności ich replikacji do własnej bazy danych czy hurtowni. Dane takie można tworzyć, odczytywać, aktualizować, usuwać i przeszukiwać przy użyciu list zewnętrznych.

Funkcja analiz biznesowych to zbiór metod, technologii i procesów umożliwiających przetwarzanie informacji przechowywanych w systemach organizacji. Łatwy dostęp do danych pozwala pracownikom podejmować właściwe decyzje. Program SharePoint jest istotnym elementem platformy analiz biznesowych firmy Microsoft, ponieważ ułatwia udostępnienie tych funkcji wszystkim pracownikom organizacji, umożliwiając podejmowanie skutecznych decyzji na podstawie kluczowych danych.

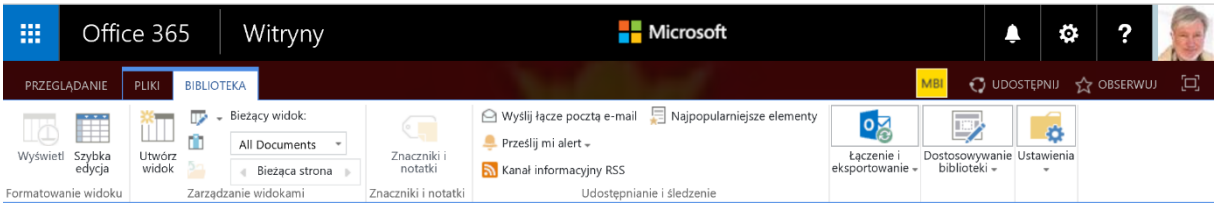
Większość organizacji przechowuje dane w różnych formatach, takich jak bazy danych, wiadomości e-mail i pliki arkuszy kalkulacyjnych. Program SharePoint ułatwia wyodrębnianie danych z różnych źródeł oraz przedstawianie ich w sposób ułatwiający analizę i podejmowanie decyzji.

Usługi *Performance Point Services* w programie SharePoint Server ułatwiają ocenę kluczowych wskaźników działalności organizacji oraz umożliwiają dogłębną analizę. Pracownicy mogą wyszukiwać trendy przy użyciu utworzonych przez siebie interakcyjnych pulpitów nawigacyjnych z kartami wyników, raportami i filtrami. Do witryn programu SharePoint można dodawać zaawansowane wykresy i łączyć je z danymi pochodzącymi z różnych źródeł, takich jak listy programu SharePoint, zewnętrzne listy danych, usługi łączności danych biznesowych, usługi Excel Services i inne składniki Web Part.

4.7.4.11. INTUICYJNA OBSŁUGA PORTALU

Dużą zaletą jest możliwość (po wykonaniu wstępnej konfiguracji) posługiwania się funkcjami portalu bez specjalnego przygotowania, bazując na znajomości zasad obsługi pakietu Office.

Dzięki wstążce programu SharePoint można szybko i łatwo znaleźć potrzebne funkcje. Prosta obsługa, polegająca na wskazywaniu i klikaniu oraz kontekstowej zmianie zawartości wstążki, sprawia, że wykonywanie złożonych zadań jest prostsze, a praca przebiega w sposób bardziej intuicyjny.

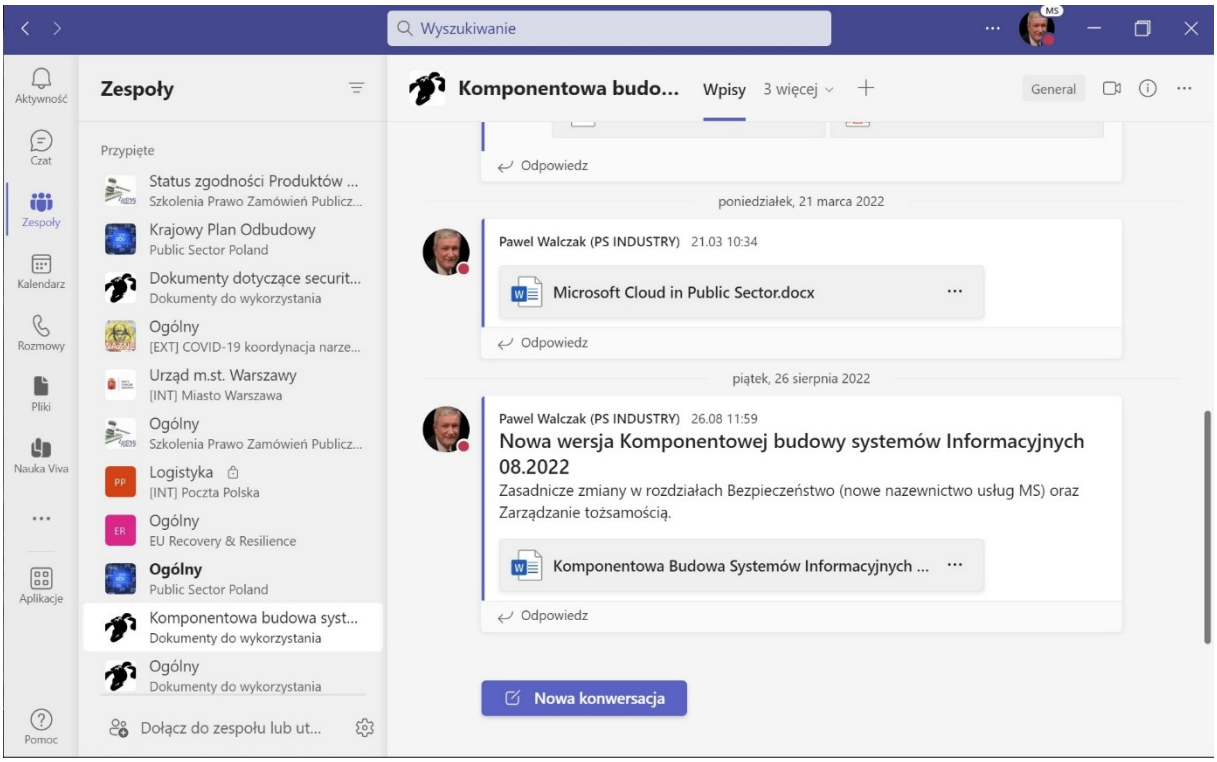


Rozwiązanie to jest w zasadzie identyczne z zawartym w narzędziach pakietu Office, a więc edycja treści do publikacji na witrynie wygląda dokładnie tak samo jak przygotowanie tekstu w MS Word.

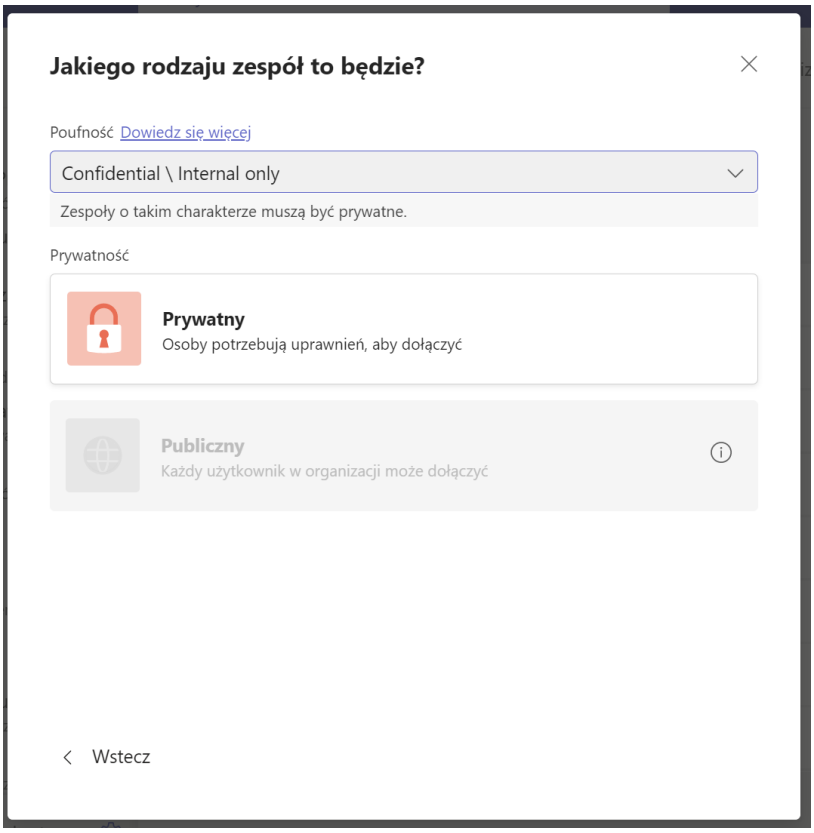
4.7.4.12. NOWOCZESNE PODEJŚCIE DO WSPÓŁPRACY W MS TEAMS

Interfejsem, który pozwala użytkownikowi na dostęp do informacji, jej publikowanie i pracę zespołową jest obecnie aplikacja MS Teams, opisana w dalszych rozdziałach. z punktu widzenia zarządzania informacją i współpracy, Teams stał się kluczowym narzędziem, upraszczającym wiele zadań i procesów. Działając jako interfejs dla usług pozostałych komponentów Office 365 umożliwia wykorzystanie wszystkich opisanych powyżej mechanizmów w spójny sposób.

Na przykład, tworzenie przestrzeni roboczych (Zespołów nazywanych też kanałami) dla wszystkich lub wybranych współpracowników wewnętrznych i zewnętrznych jest (po odpowiedniej konfiguracji Office 365) niezwykle proste i intuicyjne. W tle Teams tworzy odpowiednie struktury na SharePoint Online wykorzystując jego funkcje bez konieczności ingerencji użytkownika.



Co więcej, użytkownik tworząc nowy zespół zmuszony jest do określenia zasad bezpieczeństwa i dostępności informacji – między innymi musi dokonać klasyfikacji informacji zawartej w zespole:



4.7.4.13. ADMINISTRACJA INFORMACJĄ I BEZPIECZEŃSTWEM W MICROSOFT 365

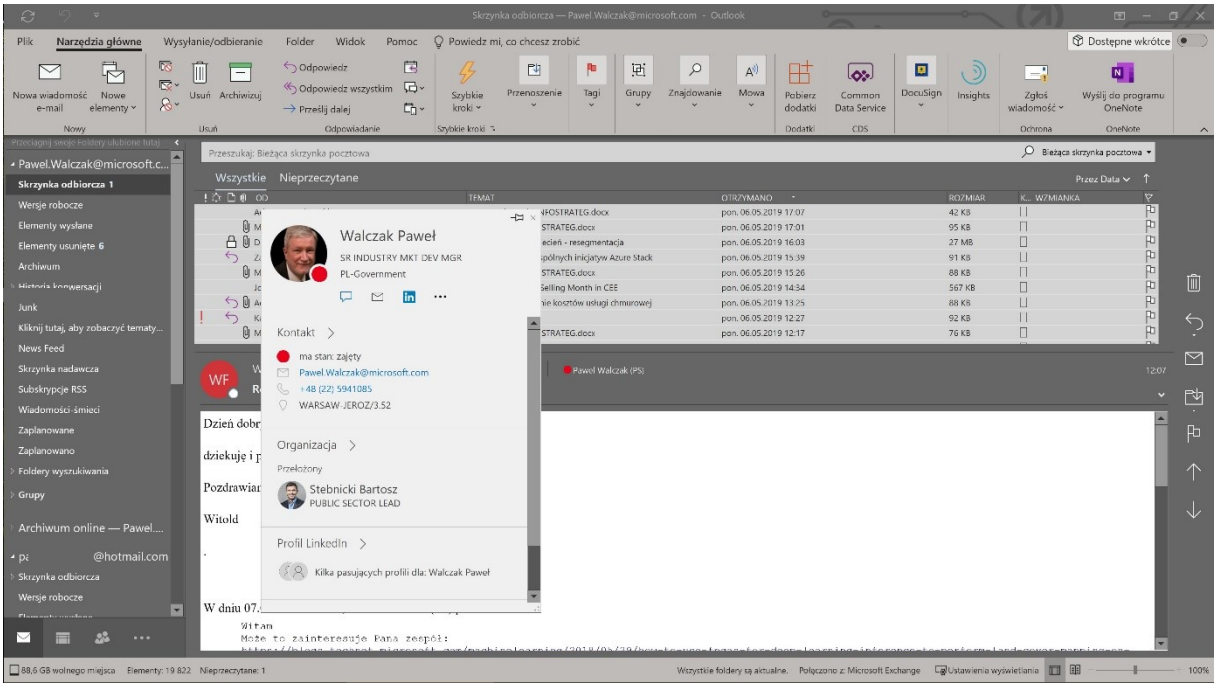
Podstawą wszystkich działań związanych z przetwarzaniem informacji jest stosowanie się do wymogów prawnych i wewnętrznych polityk organizacji. Narzędzia firmy Microsoft pozwalają na uzyskanie zgodności z takimi wymogami **pod warunkiem, że mechanizmy te zostaną odpowiednio skonfigurowane.**

Microsoft udostępnia zarówno przewodniki jak i szkolenia w tym zakresie, które powinny być wykorzystywane przez administratorów bezpieczeństwa i administratorów usług z chmury w organizacji. Brak takich ról administracyjnych i podjęcia odpowiednich działań może prowadzić do naruszeń polityk bezpieczeństwa informacji.

4.8. WSPÓŁPRACA – CZYLI MICROSOFT 365

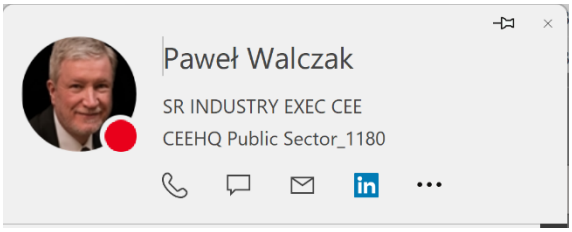
Komponenty takie jak Exchange Online, SharePoint Online, Teams i pakiet biurowy Office (lub pakiet Office 365) oraz system operacyjny Windows zainstalowane razem pozwalają uzyskać dodatkowe funkcje poprzez współdziałanie - tworząc pakiet Microsoft 365.

Typowym przykładem integracji Outlook i pozostałych komponentów Office 365 jest możliwość obserwacji danych z książki adresowej, dostępności pracowników i rozpoczęcia wielokanałowej komunikacji z nimi poprzez interfejs poczty elektronicznej.

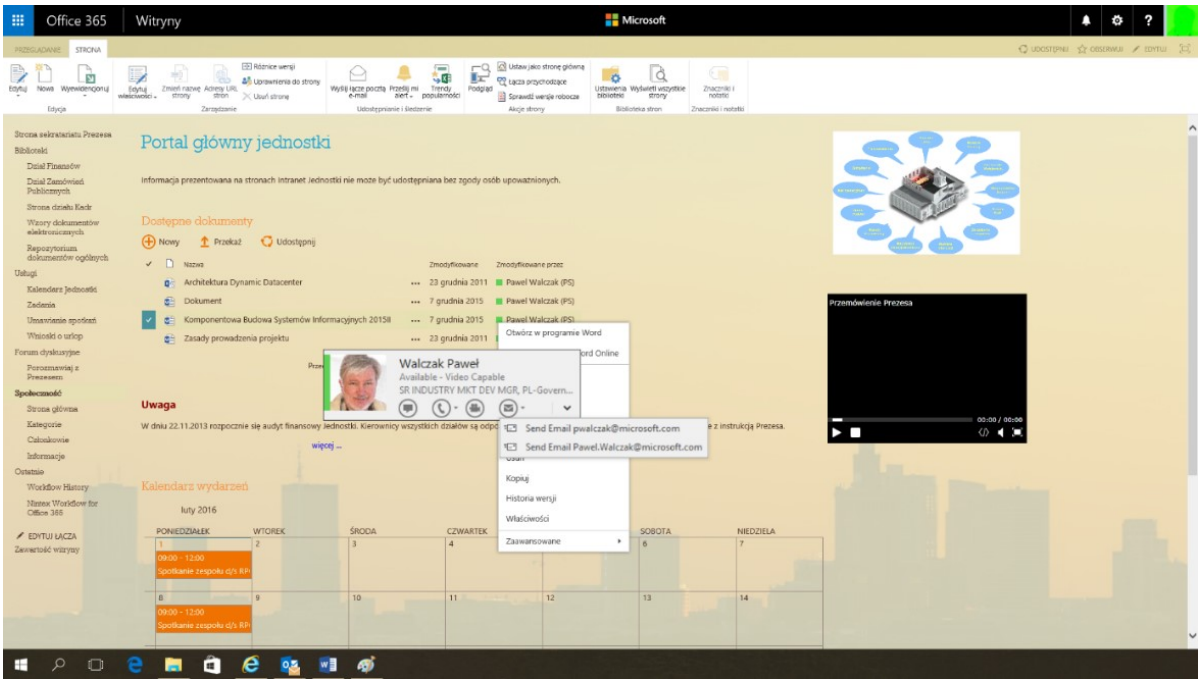


Tego typu podejście umożliwia skoncentrowanie się na samych zadaniach wykonywanych z innymi członkami zespołu, bez poszukiwania narzędzi komunikacji z nimi zawartych w różnych aplikacjach.

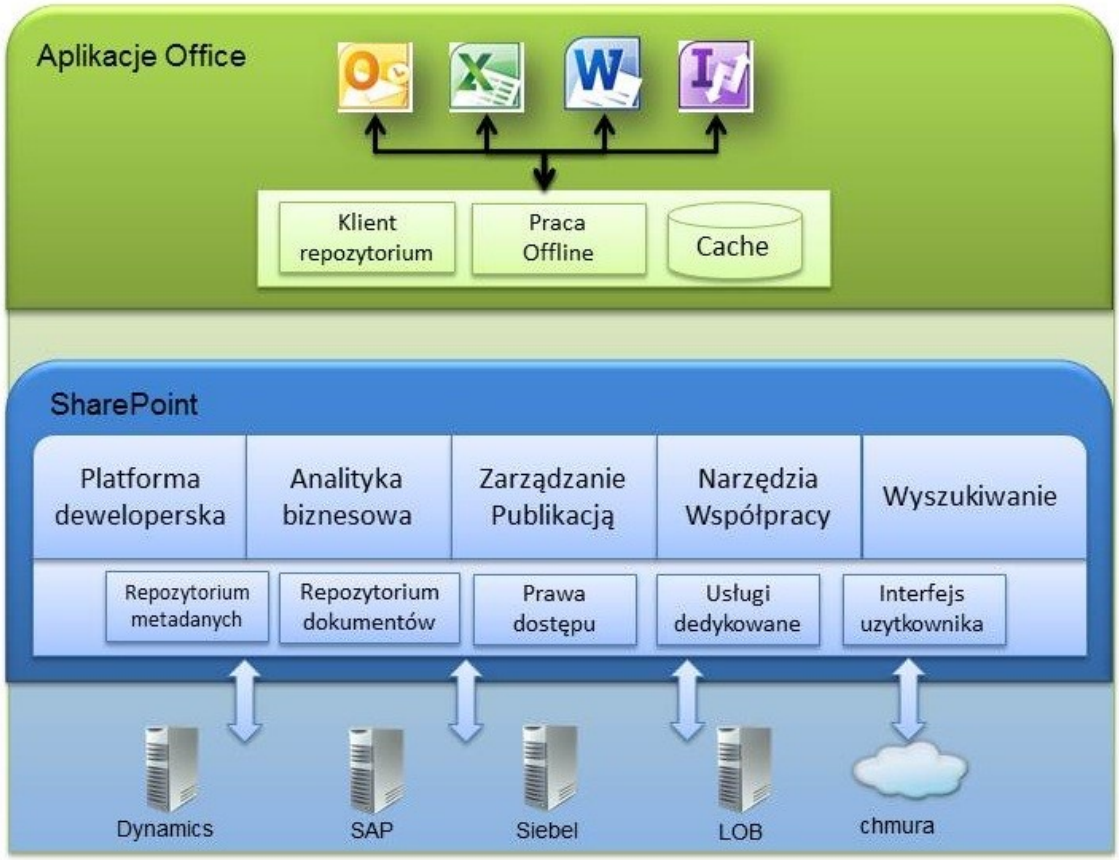
Natomiast z poziomu komunikatora Teams można wysłać wiadomość pocztową, czy sprawdzić dostępność w kalendarzu Exchange:



Podobnie wygląda integracja w portalu SharePoint. Poprzez ikonę reprezentującą dostępność autora dokumentu umieszczonego w repozytorium portalu można sprawdzić jego kalendarz, informacje o przynależności do konkretnego działu, czy też nawiązać komunikację tekstową, głosową lub video.



Przykładem mechanizmu współdziałania Office z systemami zaplecza (w tym przypadku SharePoint) pokazuje poniższa ilustracja.



Ważnym krokiem w kierunku spójnego i jednolitego sposobu obsługi aplikacji z chmury i na urządzeniach klienckich było wprowadzenie jednolitego interfejsu użytkownika, czyli MS Teams oraz nowych mechanizmów bezpieczeństwa współpracy.

4.9. PAKIET MICROSOFT 365

Pakiet usług Microsoft 365 jest zespołem narzędzi wspomagających komunikację i współpracę. Pakiet obejmuje produkty Microsoft Windows 11, Office 365 (Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft Teams) oraz - w zależności od wersji – pakiet biurowy Office oraz Microsoft EMS.

Wykorzystując usługę Microsoft 365 można w bardzo szybkim tempie i przy ograniczonym ryzyku projektowym zbudować podstawowe systemy komunikacji i współpracy przy niskich kosztach utrzymania systemu oraz zapewniając następujące korzyści:

- wysoką dostępność,
- kompleksowe bezpieczeństwo,
- uproszczone zarządzanie infrastrukturą IT.

Co daje zastosowanie usługi Microsoft 365 jako komponentu naszego systemu? Oprócz cech komponentowych opisanych dla serwerów SharePoint, Exchange czy Teams można podkreślić następujące zalety:

Dynamiczne zdalne rozwiązania

- Połączenie mocy aplikacji instalowanych na komputerach stacjonarnych z elastycznością w pełni zdalnych usług internetowych.
- Kompleksowe zintegrowanie rozwiązanie wykorzystujące rozbudowane aplikacje klienckie dobrze znane użytkownikom.
- Ujednolicony wygląd i zasady działania praktycznie na każdym urządzeniu i w każdym miejscu.
- Narzędzia do obsługi poczty e-mail, wiadomości błyskawicznych i współpracy.

Możliwości wyboru dzięki strategii Software-plus-Services

- Używanie aplikacji zainstalowanych lokalnie albo korzystanie z usług online zainstalowanych i zarządzanych w systemach firmy Microsoft oraz jej partnerów.
- Możliwość zastosowania elastycznej kombinacji rozwiązań — lokalnych oraz ulokowanych w systemach firmy Microsoft i jej partnerów.
- Dynamiczne dopasowywanie modelu wdrożenia do zmieniających się potrzeb firmy.

Łatwa instalacja i zarządzanie

- Narzędzia potrzebne organizacji do skutecznego działania oraz umożliwiające szybkie i łatwe wprowadzanie nowych funkcji bez nadmiernego obciążania wewnętrznych zasobów.
- Usługi Microsoft Online Services można synchronizować z usługami domenowymi w usłudze Active Directory, co pozwala zachować kontrolę nad zasadami dotyczącymi użytkowników i zarządzać nimi centralnie.
- Jeden zbiorczy panel administracyjny ułatwia centralne konfigurowanie i zarządzanie nowymi oraz istniejącymi użytkownikami.

4.9.1. OFFICE 365

Usługa Office 365 jest zespołem narzędzi wspomagających komunikację i współpracę. Pakiet obejmuje produkty Microsoft Exchange Online, Microsoft SharePoint Online i Microsoft Skype dla firm Online, bazujące na znanych technologiach wdrażanych dotychczas lokalnie.

Całość aktualnych informacji na temat Office 365 można znaleźć na stronie:

https://products.office.com/pl-pl/government/office-365-web-services-for-government

Wykorzystując usługę Office 365 można w bardzo szybkim tempie i przy ograniczonym ryzyku projektowym zbudować podstawowe systemy komunikacji i współpracy przy niskich kosztach utrzymania systemu oraz zapewniając następujące korzyści:

- wysoką dostępność,
- kompleksowe bezpieczeństwo,
- uproszczone zarządzanie infrastrukturą IT.

Co daje zastosowanie usługi Office 365 jako komponentu naszego systemu? Oprócz cech komponentowych opisanych dla serwerów SharePoint, Exchange czy Skype dla firm można podkreślić następujące zalety:

4.10. PLATFORMA JEDNOLITEJ KOMUNIKACJI

System wspomagający wewnętrzną komunikację w organizacji ma zapewnić pracownikom prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową, video oraz przesyłanie wiadomości tekstowych z użyciem posiadanych komputerów PC oraz urządzeń mobilnych.

Ideą implementacji platformy jednolitej komunikacji (PJK) jest współpraca różnych komponentów, wykorzystująca integrację poczty e-mail, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. PJK powinna być zintegrowana z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto PJK musi wykorzystywać mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie usług katalogowych. Wynikiem takiej integracji mają być następujące cechy systemu:

Ujednolicenie komunikacji biznesowej

- Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej.
- Ujednolicona poczta głosowa, e-mail, kontakty, kalendarz, wiadomości błyskawiczne (IM) i dane o obecności w jednym interfejsie klienckim.
- Integracja z aplikacjami pakietu biurowego z kontekstową komunikacją i z funkcjami obecności.
- Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego.
- Rozszerzalna platforma integracji narzędzi współpracy z aplikacjami biznesowymi.
- Usługi bezpieczeństwa umożliwiające chronioną komunikację wewnątrz organizacji.
- Aplikacje biznesowe dostępne bezpośrednio na urządzeniach mobilnych.
- Mobilny dostęp do ludzi i danych firmowych.
- Obniżone koszty dzięki zdalnej administracji i zarządzaniu urządzeniami.

- Niskie koszty usług telefonicznych i komunikacji między odległymi lokalizacjami.
- Wsparcie dla użytkowników niepełnosprawnych.

Zwiększenie efektywności pracy zespołów poprzez obszary robocze:

- Możliwość tworzenia ad-hoc witryn współpracy czy obszarów roboczych dla zespołów z poziomu interfejsu klienta portalu wielofunkcyjnego lub z poziomu pakietu biurowego.
- Zdecentralizowane tworzenie dokumentów dzięki obszarom roboczym zespołów, blogom i witrynom wiki.
- Strukturalne tworzenie dokumentów ze scentralizowanym przepływem pracy i kontrolą procesów.
- Funkcje sygnalizacji obecności, wiadomości błyskawicznych i konferencji bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej.
- Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych.
- Integracja zarządzania rekordami i dokumentami z aplikacjami biurowymi i bazodanowymi.
- Możliwość prostego, dostępnego dla użytkowników konfigurowania mechanizmów śledzenia i monitorowania kluczowych wskaźników wydajności.

Planując założenia do systemu warto przewidzieć obsługę następujących funkcjonalności:

- **Status obecności** – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego.
- **Krótkie wiadomości tekstowe** – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami

internetowymi (AOL, Skype, Yahoo). Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych.

- **Obsługę komunikacji głosowej** – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi, możliwość realizacji połączeń głosowych do i z sieci PSTN (publicznej sieci telefonicznej). Możliwość realizacji funkcjonalności RCC (*Remote Call Controll*) tj. zarządzania telefonem stacjonarnym firm trzecich z poziomu komunikatora. Obsługa stacjonarnych telefonów IP.
- **Obsługę komunikacji wideo** – Możliwość zestawiania połączeń wideo-telefonicznych
- **Obsługę konferencji wirtualnych** – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie z poziomu serwera WWW. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej.
- **Wsparcie dla funkcjonalności single sign-on** – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła.

4.10.1. ŚRODOWISKO PRACY ZESPOŁOWEJ I KOMUNIKACJI – CZYLI TEAMS

Aplikacja Teams dostępna w pakietach subskrypcji Office 365 i Microsoft 365 integruje różne kanały komunikacji między użytkownikami i zespołami pozwalając na wspólną pracę nad zadaniami i projektami w czasie rzeczywistym, zapewniając jednocześnie tworzenie i archiwizację niezbędnych zasobów informacyjnych.

Teams jest aplikacją pracy zespołowej, dostępną praktycznie na wszystkich platformach (łącznie z mobilnymi), korzystającą z wielu funkcji oprogramowania Office 365.

Tworzy zintegrowane środowisko pracy wykorzystujące między innymi serwery komunikacji wielokanałowej, serwery poczty elektronicznej, serwery portali wielofunkcyjnych i usługi zarządzania tożsamością użytkownika. Rozproszone dotychczas pomiędzy różnymi aplikacjami klienckimi funkcje współpracują obecnie w jednym środowisku, pozwalając na

elastyczny wybór kanałów komunikacyjnych i sposób składowania informacji. Teams porządkuje jednocześnie pracę nad jednym tematem.

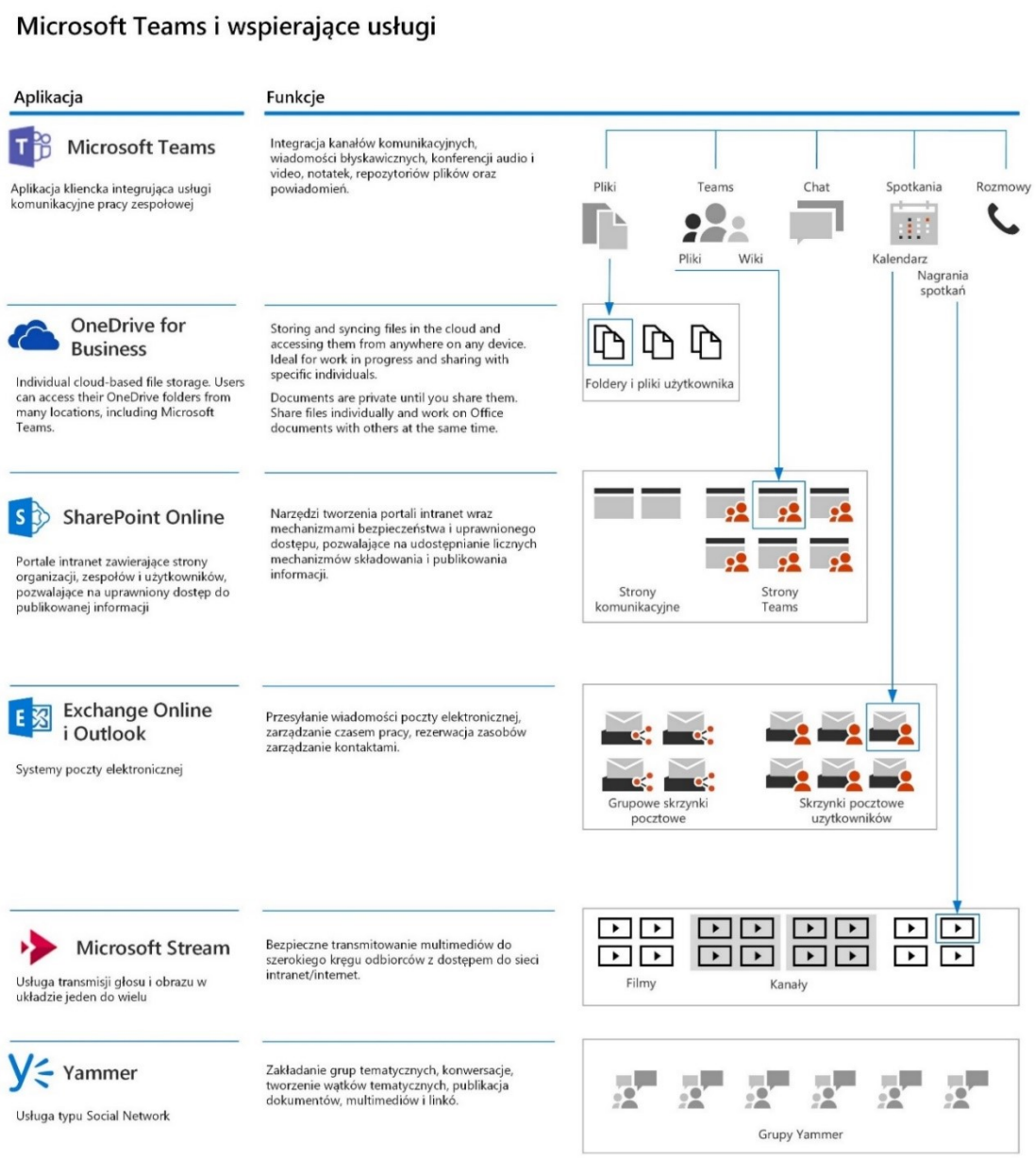
Rozbudowując możliwości starszych aplikacji klienckich Office daje możliwość:

a. komunikacji tekstowej,
b. komunikacji audio i video,
c. prowadzenia telekonferencji,
d. składowania dokumentów,
e. tworzenia notatek,
f. korespondencji poczt elektronicznej,
g. inicjacji dokumentów w oparciu o pakiet biurowy,
h. panowania czasu pracy i spotkań,
i. przydzielania zadań członkom zespołu,
j. konfiguracji powiadomień i najważniejszych informacji w interfejsie użytkownika,
k. tworzenia obszarów (kanałów) współpracy zespołowej,
l. zarządzania szkoleniami użytkowników,
m. osadzania aplikacji własnych.

Ważną funkcjonalnością Teams jest możliwość tworzenia i publikowania grup użytkowników (zespołów/kanałów) zajmujących się wspólnymi tematami z wykorzystaniem wszystkich dostępnych w narzędziu kanałów komunikacji i składowania danych wraz z integracją informacji, komunikacji, planowania i rezerwacji zasobów dla całych zespołów wokół tych tematów. Możliwe jest między innymi nadawanie uprawnień dostępu dla członków grup.

Przydatnymi funkcjami Teams są wyszukiwanie informacji i wątków tematycznych po tematach i członkach grup oraz dostępność uproszczonej wersji aplikacji na urządzenia mobilne.

Podstawowe komponenty wspierające usługę Teams, umożliwiające realizację tak szerokiego zakresu funkcji pokazane są na poniższym rysunku:



4.10.2. CHARAKTERYSTYKA USŁUG OFFICE 365

Spośród obecnie dostępnych w ofercie Microsoft planów dystrybucyjnych Office 365 można dokonać wyboru zgodnego z potrzebami danej organizacji.

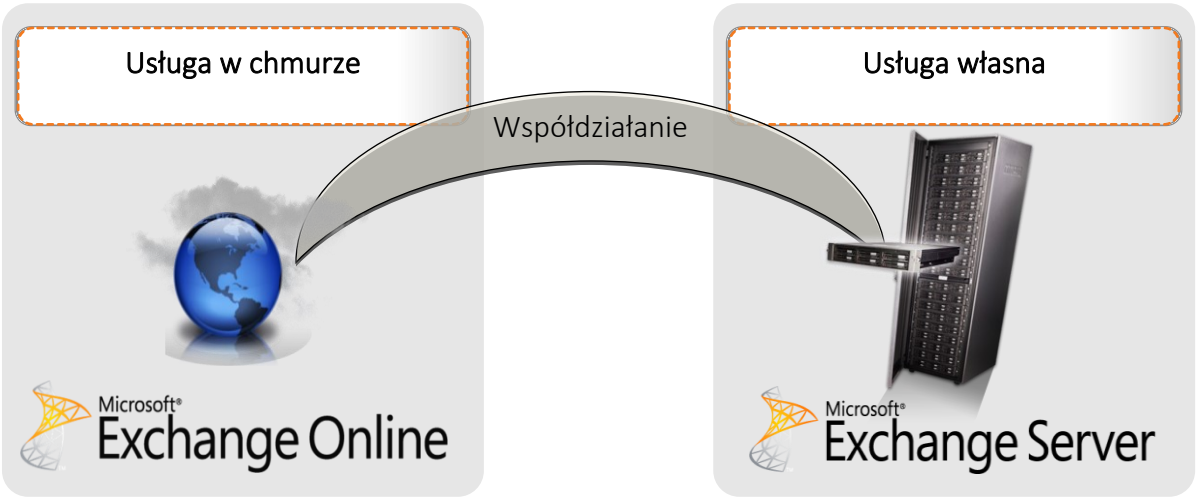
Tak więc oprócz samego Pakietu Office 365 dostępnego w postaci subskrypcji, można wybrać różnego rodzaju usługi online. Poniżej przedstawiamy krótką charakterystykę poszczególnych planów.

Składniki usług *Office 365*	E1	E3	E5
Bezpieczna poczta elektroniczna wraz z kalendarzami - *Exchange Online*	50 GB	Bez limitu	Bez limitu
Sieci socjalne, Multimedia, Portale - *Yammer, O365 Video, SharePoint Online*	●	●	●
Komunikator, Spotkania Online, Meeting Broadcast - *Skype for Business*	●	●	●
Składowanie i udostępnianie plików, Śledzenie informacji - *OneDrive for Business, Delve*	●	●	●
Subskrypcja pakietu Office - *Office 365 ProPlus*		●	●
Archiwizacja, Zarządzanie prawami dostępu, Zapobieganie wyciekom danych, Szyfrowanie		●	●
Analiza śledzonych danych, Bezpieczne załączniki			●
Zaawansowana analiza danych ad-hoc - *Power BI Pro, Delve Org Analytics*			●
Telefonia PSTN *Skype for Business*			Dodatek

4.10.2.1. EXCHANGE ONLINE

Microsoft Exchange Online to jedna z usług Microsoft Office 365 umożliwiająca obsługę poczty elektronicznej, zarządzanie czasem, zasobami oraz kontaktami i komunikacją. Funkcje Exchange Online są równoważne dla systemu Exchange wdrażanego we własnym zakresie (jako lokalny system), natomiast czas i koszt wdrożenia zostaje znacznie zredukowany.

Użycie Exchange Online może być także metodą rozbudowy własnej instalacji systemu pocztowego, na przykład dla nowych grup użytkowników.



Dostęp do usług systemu pocztowego Exchange Online jest możliwy przy pomocy:

- oprogramowania Outlook,
- przeglądarki (Outlook Web Access),
- wielu typów urządzeń mobilnych.

Typowe cechy tej usługi to:

- duże skrzynki pocztowe (od 50GB),
- standardowy i łatwy sposób obsługi poczty elektronicznej,
- obsługa najnowszych funkcji Outlook 2016 i 2019, takich jak tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari,
- współdziałanie z innymi produktami rodziny Office (SharePoint, Skype dla firm i oprogramowaniem klienckim), a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy,
- bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Ważnym elementem wszystkich usług Online firmy Microsoft są zasady bezpieczeństwa i oparcie się na wspólnym modelu praw dostępu do danych i zasobów. Usługi Online mogą wykorzystywać uwierzytelnienie poprzez lokalne usługi katalogowe (*Active Directory*), co zapewnia niezaprzeczalność praw dostępu oraz w znakomity sposób przyspiesza zakładanie kont użytkowników oraz grup z jednorodnymi prawami.

4.10.2.2. SHAREPOINT ONLINE

Microsoft SharePoint Online to jedna z usług Microsoft Office 365 umożliwiająca obsługę pracy grupowej, publikację stron, budowę repozytoriów dokumentów i systemów zarządzania informacją i jej przepływem. Funkcje SharePoint Online są równoważne dla systemu opartego o SharePoint Server wdrażanego we własnym zakresie (jako lokalny system), natomiast czas i koszt wdrożenia zostaje znacznie zredukowany.

Użycie SharePoint Online może być także metodą rozbudowy własnej instalacji systemu portali wewnętrznych, na przykład dla nowych grup użytkowników.

W strukturach jednostek administracji publicznej bardzo często wiele procesów i projektów, a nawet prostych spraw wymaga wsparcia ze strony narzędzi informatycznych. Niewystarczające już jest wspomaganie przy użyciu tradycyjnych metod, takich jak dokumenty papierowe lub choćby pocztę elektroniczną.

W praktyce poszczególni użytkownicy pracują nad dokumentami, raportami czy wnioskami w sposób całkowicie oderwany od jakichkolwiek systemów. Wykorzystują do tego znane im narzędzia pakietu Office i przygotowane już przez nich wcześniej dokumenty.

Wprowadzenie rozwiązania poszerzającego możliwości pakietu Office o współpracę z innymi użytkownikami pozwala radykalnie skrócić czas potrzebny na wypracowanie dokumentów związanych z codzienną działalnością, jak i również włączyć pracowników do jednego zespołu, jaki stanowią wszyscy pracownicy organizacji.

Zakres rozwiązań, jakie można utworzyć na bazie platformy Microsoft SharePoint Online jest bardzo rozległy. Można go podzielić na dwie podstawowe sfery – publikacji i współpracy.

Typowe narzędzia publikowania i odnajdywania informacji w organizacji to:

- Informacyjny portal intranetowy,
- Bazy wiedzy,
- Rozporządzenia dyrekcji, kierownictwa,
- Obowiązujące akty normatywne,
- Procedury postępowań,
- Szablony dokumentów,
- Kontakty do osób.

W zakresie publikacji treści na portalach SharePoint Online umożliwia wykorzystanie predefiniowanych struktur takich jak: strona użytkownika (My Site), strona zespołu (Team Site), strony intranetowe dla całej organizacji oraz strony extranet dla współdziałających

jednostek.

Współpraca wielu osób nad dokumentami lub informacjami i ich obieg:

- przygotowanie dokumentów związanych z postępowaniami,
- rejestrowanie postępowań, wniosków, decyzji,
- opracowywanie dokumentacji przetargowych, dokumentacji sądowej, wezwań, poleceń,
- planowanie kontroli, projektów, budżetów,
- zbieranie informacji i raportowanie do organów nadrzędnych,
- planowanie spotkań, ich przebiegu, publikacja omawianych dokumentów,
- zbieranie zamówień wewnętrznych, przygotowywanie dokumentacji przetargowej, zarządzanie umowami z dostawcami,
- obieg wniosków urlopowych, delegacji, rozliczeń kosztów,

- zarządzanie zasobami: salami, samochodami, projektorami, sprzętem komputerowym.

Dostęp do usług systemu SharePoint Online jest możliwy przy pomocy przeglądarki, a więc z dowolnego komputera oraz wybranych urządzeń mobilnych.

Typowe cechy tej usługi to:

- standardowy i łatwy sposób obsługi,
- obsługa SharePoint we współdziałaniu z Microsoft Office,
- współdziałanie z innymi produktami rodziny Office (Exchange, Skype dla firm i oprogramowaniem klienckim), a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy,
- bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

4.10.3. LICENCJONOWANIE I FUNKCJE PODSTAWOWYCH PRODUKTÓW MICROSOFT 365

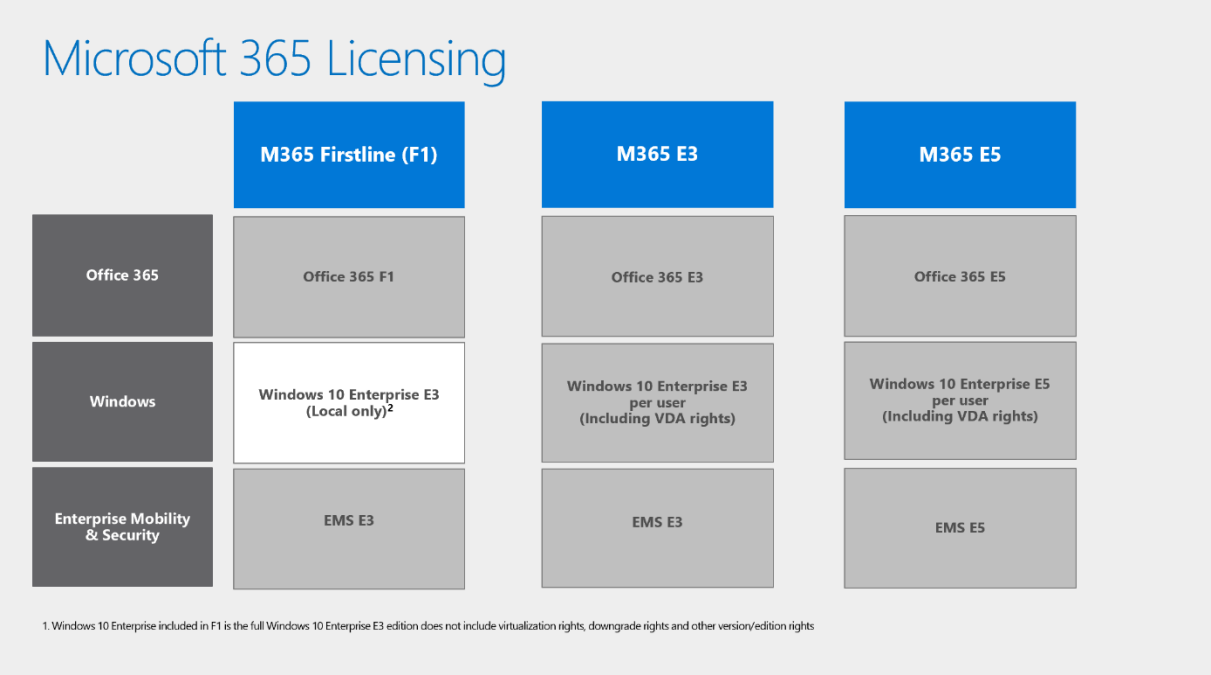
4.10.3.1. MICROSOFT 365

Microsoft 365 Plan F1, E3 i E5 składa się z trzech komponentów:

- Office 365 Plan F1, E3 i E5 (opis poszczególnych planów, znajduje się poniżej),
- Enterprise Mobility & Security Plan E3 i E5,
- Windows Enterprise Plan E3 i E5.

Szczegółowe porównanie planów Microsoft 365:

https://www.microsoft.com/pl-pl/microsoft-365/compare-all-microsoft-365-plans



4.10.3.2. ENTERPRISE MOBILITY & SECURITY E3

- Azure Active Directory Premium P1 - Bezpieczne pojedyncze logowanie do aplikacji chmurowych i lokalnych. MFA, warunkowy dostęp oraz zaawansowane raporty bezpieczeństwa.
- Azure Information Protection Premium P1 – Klasyfilkacja informacji, szyfrowanie plików we wszystkich lokalizacjach.
- Microsoft Defender for Identity - Ochrona przed zaawansowanymi atakami wykorzystująca analizę behawioralną zachowań użytkowników.
- Microsoft Intune - Zarządzanie urządzeniami i aplikacjami mobilnymi w celu ochrony danych i aplikacji korporacyjnych na dowolnym urządzeniu.
- Windows Server Cal – licencja dostępowa do AD.
- System Center Configuration Manager - zarządzanie infrastrukturą, aktualizowanie i monitorowanie konfiguracji.

4.10.3.3. ENTERPRISE MOBILITY & SECURITY E3

- Azure Active Directory Premium P2 – zawiera wszystkie funkcjonalności Planu P1, zarządzanie tożsamością i dostępem z zaawansowaną ochroną użytkowników i uprzywilejowanych tożsamości.

- Azure Information Protection Premium P2 – zawiera wszystkie funkcjonalności Planu PKlasyfilkacja informacji, szyfrowanie plików we wszystkich lokalizacjach.
- Microsoft Advanced Threat Analytics - Ochrona przed zaawansowanymi atakami wykorzystująca analizę behawioralną zachowań użytkowników.
- Microsoft Intune - Zarządzanie urządzeniami i aplikacjami mobilnymi w celu ochrony danych i aplikacji korporacyjnych na dowolnym urządzeniu.
- Windows Server Cal – licencja dostępowa do AD.
- System Center Configuration Manager – zarządzanie infrastrukturą, aktualizowanie i monitorowanie konfiguracji.
- Microsoft Cloud App Security - kontrola i ochrona aplikacji w chmurze.

Szczegółowe porównanie funkcjonalności Enterprise Mobility & Security:

https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

4.10.3.4. WINDOWS ENTERPRISE E3

- Bezpieczeństwo i zgodność z regulacjami - zaawansowane mechnizmy bezpieczeństwa dedykowane organizacjom, Windows Hello for Business[63], ochrona poświadczeń, ochrona urządzeń, blokada aplikacji.
- Zarządzanie aplikacjami i urządzeniami - ulepszone funkcje administracyjne umożliwiające zarządzanie urządzeniami i aplikacjami oraz ich wdrażania
- możliwość korzystania z VDA.

4.10.3.5. WINDOWS ENTERPRISE E5

- Bezpieczeństwo i zgodność z regulacjami - zaawansowane mechanizmy bezpieczeństwa dedykowane organizacjom, Windows Hello, ochrona poświadczeń, ochrona urządzeń, blokada aplikacji.
- Zarządzanie aplikacjami i urządzeniami - ulepszone funkcje administracyjne umożliwiające zarządzanie urządzeniami i aplikacjami oraz ich wdrażania.

[63] *https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview*

- Możliwość korzystania z VDA.
- Endpoint Detection and Response (Defender for Identity Protection) – zaawansowana ochrona przed atakami typu zero day.

Szczegółowe porównanie funkcjonalności Windows E3 i E5:

https://www.microsoft.com/pl-pl/windowsforbusiness/compare

4.10.3.6. OFFICE 365 F1

- Exchange Online – pojemność skrzynki 2GB.
- Exchange Online Protection – antyspam, antymalware.
- Skype for Business, Microsoft Teams – czat, tele-, video-konferencje, przestrzeń i narzędzia pracy wspólnej.
- Sharepoint Online – intanet, przestrzeń do pracy wspólnej.
- Yammer – korporacyjna sieć społecznościowa.
- OneDrive for Business – przestrzeń dyskowa 2GB.
- Office Mobile Apps – dostęp do aplikacji Office Online na urządzeniach mobilnych.
- Office Online – dostęp do aplikacji Office przez przeglądarkę.
- Microsoft Stream – serwis video wyłącznie do konsumpcji treści, bez możliwości publikacji.
- Moblile Device Management (MDM) dla O365.
- On-premises Active Directory synchronizacja dla single sign on.

4.10.3.7. OFFICE 365 E1

- Exchange Online – pojemność skrzynki 50GB.
- Exchange Online Protection – antyspam, antymalware.
- Skype for Business, Microsoft Teams – czat, tele-, video-konferencje, przestrzeń i narzędzia pracy wspólnej.
- Sharepoint Online – intanet, przestrzeń do pracy wspólnej.
- Yammer – korporacyjna sieć społecznościowa.

- OneDrive for Business – przestrzeń dyskowa 1GB.
- Office Mobile Apps – dostęp do aplikacji Office Online na urządzeniach mobilnych.
- Office Online – dostęp do aplikacji Office przez przeglądarkę.
- Microsoft Stream – serwis video wyłącznie do konsumpcji treści, bez możliwości publikacji.
- Moblile Device Management (MDM) dla O365.
- On-premises Active Directory synchronizacja dla single sign on.

4.10.3.8. OFFICE 365 E3

- Office 365 ProPlus - 5 PCs/Macs + 5 tabletów + 5 smartfonów w licencjonowaniu dla użytkownika.
- Exchange Online – pojemność skrzynki 100GB.
- Exchange Online Protection – antyspam, antymalware.
- Skype for Business, Microsoft Teams – czat, tele-, video-konferencje, przestrzeń i narzędzia pracy wspólnej.
- Sharepoint Online – intanet, przestrzeń do pracy wspólnej.
- Yammer – korporacyjna sieć społecznościowa.
- OneDrive for Business – przestrzeń dyskowa 5GB.
- Office Mobile Apps – dostęp do aplikacji Office Online na urządzeniach mobilnych.
- Office Online – dostęp do aplikacji Office przez przeglądarkę.
- Microsoft Stream – serwis video wyłącznie do konsumpcji treści, bez możliwości publikacji.
- Moblile Device Management (MDM) dla O365.
- On-premises Active Directory synchronizacja dla single sign on.

Dodatkowe funkcjonalności:

- Legal compliance, eDiscovery, mailbox hold - zgodność z przepisami, proces identyfikacji i dostarczania informacji elektronicznych, które mogą być wykorzystane

jako dowód w sprawach prawnych nielimitowana archiwizacja, blokada skrzynki pocztowej.

- Information protection - szyfrowanie wiadomości, zarządzanie uprawnieniami, zapobieganie utracie danych.

4.10.3.9. OFFICE 365 E5

- Office 365 ProPlus - 5 PCs/Macs + 5 tabletów + 5 smartfonów w licencjonowaniu dla użytkownika.
- Exchange Online – pojemność skrzynki 100GB.
- Exchange Online Protection – antyspam, antymalware.
- Skype for Business, Microsoft Teams – czat, tele-, video-konferencje, przestrzeń i narzędzia pracy wspólnej.
- Sharepoint Online – intanet, przestrzeń do pracy wspólnej.
- Yammer – korporacyjna sieć społecznościowa.
- OneDrive for Business – przestrzeń dyskowa 5GB.
- Office Mobile Apps – dostęp do aplikacji Office Online na urządzeniach mobilnych.
- Office Online – dostęp do aplikacji Office przez przeglądarkę.
- Microsoft Stream – serwis video wyłącznie do konsumpcji treści, bez możliwości publikacji.
- Moblile Device Management (MDM) dla O365.
- On-premises Active Directory synchronizacja dla single sign on.

Dodatkowe funkcjonalności:

- Legal compliance, Advanced eDiscovery, mailbox hold - zgodność z przepisami, proces identyfikacji i dostarczania informacji elektronicznych, które mogą być wykorzystane jako dowód w sprawach prawnych nielimitowana archiwizacja, blokada skrzynki pocztowej.
- Information protection - szyfrowanie wiadomości, zarządzanie uprawnieniami, zapobieganie utracie danych.

- Enterprise Voice w/Skype for Business (wyłącznie on-prem).
- Office 365 Cloud App Security - wykrywanie zagrożeń na podstawie user activity logs, Shadow IT dla aplikacji, kontrola dostępu do aplikacji.
- Defender for Identity - detonacji nieznanych załączników, zabezpieczanie linków pod kątem reputacji, możliwość symulowania ataków typu spear phishing, brute force czy password spray w organizacji.
- Power BI - Analiza danych i wizualizacja.
- MyAnalytics – analiza czasu pracy, produktywności, działaniach w zakresie współpracy.
- Phone System, Audioconferencing.

Szczegółowe porównanie planów Office 365:

https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/office-365-plan-options

4.10.3.10. LICENCJONOWANIE PRODUKTÓW BEZPIECZEŃSTWA MICROSOFT

Dostęp do najnowszych funkcjonalności bezpieczeństwa opisanych w dokumencie umożliwiają subskrypcje Microsoft 365 E3 oraz Microsoft 365 E5.

Poniżej prezentujemy szczegółowe porównanie funkcji zawartych w pakietach Microsoft 365 w planach E3 i E5.

		M365 E3	M365 E5
Operating System	Windows 10 Enterprise upgrade	●	●
Microsoft 365 Apps	Install Word, Excel, PowerPoint, OneNote, Outlook, Access, and Publisher on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user	●	●
	Commercial use rights for Office mobile apps and Office for the web	●	●
Email & Calendar	Exchange	●	●
Social & Intranet	SharePoint, Yammer	●	●
Meetings, Voice & Collaboration	Teams	●	●
	Phone System, Audio Conferencing		●
Files & Content	OneDrive for Business	5+ TB	5+ TB
	Microsoft Stream, Sway for Office 365, Microsoft Forms	●	●
Task Management	Planner, To-Do	●	●
Power Platform	Power Apps for Office 365, Power Automate for Office 365	●	●
Device & App Management	Microsoft 365 Admin Center, Microsoft Intune, Windows AutoPilot, Fine Tuned User Experience, Windows Analytics Device Health	●	●
	Mobile Device Management for Office 365	●	●
Security	Windows Hello, Credential Guard and Direct Access, Azure Active Directory Plan 1, Microsoft Advanced Threat Analytics, Defender Antivirus and Device Guard· Azure Information Protection Plan 1, Windows Information Protection, BitLocker	●	●
	Azure Active Directory Plan 2, Microsoft Defender Advanced Threat Protection (ATP), Office 365 ATP Plan 2, Azure ATP		●
	Cloud App Security		●
Compliance	eDiscovery Content Search, manual sensitivity and retention labels	●	●
	Office 365 Data Loss Prevention (DLP) for email and files, eDiscovery Export, eDiscovery Hold, Litigation Hold, In-Place Hold, basic Audit, Email archiving	●	●
	Automatic classification and retention, Customer Key, Advanced Message Encryption, Insider Risk Management, Communication Compliance, Information Barriers, Customer Lockbox, Privileged Access Management, Advanced Audit, Advanced eDiscovery		●
Analytics	MyAnalytics	●	●
	Power BI Pro		●

4.10.3.11. DODATKOWE FUNKCJONALNOŚCI W OFFICE E5 (NIE ZAWIERA ICH O365 E3)

- Legal compliance, Advanced eDiscovery, mailbox hold - zgodność z przepisami, proces identyfikacji i dostarczania informacji elektronicznych, które mogą być wykorzystane jako dowód w sprawach prawnych nielimitowana archiwizacja, blokada skrzynki pocztowej.
- Information protection - szyfrowanie wiadomości, zarządzanie uprawnieniami, zapobieganie utracie danych.
- Enterprise Voice.
- Office 365 Cloud App Security - wykrywanie zagrożeń na podstawie user activity logs, Shadow IT dla aplikacji, kontrola dostępu do aplikacji.
- Advanced Threat Protection - detonacji nieznanych załączników, zabezpieczanie linków pod kątem reputacji, możliwość symulowania ataków typu spear phishing, brute force czy password spray w organizacji.
- Power BI - Analiza danych i wizualizacja.
- MyAnalytics – analiza czasu pracy, produktywności, działaniach w zakresie współpracy.
- Phone System, Audioconferencing.

4.10.3.12. WINDOWS 11

Windows 11 to sprawny, bezpieczny i zarządzalny system operacyjny klasy PC. Wbudowane mechanizmy bezpieczeństwa, masowych instalacji oraz integracji z narzędziami pozwalają zbudować system, w którym komputer PC przestaje być zmorą administratorów i użytkowników, oczywiście po zastosowaniu zaleceń rozdziału „Bezpieczeństwo stacji roboczej". Dodatkowo, dotychczasowe doświadczenia wskazują, że jest to system mniej wymagający w stosunku do zasobów sprzętowych niż poprzednie wersje.

Poniżej krótko omówimy niektóre nowe cechy systemu Windows 11 (w wersji Enterprise – zalecanej dla systemów zgodnych z założeniami architektury komponentowej).

Pierwszą widoczną zmianą jest interfejs graficzny użytkownika pozwalający na obsługę:

- klasyczną przy pomocy klawiatury i myszy,
- dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.

Interfejsy te mogą być przełączane przez użytkownika, a jednocześnie w urządzeniach typu 2w1 (tablet z dołączaną klawiaturą) odpięcie czy podpięcie klawiatury może automatycznie przełączać tryb pracy interfejsu.

Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym Polskim i Angielskim, a w wersji Enterprise mamy do wyboru kilkadziesiąt pakietów językowych, które umożliwiają zmianę języka całego interfejsu poprzez zwykłe przełączenie, bez konieczności reinstalacji systemu.

Drugą ważną cechą Windows 11 jest już na etapie instalacji konieczność dokonania wyboru, jakie dane telemetryczne będą udostępniane na zewnątrz i z jakich danych (np. geolokalizacyjnych) mogą korzystać usługi i aplikacje. Standardowym ustawieniem jest NIEprzekazywanie i udostępnianie danych.

Wybory tego typu dotyczą też synchronizacji ustawień systemu operacyjnego między różnymi urządzeniami tego samego użytkownika. Włączenie takiej synchronizacji powoduje znaczące ułatwienie przy uzyskaniu tych samych ustawień czy akcesie do specyficznych zasobów (np. sieci Wi-Fi), ale z przyczyn obowiązujących w danej jednostce polityk bezpieczeństwa może nastąpić konieczność jej wyłączenia.

Dosyć zasadnicze zmiany zostały udostępnione w Windows 11 w zakresie uwierzytelniania.

Zastosowano mechanizmy uwierzytelniania w oparciu o następujące funkcje:

a. login i hasło,
b. karty z certyfikatami (smartcard),
c. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
d. wirtualnej tożsamości użytkownika potwierdzanej za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.

Dostępne są wbudowane mechanizmy wieloskładnikowego uwierzytelniania, które w połączeniu z usługą AD czy AAD dają nam możliwość dodatkowego zabezpieczenia uprawnionego dostępu do danych wrażliwych, czy objętych specjalnymi restrykcjami, bez wdrażania dodatkowych dedykowanych rozwiązań.

Podobnie jak w poprzednich wersjach mamy do dyspozycji wsparcie dla:

- uwierzytelniania na bazie Kerberos v. 5,
- uwierzytelnienia urządzenia na bazie certyfikatu,
- algorytmów Suite B (RFC 4869).

Pojawiły się jednak nowe rozwiązania w znacznym stopniu ułatwiające zarządzaniem bezpieczeństwem, takie jak:

- Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji.
- Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość

blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku.

- Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym.
- Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny.
- Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0.
- Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji.
- Możliwość konfiguracji trybu „kioskowego" dającego dostęp tylko do wybranych aplikacji i funkcji systemu.
- Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec.
- Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.

Dostępne są też jako standard różne przydatne funkcje i aplikacje:

- Klient poczty elektronicznej z kalendarzem spotkań.
- Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje.
- Wbudowany system pomocy w języku polskim ze sprawnym mechanizmem wyszukiwania.
- Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika z obsługą języka polskiego.
- Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika.

Tak jak w poprzednich wersjach mamy możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, z mechanizmem sprawdzającym, które z poprawek są potrzebne.

Istnieje też możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu.

Jako standard jest dostępna wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6 oraz wbudowane narzędzia ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.

Dalsze funkcje Windows 11 to między innymi:

- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi).
- Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.
- Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
- Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe.
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.

- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- Obsługa standardu NFC (near field communication).
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
- Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
- Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
- Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń.
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
- Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning).
- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
- Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
- Udostępnianie wbudowanego modemu.

- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
- Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).
- Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).
- Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych.
- Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.
- Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w układzie TPM (*Trusted Platform Module*) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
- Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych.
- Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
- Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
- Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB).
- Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie.

- Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
- Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching) najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
- Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
- Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC.
- Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC oraz pomiędzy dwoma różnymi politykami.
- Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
- Mechanizm umożliwiający na odzyskanie skasowanych danych z dysków twardych komputerów.
- Mechanizm umożliwiający na wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M.
- Mechanizm umożliwiający na naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.

- Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia.
- Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache".
- Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację, konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji.
- Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością.
- Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji.
- Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
- Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
- Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
- Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
- Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
- Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
- Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
- Funkcjonalność migracji ustawień aplikacji pomiędzy wieloma komputerami.

4.11. BAZY DANYCH, ANALIZA I RAPORTOWANIE

4.11.1. PODSYSTEM BAZODANOWY

Podsystem ten ma zapewnić bezpieczne składowanie danych dla wszystkich pozostałych komponentów systemu. Dodatkowo może on zawierać narzędzia raportowania i analizy danych. Poza oczywistymi funkcjami bazy danych niezwykle ważnymi obszarami dla projektantów systemów i administratorów są zarządzanie, skalowalność, wydajność, wysoka dostępność, bezpieczeństwo oraz rozwój. Skupimy się w tym wypadku na wybranych, stosunkowo nowych aspektach tych funkcji.

4.11.1.1. ZARZĄDZANIE

Jednym z ważniejszych aspektów wykorzystania systemów bazodanowych jest zarządzanie zasadami, możliwość wykonywania kwerend na wielu serwerach, serwery konfiguracji oraz technologie *Data Collector/Management Data Warehouse*. Oferują one możliwość sprawnego zarządzania rozległymi i złożonymi środowiskami bazodanowymi z setkami lub tysiącami baz danych na dziesiątkach lub nawet setkach serwerów.

Funkcja zarządzania politykami (*Policy Management*) umożliwia tworzenie i wykonywanie zasad konfiguracji na jednym lub wielu serwerach baz danych. Dzięki tym zasadom można zagwarantować, że standardowe ustawienia konfiguracji będą stosowane i utrzymywane na każdym docelowym serwerze i w każdej docelowej bazie danych.

Zasady są tworzone na podstawie predefiniowanego zestawu aspektów (ang. *facet*). Każdy aspekt zawiera podgrupę ustawień konfiguracji bazy danych oraz inne podlegające kontroli zdarzenia. Te aspekty łączymy z warunkami w celu stworzenia zasady. Warunki to dopuszczalne wartości właściwości aspektu, ustawień konfiguracyjnych lub innych zdarzeń znajdujących się w aspekcie.

Warunki stanowią również wartości wykorzystywane w filtrach zasad. Powiedzmy, że chcemy, aby zasada była wykonywana tylko w określonej bazie danych. w tym przypadku

tworzymy warunek, który zawiera nazwę bazy danych, a następnie dodajemy ten warunek do zasady.

4.11.1.2. SKALOWALNOŚĆ

Typowym jest, że środowiska bazodanowe stają się z roku na rok coraz większe. Wzrost rozmiaru środowisk bazodanowych powoduje, że potrzebujemy nowych metod oraz narzędzi w celu zapewniania skalowalności, jakiej oczekuje większość organizacji. Tak więc oczekiwane są specyficzne funkcje komponentu bazodanowego, ułatwiające rozwiązanie tych problemów.

Jednym z takich narzędzi jest wbudowany mechanizm kompresji, która umożliwia kompresowanie plików bazy danych oraz plików dziennika transakcji powiązanych ze skompresowaną bazą danych. Dobrym rozwiązaniem jest funkcja kompresji na poziomie wierszy oraz na poziomie stron, które oferują korzyści, jakich nie zapewnia nam kompresja na poziomie plików danych.

Kompresja na poziomie wierszy oraz stron redukuje wymaganą ilość miejsca na dane, a także zmniejsza ilość wymaganej pamięci, ponieważ dane w pamięci pozostają skompresowane. Skompresowane dane w pamięci skutkują zwiększeniem stopnia eksploatacji pamięci, co w wielu systemach przynosi korzyści pod względem skalowalności.

Niezwykle ważna jest też kompresja na poziomie kopii zapasowych. Choć kopie zapasowe baz danych tworzą jedynie kopię aktywnej części bazy danych, nadal oznacza to zużycie setek gigabajtów, a nawet dziesiątek terabajtów. w środowiskach bazodanowych, które zawierają więcej niż jedną kopię wieloterobajtowego pliku kopii zapasowej, kopie zapasowe często zajmują wartościową powierzchnię magazynową, która mogłaby być wykorzystywana w sposób bardziej efektywny. Jedynym rozwiązaniem jest kompresowanie plików kopii zapasowych, uwalniające część tej powierzchni, dzięki czemu może być ona wykorzystywana do przechowywania bieżących danych.

Bardzo przydatną funkcją jest definiowanie ilości zasobów, które poszczególne obciążenia robocze lub ich grupy mogą wykorzystywać podczas wykonania. Dzięki tej funkcji możemy stworzyć środowisko, w którym różne obciążenia robocze istnieją obok siebie na jednym serwerze, bez obaw, że jeden lub kilka z tych obciążeń przytłoczy serwer i obniży wydajność innych obciążeń roboczych.

Dodatkową zaletą tej funkcji jest to, że możemy bardziej efektywnie wykorzystywać całkowitą ilość zasobów, które są dostępne na serwerach baz danych.

4.11.1.3. WYDAJNOŚĆ

Wydajność komponentu bazodanowego jest zawsze, niezależnie od roli bazy danych, czynnikiem krytycznym dla wydajności całego systemu. w sytuacji, gdy w ciągu każdej sekundy realizowanych jest wiele transakcji, blokowanie, które zwykle pojawia się w ramach tych transakcji, może mieć negatywny wpływ na wydajność aplikacji bazodanowych. Komponent bazodanowy powinien być zaprojektowany i skonfigurowany tak, aby redukować całkowitą liczbę blokad utrzymywanych przez proces, poprzez eskalowanie blokad z mniejszych blokad na poziomie wierszy oraz stron do większych blokad na poziomie tabel. Jednak trzeba mieć świadomość, że ta eskalacja blokad może powodować problemy. Na przykład pojedyncza transakcja może zablokować całą tabelę i uniemożliwić innym transakcjom jej wykorzystanie.

Ważnym czynnikiem jest współpraca z mechanizmem partycjonowania tabeli, aby umożliwić silnikowi bazy eskalowanie blokad do poziomu partycji przed poziomem tabeli. Ten pośredni poziom blokowania może dramatycznie zredukować skutki eskalacji blokad w systemach, które muszą przetwarzać setki lub nawet tysiące transakcji na sekundę.

W dużym stopniu wydajność zależy też od procesora kwerend, szczególnie w sytuacjach, w których kwerenda podejmuje interakcję z partycjonowaną tabelą. Optymalizator kwerend powinien realizować wyszukiwania z wykorzystaniem partycji podobnie jak w przypadku wykorzystania poszczególnych indeksów, używając jedynie identyfikatora partycji, a nie mechanizmu partycjonowania na poziomie tabeli.

4.11.1.4. WYSOKA DOSTĘPNOŚĆ

W miarę jak środowiska bazodanowe stają się coraz bardziej złożone, a rozmiar baz danych zwiększa się, zapewnienie dostępności baz danych staje się coraz trudniejsze. Znane mechanizmy wykorzystywane w przeszłości do osiągania wysokiej dostępności są nadal wymagane. Jednak w wielu przypadkach trzeba sięgnąć po nowe rozwiązania. Jednym z nich jest implementacja mechanizmu *Database Mirroring* w celu osiągnięcia wysokiej dostępności. w nowszych rozwiązaniach tego typu redukuje się obecnie ilość informacji, przenoszonych za pośrednictwem sieci z dziennika transakcji głównej (principal) bazy danych

do dziennika transakcji lustrzanej (*mirrored*) bazy danych, kompresując informacje przed ich wysłaniem.

Dużym ułatwieniem jest możliwość naprawienia uszkodzonych stron danych w głównej bazie danych. Jeśli główna baza danych dozna uszkodzenia stron danych w związku z błędami, może zażądać świeżej kopii tych stron danych od serwerów lustrzanych. To żądanie prawidłowych stron danych powinno stanowić automatyczny proces, który pozostaje niewidoczny dla użytkowników aktualnie uzyskujących dostęp do głównych baz danych.

4.11.1.5. BEZPIECZEŃSTWO

W wielu bazach wprowadzono zabezpieczenie danych w postaci szyfrowania danych. Obecnie często szyfrowanie zostało znacznie ulepszone poprzez wprowadzenie dwóch funkcji: *Extensible Key Management oraz Transparent Data Encryption*.

Funkcja *Extensible Key Management* umożliwia zastosowanie rozszerzonej struktury do bezpiecznego magazynowania kluczy wykorzystywanych w infrastrukturze szyfrowania, nie tylko w samej bazie danych, ale również poza nią w modułach programowych od zewnętrznych dostawców lub w sprzętowym module bezpieczeństwa.

Transparent Data Encryption oferuje podniesioną elastyczność w zakresie szyfrowania danych, dzięki czemu szyfrowanie danych może stanowić właściwość bazy danych, a nie tylko wynik działania funkcji w kodzie. w efekcie administratorzy nie muszą realizować wielu zmian w strukturze bazy danych oraz kodzie aplikacji, które są konieczne, gdy szyfrowanie jest realizowane na poziomie danych.

4.11.1.6. ROZWÓJ

W nowoczesnych bazach danych istnieje wiele nowych funkcji, które zostały zaprojektowane z myślą o programistach baz danych. Obejmują one między innymi zestaw rozszerzeń języka T-SQL, a także nowe komponenty, które mogą pomóc programistom w tworzeniu i wykorzystywaniu kwerend bazodanowych.

Wielu programistów baz danych jest odpowiedzialnych za tworzenie kwerend, które służą do dostarczania danych wymaganych przez aplikacje. Znane są już narzędzia typu LINQ (*Language Integrated Query*). Dzięki niemu programiści mogą wykonywać kwerendy w bazie danych przy użyciu języka programowania zamiast zwykłych instrukcji T-SQL. Narzędzia LINQ

oferują programistom możliwość wykonywanie poleceń LINQ bezpośrednio na tabelach i kolumnach bazy. Dzięki temu tworzenie nowych kwerend danych zajmuje mniej czasu.

Coraz częściej programując z użyciem baz danych, programiści wykorzystują wysokopoziomowe obiekty, które mapują do poszczególnych tabel i kolumn bazodanowych. Obiekty te, zwane również encjami (ang. *entity*), reprezentują dane potrzebne aplikacjom bazodanowym. Dzięki temu programista nie musi rozumieć rzeczywistej struktury magazynu danych oraz schematu bazy danych. Nowe narzędzia umożliwiają programistom tworzenie kwerend bazodanowych przy użyciu encji. Abstrakcja wewnętrznej struktury bazy danych pozwala zwiększyć produktywność programistów.

Pojawiło się wiele różnych ulepszeń języka T-SQL, które mogą podwyższać efektywność programistów baz danych. Jednym z przykładów jest nowa instrukcja MERGE, która umożliwia programiście sprawdzenie czy dane istnieją, przed próbą ich wstawienia. To sprawdzenie przed wykonaniem instrukcji INSERT pozwala na modyfikację danych. Już nie trzeba tworzyć skomplikowanych złączeń, aby zmodyfikować istniejące dane i wstawić dane, które jeszcze nie istnieją - wszystko w ramach jednej instrukcji.

Ciekawym ułatwieniem jest rozdzielanie danych godziny i daty od łączonego typu danych data/godzina poprzez wprowadzenie osobnych typów danych do obsługi danych daty i godziny. Różne typy danych będą prowadziły do zwiększenia wydajności wielu kwerend, ponieważ nie będzie już konieczne wykonywanie operacji na danych przed wykorzystaniem ich w kwerendzie.

W przypadku tworzenia nowszych struktur baz danych programistom często muszą naginać strukturę w celu zaimplementowania aplikacji do obsługi map. Nowoczesne bazy danych wprowadzają nowe typy danych przestrzennych. Dwa typy danych przestrzennych: GEOGRAPHY oraz GEOMETRY umożliwiają programistom składowanie specyficznych dla lokalizacji danych bezpośrednio w bazie danych, bez konieczności dzielenia ich na formaty dopasowane do standardowych typów danych.

4.11.2. SYSTEM ANALIZY DANYCH

Rozwiązania analityczne szybko stają się kluczowym narzędziem w działalności wielu organizacji. Doprowadziło to do gwałtownego wzrostu ilości danych przechowywanych

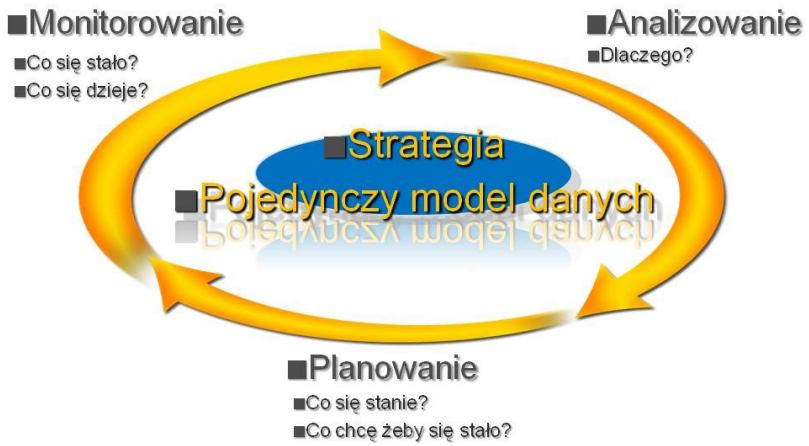
w tych systemach i konieczności wspierania większych, szybszych rozwiązań, które mogą być tworzone i rozwijane szybko i efektywnie.

System analizy danych ma umożliwić organizacji zbieranie, konsolidację, przetwarzanie i analizę danych z jednostek świadczących usługi dla obywateli i firm oraz innych instytucji. Celem działania systemu ma być optymalizacja efektywności działań administracji, analiza działania systemu obsługi interesantów, przygotowanie danych do podejmowania strategicznych decyzji w tym zakresie – w tym decyzji w zakresie budżetowania, a co za tym idzie podniesienia dostępności i jakości usług dla obywateli oraz kreowania właściwej polityki informacyjnej.

Możliwości analizy biznesowej nie stanowią nowości w produktach bazodanowych, ale ostatnio pojawiły się nowe, tanie rozwiązania wprowadzające nowe funkcje w tym zakresie.

System analizy danych ma pełnić następujące funkcje:

- Import i standaryzacja danych z podległych jednostek i instytucji zasilających w dane, z uwzględnieniem mechanizmów czyszczenia, doprowadzania do spójnej postaci oraz agregowanie.
- Hurtownię danych wraz z mechanizmami zasilania danymi przez systemy lokalne opartych na standardach WebServices i XML.
- Narzędzia analityczne umożliwiające wykonywanie analiz ad-hoc, narzędzi do raportowania otwartego, dzięki którym analitycy będą w stanie docierać do dowolnej informacji w możliwie krótkim czasie oraz narzędzia, które wspomogą ich w poszukiwaniu nieoczywistych zależności pomiędzy różnymi danymi. Aplikacja musi pozwolić im poruszać się wśród dobrze zdefiniowanych pojęć biznesowych, przechodzić od ogółu do szczegółu, nawigować w danych przy pomocy hierarchii. Narzędzia z tej grupy będą też wykorzystywane przez kierowników średniego szczebla w celu przygotowywania analiz dla kierownictwa.



- Tworzenie zrównoważonej karty wyników umożliwiającej definiowanie koncepcji efektywności działania, optymalizacji tej efektywności, usprawnianie procesu podejmowania decyzji, stosowanie kart wyników we wszystkich aspektach prowadzonej działalności, oszczędności (dzięki wykorzystaniu istniejących kompetencji i rozwiązań technicznych) zasobów ludzkich, technicznych i budżetowych.
- Przyjazne środowisko prowadzenie analiz korzystające z kreatorów, które pomagają użytkownikom w pozyskiwaniu informacji niezbędnych do zrozumienia czynników biznesowych.
- Zaawansowane funkcje analityczne i wizualizacyjne takie jak drzewa dekompozycji i mapy wpływów.
- Możliwość szybkiego wdrożenia.

W obszarze planowania i budżetowania system powinien rozwiązać najczęstsze problemy organizacji:

- Kierownicy działów mają mieć możliwość powiązania budżetów działów ze strategią organizacji i jej zadaniami.
- Sterowanie przepływem pracy ma uprościć często czasochłonne, powtarzalne i mocno obciążające od strony administracyjnej dział finansowy - procesy planowania i budżetowania.
- Skrócić cykle sprawozdawczości finansowej i konsolidacji.

- Automatycznie tworzyć raporty wymagane przepisami prawa oraz skonsolidowane wyniki dla zarządu.

Na co należy zwrócić uwagę budując komponenty analizy danych? Jednym z kluczowych parametrów jest koszt w stosunku do osiągniętego efektu. Występuje jednak wiele innych czynników wartych uwagi.

Usługi analizy danych (BI) powinny być skalowane, zapewniając wsparcie dla baz danych o rozmiarze wielu terabajtów i tysiącach użytkowników. Aby umożliwiać jednoczesną pracę wielu użytkowników, redukować konflikty i obniżać koszty, możemy skalować poziomo rozwiązanie BI. Skalowanie poziome wiąże się zazwyczaj z dodatkowym ciężarem przetwarzania i składowania, związanym z magazynowaniem i synchronizowaniem wielu wersji danych. Warto więc zapewnić sobie możliwość dzielenia jednej bazy danych w trybie tylko odczytu między kilka serwerów BI, redukując dodatkowe obciążenie.

W dzisiejszych czasach monitorowanie zasobów w czasie rzeczywistym staje się niemal niezbędne, ponieważ systemy rosną zarówno pod względem rozmiaru, jak i liczby użytkowników. Warto więc wykorzystać narzędzia dostarczające dynamicznych widoków zarządczych (DMV), podobnych do tych dostępnych w silniku bazy danych. Zapewniają one dostęp w czasie rzeczywistym do informacji o systemie korporacyjnym w celu monitorowania, analizowania i optymalizowania wydajności.

Gdy baza danych staje się coraz większa, informacje, na które oczekuje użytkownik, mogą być coraz trudniejsze do znalezienia. z pomocą przychodzą jednak perspektywy, które dostarczają możliwość filtrowania widoku modelu UDM. Oferują one wszystkie zalety magazynów danych, a jednocześnie eliminują redundantne składowanie oraz konieczność synchronizacji magazynów danych, zmniejszając koszty przetwarzania oraz usuwając problemy związane ze spójnością danych i integralnością powodowane przez składowanie wielu kopii tych samych danych.

Postępujący proces globalizacji powoduje, że rozwiązania muszą być kierowane do odbiorców na całym świecie. Dane są zazwyczaj te same w skali całego świata, ale metadane, takie jak moduły, miary, nazwy i poziomy wymiarów oraz kluczowe wskaźniki wydajności (KPI - *key performance indicators*) z reguły różnią się w zależności od wymaganej wersji językowej. Tłumaczenia, zapewniają możliwość tworzenia różnych wartości meta danych dla

każdego języka i globalnego skalowania rozwiązań. Informacje finansowe także muszą być lokalizowane, aby wyniki były prezentowane w odpowiedniej walucie. Zakładamy, że komponent BI powinien oferować szerokie możliwości tłumaczenia i konwertowania walut, oraz udostępniać użytkownikom zlokalizowane dane analityczne w odpowiedniej wersji językowej.

Warto pamiętać, że do wykorzystania informacji analitycznych w środowisku biznesowym nie wystarczy sam dostęp do danych. Użytkownicy potrzebują wsparcia dla znanych im narzędzi, a twórcy aplikacji muszą mieć możliwość integrowania danych z własnymi rozwiązaniami. Usługi BI, powinny zapewniać zoptymalizowane współdziałanie z pakietami biurowymi, dostarczając znany interfejs oraz otwartą, wbudowywaną architekturę, która umożliwia programistom integrowanie danych.

4.11.3. PLATFORMA RAPORTOWANIA

Platforma raportowania ma zapewnić wydajny, skalowalny i łatwy w użyciu zestaw narzędzi bazodanowych do budowy rozwiązań raportowych, dystrybuowanie raportów i zarządzanie nimi. Przewidziane są mechanizmy generowania raportów stałych oraz łatwego generowania raportów ad-hoc. Niezwykle ważnym elementem platformy raportowania będzie wykorzystanie tzw. kokpitów menedżerskich pozwalających ująć raporty w graficznej formie uzupełnionej wskaźnikami i danymi liczbowymi.

Platforma raportowania ma pełnić następujące funkcje:

- Przygotowywanie standardowych raportów masowych, pozwalające na uruchamiania (lub subskrybowanie) predefiniowanych, w pełni sparametryzowanych raportów, które można renderować do wielu różnych formatów (np. Excel, PDF, XML). Możliwe musi być określenie, kiedy raporty będą generowane (np. codziennie w nocy) tak, żeby w maksymalnym stopniu wykorzystać potencjał infrastruktury bazodanowej w urzędzie oraz zapewnienie mechanizmów wersjonowania wygenerowanych raportów z dostarczaniem na żądanie np. w postaci załącznika do listu elektronicznego.
- Istotna jest również możliwość rozbudowywania platformy o nowe formaty, do jakich można renderować raporty oraz o mechanizmy dostarczania gotowych, wygenerowanych raportów wraz z funkcjonalnością WebServices.

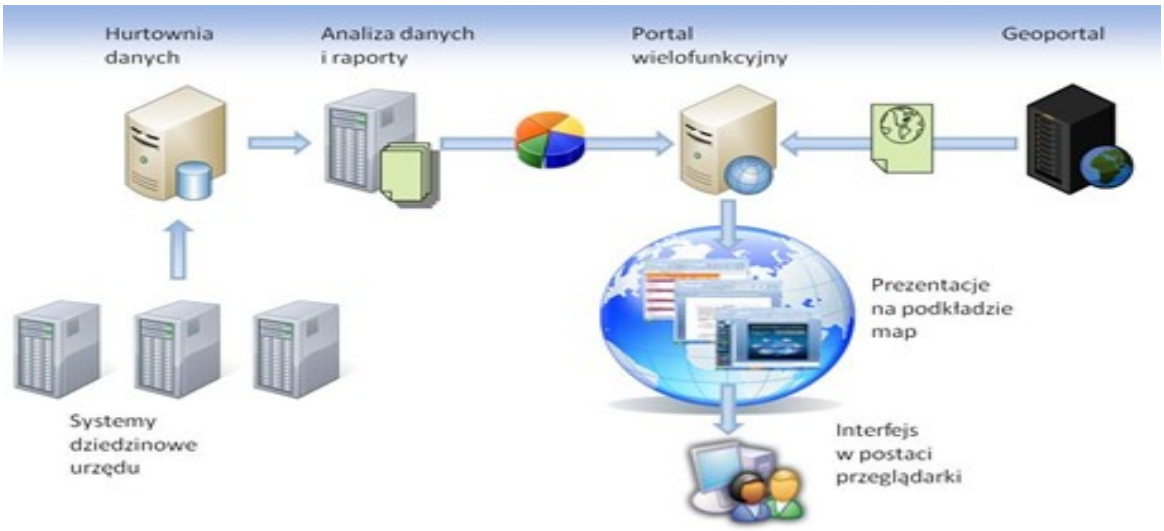
- Drukowanie niezależnie od formatu końcowego raportu z dostępnością parametrów wielowartościowych, sortowanie (także wg. wielu kolumn na raporcie i bez wykonywania dodatkowych zapytań do źródła danych).
- Edytor wyrażeń oraz kreator zapytań opartych o wielowymiarowe źródła danych.
- Proste narzędzia do budowy raportów ad-hoc.

4.11.4. PODSYSTEM GRAFICZNEJ PREZENTACJI ANALIZY DANYCH

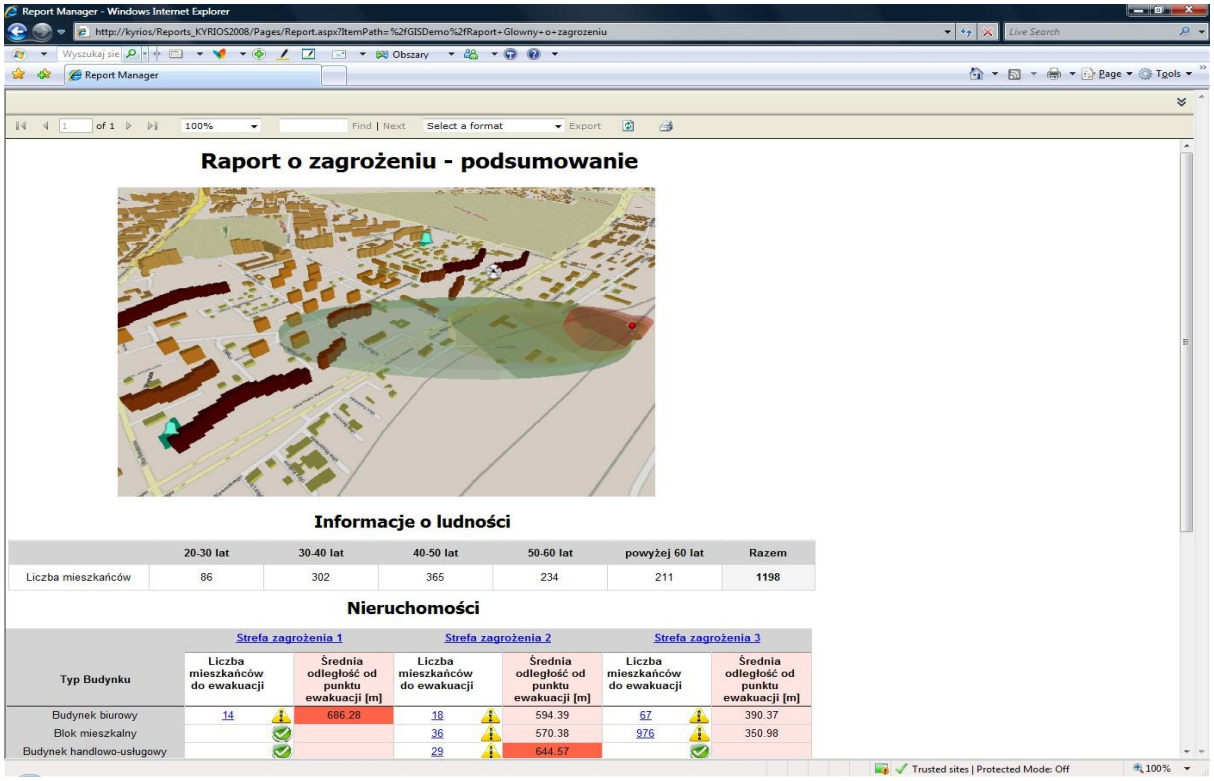
Podsystem graficznej prezentacji analizy danych (GPAD) ma zapewnić możliwość graficznej prezentacji wyników analizy danych na platformie systemów informacji przestrzennej. Coraz częściej wszelkie usługi informacyjne Wiele strategicznych decyzji dotyczących rozwoju, planowania budżetu czy też efektywnego wykorzystania istniejących zasobów wymaga analizy danych w ujęciu przestrzennym. Klasycznym przykładem może być planowanie tras i czasu dojazdu karetek pogotowia do różnych punktów adresowych, planowanie lokalizacji infrastruktury edukacyjnej, czy też rozbudowy niezbędnej infrastruktury w ramach tworzenia Planów Zagospodarowania Przestrzennego. Ponadto narzędzia tego typu pozwalają na szybkie i trafne podejmowanie decyzji w przypadku różnego rodzaju zagrożeń (powodzi, pożarów, epidemii) czy też imprez masowych.

System GPAD będzie opierać się na komponencie bazodanowym, raportowania i analizy danych. Założeniem jest stworzenie prostego, elastycznego i stosunkowo łatwo modyfikowalnego mechanizmu prezentacji analiz.

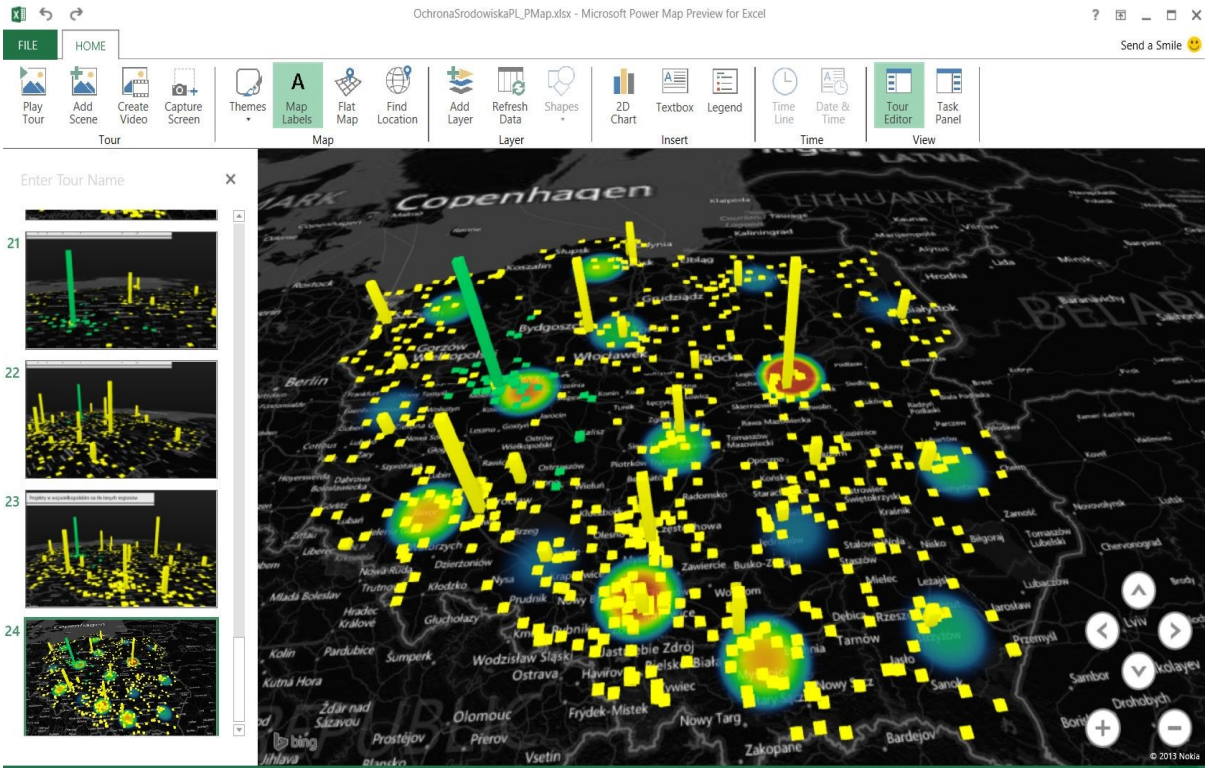
Ogólny schemat działania komponentu GPAD można przedstawić następująco:

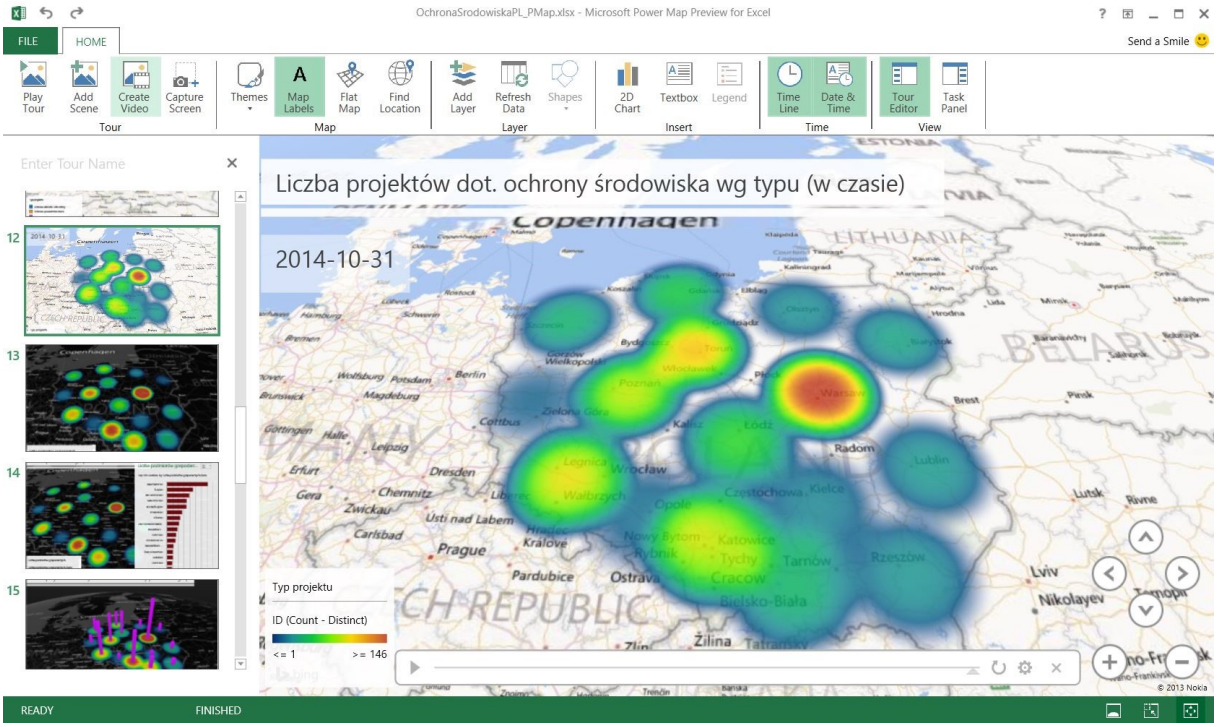


Przykładem zastosowań prezentacji analizy danych w układzie przestrzennym są następujące scenariusze zawierające statyczne raporty lub dynamiczne wizualizacje:



Bardzo często interfejsem dla prezentowanania analiz i raportów jest Microsoft Excel:





4.11.5. BAZY, ANALIZA DANYCH I RAPORTOWANIE – CZYLI SQL SERVER

Serwer relacyjnej bazy danych SQL Server 2019 jest najnowszym produktem Microsoft w technologii bazodanowej. Nie ogranicza się on do samego silnika bazy danych, ale zawiera też liczne rozszerzenia i narzędzia typu *Data Mining*, analiz biznesowych czy raportowania.

Najważniejszymi funkcjonalnie narzędziami SQL Server są:

Silnik bazy danych - Database Engine

składujący, przetwarzający i zabezpieczający dane. w aktualnej wersji znajduje się wiele rozszerzeń i ulepszeń, takich jak optymalizacja przetwarzania tablic w pamięci bazująca na In-Memory OLTP, wsparcie dla modelu przechowywania niestrukturalnych plików binarnych w usłudze Azure (Azure Blob Storage), wsparcie dla procedury składowania (*backup*) na adres sieciowy (*Backup to URL*), szyfrowanie składowanych plików (backup), wsparcie dla estymacji mocy zbioru matematycznego (*cardinality estimation logic*) optymalizujące planowanie zapytań i zwiększające wydajność realizacji zapytań.

Programowanie w języku R - R Services

Usługa udostępniająca możliwość wprowadzenia własnych modeli w popularnym języku R wywołującym procedury SQL.

Usługa spójności danych Data Quality Services

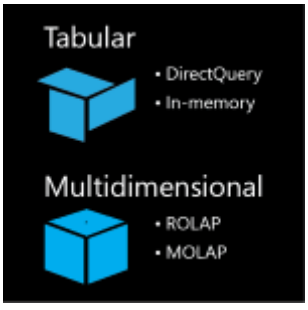
SQL Server Data Quality Services (DQS) umożliwiająca utrzymanie i czyszczenie danych referencyjnych w oparciu o logikę korekcji danych.

Usługa integracji danych - Integration Services

zapewniające wsparcie dla integracji i czyszczenia danych na etapie ich ekstrakcji, transformacji i pobierania (ETL) przy tworzeniu hurtowni danych.

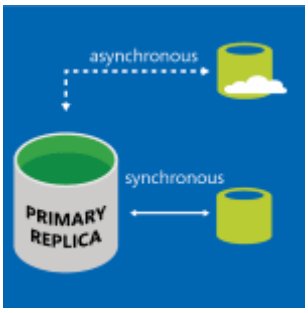
Usługa zarządzania danymi referencyjnymi - Master Data Services

pozwalająca na oparcie się w analizach, raportach i zasilaniu wszystkich systemów o aktualne i niezaprzeczalne dane referencyjne.



Usługa analizy danych - Analysis Services

Bardzo rozbudowane rozwiązanie klasy BI zawierająca też mechanizmy drążenia danych i Data Mining.



Usługa replikacji danych - Replication
pozwalająca na kopiowanie i dystrybucję danych i obiektów baz danych pomiędzy bazami danych i zapewniająca synchronizację danych dla utrzymania ich spójności i aktualności.

Usługa raportowania - Reporting Services
udostępniająca mechanizmy kreowania raportów ad-hoc i stałych wraz zachowaniem ich bezpieczeństwa i mechanizmów subskrypcji dla wybranych użytkowników.

Dzięki bardzo elastycznej architekturze SQL Server umożliwia budowanie systemów do zarządzania danymi o dowolnej skali. Całe środowisko może działać na jednym dużym serwerze lub skalować się w ramach farmy mniejszych, zcentralizowanych lub rozproszonych instancji.

Jedna instancja SQL Server może obejmować wiele maszyn (fizycznych lub wirtualnych) realizujących poszczególne usługi. Również same bazy danych można dzielić i uruchamiać partycje na oddzielnych serwerach. Bazy danych mogą replikować się w trybie transakcyjnym lub cyklicznie w ramach dowolnie zdefiniowanej topologii. Elastyczność w dziedzinie skalowania jest jedną z najważniejszych zalet SQL Server.

Bardzo ciekawą cechą z punktu widzenia użytkowników i administratorów SQL Server jest możliwość przypisania poszczególnym aplikacjom, procesom, a nawet konkretnym poleceniom SQL limitów zasobów, z jakich mogą korzystać. Dla każdego zasobu – takiego jak moc obliczeniowa, pasmo I/O, pamięć RAM, zasoby dyskowe – można zdefiniować hierarchię priorytetów obsługi różnych typów obciążeń, konkretnych zadań lub nawet ich fragmentów. w rezultacie, wyniki analiz dostępne są na czas – nawet wtedy, gdy w tle odbywa się intensywne przetwarzanie, np. aktualizacja indeksów, odtwarzanie baz czy raportowanie. SQL Server zawiera także narzędzia, które ułatwiają wykrywanie i usuwanie zakleszczeń baz danych.

SQL Server umożliwia centralizowanie i konsolidowanie informacji ze wszystkich systemów i aplikacji, bez względu na typ i format danych. w nowym centralnym repozytorium można gromadzić ujednolicone informacje z baz danych, dokumentów biurowych, plików o dowolnej strukturze, strumieni danych itd. Wszystkie dane można poddać jednolitym regułom przetwarzania i udostępniania do celów transakcyjnych, analitycznych, prognostycznych, raportowych i innych. Zgromadzone dane można spójnie przeszukiwać, zabezpieczać, odtwarzać i udostępniać użytkownikom zgodnie z nadanymi im uprawnieniami.

4.11.5.1. BEZPIECZEŃSTWO DOSTĘPU

SQL Server zapewnia wysoki poziom zabezpieczeń w zakresie uprawnionego dostępu do danych. Oprócz serwerów Urzędu Certyfikacji dla środowisk PKI, platforma zawiera obecnie własny, rozbudowany mechanizm do zarządzania kluczami kryptograficznymi. Dużym ułatwieniem jest wsparcie dla szyfrowania wszystkich danych w czasie rzeczywistym (programowo lub z wykorzystaniem akceleratorów sprzętowych). Szyfrowanie dotyczy zarówno danych przechowywanych na dyskach, jak i w bieżąco wykorzystywanych buforach przechowywanych w pamięci RAM serwera. w połączeniu z wielowarstwowymi mechanizmami kontroli dostępu, zarządzania prawami do informacji i uwierzytelniania, obsługą nowoczesnych protokołów WS-Security, SQL Server 2016 stanowi najbezpieczniejsze spośród dostępnych na rynku środowisk do zarządzania danymi.

4.11.5.2. BEZPIECZEŃSTWO DANYCH

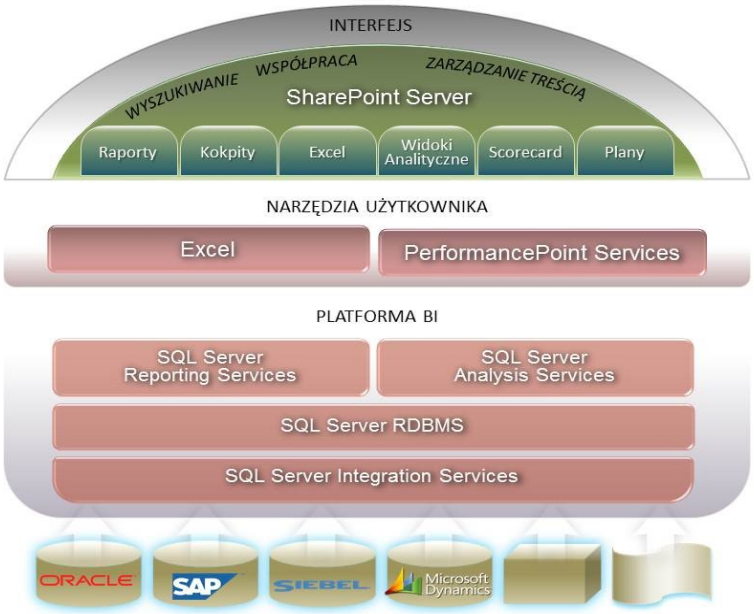
Ważnym krokiem w rozwoju SQL Serwer jest implementacja mechanizmu *Database Mirroring* w celu osiągnięcia wysokiej dostępności. w nowszych rozwiązaniach tego typu redukuje się obecnie ilość informacji, przenoszonych za pośrednictwem sieci z dziennika transakcji głównej (principal) bazy danych do dziennika transakcji lustrzanej (mirrored) bazy danych, kompresując informacje przed ich wysłaniem.

Dużym ułatwieniem jest możliwość naprawienia uszkodzonych stron danych w głównej bazie danych. Jeśli główna baza danych dozna uszkodzenia stron danych w związku z błędami, może zażądać świeżej kopii tych stron danych od serwerów lustrzanych. To żądanie prawidłowych stron danych powinno stanowić automatyczny proces, który pozostaje niewidoczny dla użytkowników aktualnie uzyskujących dostęp do głównych baz danych.

4.11.5.3. ANALITYKA BIZNESOWA

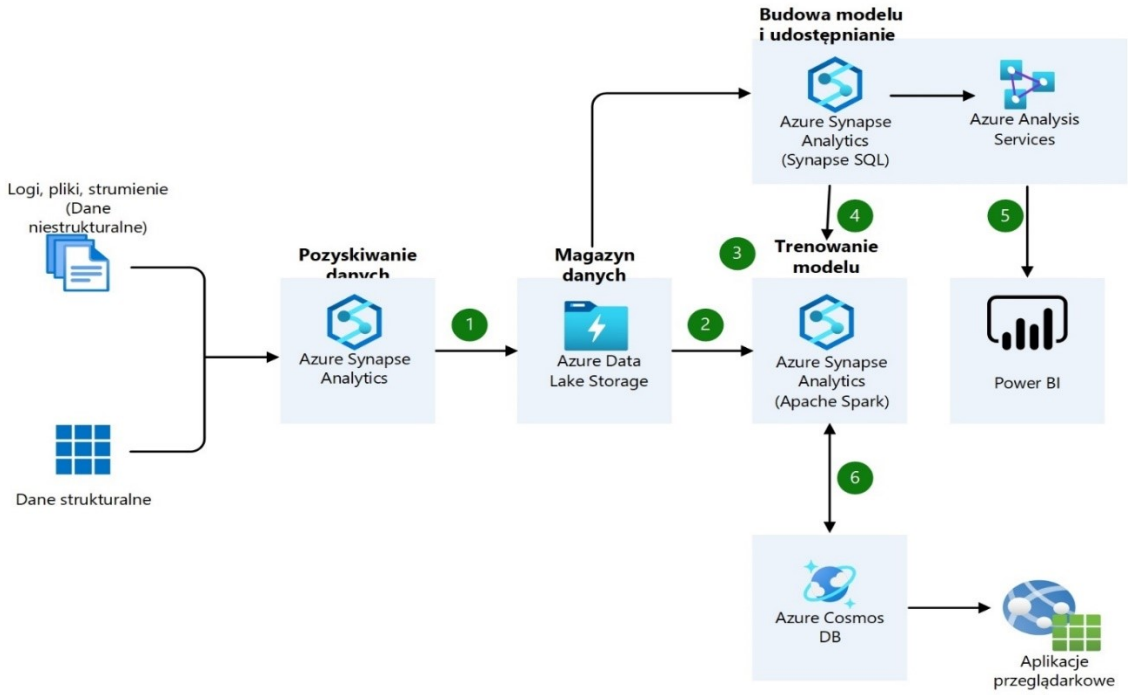
Wraz z edycjami Enterprise i BI SQL Server dostarczany jest moduł BI o bardzo szerokich możliwościach, poszerzonych dodatkowo poprzez integrację z innymi systemami i aplikacjami Microsoft Office. Użytkownicy Microsoft Excel mogą bezpośrednio łączyć się z bazami analitycznymi SQL Server Analysis Services i dokonywać analiz na danych za pomocą znanego im mechanizmu tabeli przestawnej czy Power Pivot – mechanizmu poszerzającego możliwości tabeli przestawnej, umożliwiający pracę na dużej liczbie danych i łączenie danych ze źródeł zewnętrznych.

Użytkownicy biznesowi mogą także bezpośrednio odwoływać się w swoich analizach do zaawansowanych algorytmów analitycznych dostępnych na platformie SQL Server. Platforma ta umożliwia generowanie raportów w formacie Microsoft Word i ich bezpośrednie publikowanie za pośrednictwem Microsoft SharePoint Server lub przy udziale komponentu Performance Point Services osadzonego w SharePoint Server. Ogólną koncepcję wykorzystania rozwiązania SQL BI przedstawia poniższy rysunek.

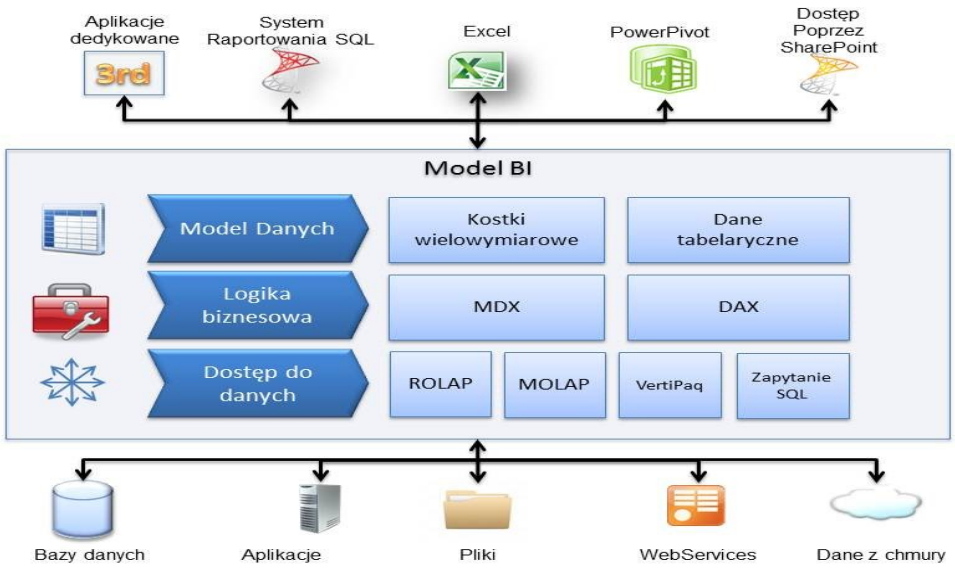


Można stwierdzić, że tego typu mechanizmy dawały potężne możliwości analizy danych – jeszcze parę lat temu. Obecnie dostępne narzędzia platformy Azure, dają dużo większe możliwości, przy radykalnym skróceniu czasu potrzebnego na budowę funkcji analizy danych, poprzez korzystanie z dostępnych, konfigurowalnych i skalowalnych komponentów –

pozwalając przygotować całość infrastruktury analizy danych nie w miesiące, ale w dni. Przykładową architekturę opartą o usługi Azure prezentujemy poniżej.

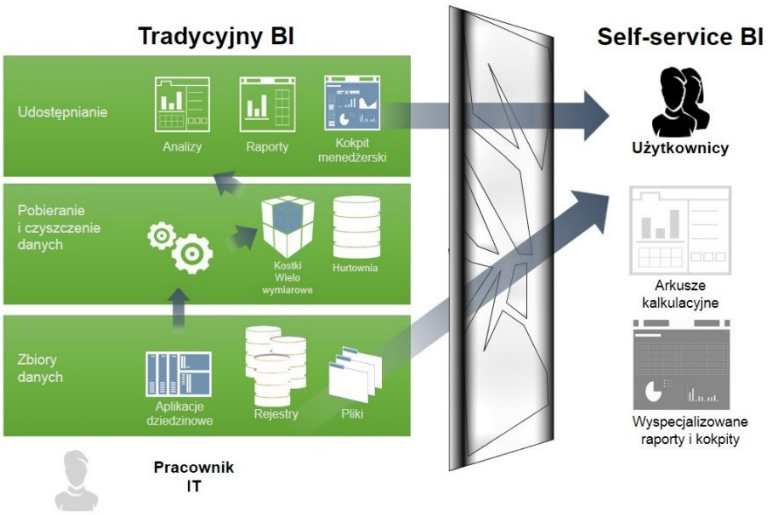


Duża elastyczność zawartych w SQL Server narzędzi analizy danych umożliwia dostęp do wyników analizy poprzez wiele standardowych interfejsów lub poprzez dedykowane aplikacje łączące się z SQL poprzez usługi sieciowe. Istnieje też w wiele mechanizmów zasilania danymi silnika analiz[64]:



[64] *Alan Merrihew, Connected Government Framework Reference Architecture, Microsoft 2012*

Ważną zmianą w podejściu do udostępniania narzędzi analiz, jest przejście od tradycyjnego modelu, w którym konieczne jest nieustanne zaangażowanie pracowników IT i specjalistów bazodanowych, do modelu samoobsługowego. Model samoobsługowy umożliwia użytkownikom nieznającym tajników narzędzi analitycznych, struktury danych i uprawnień, na wykonanie raportów i analiz w prosty sposób.



Tego typu scenariusze mogą być realizowane za pomocą SQL Server, SharePoint Server i Excel lub usługi platformy Azure.

4.11.5.4. EKSPLORACJA DANYCH

Skuteczne zarządzanie wiedzą w instytucjach administracji państwowej wymaga wykorzystania zaawansowanych narzędzi do gromadzenia i przetwarzania danych, zamiany tych danych w informacje, umieszczania tych informacji w odpowiednim kontekście, a następnie przetwarzania tych informacji w wiedzę, wykorzystywaną do analizy istniejących procesów biznesowych. Analiza powinna obejmować fakty, na podstawie których można planować długofalowe strategie biznesowe, wyszukiwać procesy, które wymagają przeformułowania oraz tworzyć nowe procesy, usprawniające funkcjonowanie instytucji i ludzi zaangażowanych w realizację wyznaczonych celów.

Algorytmy eksploracji danych (*Data Mining*[65]) wyszukują nieoczywiste zależności w danych oraz śledzą trendy, dzięki czemu można zbudować model analityczny. Model służy do

[65] *Sławomir Strzykowski, Modele zasilania danymi, Microsoft 2008*http://www.microsoft.com/poland/technet/article/art019.mspx

klasyfikowania, przewidywania i planowania działań przyszłych w oparciu o istniejące informacje. Najczęściej używanymi z zaimplementowanych w SQL Server algorytmów *Data Mining* są drzewa decyzyjne, grupowanie (analiza skupień), szeregi czasowe, reguły asocjacyjne i sieci neuronowe.[66] Najbardziej zaawansowane mechanizmy *Data Mining* dostępne są jako gotowe usługi w *Azure Machine Learning*.[67]

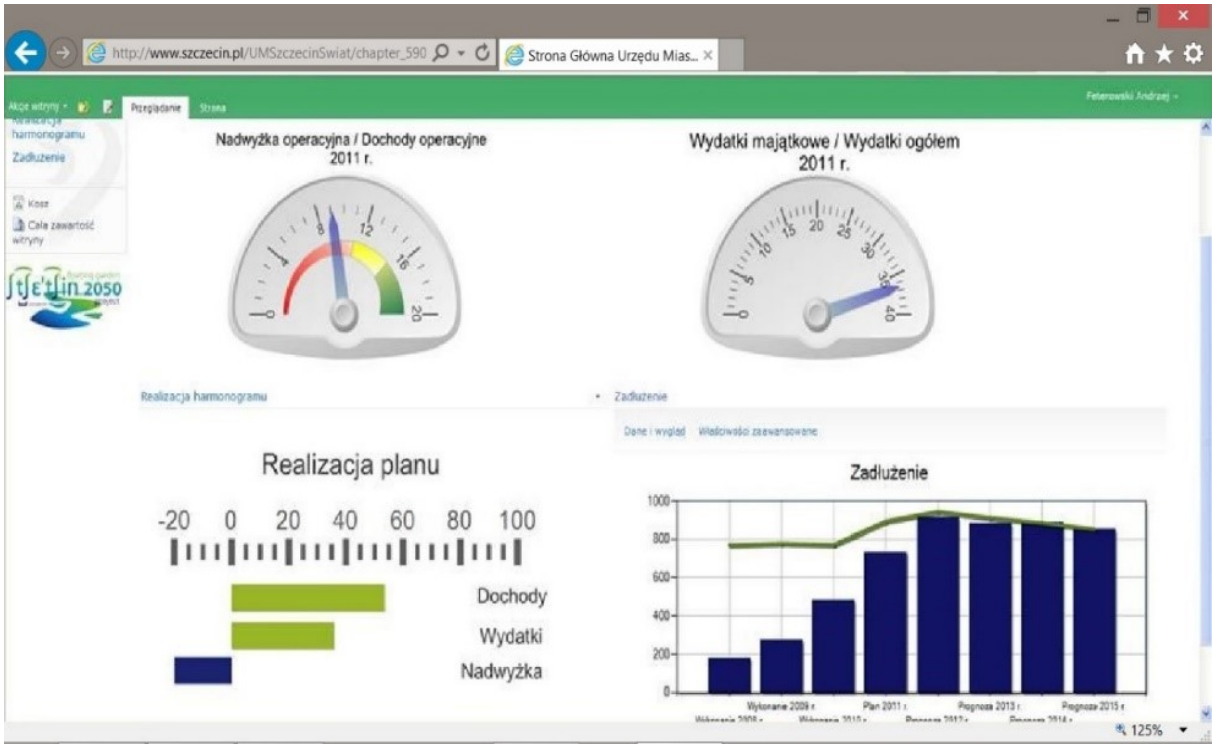
4.11.5.5. RAPORTOWANIE

SQL Server umożliwia gromadzenie danych na potrzeby analiz i raportowania zarówno w formie tradycyjnej hurtowni danych, jak i w formie widoków mapujących oryginalne źródła danych prezentowanych na przykład na platformie SharePoint. Tak przygotowane scenariusze można wykorzystywać jednocześnie. w tym drugim przypadku możliwe jest uproszczenie analiz i raportowania dziedzinowego wykonywanego w ramach narzędzi dostarczanych wraz z aplikacjami. Mapowanie oryginalnych metadanych na zdefiniowane w widokach przyjazne nazwy pól i obiekty logiczne, takie jak klient, zamówienie, faktura itp. umożliwia łatwiejsze utrzymanie i wprowadzanie zmian w procesach analizy i podejmowania decyzji bez prowadzenia prac programistycznych czy angażowania wykonawcy wdrożonego systemu. Oprócz klasycznych raportów tabelarycznych możliwe jest wykorzystanie gotowych wizualizacji danych, przyspieszających ocenę danych i związanych z nimi procesów:

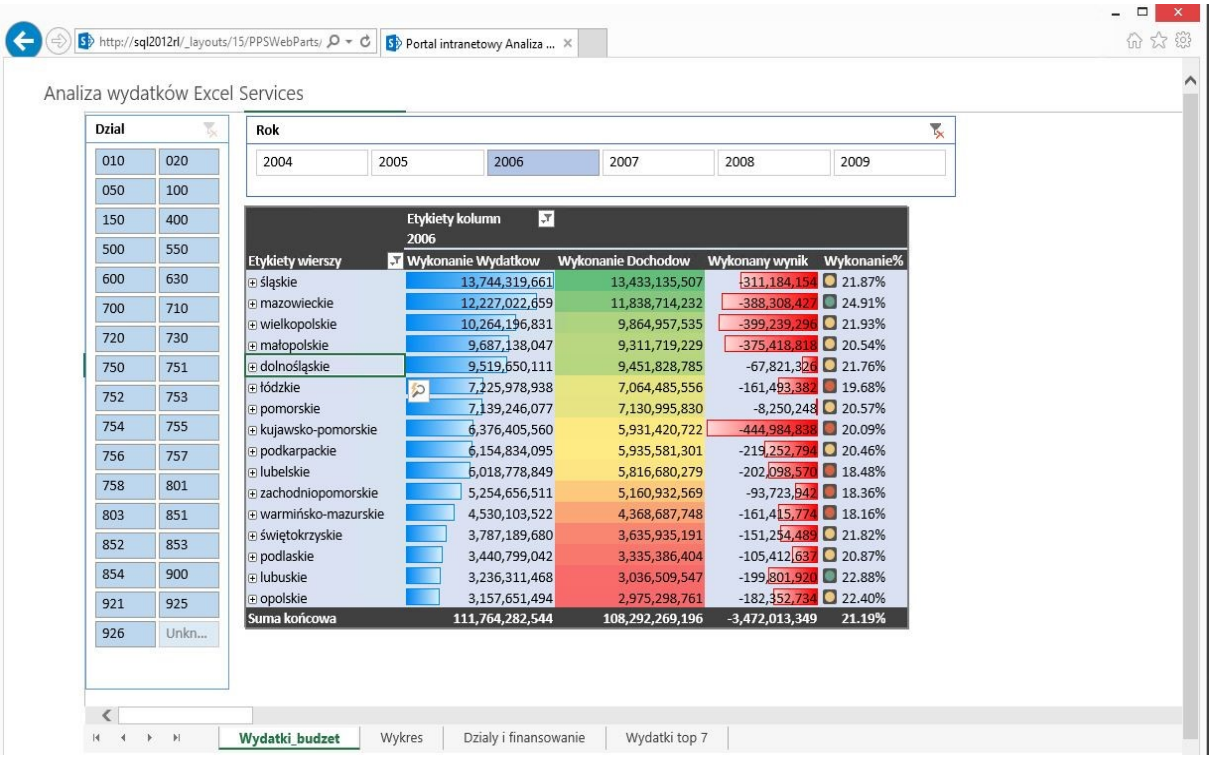
[66] https://docs.microsoft.com/en-us/sql/analysis-services/data-mining/data-mining-ssas?view=sql-server-2017
[67] https://azure.microsoft.com/en-us/services/machine-learning-studio/

Dodatkowo dostępne są predefiniowane narzędzia wizualizacji raportów o bardziej klasycznej formie:

Praktycznym przykładem tworzenia tzw. kokpitów menedżerskich jest zastosowanie opisywanych narzędzi w Urzędzie Miasta Szczecin dla monitoringu stanu finansów miasta:



Podobnie jak w prezentowanych już uprzednio przykładach typowym interfejsem dla narzędzi analitycznych i raportowych jest Excel lub Excel Services, czyli usługa portalu SharePoint. Mamy więc do wyboru oparcie się na aplikacji zainstalowanej na naszym urządzeniu lub oparcie się o model korzystania z usług portalu przez przeglądarkę. Oczywiście można łączyć obydwa modele, uzależniając na przykład ich wykorzystanie od dostępności łącza i wybierając między pracą on-line lub off-line.



4.11.5.6. ZARZĄDZANIE

Narzędzia zarządzania serwerami SQL pozwalają na objęcie zakresem działania zarówno instancji serwerów SQL, plików baz danych, jak i informacji o wykorzystaniu zasobów obliczeniowych (procesora) oraz dyskowych (*storage*). Najważniejszym celem jest centralizacja zarządzania. w SQL Server zawarty jest wprowadzony w wersji SQL Server 2008 R2 pojedynczy punkt zarządzania/wdrożenia (*single unit of deployment*). Dzięki zastosowaniu wspomnianego rozwiązania zwiększy się wydajność pracy administratorów w zakresie zmian, podnoszenia wersji i monitorowania wielu serwerów jednocześnie. Wprowadzono między innymi takie narzędzia jak:

- **Control Point Explorer** (CPE), który wykorzystywany jest jako punkt wejścia (*entry point*) i umożliwia zarządzanie grupą serwerów.

- **SQL Server Control Point** (SCP), który jest instancją SQL Server przeznaczoną do utrzymywania relacji z innymi instancjami serwerów SQL (zarządzanymi przez SQL Server Utility).
- **Managed Server Group** opisuje grupę serwerów SQL (instancji serwerów SQL) podłączonych do SQL Server Control Point, gdzie gromadzone są dane o wykorzystaniu ich zasobów.

4.11.6. ANALIZA I RAPORTOWANIE DANYCH W AZURE

Wymienione uprzednio narzędzia pobierania, przetwarzania, analizy i raportowania danych pozwalają na budowę niezwykle zaawansowanych systemów. Niestety, budowa takich systemów związana jest z dużymi nakładami na budowę infrastruktury, jej utrzymanie i rozwój.

Alternatywą dla tych kosztów i długiego czasu na przygotowanie tej infrastruktury, jest wykorzystanie gotowych usług zawierających narzędzia pobierania, ładowania, czyszczenia, filtrowania, analizy i raportowania danych.

Bardzo szeroki zakres tego typu narzędzi dostępny jest w usłudze Azure.[68]

4.11.6.1. AZURE DATA FACTORY

Niezwykle przydatną przy analizie danych usługą jest Azure Data Factory (ADF)[69], pozwalającą na pobieranie danych z wielu ustrukturyzowanych i nieustrukturyzowanych źródeł danych, transformowanie ich i składowanie w Azure do dalszej analizy. w skrócie – ADF służy do produkcji wiarygodnych informacji z różnych zbiorów surowych danych.

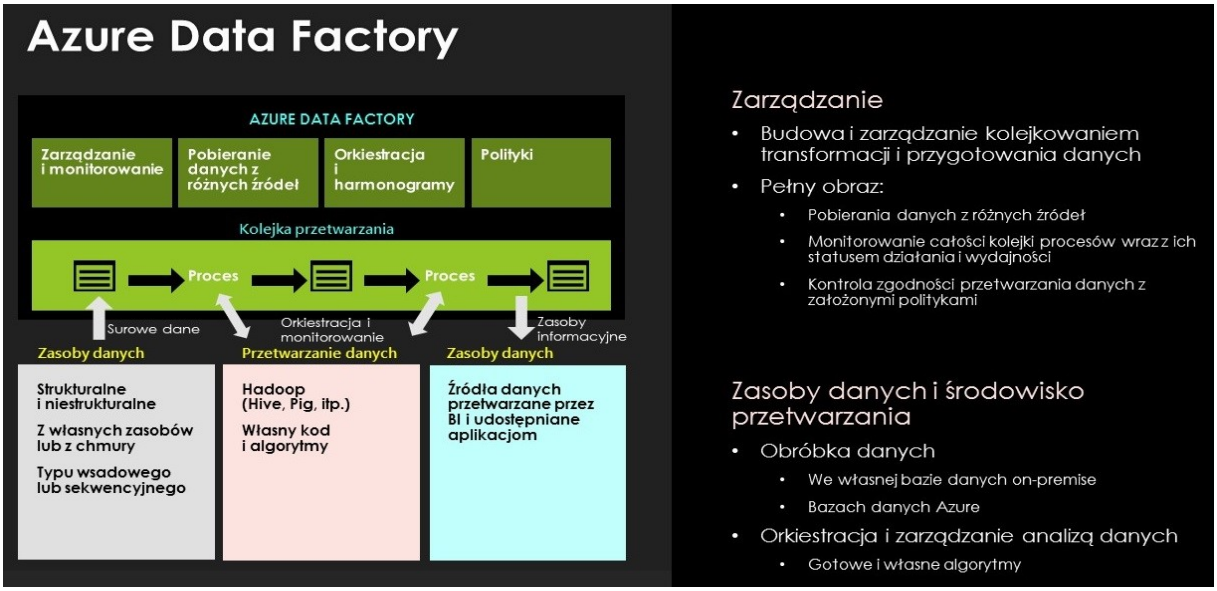
W trakcie ładowania danych możliwa jest ich wstępna obróbka, czyszczenie i partycjonowanie.

W dalszych etapach ADF pozwala na orkiestrację i zarządzanie transformacją, a następnie analizą danych. Dostępnych jest wiele gotowych algorytmów przekształceń i transformacji oraz możliwość implementacji własnych algorytmów.

[68] https://azure.microsoft.com/en-us/documentation/scenarios/data-analytics/
[69] https://docs.microsoft.com/pl-pl/azure/data-factory/

Tak przygotowany zasób danych może podlegać analizie (BI) dostępnej w Azure, a następnie może być publikowany w formie raportów lub udostępniany różnego typu aplikacjom.

Całość wymienionych procesów i kolejki tych procesów może być monitorowana i analizowana w celu usunięcia błędów, lub modyfikacji zastosowanych algorytmów.

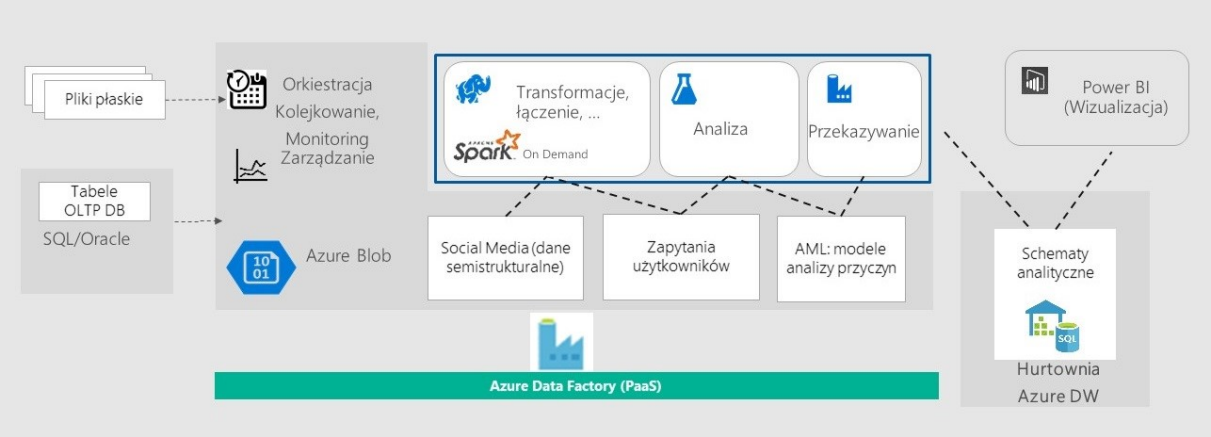


Takie podejście umożliwia szybkie „złożenie” z gotowych komponentów zaawansowanych systemów pobierających praktycznie dowolne dane (relacyjne i nierelacyjne, strukturalne i niestrukturalne, dostępne w postaci data-lake czy też strumieni danych w czasie rzeczywistym) z dowolnych źródeł, czyszczenie danych, budowę hurtowni i baz tymczasowych (staging), budowę modeli danych i przekazywanie do narzędzi typu BI udostępniających kokpity zarządcze, raporty stałe i ad-hoc.

Procesy takie są możliwe dzięki następującym narzędziom:

Oczywiście na każdym z poziomów obróbki danych zastosowane są mechanizmy niezaprzeczalnego dostępu do danych, monitorowania i realizacji zasad rozliczalności.

Dobrym przykładem wykorzystania narzędzi Azure jest schemat zaawansowanej hurtowni danych:



4.11.6.2. ANALIZY STRUMIENIOWE

Analiza strumieniowa pozwala na dokonywanie analizy danych pochodzących z wielu różnych źródeł, często raportujących w czasie rzeczywistym, takich jak czujniki, różnego rodzaju urządzenia, aplikacje itp. Pozwala kreować dynamiczną informację i monitorować wiele obiektów i wyciągać wnioski dotyczące zjawisk masowych – np. związanych z Internetem rzeczy. Pozwala to na obserwowanie dynamiki zjawisk, porównywanie wielu strumieni danych między sobą lub z przygotowanym uprzednio modelem umożliwiając wykrywanie prawidłowości, zależności zjawisk lub wykrywanie nieprawidłowości.

Dane pobierane ze źródeł mogą być transformowane w locie za pomocą gotowych lub tworzonych przez użytkownika algorytmów. Ważną cechą usługi opartej na Azure jest możliwość praktycznie nieograniczonego skalowania.

4.11.6.3. AZURE DATA LAKE ANALYTICS

Azure data lake analitics to wysoce skalowalna usługa pozwalająca na analizę dużych wolumenów danych niestrukturalnych i strukturalnych, czasem pochodzących z wielu źródeł. Niezwykłą zaletą tej usługi jest automatyczne łączenie się z wcześniej zdefiniowanymi zasobami danych, do których mamy uprawnienia, a następnie – po wykonaniu analiz – odłączanie tych źródeł. Ważną składową tej usługi jest pełna integracja z narzędziami Visual Studio, pozwalająca na łatwe debugowanie i optymalizację kodu stosowanego w analizie.

Dodatkowo możliwe jest wykorzystanie języka zapytań U-SQL.

Podobnie jak inne usługi Azure DLA bazuje na Active Directory, co daje możliwość łatwego zarządzania prawami użytkowników i uzyskanie potwierdzenia niezaprzeczalności ich działań.

4.11.6.4. AZURE SQL DATA WAREHOUSE

Azure SQL Data Warehouse to wysoce zaawansowana, skalowalna usługa hurtowni danych bazująca na mechanizmach SQL Server. Pozwala ona przetwarzać peta bajty danych, w tym w modelu masowego przetwarzania równoległego bez konieczności budowania własnej infrastruktury hurtowni z zasobów dyskowych. Umożliwia posługiwanie się językiem T-SQL i integrowanie wyników zapytań dla danych strukturalnych i niestrukturalnych z tzw. *Azure blob storage*[70].

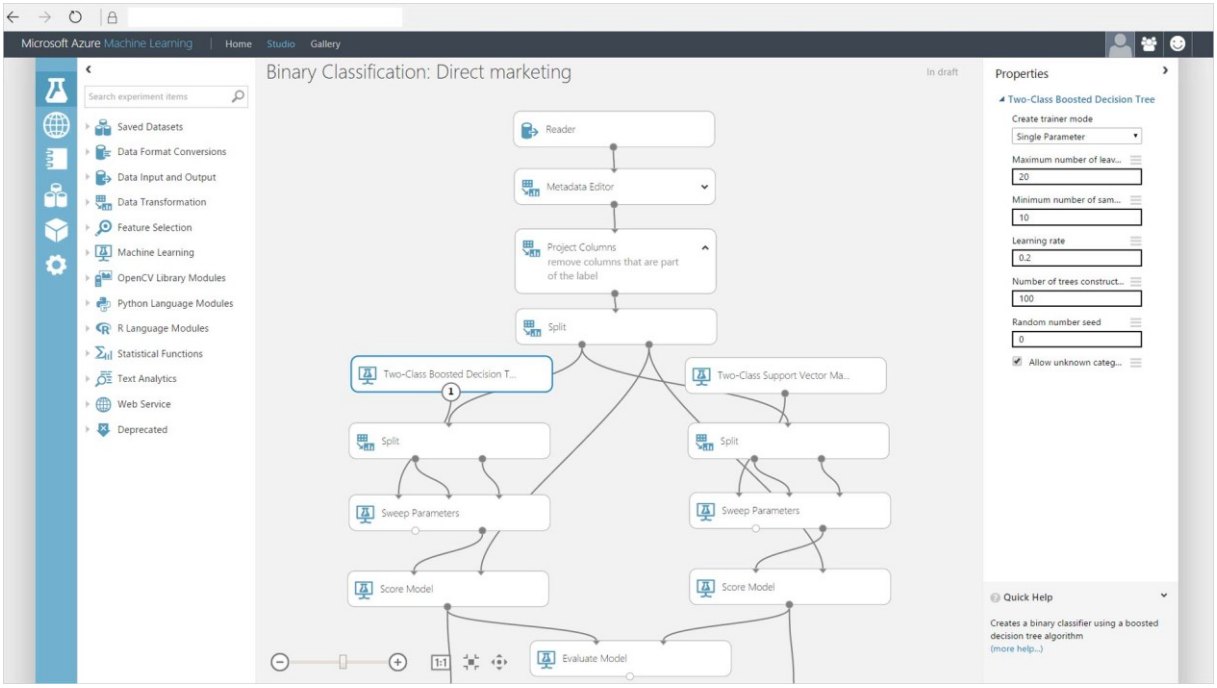
Z uwagi na zastosowanie tych samych rozwiązań co w SQL Server instalowanym lokalnie, możliwe jest budowanie hybrydowych rozwiązań przenoszenia i ekstrakcji danych, transformacji i ładowania danych z wykorzystaniem ETL – pomiędzy środowiskami własnymi i Azure.

Oczywiście, jedną z zalet takiej hurtowni jest możliwość uruchomienia jej w kilka minut.

4.11.6.5. AZURE MACHINE LEARNING

Bardzo często zbiory danych które posiadamy zawierają ciekawe, czasem wręcz niespodziewane informacje, użyteczne dla użytkownika. Wydobycie tych informacji o pewnych prawidłowościach czy trendach wymaga zastosowania zaawansowanych algorytmów, bardzo często niedostępnych dla zainteresowanych z uwagi na koszt masowego przetwarzania danych. Usługa Azure Machine Learning[71] pozwala na przetworzenie wolumenu danych, które posiadamy, z zastosowaniem wielu różnych metod statystycznych w poszukiwaniu zależności i prawidłowości.

[70] https://azure.microsoft.com/en-us/documentation/articles/storage-dotnet-how-to-use-blobs/#what-is-blob-storage
[71] https://azure.microsoft.com/en-us/services/machine-learning-studio/



Możliwości i skala takich analiz są praktycznie nieograniczone zarówno ze względu na skalę jak i na stosowane algorytmy – gotowe lub własne.

4.11.6.6. POWER BI

Usługa Power BI (PBI) to zbiór usług oprogramowania, aplikacji i konektorów, które współpracują ze sobą, aby przekształcić niepowiązane źródła danych w spójne, i interaktywne szczegółowe raporty. Dane wykorzystywane przez Power BI do tworzenia raportu mogą pochodzić z wielu źródeł, np. arkusza kalkulacyjnego Excel, chmurowych i lokalnych hybrydowych zasobów danych. Usługa Power BI umożliwia łatwe łączenie się ze źródłami danych, wizualizowanie i odkrywanie ważnych elementów oraz udostępnianie ich dowolnej osobie lub wszystkim osobom.

Power BI[72] to zaawansowana usługa wizualizacji, raportowania i analizy danych składająca się z trzech głównych komponentów:

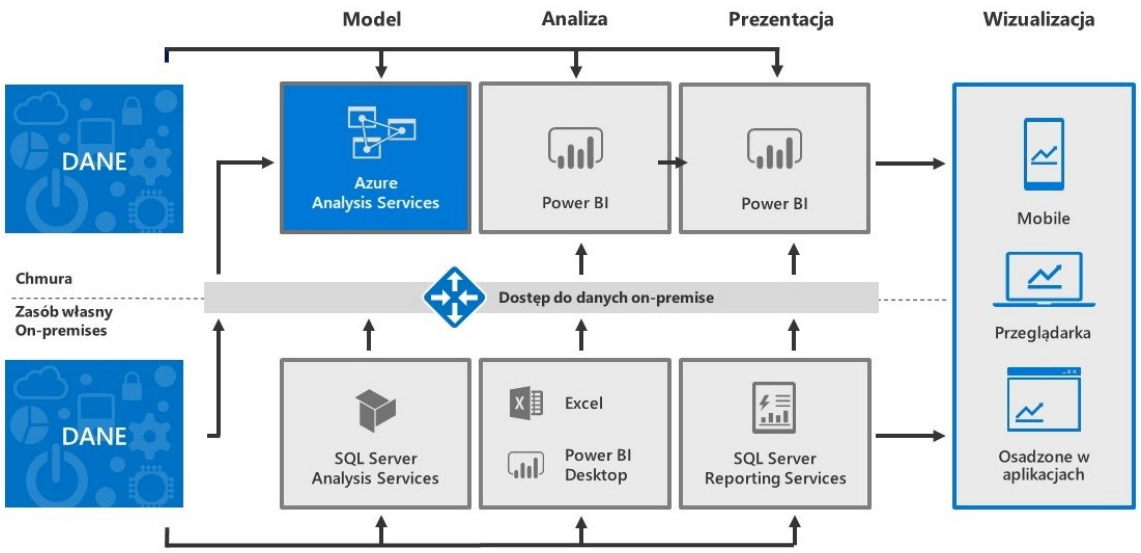
- Datasets – czyli różnych lokalnych i zewnętrznych zbiorów danych importowanych lub udostępnianych przez podłączenie do PBI i tworzących zbiór danych do analiz.
- Dashboards – pulpitów informacyjnych udostępniających w jednym lub wielu okienkach wyniki analizy zbioru danych (*dataset*) w formie graficznej lub

[72] https://powerbi.microsoft.com/en-us/documentation/powerbi-service-get-started/

alfanumeryczne. Pulpity informacyjne są zwykle konfigurowane pod względem zawartości i formy jej prezentacji dla danej roli w organizacji. Pozwalają one szybko uzyskać aktualną i wiarygodną informację pochodzącą bezpośrednio z systemów zaplecza i źródeł zewnętrznych. Dodatkowo pulpity umożliwiają zmianę formy prezentacji, zakresu analizowanych danych, filtrowanie oraz drążenie danych pozwalające zapoznać się ze szczegółowymi informacjami z wykorzystywanego modelu.

- Reports – raporty stałe i generowane ad-hoc pozwalające na przedstawienie wyników analiz w formie graficznej lub alfanumerycznej. Raporty można udostępniać w dwóch trybach – odczytu i edycji. w rzeczywistości, tryb odczytu, jest ograniczeniem uprawnień użytkowników do modyfikacji raportu. Raporty są zwykle podstawą treści pulpitów informacyjnych i mogą stanowić składową wielu różnych pulpitów.

Ciekawym rozwiązaniem jest hybrydowe połączenie możliwości analizy danych w modelu klasycznym wykorzystującym SQL Server BI i Reporting Services oraz Azure Analysis Services[73] z PowerBI.



4.11.6.7. MICROSOFT PURVIEW

Prawidłowe zarządzanie danymi, a co za tym idzie efektywne działanie i bezpieczeństwo danych, jest dużym wyzwaniem bez odpowiednich narzędzi ich wykrywania, katalogowania, wyszukiwania i udostępniania. Bardzo często dane są rozproszone w wielu systemach i usługach własnych i zewnętrznych, dublują się, mają różne poziomy poufności, a zawsze wymagają ochrony adekwatnej do ich wagi. Podstawą efektywnego działania jest uprawniony dostęp użytkowników do danych, które są aktualne, referencyjne, a jednocześnie dostępne w takiej jednolitej postaci dla odpowiednich komponentów systemów teleinformatycznych.

Odpowiedzią na tego typu oczekiwania w zakresie zarządzania danymi może być usługa Microsoft Purview oferowana z platformy Azure, której funkcje z zakresu cyberbezpieczeństwa zostały opisane w rozdziale „Bezpieczeństwo”. Pozwala ona uprawnionym użytkownikom na zarządzanie metadanymi w środowiskach opartych o własną infrastrukturę jak i w usługach typu *cloud* różnych dostawców.

[73] https://azure.microsoft.com/en-us/services/analysis-services/#overview

Microsoft Purview to rodzina rozwiązań do zarządzania danymi, zarządzania ryzykiem i zgodnością, które mogą pomóc organizacji w zarządzaniu i ochronie całego zasobu danych oraz zarządzaniu nim. Rozwiązania Microsoft Purview zapewniają kompleksowość podejścia do udostępniania właściwych danych w sposób uprawniony użytkownikom zdalnym, czy problemu fragmentacji danych w organizacji.

Microsoft Purview łączy dawne rozwiązania i usługi Azure Purview i Microsoft 365 wspomagając:

- uzyskanie wglądu w strukturę zasobów danych w całej organizacji,
- umożliwianie uprawnionego dostępu do danych,
- klasyfikację danych,
- ochronę poufnych danych i zarządzanie nimi w chmurach, aplikacjach i punktach końcowych,
- kompleksowe zarządzanie ryzykiem związanym z ochroną danych oraz zgodnością z przepisami i politykami.

Zastosowanie narzędzi Purview pozwala na optymalizację ogólnej architektury systemów, deduplikację danych, ich właściwą ochronę oraz ujednolicenie procesów biznesowych opartych o uprawnienia, a co za tym idzie – bezpieczny dostęp do aktualnych i referencyjnych danych. Jest też nieocenioną pomocą przy definiowaniu architektury nowych, jak i modernizowanych systemów i usług. Należy podkreślić, że tego typu podejście jest zgodne z większością wymagań w zakresie zasad interoperacyjności i cyberbezpieczeństwa – między innymi rozp. w sprawie Krajowych Ram Interoperacyjności i minimalnych wymagań dla systemów teleinformatycznych, ustawą o cyberbezpieczeństwie czy też RODO.

Głównymi funkcjami Purview są:

- wykrywanie zasobów danych,
- wykrywanie źródeł ich pochodzenia,
- klasyfikacja danych,
- tworzenie mapy naszych zasobów danych z miejscami ich położenia.

4.11.6.7.1. AUTOMATYCZNE WYKRYWANIE DANYCH

Podstawą właściwego zarządzania danych jest wykrycie miejsca ich składowania, ich źródeł i sposobu ich używania – w tym procesów, które z nich korzystają. Funkcja automatycznego wykrywania danych usługi Purview pozwala zrealizować te zadania zarówno przy inicjalnym mapowaniu danych, jak też w trakcie użytkowania i rozwoju wykorzystywanych systemów.

W trakcie tego procesu możliwe jest:

- wykrycie danych i źródeł ich pochodzenia,
- zautomatyzowanie zarządzania metadanymi w wielu źródłach danych,
- klasyfikacja danych z użyciem wbudowanych lub definiowanych we własnym zakresie schematów klasyfikacji,
- właściwe oznakowanie danych wrażliwych.

4.11.6.7.2. BUDOWA MAPY DANYCH

Drugim etapem po wykryciu i klasyfikacji danych jest budowa ich mapy w systemach i usługach dzięki usłudze Purview. Głównymi jej funkcjami są:

- budowa mapy położenia danych, ich źródeł, sposobu użycia oraz zależności między zasobami danych,
- automatyzacja i zarządzanie metadanymi z wielu źródeł,
- ciągła automatyczna lub ręczna klasyfikacja danych wraz z ich odpowiednim oznakowaniem i ujednoliceniem tej klasyfikacji w różnych systemach,
- integracja poprzez API z systemami Apache Atlas.

4.11.6.7.3. KATALOGOWANIE I DOSTĘP DO DANYCH

Po utworzeniu dynamicznej mapy danych konieczne jest udostępnienie narzędzi ułatwiających uprawnione ich wykorzystanie przez użytkowników. w tym zakresie Purview umożliwia:

- wyszukiwanie danych w oparciu o metadane, słowa kluczowe i pojęcia,
- rozpoznawanie danych poprzez dołączone metadane i opisy,
- ustalanie poziomu poufności danych,

- ustalanie pochodzenia danych wraz z graficzną wizualizacją źródeł i przepływów,
- właściwy dobór danych do procesów biznesowych oraz analizy.

4.11.6.7.4. MONITOROWANIE WYKORZYSTANIA DANYCH

W trakcie wykorzystywania odpowiednio wykrytych, oznakowanych i skatalogowanych danych Purview umożliwia:

- ciągły proces monitoringu wykorzystania – od źródeł surowych danych, poprzez przekształcenia, do ich prezentacji i raportowania,
- użycie mechanizmów platformy Azure w celu pobierania, czyszczenia i integracji danych z różnych źródeł,
- wykrywanie już istniejących analiz i raportów, aby uniknąć ich duplikacji.

4.12. ZARZĄDZANIE JEDNOSTKĄ

Coraz częściej efektywne zarządzanie przedsiębiorstwem czy instytucją wymaga wsparcia zaawansowanych narzędzi klasy ERP i CRM.

Wdrożenie tego typu rozwiązań jest niezwykle trudne – nie z przyczyn technicznych, ale raczej z uwagi na konieczność dokonania szczegółowych analiz, a często wprowadzenia zasadniczych zmian organizacyjnych i sposobu funkcjonowania podmiotu.

Ważnym jest stosowanie metodyk i narzędzi pozwalających na etapowe wdrażanie komponentów systemu zarządzania przedsiębiorstwem, przy utrzymaniu założonej wizji rozwoju i interoperacyjności poszczególnych modułów.

Zasadniczymi częściami optymalnego rozwiązania są komponenty zarządzania relacjami (CRM/XRM) i komponenty określane zwykle jako ERP (kadry, płace, środki, itd.).

4.12.1. ZARZĄDZANIE RELACJAMI Z KLIENTEM

Głównym celem wdrożenia wielu systemów jest zapewnienie interesantom (klientom wewnętrznym i zewnętrznym), efektywnego i zunifikowanego sposobu kontaktu z naszą organizacją (urzędem lub przedsiębiorstwem), opisu zasobów (ludzkich i materialnych) oraz stworzenia relacji między nimi.

W takim modelu – organizacji nastawionej na świadczenie usług – konieczne jest zbudowanie struktury organizacyjno-technicznej umożliwiającej minimalizację interakcji z interesantem i wyeliminowanie konieczności dostarczania przez interesanta dokumentów i załączników będących już w posiadaniu naszej organizacji. Koncepcyjnie jest to realizacja założenia budowy systemu dla klientów, a więc dostosowująca projekt organizacyjno-techniczny do tego priorytetu.

Dodatkowymi założeniami tego komponentu są:

- stworzenie struktury Działu Obsługi Klientów (centrum kontaktów), który będzie reprezentował sprawy interesantów wobec różnych jednostek organizacji lub wobec podmiotów zewnętrznych,
- stworzenie zestandaryzowanych i jednolicie obsługiwanych form kontaktu z organizacją, niezależnie od rodzaju wnoszonej sprawy,

- stworzenie uniwersalnych baz wiedzy dla centrum kontaktów,
- sożliwość uzyskania w dalszych etapach gwarantowanego czasu odpowiedzi lub załatwienia sprawy,
- możliwość monitorowania statusu sprawy przez interesanta,
- odciążenie interesantów poprzez zmniejszenie liczby interakcji.

Trzeba dodać, że koncepcja ta jest zgodna dyrektywą „usługową" UE:
- http://ec.europa.eu/internal_market/services/services-dir/index_en.htm

Wdrożenie nowych usług elektronicznych w takim kształcie, będzie niosło za sobą korzyści i usprawnienie procesów zaimplementowanych w poszczególnych komórkach organizacyjnych, ułatwiając i przyspieszając codzienną pracę, zwłaszcza osób odpowiedzialnych za ich rozwiązywanie w poszczególnych obszarach merytorycznych.

4.12.2. WIELOKANAŁOWA PLATFORMA KONTAKTU

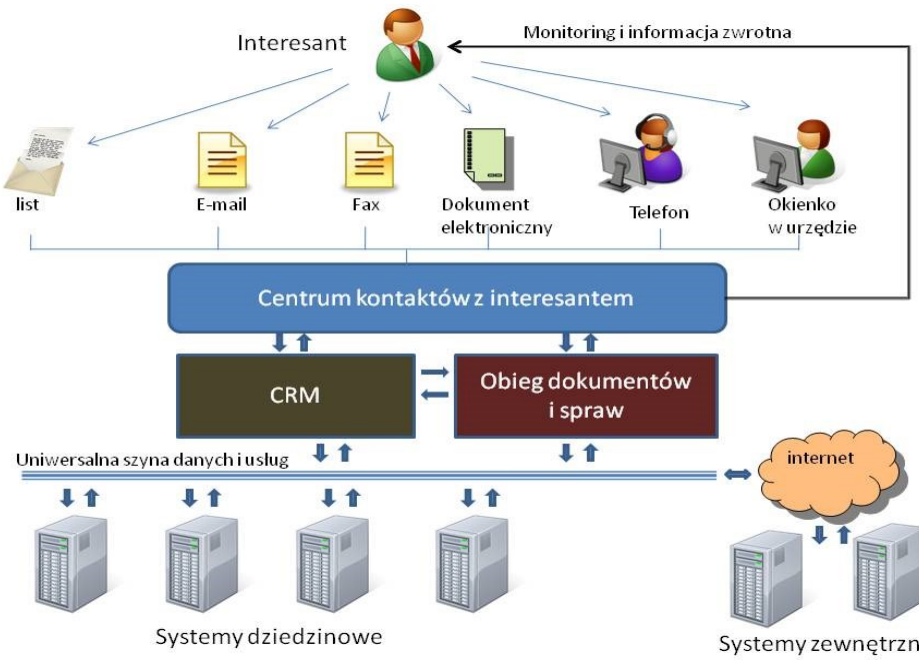
Podstawą rozwiązania problemów z obsługą różnych form kontaktu z interesantami jest wielokanałowy (w tym klasyczny) dostęp do usług świadczonych klientom. Tak więc stawianymi założeniami będą:

- obsługa różnego typu komunikacji i wymiany informacji (bezpośredniej, telefonicznej, przy pomocy dokumentów elektronicznych i papierowych),
- ujednolicenie procedur obsługi spraw po ich zarejestrowaniu,
- wykorzystanie zalet komponentu zarządzania relacjami.

Zwyczajowo sposób świadczenia usług na platformie elektronicznej jest kojarzony z dokumentami elektronicznymi przekazywanymi za pomocą Internetu. Rozwój technologii telekomunikacyjnych pozwala jednak myśleć o nowych kanałach komunikacji i platformach, na których można udostępniać usługi publiczne. Dobrym przykładem takiej nowej platformy jest telefonia komórkowa. Rosnące możliwości transmisyjne sieci komórkowych, wdrożenie UMTS, a także rosnące możliwości samych telefonów pozwala już realnie myśleć o udostępnieniu niektórych usług za pomocą telefonów.

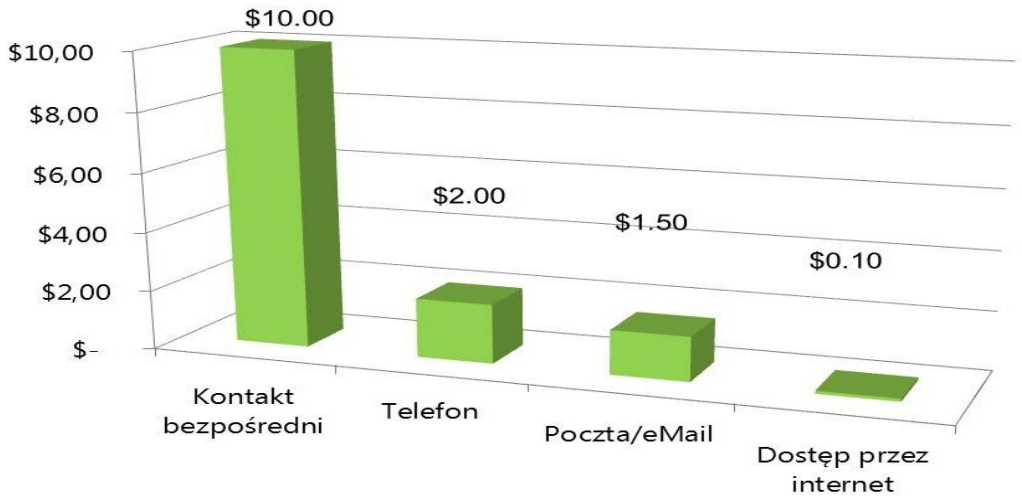
Należy także pamiętać o tym, że dostęp do Internetu, a co za tym idzie usług świadczonych za pomocą tego medium, dostęp ma mniejsza część naszego społeczeństwa. Skupiając się

tylko na tej części społeczeństwa, która ma dostęp do Internetu i odpowiednio potrafi korzystać z Internetu skazuje pozostałych na wykluczenie cyfrowe. Stawia też pod znakiem zapytania wydatkowanie środków publicznych na realizacje projektów, z których korzystać może tylko część społeczeństwa. Wykorzystanie usług telefonii komórkowej, mobilnego Internetu oraz możliwości, jakie daje interaktywna cyfrowa telewizja, to kierunki, w których zmierzać powinna funkcjonalność systemów, aby uczynić swoje usługi jak najbardziej dostępnymi. Jednym z beneficjentów takiego podejścia jest administracja publiczna, która może skorzystać na wykorzystaniu nowych technologii, szczególnie mobilnych. Wiele z zadań realizowanych przez administrację wymaga mobilności, a jednocześnie stawia wysokie wymagania dotyczące dostępu do danych i dokumentowania pracy. w takich wypadkach tylko dostęp do aplikacji mobilnych pozwala pogodzić ze sobą tak sprzeczne wymagania.



Powstawanie nowych kanałów komunikacji z interesantami niesie też możliwość obniżenia kosztów ich obsługi. Przedstawiony poniżej diagram pokazuje opracowane na bazie doświadczeń projektowych uśrednione koszty różnych form przekazywania informacji.[74]

[74] *Marcin Ozurkiewicz, Centrum kontaktu z mieszkańcem.*



Platforma wielokanałowej komunikacji daje możliwość udostępnienia wszelkich form interakcji i wymiany informacji, ale dla pełnej implementacji takich rozwiązań konieczna jest integracja wewnętrzna obecnie istniejących systemów, co jest procesem skomplikowanym i długotrwałym, głównie z przyczyn organizacyjno-prawnych.

4.12.3. ZARZĄDZANIE RELACJAMI - CZYLI DYNAMICS CRM

Microsoft Dynamics 365 zawiera komponent CRM (*Customer Relationship Management*), który jest elastycznym i łatwo konfigurowalnym systemem zarządzania relacjami z klientami.

Nie należy jednak utożsamiać jego funkcjonalności wyłącznie z klasycznymi zastosowaniami typu CRM mającymi zastosowanie w komercyjnych centrach obsługi klienta.

Dynamics CRM pozwala poprzez konfigurację wbudowanych narzędzi opisywać dowolne obiekty (osoby, budynki, urządzenia, elementy infrastruktury) i przyporządkowywać związane z nimi relacje, procesy czy zadania.

Ważną jego zaletą jest możliwość bardzo szybkiego prototypowania rozwiązań bez konieczności użycia narzędzi programistycznych.

Jednocześnie zapewnia bardzo szeroką skalowalność, od małych organizacji i kilku użytkowników do farm obsługujących wiele jednostek z kilkuset tysiącami jednoczesnych użytkowników. w tym ostatnim przypadku przydaje się cecha architektury CRM, pozwalająca uruchomić w jednym wysokodostępnym środowisku uruchomić wiele niezależnych instancji CRM o różnych funkcjach lub różnych zasobach danych – podobnie jak dla rozwiązań opartych o farmy SharePoint.

4.12.3.1. PODSTAWOWE FUNKCJE

Dzięki gotowym mechanizmom tworzenia strukturalnego opisu dowolnego obiektu oraz łatwego definiowania i przyporządkowywania do niego dowolnych zdarzeń, zadań, relacji czy procesów można w bardzo szybki i efektywny sposób kreować różne scenariusze usługowe:

- kompleksowej obsługi klienta urzędu wraz historią wszystkich jego interakcji,
- obsługi klientów wewnętrznych (pracowników),
- zarządzania i wykorzystania różnego typu zasobów (samochodów, budynków, sal).

Pomysły na wykorzystania systemu CRM są właściwie ograniczone tylko i wyłącznie pomysłowością użytkownika.

Dodatkowo system CRM posiada wiele usług pomocniczych takich jak:

- narzędzia integracji z użyciem web services,
- dostęp do zewnętrznych baz danych,
- wsparcie dla otwartych standardów,
- raportowanie,
- przepływy pracy,
- tworzenie i udostępnianie baz wiedzy,
- narzędzia programistyczne.

Przykładowe usługi, które można zrealizować poprzez Dynamics CRM w modelu obsługi klienta urzędu wyglądają następująco:

- Tworzenie bazy danych obywateli i ich spraw.
- Możliwość monitorowania poprzez CRM statusu spraw klientów z udzielaniem informacji o statusie:
    - przez urzędnika,
    - poprzez portal Urzędu,
    - poprzez skrzynkę podawczą.
- Możliwość wprowadzenia do systemu CRM informacji (baz wiedzy) o:

    - sposobie załatwiania spraw,
    - lokalnych regulacjach,
    - kompetencjach poszczególnych jednostek w Urzędzie,
    - danych teleadresowych w Urzędzie.
- Procesowanie zgłoszeń/spraw w następujący sposób:
    - przejęcie i zarejestrowanie danych obywatela (lub ich potwierdzenie),
    - zarejestrowanie sprawy,
    - przekazanie informacji o sposobie załatwienia sprawy lub uruchomienie „ręczne” sprawy poprzez przekazanie do odpowiedniej jednostki (mail, dokument papierowy, lun poprzez końcówkę systemu),
    - informowanie o statusie sprawy,
    - w przypadkach uzasadnionych – przekazywanie informacji do 112.
- Badanie poziomu satysfakcji mieszkańców
- Analiza danych zawartych w CRM pod kątem wydajności i efektywności obsługi mieszkańców.
- Tworzenie listy zgłoszeń priorytetowych lub przewlekłych, eskalacja spraw na wyższy poziom decyzyjny.
- Integracja CRM z system obiegu dokumentów i archiwum elektronicznym
- Integracja CRM z całością funkcjonalności systemów danej jednostki.

4.12.3.2. INTERFEJS UŻYTKOWNIKA

Typowym interfejsem pozwalającym korzystać z CRM jest przeglądarka. Wpisuje się to w standardowe podejście firmy Microsoft, dające prosty, a zarazem łatwy i podobny w obsłudze interfejs umożliwiający dostęp z wewnątrz i z zewnątrz organizacji, a zarazem niskie koszty wdrożenia i szkolenia użytkowników.

Standardowym interfejsem w modelu off-line jest MS Outlook pozwalający w prosty, znany z obsługi poczty elektronicznej sposób korzystać z funkcji CRM.

Często spotykanym rozwiązaniem jest wykorzystanie mechanizmów integracji z portalem wielofunkcyjnym SharePoint. w takim modelu użytkownik korzystający z portalu otrzymuje zadania, formularze czy treści publikowane przez CRM.

Tego typu rozwiązania można budować w oparciu o CRM– usługi Dynamics 365[75].

4.12.4. SYSTEM KLASY ERP

Podstawowymi założeniami budowy komponentu ERP jest budowa systemu pozwalającego na zarządzanie krytycznymi zasobami Zamawiającego (tj. finansami, środkami trwałymi czy pracownikami) wraz z niezbędnymi narzędziami analitycznymi i raportowymi. Założeniem jest też oparcie się na komponentowym modelu usług, z zachowaniem zasad interoperacyjności, skalowalności i bezpieczeństwa.

Wdrożenie ERP ma zapewnić jasny, efektywny i zunifikowany dostęp do danych, ich kolekcjonowanie, analizę i raportowanie, wprowadzić mechanizmy efektywnej komunikacji i pracy grupowej, a przede wszystkim umożliwić realizowanie podstawowych zadań statutowych.

W ramach budowy konkretnych funkcjonalności ERP należy uwzględnić integrację istniejących i planowanych usług pomocniczych, bez których pełne i efektywne wykorzystanie usług ERP nie jest możliwa. Usługi pomocnicze te obejmują zakresem funkcjonalnym:

- standaryzację zarządzania tożsamością użytkowników (pracowników),
- standaryzację interfejsu użytkownika,
- współdzielenie i obieg informacji:
  - wykorzystanie przestrzeni roboczych i bibliotek dokumentów dla instytucji, projektów, zespołów i pracowników,
  - standaryzację dokumentów i formularzy elektronicznych w ramach standardu Zamawiającego,
  - wykorzystanie mechanizmów typu workflow,

[75] https://www.microsoft.com/en-gb/dynamics365/home

    - wykorzystanie PKI,
    - wykorzystanie systemu poczty elektronicznej i integrację jej z innymi usługami.
- integrację systemów zastanych w niezbędnym zakresie,
- przyjęcie założeń umożliwiających budowę uniwersalnej szyny usług i zarządzanie usługami,
- monitorowanie statusu procesów i spraw.

Z punktu widzenia architektury ERP postawiono następujące założenia:

- posługiwanie się otwartymi standardami w wymianie informacji, umożliwiające realizację zasad interoperacyjności na wszystkich jej poziomach, takimi jak:
    - usługi sieciowe (Web Services),
    - dokumenty w formacie XML oparte o schematy XML ,
    - wizualizacja dokumentów w dowolnej przeglądarce internetowej,
    - formularze dostępne w dowolnej przeglądarce internetowej.
- możliwość komunikacji i integracji w warstwie przepływu informacji z dowolną technologią,
- łatwość integracji z przyszłymi centralnymi systemami administracji publicznej,
- wysoka skalowalność wydajnościowa i funkcjonalna,
- łatwość wdrożenia zaimplementowanych funkcjonalności w krótkim czasie,
- modularność systemu,
- możliwość modyfikacji sposobu działania systemu przez uprawnionych użytkowników bez konieczności ingerencji firm zewnętrznych,
- otwartość na dalszą rozbudowę,
- prostota obsługi.

Typowymi modułami systemów klasy ERP są:

- księga główna,

- środki trwałe,
- remonty i naprawy,
- kasa,
- materiałówka,
- służba eksploatacyjna,
- kadry,
- archiwum akt pracowników,
- płace,
- ewidencja czasu pracy,
- sprawy socjalne,
- sprawozdania i analiza danych.

Rozpoczynając budowę systemu klasy ERP lub zamawiając go jako usługę z chmury warto sprecyzować następujące wymagania:

a) System musi być „otwarty", tzn. zapewniać możliwość rozbudowy, dokonywania zmian oraz współpracy z innym oprogramowaniem, będącym w dyspozycji danej jednostki obecnie oraz pozyskanymi w przyszłości oraz umożliwiać modyfikowanie parametrów, raportów, itp. we własnym zakresie.

b) System musi być dostarczony wraz ze środowiskiem rozwojowym umożliwiającym samodzielną rozbudowę funkcjonalną i zapewniać tzw. zintegrowane środowisko rozwojowe (*Integrated Developement Enviroment*).

c) System musi posiadać architekturę co najmniej trójwarstwową i umożliwiać jego obsługę poprzez przeglądarki stron WWW oraz powinien oferować mechanizmy umożliwiające realizację dostępu do jego zasobów poprzez urządzenia mobilne. Architekturę trójwarstwową definiujemy jako system stworzony zgodnie z modelem trójwarstwowym, w którym można wyróżnić następujące grupy funkcjonalne, zwane warstwami:

    a. warstwa danych – w warstwie tej wyróżnia się elementy aplikacji operujące na danych pobranych z bazy danych. Mechanizmy zawarte w tej warstwie są

bezpośrednio odpowiedzialne za prawidłowy zapis, odczyt oraz modyfikację danych w bazie danych;

b. warstwa aplikacji – zawiera mechanizmy odpowiedzialne za pobranie danych z warstwy bazy danych, odpowiednie ich przetwarzanie oraz przygotowanie danych do przekazania ich do warstwy prezentacji. Ponadto w warstwie tej znajdują się mechanizmy operujące na danych dostarczonych z warstwy prezentacji, odpowiednie ich przygotowanie i przekazanie do warstwy bazy danych;

c. warstwa prezentacji – zawiera mechanizmy odpowiedzialne za komunikację z użytkownikiem. Dane z warstwy prezentacji przekazywane są do warstwy aplikacji oraz dane z warstwy aplikacji mogą zostać przekazane do warstwy prezentacji.

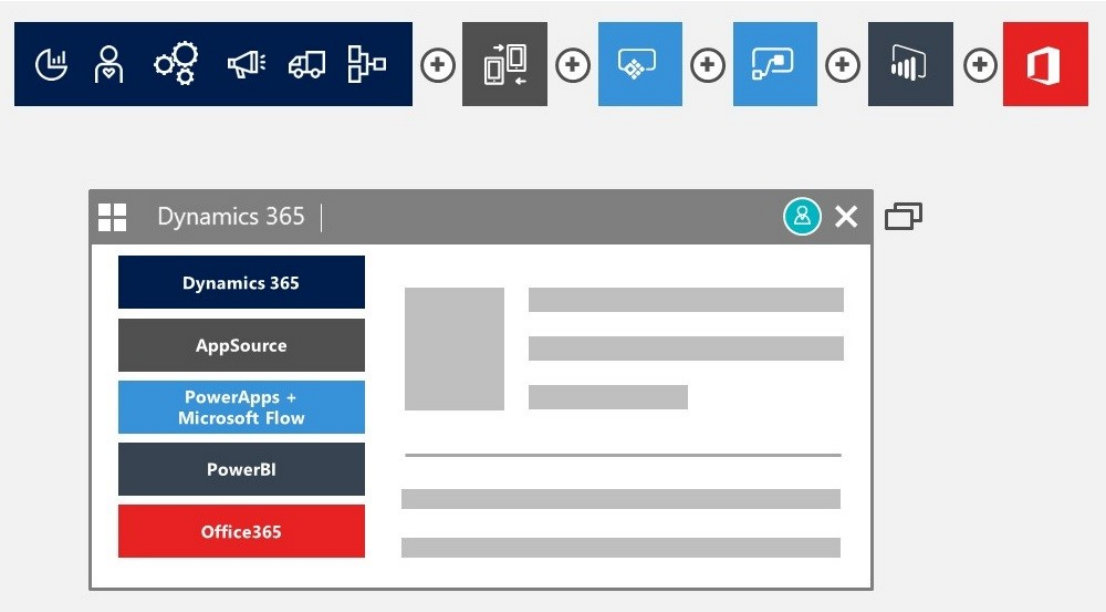
4.12.5. USŁUGI ZARZĄDZANIA JEDNOSTKĄ, CZYLI DYNAMICS 365

Subskrypcja Dynamics 365 dostarcza funkcjonalność systemów klasy ERP i CRM w postaci usługi hostowanej z centrów przetwarzania Microsoft i pozwala na szeroką konfigurację pozwalającą na dostosowanie do wymagań klientów. Dodatkowym plusem tej subskrypcji jest możliwość zainstalowania tych rozwiązań we własnych środowiskach serwerowych lub utworzenia rozwiązań hybrydowych on premises-chmura.

W stosunku do opisywanych powyżej rozwiązań, Dynamics 365 uzupełniony jest o wiele funkcji zarządzania, monitorowania bezpieczeństwa, skalowania czy usług analizy danych, jak na przykład Power BI.

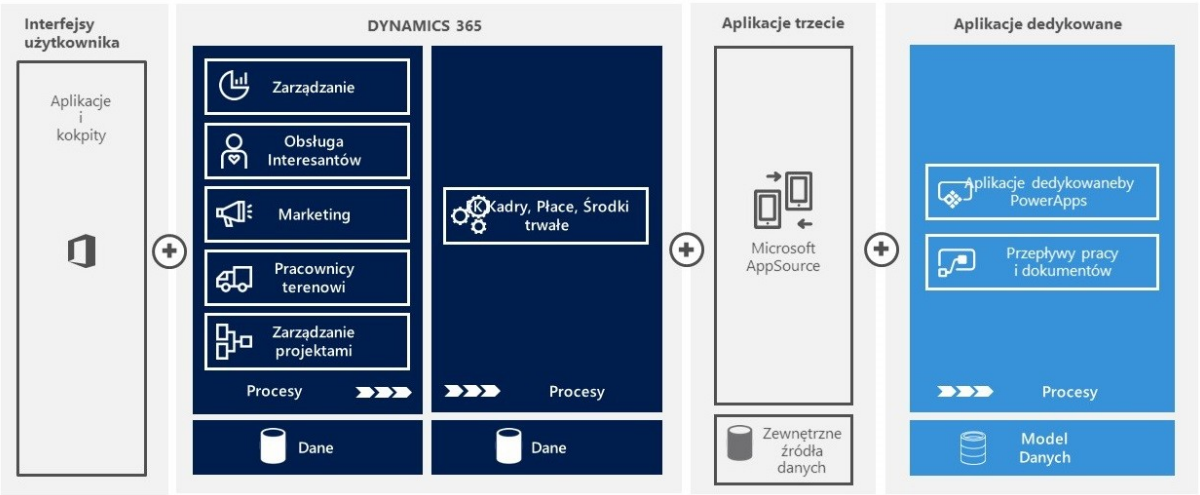
W zależności od typu subskrypcji, użytkownik może korzystać w różnym zakresie z funkcji ERP, CRM, raportowania czy analizy danych. w związku z tym Dynamics 365 stał się usługą (czy też zespołem usług) skalowalną zarówno wydajnościowo jak i funkcjonalnie.

Ważną cechą tej usługi jest też natywna integracja z innymi usługami Microsoft w modelu komponentowo-usługowym.



Oczywiście usługa Dynamics 365 korzysta z Azure Active Directory pozwalając na niezaprzeczalność i rozliczalność działań użytkowników, a w modelu hybrydowym – na wykorzystanie modelu pojedynczego logowania z własnego Active Directory. Możliwe jest też uruchomienie uwierzytelniania wieloskładnikowego dla dostępu dla szczególnie chronionych danych czy usług.

Szczególnie przydatną jest możliwość płynnego pokrycia całego procesu biznesowego przez różne komponenty dopasowując ich wykorzystanie do zaistniałych potrzeb.



Wdrażając Dynamics 365 należy pamiętać, że z jednej strony projektowanie obsługi procesów w części CRM jest niezwykle proste i szybkie, z drugiej strony, część ERP wymaga zwykle dedykowanych dla danego wertykału rozszerzeń pisanych przez partnerów Microsoft.

4.13. POCZTA ELEKTRONICZNA

4.13.1.1. PODSTAWOWE WYMAGANIA DLA SYSTEMU POCZTY

System poczty elektronicznej (e-mail) ma spełniać oczekiwania różnych grup użytkowników (wewnętrznych i zewnętrznych), biorących udział w procesach komunikacyjnych umożliwiając ochronę, zgodną z wymogami organizacji, dostęp do informacji z dowolnego miejsca oraz potrzebną działom IT wydajność operacyjną.

System poczty ma dostarczać usługi pracy grupowej i poczty elektronicznej w oparciu o usługi katalogowe i integrować się w pełni z katalogiem UK, przechowując w nim zarówno dane konfiguracyjne usług jak i dane skrzynek pocztowych użytkowników.

Organizacja serwera poczty ma objąć swoim zakresem cały las UK, w którym dokonana została instalacja serwera poczty (tryb *forest wide*). Oznacza to, że w środowisku jednego lasu z wieloma domenami istnieje tylko jednak organizacja serwera poczty, w której skrzynki mogą posiadać użytkownicy z wszystkich domen tego lasu.

Proponowane jest zbudowanie jednolitej infrastruktury dostępu do usług pocztowych i pracy grupowej dla użytkowników systemu informatycznego. Serwer poczty może być użyty jako serwer przechowujący dane użytkowników i obsługujący ich zapytania, jak i do budowy platformy usług internetowych związanych z dostępem do poczty elektronicznej.

Serwery poczty mogą pełnić dwie główne role:

- serwerów przechowujących dane użytkowników (*mailbox server*),
- serwerów usług internetowych.

Serwery przechowujące dane użytkowników udostępniają dostęp do zasobów serwera poczty oraz wymianę informacji wewnątrz organizacji pomiędzy użytkownikami. Każdy z użytkowników posiada skrzynkę pocztową umiejscowiona na jednym z serwerów zawierających skrzynki pocztowe w organizacji poczty.

Użytkownik posiada możliwość dostępu do swojej skrzynki niezależnie od lokalizacji w sieci organizacji.

W celu zapewnienia odpowiedniej jakości dostępu do usług poczty użytkownikom systemu informatycznego jednostki proponowane jest umiejscowienie serwera pocztowego pełniącego rolę serwera skrzynek pocztowych użytkowników:

- w centrali jednostki,
- w uzasadnionych przypadkach w każdym oddziale (lokalizacja odległa).

Na serwerach tych umieszczone zostaną skrzynki pocztowe użytkowników odpowiednich podległych urzędów oraz placówek terenowych.

Użytkownicy będą wewnątrz sieci jednostki uzyskiwali dostęp do usług poczty korzystając z klienta usług i protokołu MAPI.

System poczty dostarczy możliwości budowania rozwiązań w topologii *front-end* \ *back-end* pozwalając na udostępnieni w sieci Internet usług dla użytkowników poczty oraz wymianę poczty elektronicznej z organizacjami zewnętrznymi. w przypadku sieci urzędu docelowo w sieci Internet i użytkownikom zdalnym mają zostać udostępnione dwie usługi:

- Bramka SMTP.
  Bramka SMTP jest elementem koniecznym, aby umożliwić wymianę poczty z siecią Internet. Bramka SMTP zbudowana zostanie w oparciu o serwery poczty pracujące w konfiguracji front-end. Serwery te nie utrzymują lokalnie zasobów skrzynek użytkowników, lecz pośredniczą w wymianie poczty pomiędzy organizacją wewnętrzną a siecią Internet. w celu zapewnienia ciągłości wymiany poczty sugerowane jest zbudowanie rozwiązania bramki internetowej w konfiguracji *fail-over*. Możliwe jest poprzez zrównoważenie obciążenia sieciowego dla dwóch serwerów poczty pracujących równocześnie lub poprzez Udostępnienie dwóch serwerów poczty niezależnie w sieci Internet i odpowiednią konfiguracje ustawień DNS dla domen obsługiwanych przez organizację.
- Dostęp do poczty poprzez WWW.
  Usługi dostarczą użytkownikom możliwości skorzystania z zasobów serwera poczty poprzez przeglądarkę Internetową. w celu zapewnienia takiego dostępu

użytkownikom zaleca się instalację i konfigurację jako serwera dostępu przez WWW osobnego serwera w ramach zasobów informatycznych jednostki.

Ze względu na bezpieczeństwo oraz zapewnienie odpowiedniej funkcjonalności klientom usług poczty zaleca się Udostępnienie użytkownikom serwera poczty dostępu do następujących usług spoza sieci jednostki:

- połączenia z serwerem poczty poprzez interfejs przeglądarki,
- połączenia z serwerem poczty z poziomu klienta (np. typu Outlook) poprzez RPC\HTTPS.

W celu wymiany danych z serwerami poczty internetowej w sieci Internet zbudowana zostanie bramka SMTP oparta o dwa serwery poczty. Serwery te nie będą utrzymywały skrzynek użytkowników.

W celu zapewnienia ochrony antywirusowej dla poczty elektronicznej zalecane jest zainstalowanie oprogramowania antywirusowego na każdym serwerze poczty.

Dodatkowo w przypadku poczty przychodzącej z sieci Internet poprzez protokół SMTP zalecane jest przekazanie poczty poprzez dodatkowy serwer SMTP, na którym również zainstalowane zostanie oprogramowanie antywirusowe.

W celu zapewnienia ochrony użytkowników serwera poczty przed niechcianą pocztą (*spam*) konieczne jest zastosowanie następujących mechanizmów:

- *Inteligent Messsage Filtering* (IMF): mechanizm pozwalający na filtrowanie niechcianej poczty przez serwer poczty na podstawie pobieranych, lub tworzonych przez użytkowników sygnatur wiadomości spam,
- *SenderID*: technologia pozwalająca na uwierzytelnienie źródła pochodzenia przesyłki elektronicznej.

4.13.1.2. FUNKCJONALNOŚCI SYSTEMU POCZTY ELEKTRONICZNEJ

Sprawny system obsługi poczty powinien charakteryzować się następującymi cechami:

Funkcjonalność podstawowa:

1. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych.

2. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata.
3. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami.
4. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia.
5. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

Funkcjonalność wspierająca pracę grupową:

1. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości.
2. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu.
3. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze.
4. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone.
5. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania.
6. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.
7. Obsługa list i grup dystrybucyjnych.

Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:

1. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie, archiwizacja.

2. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników.

Wsparcie dla użytkowników mobilnych:

1. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej.
2. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem.
3. Możliwość „lekkiej" synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.).
4. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu PDA, Smartphone.
5. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej.
6. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej.

4.13.2. POCZTA ELEKTRONICZNA I REZERWOWANIE ZASOBÓW – CZYLI EXCHANGE

System Microsoft Exchange stanowi podstawę sprawnego i wysokodostępnego systemu poczty elektronicznej. System Exchange oferuje bogaty wybór scenariuszy wdrażania, pełny dostęp użytkowników do funkcji za pośrednictwem komputera stacjonarnego, przeglądarki i urządzenia przenośnego, a także wbudowaną ochronę informacji i możliwości kontroli. Najważniejsze, wpływające na funkcjonalność komponentu poczty elektronicznej cechy serwera Exchange można podzielić na kilka kategorii:

4.13.2.1. PODSTAWOWE CECHY EXCHANGE

Ponieważ system Exchange dostępny jest zarówno, jako oprogramowanie lokalne, jak i usługa on-line, każda organizacja może wybrać właściwy dla siebie sposób jego wdrożenia lub rozwiązanie hybrydowe.

Exchange Server zapewnia uproszczone rozwiązanie, jeśli chodzi o wysoką dostępność i przywracanie sprawności systemu po awarii. Tym samym pozwala osiągnąć wysokie standardy niezawodności, zapewniające ciągłość działania. Rezultatem takiego podejścia są:

- Możliwość rezygnacji z wdrażanie złożonych i kosztownych rozwiązań opartych na klastrach.
- Możliwość automatycznej replikacji baz danych skrzynek poczty elektronicznej i działanie trybu awaryjnego przy użyciu zaledwie dwóch serwerów lub pomiędzy rozproszonymi geograficznie centrami obsługi danych.
- Zapewnienie ciągłej dostępności systemu i jego szybkie przywracanie dzięki wielokrotnym kopiom baz danych poszczególnych skrzynek poczty elektronicznej zarządzanym przez Exchange.
- Ograniczenie zakłóceń działalności użytkowników podczas przenoszenia skrzynek poczty elektronicznej, co pozwoli na przeprowadzanie zadań migracyjnych oraz konserwacyjnych zgodnie z planem.
- Wyeliminowanie przypadków zaginięcia wiadomości email z powodu aktualizacji lub awarii serwera transportowego dzięki nowym, wbudowanym funkcjom redundancji, zaprojektowanym tak, aby w inteligentny sposób przekierowywać wiadomości inną, dostępną drogą.

System Exchange oferuje wbudowaną funkcję archiwizacji wiadomości email, która pomaga w rozwiązaniu problemów związanych ze zgodnością i ujawnianiem informacji. Umożliwia obsługę funkcji ochrona i kontrola informacji, która upraszcza szyfrowanie, moderowanie i blokowanie wiadomości email o poufnej lub nieodpowiedniej treści na podstawie danych nadawcy, odbiorcy i słów kluczowych. Funkcja ta:

- Łączy system Exchange z usługami katalogowymi *Active Directory* i *Active Directory Rights Management Services* (AD RMS), pozwalając na automatyczne zastosowanie

usługi zarządzanie prawami do informacji (*Information Rights Management* – IRM) w celu ograniczenia wykorzystania danych zawartych w wiadomości i dostępu do nich.

- Pozwala partnerom i klientom odczytywać i odpowiadać na wiadomości chronione przez funkcję IRM, nawet jeżeli nie posiadają oni usługi AD RMS.
- Umożliwia osobom uprawnionym przeglądanie wiadomości oraz zezwalanie na ich przekazywanie lub blokowanie.

Pamiętać należy, wszystkie wymienione funkcje i mechanizmy poczty elektronicznej możemy uzyskać wdrażając subskrypcje gotowej, bezpiecznej i skalowalnej usługi Exchange Online, która dodatkowo może być uzupełniona dodatkowym zestawem narzędzi i usług.

4.14. INTEGRACJA SYSTEMÓW WEWNĘTRZNYCH I ZEWNĘTRZNYCH

Przeniesienie realizacji usług na platformę elektroniczną powinno odbyć się z wykorzystaniem wszelkich dostępnych środków komunikacji i wymiany danych. Realizacji usług tylko i wyłącznie za pomocą formularzy elektronicznych stawia poza nawiasem dostępu tak dużą grupę potencjalnych klientów, że trudno taki pomysł uznać za słuszny w aspekcie rozpatrywania ekonomicznego efektu inwestycji. Na szczęście istnieje coraz więcej środków technicznych za pomocą, których można realizować usługi. Dla dalszego pomyślnego rozwoju elektronicznych usług konieczne jest osiągnięcie efektu synergii pomiędzy wykorzystaniem różnego rodzaju technik komunikacji. Ponadto wiele procesów wkracza poza zakres działania jednej organizacji, konieczna jest więc sprawna wymiana danych i dokumentów z systemami zewnętrznymi.

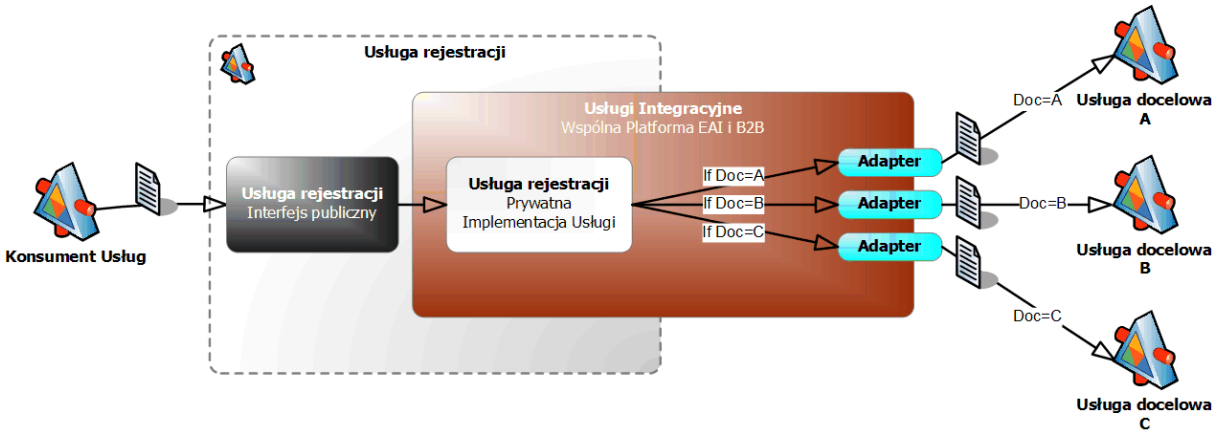
Przy takim podejściu kluczowym problemem jest połączenie wszystkich informacji dotyczących obsługi procesów zachodzących w jednostce, w szczególności tych, które wymagają interakcji różnych systemów (wewnętrznych i zewnętrznych) oraz wykorzystania różnych źródeł danych. Uzyskanie bezpośredniej interoperacyjności pomiędzy systemami

opartymi na standardach to ważny cel w budowaniu systemu, jednak integracja z istniejącymi systemami i usługami — rozwiązaniami bardzo zróżnicowanymi, tworzonymi na zamówienie albo produktami gotowymi — jest sporym wyzwaniem. Prawdopodobnie systemy te z wolna będą uzyskiwały możliwość komunikacji z wykorzystaniem usług *Web Service* — o ile w ogóle taka możliwość się pojawi. Szczegółową dyskusję nad implementacją założeń interoperacyjności można znaleźć w dokumencie „Ramy Interoperacyjności Systemów Administracji" – RISA. w niniejszym opracowaniu skupimy się na interoperacyjności technicznej i integracji.

W ramach wspólnej platformy komponentowej, usługi integracyjne umożliwiają integrację z systemami wykorzystującymi różnorodne mechanizmy, takie jak:

- SOAP — do komunikacji z usługami Web Service,
- HTTP — proste publikowanie dokumentów na serwerach internetowych, często w formacie XML,
- FTP — do transmisji plików zawierających duże ilości danych,
- mechanizmy kolejkowania, takie jak MSMQ,
- pliki w lokalnych lub sieciowych systemach plików,
- zapytania do baz danych z wykorzystaniem technologii ODBC i OLEDB,
- SMTP i POP3 — do dostępu do poczty elektronicznej i wysyłania wiadomości e-mail,
- niestandardowe interfejsy API — czasami oferowane przez producentów oprogramowania w celu umożliwienia klientom dostępu do danych w zorganizowany i wspierany sposób.

Na ilustracji przedstawiono strukturę logiczną platformy usług integracyjnych. Adaptery to komponenty zapewniające obsługę konkretnego protokołu lub komunikację z interfejsem API. Implementacje czarnej i białej skrzynki są logicznie elementami usługi rejestracji, jednak implementacja białej skrzynki może korzystać z platformy usług integracyjnych w zakresie komunikacji z usługami urzędu.



4.14.1.1. ZAKRES I HARMONOGRAM INTEGRACJI

Przystępując do projektowania i budowy komponentu integracyjnego, należy sobie zdawać sprawę, że o ile od strony technologicznej nie jest to już teraz trudny projekt, o tyle strona organizacyjno-prawna stawia przed nami wiele wyzwań. Szczególnie trudne są do określenia w czasie i budżecie te projekty, które przewidują integrację wielu różnych systemów wewnętrznych i zewnętrznych. Systemy te zwykle nie były tworzone zgodnie z zasadami interoperacyjności, nie posiadają uznanych standardów i interfejsów komunikacji, nie posługują się jednym, zdefiniowanym meta standardem, a co gorsza, zwykle są osadzone w kontekście zawartych umów dotyczących opieki serwisowej i odpowiedzialności wykonawcy za ich działanie. Wynikiem takich uwarunkowań jest to, że fizyczna integracja wielu systemów staje się przedsięwzięciem ryzykownym, trudnym do budżetowania i osadzenia w konkretnych ramach czasowych.

Proponowanym wyjściem jest budowa podstawowych mechanizmów integracyjnych i opublikowanie standardów, do których stopniowo będą dołączać się poszczególni uczestnicy zaplanowanych procesów wraz wymaganymi modyfikacjami techniczno-organizacyjnymi.

Początkiem tych działań jest:

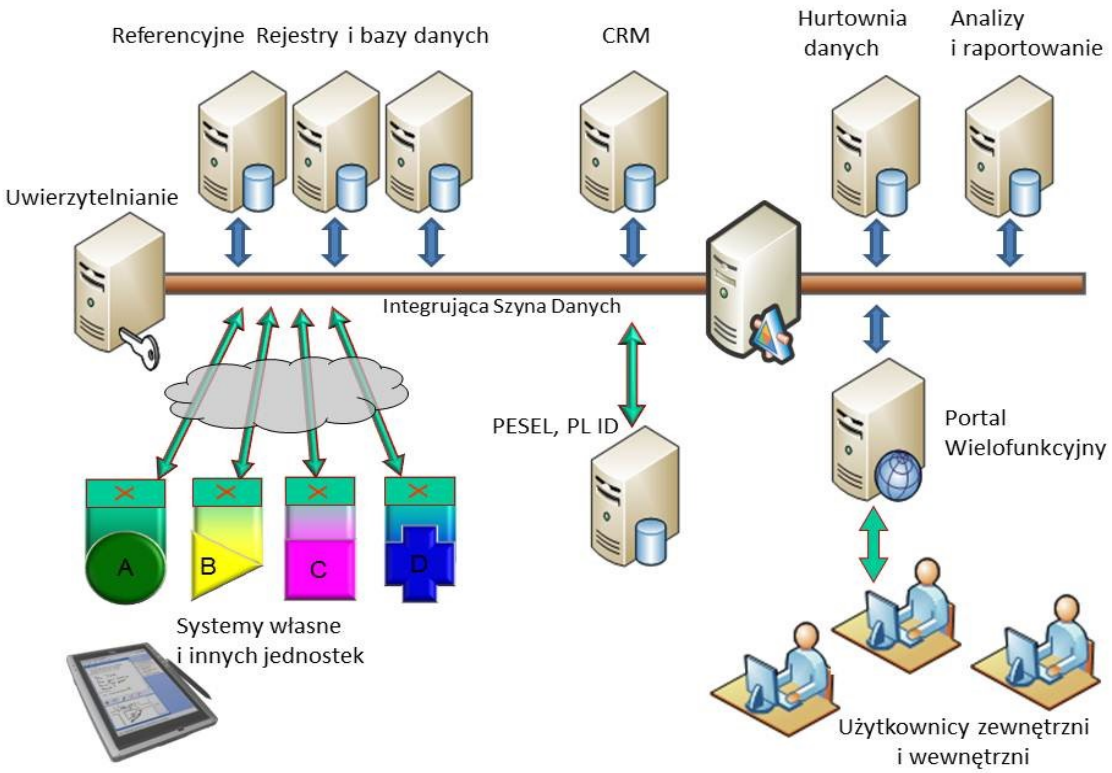
- ustalenie i opublikowanie meta standardu danych, który powinien bazować na meta standardzie opublikowanym w systemie ePUAP,
- budowa i opublikowanie niezbędnych słowników,
- ustalenie i opublikowanie specyfikacji interfejsów komunikacyjnych,
- ustalenie i opublikowanie zasad dostępu do danych i systemu uwierzytelniania,

- fizyczna budowa szyny danych i usług pozwalająca na integrowanie kolejnych usług i systemów.

Po określeniu powyższych standardów, można zdefiniować wymagania dla wszystkich dostawców nowych systemów oraz wykonawców odpowiedzialnych za modyfikacje i utrzymanie istniejących systemów.

Ważnym aspektem takiego planu jest to, aby realistycznie zaplanować wdrażanie i działanie usług bazujących na mechanizmach integracji, a więc wypracować harmonogram, w którym wdrażanie tych usług będzie podążało za możliwościami wykonawczymi w zakresie zmian w systemach i w organizacji pracy.

Przyjmując powyższe założenie można zacząć budować centralny model szyny danych i usług, nie zapominając o jednoczesnej budowie odpowiednich komponentów bezpieczeństwa, uwierzytelniania, wyszukiwania i modelu dostępu do danych.



Na powyższym rysunku zaproponowano model z użyciem integrującej szyny danych. Warto zwrócić uwagę na jeszcze jeden ważny problem. Bardzo atrakcyjnym wydaje się zawsze scenariusz centralizacji danych, a więc replikacji wielu baz danych z systemów własnych

i zewnętrznych wraz z procesem uspójnienia ich z wykorzystaniem mechanizmów ETL i logiki rozmytej.

Nie zawsze jest to jednak możliwe i to z kilku powodów. Po pierwsze, nie zawsze regulacje prawne pozwalają na tego typu centralizację danych. Po drugie nie pozwalają na to względy bezpieczeństwa danych. Po trzecie budowa wielkich hurtowni może wykraczać poza budżet zaplanowany w projekcie.

W takich przypadkach należy zastanowić się nad utworzeniem baz danych zawierających zindeksowaną informację na temat tego GDZIE znajdują się jej źródła oraz wytworzeniem mechanizmów bezpiecznego dostępu do tych źródeł dla osób (systemów) uprawnionych.

4.14.1.2. STWORZENIE ZALECEŃ DLA PRZEBUDOWY I BUDOWY NOWYCH APLIKACJI LOKALNYCH

W ramach implementacji systemu niezbędnym jest opracowanie dokumentu architektury referencyjnej, opartej o usługi sieciowe (*WebServices*) i elementy architektury zorientowanej na usługi (SOA), która umożliwi wszystkim podmiotom objętym działaniem systemu i wykonawcom systemów teleinformatycznych dla tych podmiotów, budowanie rozwiązań według konkretnych zaleceń.

Dokument ten powinien określić następujące reguły architektury systemów:

- Reguły rządzące architekturą —ogólne zasady projektowania oraz architektury zorientowanej na usługi (*Service Oriented Architecture* — SOA), na której oparta jest cała platforma.
- Hub usług— jak zapewnić wspólną infrastrukturę, z której może korzystać wielu dostawców usług.

Ponadto zdefiniowane być muszą usługi platformy - opis poszczególnych usług zapewnianych przez system. Usługi te to między innymi:

- usługi zarządzania tożsamością,
- usługi zachowania poufności i bezpieczeństwa,
- usługi prezentacji i punktu dostępu,
- usługi publikacji i wyszukiwania usług,

- usługi dostępu do rejestrów i baz danych,
- usługi integracyjne,
- usługi operowania danymi,
- usługi zarządzania systemem,
- usługi komunikacyjne.

4.14.2. INTEGRACJA SYSTEMÓW WEWNĘTRZNYCH I ZEWNĘTRZNYCH – CZYLI BIZTALK SERVER

Jednym z najważniejszych postulatów projektów integracyjnych jest użycie standardowych, przewidywalnych w swoim rozwoju narzędzi integracyjnych, dobrze obudowanych dokumentacją wdrożeniową i eksploatacyjną.

Takie podejście obniża koszty wdrożenia i eksploatacji systemów informacyjnych oraz minimalizuje ryzyko projektowe pozwalając na osiągnięcie efektów w założonym czasie i budżecie.

BizTalk Server jest narzędziem pozwalającym na łączenie różnych systemów wewnętrznych i zewnętrznych i umożliwiającym zarządzany przepływ informacji między nimi. Stanowi podstawę budowy systemów integracyjnych takich jak uniwersalna szyna danych oraz pozwalających na wdrożenie założeń architektury zorientowanej na usługi *Service-Oriented Architecture* (SOA)[76]. Tak więc, z jednej strony BizTalk jest narzędziem łączenia i integracji dotychczas niezależnie działających aplikacji wraz z ustanawianiem reguł biznesowych, standardów i interfejsów tej komunikacji. z drugiej strony może pełnić taką samą rolę w stosunku do całych systemów, pomiędzy którymi trzeba zbudować mechanizmy wymiany danych czy wspólnych usług.

Dzięki serwerowi BizTalk wymiana informacji pomiędzy systemami w złożonej infrastrukturze bazuje na branżowych standardach i wzorcach architektonicznych takich jak (SOA), *Enterprise Application Integration* (EAI), *Business-to-Business* (B2B), *Complex Event Processing* (CEP), *Enterprise Services Bus* (ESB), *Web Services, Society for Worldwide Interbank Financial Telecommunication* (SWIFT), *Health Level Seven* (HL7), *Health Insurance*

[76] http://pl.wikipedia.org/wiki/Architektura_zorientowana_na_us%C5%82ugi

Portability and Accountability Act (HIPAA) i innych. BizTalk Server jest kluczowym komponentem budowy tego typu rozwiązań.

Dodatkowo umożliwia konwersję między formatami danych, komunikację między systemami wykorzystującymi różne protokoły komunikacyjne lub formaty wiadomości *Electronic Data Interchange* (EDI). Zapewnia także dodatkową warstwę sterowania procesami oraz ochrony i integralności danych.

Funkcjonalność BizTalk Server to między innymi:

- definiowanie procesów biznesowych (BPM, Workflow),
- orkiestracja poprzez łączenie w logiczne ciągi szeregu obiektów i akcji,
- budowa schematów XSD poprzez graficzne definiowanie ich elementów i hierarchii,
- mapowanie strukturalnej informacji z wielu dokumentów źródłowych na wynikowe,
- translacja danych pomiędzy różnymi formatami,
- walidacja struktur i słowników,
- przetwarzanie reguł biznesowych,
- monitorowanie aktywności biznesowej (BAM),
- konfigurowanie relacji z partnerami,
- logowanie zdarzeń i debugowanie,
- statystyki i raportowanie pracy,
- integracja z MS Office/InfoPath,
- wsparcie usługi jednokrotnego logowania,
- prosta administracja.

W skład technologii integracyjnych Microsoftu oprócz BizTalk-a wchodzą:

- Windows Server AppFabric,
- Windows Azure AppFabric,
- Enterprise Service Bus (ESB),
- StreamInsight,

- Master Data Services,
- SQL Server Integration Services (SSIS).

Główne zalety wykorzystania BizTalk Server:

- Umożliwia efektywną komunikację zarówno wewnątrz organizacji, jak i z podmiotami zewnętrznymi.
- Nie tylko łączy ze sobą aplikacje i systemy, ale także pozwala definiować procesy biznesowe w firmie, łączyć je z ludźmi i systemami oraz zarządzać zdarzeniami i podstawowymi wskaźnikami wydajności wewnątrz każdego procesu w celu zagwarantowania efektywnego i wydajnego działania przedsiębiorstwa.
- Automatyzacja komunikacji z aplikacjami innych organizacji oraz pomiędzy aplikacjami wewnątrz firmy. Usługi integracyjne BizTalk Server skracają czas potrzebny na integrację rozwiązań, zmniejszając tym samym nakład niezbędnych prac administracyjnych IT.
- BizTalk Server wykorzystuje standardowe technologie, takie jak XML i usługi sieciowe (Web Services).
- Zapewnia świetną ekonomię zarządzania procesami biznesowymi i skalowalność, dzięki której małe, średnie i duże organizacje mogą w łatwy i ekonomiczny sposób instalować, konfigurować i dostosowywać rozwiązania integracyjne.
- Dzięki wykorzystaniu standardowego zestawu usług wielokrotnego użycia, można obniżyć koszty i skrócić czas zwrotu z inwestycji w automatyzację procesów biznesowych, upraszczając przy tym zarządzanie i obniżając koszty utrzymania.
- Integratorom systemów pozwala budować szyte na miarę rozwiązania dla każdej branży w dowolnym rejonie geograficznym.
- Umożliwia mapowanie procesów biznesowych w formie graficznej, dzięki czemu personel biznesowy może z łatwością analizować i dostosowywać procesy biznesowe w organizacji. Po skonfigurowaniu procesów biznesowych, użytkownicy mogą na bieżąco monitorować aktywność biznesową, w czasie rzeczywistym pobierać informacje o stanie oraz otrzymywać powiadomienia o interesujących ich wydarzeniach lub punktach krytycznych poszczególnych procesów.

- Zapewnia stosunkowo niskie koszty wdrożenia.
- Dzięki modułowej konstrukcji, pozwalającej między innymi na dodawanie wtyczek (adapterów) niezależnych producentów, ułatwia zmiany w strukturze komunikatu i standaryzacji.
- Udostępnia bogate środowisko programistyczne – Visual Studio.
- Uniezależnia od sieciowej platformy sprzętowej - brak konieczności instalacji sieci prywatnych lub VPN.

Dodatkową, ważną funkcją BizTalk jest wspieranie RFID. Możliwość identyfikacji z wykorzystaniem RFID otwiera szerokie możliwości monitorowania towarów w czasie rzeczywistym obiektów. Microsoft zakłada dostarczanie rozwiązań SOA pomagające użytkownikom przesiewać (filtrować) z masy danych RFID etykiety i czujniki w celu przekształcenia ich w informacje wspomagające procesy logistyki i zarządzania. Biz Talk RFID łatwo włącza inteligentne urządzenia (*at the edge*), które mogą być obserwowane i podłączone jako urządzenia sieciowe, do procesu monitorowania czy logistyki.

4.15. SERWEROWE SYSTEMY OPERACYJNE - CZYLI WINDOWS SERVER

Windows Server jest stale rozwijany w zakresie funkcji i efektywności zarządzania.[77] Oprócz standardowej funkcji serwerowego systemu operacyjnego posiada narzędzia wirtualizacji, zasoby sieci Web, usprawnienia zarządzania oraz integrację z platformami Online pomagającą oszczędzić czas i ograniczyć koszty wdrożenia. Wiele usług Windows Serwer zostało opisanych w poprzednich rozdziałach dotyczących usługi katalogowej, centrum certyfikacji czy bezpieczeństwa.

[77] *Część informacji o funkcjach Windows Server znajduje się w rozdziale „Usługi katalogowe – czyli Active Directory".*

Liczba edycji Windows Server oraz ról, w jakich to narzędzie możemy zastosować sprawia, że mamy do dyspozycji jeden z najbardziej rozwiniętych i elastycznych systemów operacyjnych dla środowisk serwerowych.

Zawartych jest w nim wiele przydatnych rozwiązań.

- Kontenery Windows Server (*Windows Server Containers*) – są to wyizolowane, zarządzalne przestrzenie pozwalające na uruchamianie aplikacji w sposób niewpływający na resztę systemu.
- Możliwość rozbudowy klastra typu *Failover* bez konieczności przerywania jego pracy.
- Udoskonaleniom uległa usługa *Remote Desktop Services*, gdzie między innymi wprowadzono wsparcie dla aplikacji wykorzystujących OpenGL i OpenCL.
- Nowe funkcje usługi zasobów dyskowych (*Storage Services*) pozwalają obecnie na tworzenie polityk typu QoS dla zasobów dyskowych i przypisywanie ich do wirtualnych dysków na maszynach wirtualnych działających w oparciu o Hyper-V.
- Najnowsza wersja usług sieciowych wspiera obecnie tunelowanie *Generic Routing Encapsulation (GRE)* oraz udoskonalone zarządzanie adresami IP, DNS i DHCP.

Windows Server jest dostępny w kilku wersjach. Najważniejsze z nich to Windows Server Datacenter i Windows Server Standard. Podstawowe różnice pomiędzy tymi wersjami to dodatkowe funkcje w Windows Server Datacenter - między innymi:

- Licencyjne uprawnienie do uruchamiania nielimitowanej liczby maszyn wirtualnych na wersji Datacenter i dwóch maszyn wirtualnych na wersji Standard. Wskazuje to jasno, że wersja Datacenter jest przewidziana do użycia w serwerowniach i centrach przetwarzania wykorzystujących technologię wirtualizacji.
- Chronione maszyny wirtualne z administracyjnymi uprawnieniami dotyczącymi samej maszyny wirtualnej – bez uprawnień do zarządzania środowiskami, na których są one osadzone.
- Rozszerzone mechanizmy zarządzania zasobami dyskowymi, takie jak *Storage Spaces Direct* i *Storage Replica.*
- Dodatkowe narzędzia wirtualnej infrastruktury sieciowej, takie jak *Network Controller*, *Software Load Balancer* i *Multi-tenant Gateway*.

Poniżej przedstawimy wybrane funkcje czy rozszerzenia wbudowane w Windows Server 2022:

- Wydajne i wszechstronne narzędzia, takie jak nowa wersja Internet Information Services (IIS), uaktualniona konsola Server Manager, platforma Hyper-V oraz środowisko Windows PowerShell współpracują ze sobą, zapewniając użytkownikom większą kontrolę, podniesioną wydajność oraz możliwość szybszej niż kiedykolwiek reakcji na potrzeby biznesowe.
- W Windows Serwer (podobnie jak w Windows 11) mamy udostępniony nowy, poprawiony *BitLocker*. Poprzednie wersje Windows Server (podobnie jak w Windows Vista i 7) oferowały zaszyfrowanie całego dysku, razem z pustym miejscem. w Windows Server 2022 i Windows 11 możliwe jest wybranie szyfrowania tylko używanych bloków, dzięki czemu działa ono znacznie szybciej.
- Zwiększono znacznie możliwości skalowania platformy osadzonej na Windows Server. Mamy obecnie możliwość wykorzystania do 320 logicznych procesorów oraz i do 4 TB pamięci RAM w środowisku fizycznym.
- Ponadto, w środowiskach zwirtualizowanych możemy wykorzystać do 64 procesorów wirtualnych, 1 TB pamięci RAM i dysku o pojemności do 64 TB dla każdego wirtualnego serwera.
- W przypadku budowy dużych środowisk z elementami niezawodnościowymi mamy możliwości budowania klastrów składających się z maksymalnie 64 węzłów, z możliwością uruchomienia do 8000 maszyn wirtualnych.
- Ciekawym rozwiązaniem jest możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

4.16. WIRTUALIZACJA - HYPER-V I AZURE

4.16.1. WIRTUALIZACJA CENTRUM PRZETWARZANIA

Microsoft Hyper-V jest jedną z usług systemów operacyjnych Windows Server oraz Windows pozwalająca na wirtualizację. Szczególnie interesującym składnikiem dla założeń budowy komponentowego centrum przetwarzania danych jest wirtualizacja środowisk serwerowych.

Niezwykle dynamiczny rozwój technologii wirtualizacyjnych spowodował, że w obecnej chwili wykorzystują je praktycznie wszystkie duże centra przetwarzania. Trudno sobie też wyobrazić inny model dla tych największych Data Center, obsługujących miliony użytkowników.

Szczególnie zalecaną wersją w takich przypadkach jest Windows Server Datacenter, pozwalający na tworzenie nielimitowanej liczby maszyn wirtualnych na fizycznym serwerze. Oczywistym składnikiem środowisk wirtualnych jest też System Center Datacenter, którego funkcje opisano w jednym z rozdziałów.

Wirtualizacja na bazie Hyper-V ma szczególne znaczenie w budowie centrów przetwarzania w modelu chmury prywatnej zgodnie z metodyką Dynamic Datacenter i rozwiązaniach hybrydowych z wykorzystaniem własnej infrastruktury i usług platformowych z chmury publicznej – np. Windows Azure. Takie połączenie pozwala na bardzo wysoką elastyczność bezpiecznego przenoszenia maszyn wirtualnych nie tylko pomiędzy własnymi maszynami fizycznymi, ale też środowiskiem Windows Azure i własnym centrum przetwarzania.

Głównymi obszarami wirtualizacji Hyper-V są maszyny wirtualne, sieci wirtualne i wirtualne zasoby dyskowe.

4.16.2. WIRTUALIZACJA ŚRODOWISK KLIENCKICH (VDI)

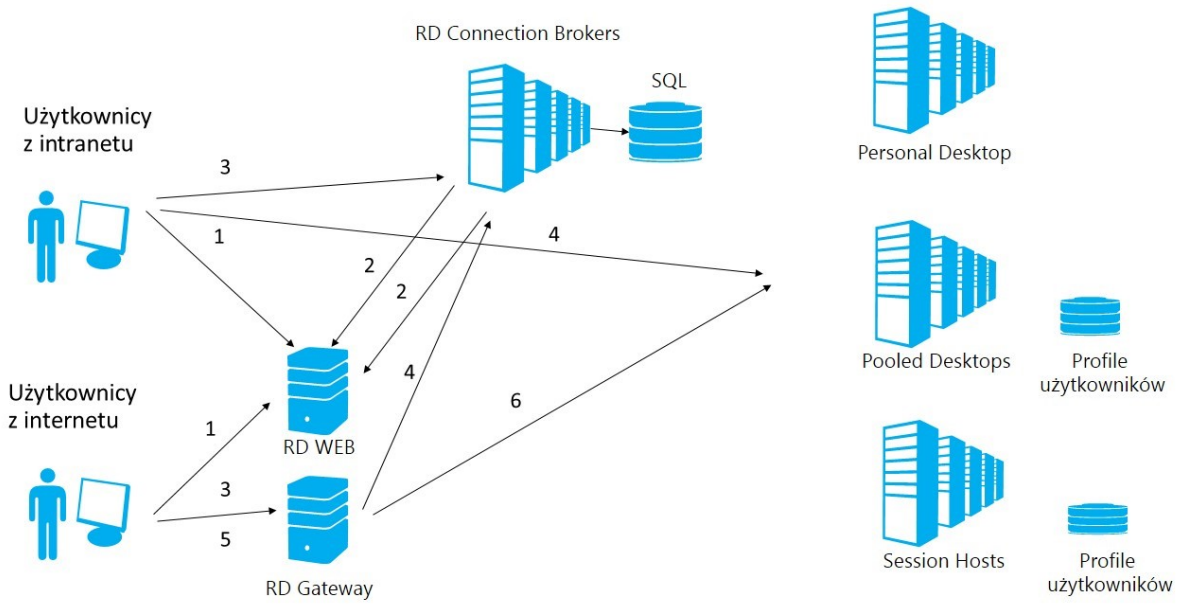
Jednym z typowych zastosowań mechanizmu Hyper-V jest wirtualizacja środowisk klienckich (*Virtual Desktop Infrastructure* VDI). VDI umożliwia uruchomienie klienckich systemów operacyjnych Windows jako maszyn wirtualnych na serwerach w centrum przetwarzania.

Użytkownik ma do nich dostęp z komputera PC, cienkiego klienta lub innych urządzeń klienckich spełniających wymagania.

W rozwiązaniu takim wykorzystywany jest standardowy mechanizm Hyper-V będący usługą Windows Server wraz z usługą *Remote Desktop Services* (RDS). Wdrożenie tego typu rozwiązania jest wspomagane przez *Microsoft Desktop Optimization Pack* (MDOP) oraz *System Center Management Suite*.

W ramach rozwiązania VDI dostępne są trzy scenariusze użycia:

- Środowiska dostępne w ramach sesji RDS.
- Dostęp do współdzielonych maszyn wirtualnych.
- Dostęp do dedykowanych użytkownikowi maszyn wirtualnych.



Przy wyborze jednego z dostępnych scenariuszy trzeba wyważyć wymagania użytkowników wynikające z funkcjonalności i bezpieczeństwa. Na przykład, częstym scenariuszem hybrydowym jest dostarczenie dedykowanych maszyn wirtualnych, wymagających dużych zasobów (przestrzeni dyskowej, zasobów serwerowych) kadrze kierowniczej i specjalnym użytkownikom, a reszcie użytkowników – maszyn współdzielonych.

Microsoft Desktop Virtualization upraszcza zarządzanie poprzez połączenie środowiska IT w jedną infrastrukturę obejmującą zarówno zasoby fizyczne, jak i wirtualne. Umożliwia błyskawiczne dostarczenie aplikacji i środowisk roboczych, co pozwala nowym użytkownikom na natychmiastowe rozpoczęcie pracy. Dodatkowo umożliwia działowi IT udostępnianie starszych aplikacji zgodnych z wcześniejszymi wersjami klienckich systemów

operacyjnych. Dzięki narzędziom zarządzającym System Center, Microsoft Desktop Virtualization automatycznie wykrywa konfigurację urządzeń i stan sieci, aby dostarczyć każdemu użytkownikowi najbardziej dopasowaną usługę w ramach przysługujących mu uprawnień.

5. ROZWIĄZANIA Z CHMURY - PIERWSZY WYBÓR

Jednym z ważnych założeń planowania komponentowej architektury teleinformatycznej powinna być zasada oparcia się na rozwiązaniach, które mogą być budowane w ramach własnej infrastruktury, jak też hostowane przez różnych dostawców lub inne organizacje. Model taki pozwala elastycznie decydować – czy budujemy dany komponent sami, licząc się z ryzykiem projektu, czasem wdrożenia i kosztami utrzymania, czy zamawiamy wymaganą funkcjonalność na zewnątrz – jako usługę.

Założeniem praktycznie wszystkich dostępnych obecnie produktów Microsoft jest możliwość wykorzystania ich zarówno poprzez klasyczną implementację w ramach własnej infrastruktury (*on-premise*), jak i pozyskanie opartej na nich funkcjonalności w trybie hostowanej usługi. w modelu usługowym można skorzystać z oferty chmury publicznej *Microsoft Cloud*[78], jak też z oferty partnerów Microsoft, bardzo zróżnicowanej w zakresie funkcjonalnym i wydajnościowym.

Przy korzystaniu usług z „chmury" możliwe jest też integrowanie usług własnej i hostowanej infrastruktury, co w przypadku produktów Microsoft jest proste i nieobarczone ryzykiem kłopotów techniczno-organizacyjnych.

Taki mieszany model będzie najprawdopodobniej najczęściej wybierany, choćby z powodu już istniejących w organizacji rozwiązań. Za każdym razem istnieje jednak możliwość wyboru:

- zakup aplikacji jako pakietu usług (Microsoft Cloud),
- zakup platformy jako pakietu usług (Microsoft Cloud),
- zakup aplikacji jako pakietu usług (Partner Microsoft),
- zakup platformy jako pakietu usług (Partner Microsoft),
- oparcie się o własne zasoby,

[78] https://azure.microsoft.com/pl-pl/overview/what-is-azure/

- połączenie tych modeli.

Dostępne są w tej chwili modele oparte o własną infrastrukturę, chmurę publiczną i chmurę prywatną.

Usługi z chmury Microsoft są połączeniem znanych, standardowych technologii oraz zaawansowanych rozwiązań organizacyjno-technicznych w centrach przetwarzania wspartych najwyższym dostępnym poziomem bezpieczeństwa.

Poniżej prezentujemy przykładowe scenariusze wykorzystania usług chmury publicznej Microsoft.

Typ zadania	**Sposób realizacji**
Zdalna praca zespołowa Komunikacja Spotkania Wspólna praca z dokumentami, konferencje	***Microsoft Teams*** Komunikacja typu chat, głosowa, wideo, dzielenie się dokumentami i aplikacjami, wspólna praca na dokumentach, telekonferencje, transmisja spotkań, udostępnianie pulpitu – w modelach jeden do jeden, jeden do wielu i wielu do wielu. Daje możliwość: n. komunikacji tekstowej, o. komunikacji audio i video, p. prowadzenia telekonferencji, q. składowania dokumentów, r. tworzenia notatek, s. korespondencji poczt elektronicznej, t. inicjacji dokumentów w oparciu o pakiet biurowy, u. panowania czasu pracy i spotkań, v. przydzielanie zadań członkom zespołu, w. konfiguracja powiadomień i najważniejszych informacji w interfejsie użytkownika.

Typ zadania	Sposób realizacji
	Dostępne z dowolnego urządzenia typu komputer, tablet, smartphone. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5
Praca zdalna z komputera w domu	***Pulpit wirtualny systemu Windows*** Umożliwia pracę zdalną na maszynie wirtualnej osadzonej na platformie Azure. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE Usługa w podstawowej konfiguracji dostępna bezpłatnie dla celów walki i zapobiegania COVID-19 bezpłatnie w okresie 6-ciu miesięcy.
Wirtualna informacja (BOT) - dla opieki zdrowotnej - dla dowolnych jednostek administracji	Azure Bot Wirtualni asystenci udzielający odpowiedzi na pytania zadawane językiem naturalnym. Dzięki komponentom uczenia maszynowego umożliwiają szybkie stworzenie efektywnych narzędzi informujących. Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Wirtualna pomoc	***Microsoft Teams***

Typ zadania	Sposób realizacji
zdrowotna Wirtualna wizyta w urzędzie	Umożliwiająca wirtualne spotkanie z lekarzem czy urzędnikiem komunikacja typu chat, głosowa, wideo, dzielenie się dokumentami. Dostępne z dowolnego urządzenia typu komputer, tablet, smartphone. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5
Obiegi dokumentów	***Microsoft Office 365*** Pozwala na tworzenie procesów workflow stałych i ad-hoc wraz z ścieżkami akceptacyjnymi i wykorzystaniem podpisu elektronicznego od zewnętrznego dostawcy. Podstawowymi elementami obiegu informacji i dokumentów są następujące struktury, opierające się na komponencie SharePoint Online: - repozytoria dokumentów i wzorów dokumentów elektronicznych, - repozytoria metadanych słownikowych i słów kluczowych, - środowisko definiowania i zarządzania metadanymi i ich zestawami, - środowisko definiujące zasady zarządzania dokumentami i cyklem ich życia, - silnik obiegu informacji (*Workflow*),

Typ zadania	Sposób realizacji
	- formularze elektroniczne (wzory dokumentów), - narzędzia wyszukiwania informacji i dokumentów. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5
Pierwsza linia wsparcia dla pracowników dla obywateli	***Microsoft Teams*** Możliwość utworzenia centrów wsparcia i konsultacji dla dowolnych procesów, zarówno w zakresie informacji jak i wsparcia zdalnego. Komunikacja typu chat, głosowa, wideo, dzielenie się dokumentami udostępnianie pulpitu. Dostępne z dowolnego urządzenia typu komputer, tablet, smartphone. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5
Zdalna nauka	***Microsoft Teams*** Usługi Microsoft Teams i Office 365 ułatwiają naukę z domu dzięki możliwości prowadzenia połączeń grupowych i indywidualnych, a także współpracy w czasie rzeczywistym z aplikacjami pakietu Office dla sieci Web, w tym Word, Excel i PowerPoint.

Typ zadania	Sposób realizacji
	Możliwość organizacji testów i sprawdzania wiedzy. Dla nauczycieli dostępne są obszerne szkolenia wspierające uczenie zdalne, za pomocą seminariów internetowych i pomocy technicznej społeczności programu Microsoft Educator. Komunikacja typu chat, głosowa, wideo, dzielenie się dokumentami udostępnianie pulpitu. Dostępne z dowolnego urządzenia typu komputer, tablet, smartphone. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5
Tożsamość cyfrowa uczniów	***Azure Active Directory*** Jednym z większych wyzwań powodujących nadmierne nakłady pracy w jednostkach edukacyjnych każdego szczebla jest konieczność „ręcznego” wpisywania danych ucznia do kilku różnych systemów. Osadzenie uzupełnialnego na poszczególnych etapach cyfrowego profilu danych ucznia w Azure AD umożliwiłoby automatyzację tego procesu i wprowadzenie zasad niezaprzeczalności. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5 Azure

Typ zadania	Sposób realizacji
Koordynacja działań z pracownikami terenowymi	***Power Apps*** Narzędzia pozwalające na szybkie utworzenie aplikacji mobilnych dla pracowników w terenie dla kontaktu, dostarczania informacji (dwukierunkowo), wysyłania zleceń, potwierdzania wykonania, włączenie komponentu geolokalizacji i map. Dostępne wsparcie zespołów Microsoft. Zawarte w produktach: PowerApps Pakiety Azure w licencjonowaniu CSP, AD, SCE
Bezpieczna poczta elektroniczna	***Microsoft 365 i Office 365*** Gotowa usługa poczty elektronicznej oparta o Exchange Online wraz zarządzaniem czasem poprzez kalendarze użytkowników i planowaniem spotkań. Zawiera usługę bezpiecznego uwierzytelnienia AAD. Dostępne szkolenia i wsparcie wdrożenia. Zawarte w produktach: Microsoft 365 E3, E5, A3 i A5 Office 365 E1, E3, E5, A1, A3, A5

Typ zadania	Sposób realizacji
Maszyny wirtualne	***Azure*** Jedną z podstawowych usług infrastrukturalnych w Azure są wirtualne serwery pozwalające wykorzystać system operacyjny Windows Server jak i liczne dystrybucje systemu Linux. Maszyny wirtualne – wraz z innymi usługami infrastrukturalnymi (sieci, storage, monitorowanie, usługi bezpieczeństwa) – umożliwiają efektywne wdrożenie rozwiązania zbudowanego w oparciu o 'klasyczną' architekturę (w przeciwieństwie do chmurowych wzorców architektonicznych. Pozwala to w szczególności na błyskawiczne uruchomienie rozwiązań projektowanych z myślą o wdrożeniu we własnej serwerowni oraz wszelkie warianty wdrożenia hybrydowego (część komponentów we własnej serwerowni, część w Azure – choćby z przyczyn wydajnościowych). Więcej informacji o usłudze maszyn wirtualnych można znaleźć pod poniższym linkiem: https://azure.microsoft.com/pl-pl/services/virtual-machines/ Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Środowiska testowe i rozwojowe	***Azure*** Środowiska testowo-rozwojowe oparte o Azure tworzą (bo pozostające poza infrastrukturą klienta), szybkie w uruchomieniu i konfiguracji oraz skalowalne zgodnie z potrzebami środowisko uruchamiania środowisk deweloperskich i testowych. Środowisko może zostać wydzielone dla wykonawcy lub kilku wykonawców. Scenariusz taki jest możliwy zarówno dla procesu wytwórczego wspartego narzędziami Visual Studio (możliwa pełna kontrola nad

Typ zadania	Sposób realizacji
	bezpieczeństwem i poprawnością procesu wytwórczego wykonawcy lub kilku wykonawców) jak i osadzania gotowych prototypów rozwiązań dostawców. Drugim etapem wykorzystania takich środowisk są testy funkcjonalne i wydajnościowe, a po ich zakończeniu gotowe aplikacje (usługi) mogą być, dzięki wsparciu narzędzi Azure, przenoszone do środowisk produkcyjnych na Azure lub on-premise. Środowiska te dodatkowo umożliwiają efektywną kosztowo realizację typowego scenariusza rozwoju aplikacji, gdzie po zakończeniu testów maszyny wirtualne podlegają zamrożeniu (z minimalną opłatą związaną z ich przechowywaniem), a przy rozpoczęciu następnego cyklu rozwojowego są ponownie uruchamiane – w gotowej postaci tożsamej ze środowiskami produkcyjnymi. Scenariusze takie dotyczą procesu wytwórczego dedykowanych aplikacji (.Net i open source) oraz aplikacji opartych o oprogramowanie standardowe. Zalety: 1. błyskawiczne tempo uruchamiania środowisk, 2. praktycznie nieograniczona skalowalność, 3. niskie koszty wytworzenia i eksploatacji, 4. bezpieczna separacja od środowisk produkcyjnych, 5. wsparcie dla przenoszenia do środowisk produkcyjnych, 6. efektywne kosztowo przechowywanie „zamrożonych” środowisk testowo – rozwojowych,

Typ zadania	Sposób realizacji
	7. zespół narzędzi analizy zachowania aplikacji. Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Bezpieczny magazyn danych	***Azure*** Pozwala na szybkie utworzenie bezpiecznych przestrzeni na dane archiwalne (w tym miejsce na backup) lub współpracujące z maszynami wirtualnymi to w szczególności na błyskawiczne uruchomienie rozwiązań wdrożenia hybrydowego (część komponentów we własnej serwerowni, część w Azure). Więcej informacji można znaleźć pod poniższym linkiem: Magazyn dysków Usługa Azure Backup Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Moc obliczeniowa	***Azure*** Pozwala na szybkie utworzenie i konfigurację szerokiego zakresu komponentów systemów informatycznych, takich jak: Aprowizacja maszyn wirtualnych z systemami Windows i Linux w kilka sekund. Uproszczenie wdrażania i obsługi platformy Kubernetes oraz zarządzania nią. Opracowywanie mikro usług i organizowanie kontenerów w systemie Windows lub Linux. Szybko twórz zaawansowane internetowe i mobilne aplikacje w chmurze.

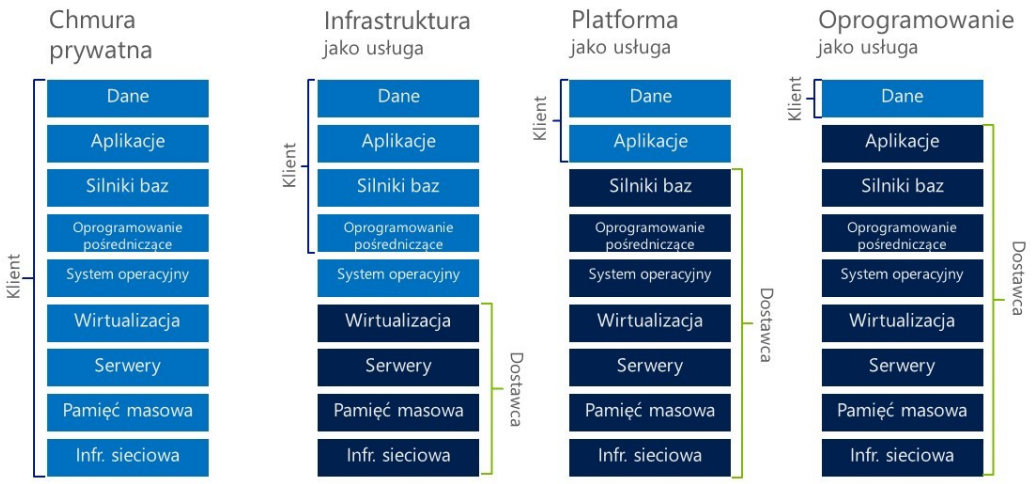
Typ zadania	Sposób realizacji
	Tworzenie, używanie oraz optymalizowanie klastrów HPC i dużych klastrów obliczeniowych w dowolnej skali oraz zarządzanie nimi. Natywnie uruchamiaj obciążenia VMware na platformie Azure. Dedykowany serwer fizyczny do hostowania maszyn wirtualnych platformy Azure dla systemów Windows i Linux. Więcej informacji można znaleźć pod poniższym linkami: Virtual Machines Azure Kubernetes Service (AKS) Service Fabric App Service Azure CycleCloud Rozwiązanie Azure VMware firmy CloudSimple Dedykowany host platformy Azure Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Usługi aplikacyjne	***Azure*** Szybkie tworzenie całych rozwiązań i usług takich jak: Zaawansowane internetowe i mobilne aplikacje w chmurze. Proste i bezpieczne interfejsy API lokalizacji umożliwiają dodawanie kontekstu geoprzestrzennego do danych. Wysyłanie powiadomień wypychanych dla każdej platformy, z dowolnego zaplecza. Bezpieczne publikowanie interfejsów API dla deweloperów,

Typ zadania	Sposób realizacji
	partnerów i pracowników w odpowiedniej skali. Tworzenie, testowanie, monitorowanie aplikacji mobilnych i klasycznych. Szybsze tworzenie aplikacji mobilnych z obsługą chmury. Więcej informacji można znaleźć pod poniższym linkami: App Service Azure Maps Notification Hubs API Management Centrum aplikacji programu Visual Studio Xamarin Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Usługi bezpieczeństwa dla rozwiązań własnych i w chmurze	***Azure*** Szybkie wdrażanie zaawansowanych usług bezpieczeństwa danych i usług takich jak: Synchronizowanie katalogów lokalnych i obsługa logowania jednokrotnego. Lepsza ochrona poufnych informacji — zawsze i wszędzie. Przyłącz maszyny wirtualne platformy Azure do domeny bez kontrolerów domeny. Ochrona i zachowywanie kontroli nad kluczami i innymi wpisami tajnymi.

Typ zadania	Sposób realizacji
	Uzyskaj ujednolicone zarządzanie zabezpieczeniami i zaawansowaną ochronę przed zagrożeniami w obciążeniach chmury hybrydowej. Zarządzaj w chmurze używanymi sprzętowymi modułami zabezpieczeń. Więcej informacji można znaleźć pod poniższym linkami: Azure Active Directory Azure Information Protection Azure Active Directory Domain Services Key Vault Security Center Dedykowany moduł HSM platformy Azure Zawarte w produktach: Pakiety Azure w licencjonowaniu CSP, AD, SCE
Wsparcie techniczne	***Premier Support*** Wsparcie techniczne proaktywne i reaktywne dla technologii Microsoft. Zawarte w produktach: Pakiety Premier Support

5.1. USŁUGA AZURE

Usługa Microsoft Azure[79] to platforma przetwarzania w chmurze, która umożliwia łatwe, bezpieczne i szybkie tworzenie oraz uruchamianie własnych aplikacji. Ogólnie mówiąc możemy potraktować ją jako wysokodostępne, skalowalne i bezpieczne zewnętrzne centrum przetwarzania danych, wyposażonych we wszystkie niezbędne elementy do uruchamiania aplikacji, utrzymania i monitorowania systemu, składowania danych (backup) i mechanizmów bezpieczeństwa na styku z Internetem. Wśród wszystkich podstawowych modeli przetwarzania w chmurze, Azure może realizować wszystkie trzy (IAAS, PAAS, SAAS). Poniższy rysunek przedstawia typowy podział zadań między dostawcę usługi i jego klienta w tych modelach.



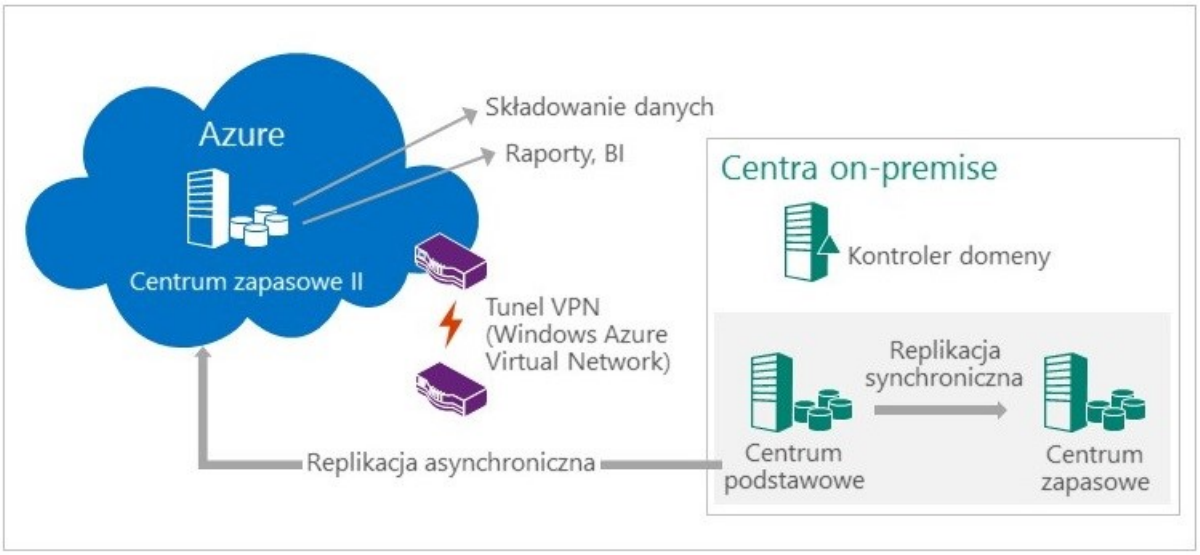
Platforma Azure to jedyna duża platforma chmury oceniana przez firmę Gartner jako jednoczesny lider usług IaaS (infrastruktury jako usługi) i PaaS (platformy jako usługi). Opiera się na rosnącej globalnej sieci centrów danych zarządzanych przez firmę Microsoft w 19 regionach. Dzięki temu spełnione są postulaty bezpieczeństwa danych rozproszonych geograficznie, a jednocześnie dostęp do usług nie jest limitowany zbyt dużą odległością. Dodatkowo, mając na uwadze specyficzne regulacje prawne, firma Microsoft daje klientom możliwość określenia, w jakich regionach mają być przechowywane i przetwarzane ich dane. Na przykład, uruchamiając usługę na Azure można zastrzec sobie możliwość korzystania tylko

[79] http://azure.microsoft.com/pl-pl/

i wyłącznie z Europejskich centrów przetwarzania położonych w Amsterdamie i Dublinie. Liczba usług w ramach Microsoft Azure rośnie praktycznie, co miesiąc, w związku z tym ograniczymy się do przedstawienia tych najpopularniejszych, które mogą być przyczynkiem do budowy komponentowego modelu usług IT. Poniżej przedstawimy skróconą listę dostępnych usług, które można wybrać z witryny Azure[80]:

Wiele ze scenariuszy wykorzystania Microsoft Azure jest szczegółowo opisanych, a co więcej posiadają one wsparcie odpowiednich narzędzi wraz planami wsparcia technicznego. Przykładowo uruchomienie farmy serwerów SharePoint polega na wyborze odpowiedniego scenariusza, dzięki czemu po kliknięciu tworzy się farma wielofunkcyjnego portalu, składająca się z dziewięciu maszyn.

Bardzo ciekawym i dobrze oprzyrządowanym scenariuszem jest tworzenie centrum zapasowego w chmurze dla prywatnego centrum przetwarzania. Ogólną idee takiej usługi przedstawia poniższy rysunek.



Jedną z najszerzej wykorzystywanych funkcji Azure jest Azure Active Directory (AAD), czyli usługa zarządzania tożsamością i dostępem w chmurze. Pozwala więc ona na wykorzystanie większości funkcji AD, bez budowy całej związanej z tym infrastruktury i jej utrzymania. Usługa ta test też podstawą infrastrukturalną dla wszystkich pozostałych funkcjonalności chmury Microsoft.

[80] https://docs.microsoft.com/pl-pl/azure/

Dodatkowo AAD oferuje gotowe mechanizmy w zakresie:

- Wieloskładnikowego uwierzytelniania.
- Opartego na unikalnych poświadczeniach z własnego AD uwierzytelnienia do aplikacji posiadających jedno konto dostępowe.
- Raportowania i powiadamiania o zagrożeniach umożliwiającego ich stały monitoring.
- Zaawansowanej samoobsługi użytkowników, między innymi resetu hasła, zarządzania uprawnieniami w grupach czy też delegacji uprawnień.
- Zarządzania tożsamością dla systemów własnych i usług w chmurze.

Istotnym zagadnieniem dla każdego kto podejmuje decyzję o wykorzystaniu konkretnej usługi jest możliwość potencjalnego przeniesienia w przyszłości budowanych usług i danych do innych środowisk – na przykład wskutek potrzeby zmiany dostawcy centrum przetwarzania. Niezbędne jest w takim przypadku oparcie się o standardowe rozwiązania, które pozwalają na dokonanie takiej operacji – w szczególności oparcie się o ogólnie przyjęte standardy. Usługa Azure oparta jest na standardach przemysłowych w zakresie norm bezpieczeństwa i dostępności, przenoszenia danych i komunikacji, interoperacyjności, narzędzi programistycznych czy stosowania na tej platformie wielu różnych standardowych technologii. Wykorzystywane są między innymi takie standardy jak:

- ISO 27001, ISO 27002, ISO 27017, ISO 27018,
- TDS (tabular data stream),
- Open Authentication Standard – OAuth,
- OData,
- REST API.

W zakresie interoperacyjności:

- HTTP(S),
- XML wraz z XAdES,
- SOAP,
- Docker.

W zakresie programowania

- Java,
- .NET,
- PHP,
- Python,
- Język C,
- Node.js,
- Visual Studio & Eclipse tools.

Możliwe jest wykorzystanie standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB czy mojo.

Dodatkowo stosowane są w Azure rozwiązania typu AMQPS, MQTT, DataLake – U-SQL, Stream Analitics – T-SQL, Hadoop – R Server, R Scripting/Spark czy MapReduce.

5.1.1. PRZYKŁADOWE SCENARIUSZE UŻYCIA AZURE

Możliwości wykorzystania usług Azure są praktycznie nieograniczone. Poniżej przedstawiamy kilka przykładów scenariuszy wykorzystania tych usług w postaci generycznej, bazującej na gotowych mechanizmach tej platformy[81].

5.1.1.1. ZARZĄDZANIE TOŻSAMOŚCIĄ UŻYTKOWNIKÓW – AAD

Jedną z najszerzej wykorzystywanych funkcji Azure jest Azure Active Directory (AAD), czyli usługa zarządzania tożsamością i dostępem w chmurze. Pozwala więc ona na wykorzystanie większości funkcji AD, bez budowy całej związanej z tym infrastruktury i jej utrzymania. Usługa ta test też podstawą infrastrukturalną dla wszystkich pozostałych funkcjonalności chmury Microsoft.

Dodatkowo AAD oferuje gotowe mechanizmy w zakresie:

- wieloskładnikowego uwierzytelniania;

[81] *Scenariusze przygotowane przez zespół Piotr Boniński, Marcin Fryzik, Tomasz Kopacz, Paweł Walczak – Microsoft 2016*

- opartego na unikalnych poświadczeniach z własnego AD uwierzytelnienia do aplikacji posiadających jedno konto dostępowe;
- raportowania i powiadamiania o zagrożeniach umożliwiającego ich stały monitoring;
- zaawansowanej samoobsługi użytkowników, między innymi resetu hasła, zarządzania uprawnieniami w grupach czy też delegacji uprawnień;
- zarządzania tożsamością dla systemów własnych i usług w chmurze.

Istnieje wiele scenariuszy funkcjonalnych, dla których uzasadnione jest wykorzystanie usługi przechowujące informacje o tożsamości użytkowników opartej o infrastrukturę wyniesioną do zewnętrznego centrum przetwarzania. Przykładami takich scenariuszy są:

1. Udostępnianie naszych usług i danych użytkownikom zewnętrznym, zwykle za pośrednictwem sieci Internet. w większości przypadków musimy zapewnić niezaprzeczalność i bezpieczeństwo takiego dostępu na bazie usługi katalogowej i zarządzania prawami dostępu użytkowników. Jednocześnie dobrą praktyką jest wyizolowanie takiej usługi katalogowej od usługi obsługującej użytkowników wewnętrznych. Oznacza to konieczność zbudowania własnej infrastruktury usługi zarządzania tożsamością i dostępem i utrzymanie jej lub skorzystanie z gotowego rozwiązania takiego jak Azure Active Directory (AAD).
2. Budowa systemu na bazie hostowanej usługi platformowej (np. Azure), gdzie najprościej jest wykorzystać usługę katalogową dostarczaną z platformą.
3. Izolacja użytkowników mobilnych dostających się do zasobów wewnętrznych poprzez Internet. Użycie usługi katalogowej z chmury daje możliwość niezaprzeczalnego dostępu do takich zasobów, weryfikowanego poza systemami wewnętrznymi.
4. Projekty krótkotrwałe, w których trzeba zapewnić niezaprzeczalność praw dostępu do danych i usług, a nie opłaca się na krótki okres budować specjalnej, wydzielonej infrastruktury.
5. Uwierzytelnianie użytkowników do zewnętrznej usługi lub pomiędzy różnymi systemami w modelu pojedynczego logowania (single sign-on).

Poza oczywistą korzyścią korzystania z gotowej, sprawdzonej i audytowanej usługi, AAD posiada wszystkie funkcje pozwalające na posługiwanie się tożsamością cyfrową. Co więcej możliwe jest bezpieczne tworzenie środowisk hybrydowych, w których bazując na uwierzytelnieniu użytkownika poprzez własną usługę katalogową, logujemy się do systemów bazujących na AAD zawierającego profil tego samego użytkownika. Można tu wykorzystać dwa scenariusze:

- Stworzenie relacji wzajemnego zaufania pomiędzy AD i AAD.
- Wykorzystanie mechanizmu bazującego skrócie skrótu tokenu generowanego przez AD i uwierzytelnianiu użytkownika na tej bazie w AAD.

Takie wykorzystanie AAD może też być przydatne, kiedy organizacja korzysta z jednego konta w dowolnej zewnętrznej usłudze (np. Facebook). Pozwala na zalogowanie się do niej każdego uprawnionego użytkownika poprzez własne, organizacyjne poświadczenia, które w AAD są mapowane na zdefiniowane uprzednio poświadczenia do zewnętrznej usługi, eliminując konieczność przekazywania użytkownikom tego samego loginu i hasła.

Dużym ułatwieniem dla administratorów jest to, że AAD zawiera mechanizmy samoobsługi użytkowników, np. zmiana hasła, reset hasła czy tworzenie grup użytkowników na bazie udzielonych uprawnień.

Dodatkowo AAD posiada wbudowane, definiowalne mechanizmy uwierzytelniania wieloskładnikowego, co może być wykorzystane w dowolnych scenariuszu dla ochrony danych wrażliwych.

Mechanizmy zarządzania tożsamością w AAD można zastosować w połączeni z praktycznie dowolnymi środowiskami własnymi czy aplikacjami dzięki zastosowaniu standardowych protokołów takich jak SAML 2.0, WS-Federation, czy OpenID Connect. Poprzez wsparcie dla OAuth 2.0 możliwe jest pisanie własnych aplikacji i interfejsów komunikacyjnych wykorzystujących AAD.

Przydatnym rozwiązaniem jest to, że niekoniecznie musimy wykorzystywać certyfikaty do uwierzytelniania z CA będącego składową AAD. Możemy zastosować własne certyfikaty, z całą konsekwencją konieczności obsługi życia certyfikatu.

5.1.1.2. WIRTUALNE MASZYNY W AZURE

Jedną z podstawowych usług infrastrukturalnych w Azure są wirtualne serwery pozwalające wykorzystać system operacyjny Windows Server jak i liczne dystrybucje systemu Linux.

Maszyny wirtualne – wraz z innymi usługami infrastrukturalnymi (sieci, storage, monitorowanie, usługi bezpieczeństwa) – umożliwiają efektywne wdrożenie rozwiązania zbudowanego w oparciu o 'klasyczną' architekturę (w przeciwieństwie do chmurowych wzorców architektonicznych. Pozwala to w szczególności na błyskawiczne uruchomienie rozwiązań projektowanych z myślą o wdrożeniu we własnej serwerowni oraz wszelkie warianty wdrożenia hybrydowego (część komponentów we własnej serwerowni, część w Azure – choćby z przyczyn wydajnościowych).

Więcej informacji o usłudze maszyn wirtualnych można znaleźć pod poniższym linkiem:

https://azure.microsoft.com/pl-pl/services/virtual-machines/

Warto tu podkreślić, że tworząc maszynę w Azure, możemy bazować na jednym z tysięcy predefiniowanych obrazów takich maszyn, w szczególności z preinstalowanym oprogramowaniem systemowym typu bazy danych, serwery aplikacyjne, mechanizmy bezpieczeństwa. w przypadku oprogramowania Microsoft, takiego jak Windows Server, SQL Server czy Biztalk Server – może ono być w pełni licencjonowane z Azure, bez konieczności posiadania na nie licencji a priori przez klienta.

5.1.1.3. PRZESTRZEŃ DO SKŁADOWANIA DANYCH

Platforma Azure oferuje szereg różnych mechanizmów do składowania danych, optymalnych pod różne scenariusze wykorzystania. Poniższa tabela przedstawia główne rodzaje tej przestrzeni, wraz z linkami do dokładniejszej dokumentacji.

Scenariusz	**Rodzaj storage**
Skalowalny i bezpieczny magazynu dla dysków maszyn wirtualnych	Magazyn dysków
Skalowalny i bezpieczny magazynu dla maszyn ogólnego przeznaczenia	Blob Storage

Scenariusz	Rodzaj storage
Skorzystaj z ekonomicznego przechowywania danych rzadko używanych	Magazyn archiwum
Magazyn dla komunikacji między aplikacjami opartej na komunikatach	Queue Storage
Urządzenia i rozwiązania do transferu danych na platformę Azure i do funkcji obliczeniowej Edge	Data Box
Zaawansowane udziały plików, dostępne również natywnymi mechanizmami systemu Linux	Azure NetApp Files
Buforowanie plików na potrzeby obliczeń o wysokiej wydajności (HPC)	Azure HPC Cache

5.1.1.4. MOC OBLICZENIOWA

Rodzaj storage	Scenariusz
Virtual Machines	Aprowizacja maszyn wirtualnych z systemami Windows i Linux w kilka sekund
Azure Kubernetes Service (AKS)	Uproszczenie wdrażania i obsługi platformy Kubernetes oraz zarządzania nią
Service Fabric	Opracowywanie mikro usług i organizowanie kontenerów w systemie Windows lub Linux
App Service	Szybko twórz zaawansowane internetowe i mobilne aplikacje w chmurze
Azure CycleCloud	Tworzenie, używanie oraz optymalizowanie klastrów HPC i dużych klastrów obliczeniowych w dowolnej skali oraz

Rodzaj storage	Scenariusz
	zarządzanie nimi
Rozwiązanie Azure VMware firmy CloudSimple	Natywnie uruchamiaj obciążenia VMware na platformie Azure
Dedykowany host platformy Azure	Dedykowany serwer fizyczny do hostowania maszyn wirtualnych platformy Azure dla systemów Windows i Linux

5.1.1.5. USŁUGI SKŁADOWANIA DANYCH

Rodzaj storage	Scenariusz
Konta magazynu	Niezawodny magazyn danych w chmurze o wysokim stopniu dostępności i skalowalności
Usługa Azure Backup	Uprość ochronę danych przed oprogramowaniem wymuszającym okup
Data Box	Urządzenia i rozwiązania do transferu danych na platformę Azure i do funkcji obliczeniowej Edge
Avere vFXT for Azure	Uruchamiaj oparte na plikach obciążenia o wysokiej wydajności w chmurze
Azure NetApp Files	Udziały plików platformy Azure klasy korporacyjnej obsługiwane przez usługę NetApp

5.1.1.6. USŁUGI APLIKACYJNE

Rodzaj storage	Scenariusz
App Service	Szybko twórz zaawansowane internetowe i mobilne aplikacje w chmurze

Rodzaj storage	Scenariusz
Azure Maps	Proste i bezpieczne interfejsy API lokalizacji umożliwiają dodawanie kontekstu geoprzestrzennego do danych
Notification Hubs	Wysyłanie powiadomień wypychanych dla każdej platformy, z dowolnego zaplecza
API Management	Bezpieczne publikowanie interfejsów API dla deweloperów, partnerów i pracowników w odpowiedniej skali
Centrum aplikacji programu Visual Studio	Twórz, testuj, wydawaj i monitoruj swoje aplikacje mobilne i klasyczne w sposób ciągły
Xamarin	Szybsze tworzenie aplikacji mobilnych z obsługą chmury

5.1.1.7. SIEĆ

Rodzaj storage	Scenariusz
Content Delivery Network	Bezpieczne i niezawodne dostarczanie zawartości o szerokim zasięgu globalnym
System DNS Azure	Hostowanie domeny systemu DNS na platformie Azure
Traffic Manager	Kierowanie ruchem przychodzącym w celu uzyskania wysokiej wydajności i dostępności
Load Balancer	Zapewnij swoim aplikacjom wysoką dostępność i wydajność sieci
VPN Gateway	Ustanawianie bezpiecznej łączności między środowiskami lokalnymi
Application Gateway	Tworzenie bezpiecznych, skalowalnych frontonów internetowych o wysokiej dostępności na platformie

Rodzaj storage	Scenariusz
	Azure
Ochrona przed atakami DDoS na platformie Azure	Chroń aplikacje przed atakami DDoS (Distributed Denial of Service, rozproszona odmowa usługi)
Network Watcher	Rozwiązanie do monitorowania i diagnostyki wydajności sieci
Azure Firewall	Natywne niewymagające obsługi funkcje zapory o wysokiej dostępności i nieograniczonej skalowalności w chmurze
Wirtualna sieć WAN	Optymalizacja i automatyzacja łączności między oddziałami za pośrednictwem platformy Azure
Azure Front Door	Skalowalny punkt dostarczania z rozszerzonymi zabezpieczeniami na potrzeby globalnych aplikacji internetowych opartych na mikro usługach
Azure Bastion	Prywatny i w pełni zarządzany dostęp RDP i SSH do maszyn wirtualnych

5.1.1.8. USŁUGI DLA SCENARIUSZY HYBRYDOWYCH

Rodzaj storage	Scenariusz
Azure DevOps	Usługi dla zespołów do udostępniania kodu, śledzenia pracy i dostarczania oprogramowania
Usługa ExpressRoute systemu Azure	Dedykowane połączenia światłowodowe sieci prywatnej z systemem Azure
Security Center	Uzyskaj ujednolicone zarządzanie zabezpieczeniami i zaawansowaną ochronę przed zagrożeniami

Rodzaj storage	Scenariusz
	w obciążeniach chmury hybrydowej
Azure Database for PostgreSQL	Zarządzana usługa bazy danych PostgreSQL dla deweloperów aplikacji
Azure Sentinel	Zacznij korzystać z natywnego dla chmury zarządzania informacjami i zdarzeniami zabezpieczeń oraz inteligentnej analizy zabezpieczeń, aby ułatwić ochronę swojego przedsiębiorstwa

5.1.1.9. USŁUGI INTEGRACYJNE

Rodzaj storage	Scenariusz
Logic Apps	Automatyzowanie dostępu do danych i korzystania z nich w ramach wielu chmur bez konieczności pisania kodu
Service Bus	Połączenia między aplikacjami w środowiskach chmur prywatnych i publicznych

5.1.1.10. KONTENERY

Rodzaj storage	Scenariusz
Azure Kubernetes Service (AKS)	Uproszczenie wdrażania i obsługi platformy Kubernetes oraz zarządzania nią
Container Registry	Przechowywanie obrazów kontenerów i zarządzanie nimi w różnych typach wdrożeń platformy Azure
Azure Red Hat OpenShift	W pełni zarządzana usługa OpenShift obsługiwana wspólnie z firmą Red Hat

5.1.1.11. USŁUGI BEZPIECZEŃSTWA

Rodzaj storage	Scenariusz
Azure Active Directory	Synchronizowanie katalogów lokalnych i obsługa logowania jednokrotnego
Azure Information Protection	Lepsza ochrona poufnych informacji — zawsze i wszędzie
Azure Active Directory Domain Services	Przyłącz maszyny wirtualne platformy Azure do domeny bez kontrolerów domeny
Key Vault	Ochrona i zachowywanie kontroli nad kluczami i innymi wpisami tajnymi
Security Center	Uzyskaj ujednolicone zarządzanie zabezpieczeniami i zaawansowaną ochronę przed zagrożeniami w obciążeniach chmury hybrydowej
Dedykowany moduł HSM platformy Azure	Zarządzaj w chmurze używanymi sprzętowymi modułami zabezpieczeń
VPN Gateway	Ustanawianie bezpiecznej łączności między środowiskami lokalnymi
Application Gateway	Tworzenie bezpiecznych, skalowalnych frontonów internetowych o wysokiej dostępności na platformie Azure
Ochrona przed atakami DDoS na platformie Azure	Chroń aplikacje przed atakami DDoS (Distributed Denial of Service, rozproszona odmowa usługi)
Azure Sentinel	Zacznij korzystać z natywnego dla chmury zarządzania informacjami i zdarzeniami zabezpieczeń oraz inteligentnej analizy zabezpieczeń, aby ułatwić ochronę swojego przedsiębiorstwa

5.1.1.12. USŁUGI CIĄGŁOŚCI DZIAŁANIA I AUTOMATYZACJI

Rodzaj storage	Scenariusz
Usługa Azure Backup	Uprość ochronę danych przed oprogramowaniem wymuszającym okup
Azure Site Recovery	Nieprzerwana praca firmy dzięki wbudowanej funkcji odzyskiwania po awarii
Scheduler	Uruchamianie zadań na podstawie prostych lub złożonych powtarzanych harmonogramów
Automation	Uproszczenie zarządzania chmurą poprzez automatyzację procesów
Azure Monitor	Możliwość pełnej obserwacji aplikacji, infrastruktury i sieci
Network Watcher	Rozwiązanie do monitorowania i diagnostyki wydajności sieci

5.1.1.13. AZURE JAKO STANDARDOWY SKŁADNIK PROJEKTU DLA BUDOWY ŚRODOWISK DEVELOPERSKO-TESTOWYCH ORAZ ŚRODOWISK INTERAKCJI Z UŻYTKOWNIKAMI (PODMIOTAMI) ZEWNĘTRZNYMI

Środowiska testowo-rozwojowe oparte o Azure tworzą (bo pozostające poza infrastrukturą klienta), szybkie w uruchomieniu i konfiguracji oraz skalowalne zgodnie z potrzebami środowisko uruchamiania środowisk deweloperskich i testowych. Środowisko może zostać wydzielone dla wykonawcy lub kilku wykonawców. Scenariusz taki jest możliwy zarówno dla procesu wytwórczego wspartego narzędziami Visual Studio (możliwa pełna kontrola nad bezpieczeństwem i poprawnością procesu wytwórczego wykonawcy lub kilku wykonawców) jak i osadzania gotowych prototypów rozwiązań dostawców.

Drugim etapem wykorzystania takich środowisk są testy funkcjonalne i wydajnościowe, a po ich zakończeniu gotowe aplikacje (usługi) mogą być, dzięki wsparciu narzędzi Azure, przenoszone do środowisk produkcyjnych na Azure lub on-premise.

Środowiska te dodatkowo umożliwiają efektywną kosztowo realizację typowego scenariusza rozwoju aplikacji, gdzie po zakończeniu testów maszyny wirtualne podlegają zamrożeniu (z minimalną opłatą związaną z ich przechowywaniem), a przy rozpoczęciu następnego cyklu rozwojowego są ponownie uruchamiane – w gotowej postaci tożsamej ze środowiskami produkcyjnymi.

Scenariusze takie dotyczą procesu wytwórczego dedykowanych aplikacji (.Net i open source) oraz aplikacji opartych o oprogramowanie standardowe.

Zalety:

- Błyskawiczne tempo uruchamiania środowisk.
- Praktycznie nieograniczona skalowalność.
- Niskie koszty wytworzenia i eksploatacji.
- Bezpieczna separacja od środowisk produkcyjnych.
- Wsparcie dla przenoszenia do środowisk produkcyjnych.
- Efektywne kosztowo przechowywanie „zamrożonych" środowisk testowo – rozwojowych.
- Zespół narzędzi analizy zachowania aplikacji.

Niezbędne produkty: Azure MC, Visual Studio.

5.1.1.14. OBNIŻENIE KOSZTÓW STANOWISK DLA PROGRAMISTÓW

Przy tworzeniu oprogramowania ważne jest, aby programista nie miał problemu ze środowiskiem pozwalającym na używanie najnowszych wersji oprogramowania rozmaitych narzędzi. Możliwe jest wykorzystanie „starych" maszyn i zwiększenie ich mocy przy wykorzystaniu Azure. Koszt z modelu Capex przechodzi do Opex.

Ważniejsze cechy:

- Możliwość używania najnowszych wersji Visual Studio bez ryzyka, że wpłynie się na działanie starszych środowisk.
- Możliwość posiadania przygotowanych obrazów per projekt / technologia co bardzo ułatwi pracę, gdy pojedynczy developer opiekuje się wieloma projektami w różnych technologiach/wersjach.

- Niezależność od wieku/typu/parametrów używanych laptopów / ultrabooków.

Używane narzędzia i technologie:

- Visual Studio Enterprise wraz z licencją MSDN pozwalającą właścicielowi na nieograniczone uruchamianie środowisk developerskich i testowych.
- Maszyny wirtualne w Azure oraz DevTest Lab: https://azure.microsoft.com/en-us/documentation/services/devtest-lab/. Zapewniają automatyczne mechanizmy obniżające koszty, takie jak zamykanie instancji, gdy nie są potrzebne, zarządzanie centralnym repozytorium obrazów itp.

5.1.1.15. INFRASTRUKTURA DO WYKONANIA TESTÓW OBCIĄŻENIOWYCH TWORZONYCH APLIKACJI

Testy obciążeniowe są niezbędnym elementem procesu developerskiego, jednak z uwagi na ograniczenia sprzętowe często są pomijane. w oparciu o usługi Azure możliwe jest rozwiązanie, które pozwoli sprawdzić skalowalność tworzonych aplikacji lub aplikacji otrzymywanych od zewnętrznych dostawców.

Ważniejsze cechy:

- Możliwość przetestowania czy aplikacja jest w stanie obsłużyć zadaną liczbę użytkowników.
- Sprawdzenie, jakie muszą być parametry maszyn dla większej / mniejszej liczby użytkowników (by sprawdzić jak aplikacja się skaluje).
- Testy pozwolą także oszacować jakie naprawdę są potrzebne parametry sprzętowe maszyn dla konkretnej liczby użytkowników.
- Zarządzanie procesem testowym co pozwala zapewnić powtarzalność wyników.
- Wykonywane testy można łatwo powtórzyć w sytuacji, gdy kolejna wersja rozwiązania ma dodatkowe funkcjonalności – i warto sprawdzić, czy nie mają one wpływu na wydajność.

Używane narzędzia i technologie:

- Visual Studio Enterprise wraz z licencją MSDN pozwalającą właścicielowi na nieograniczone uruchamianie środowisk developerskich i testowych. w tym stawianie środowisk dla SharePoint Server czy SQL Server.
- Visual Studio Team Services zawierającą usługę Load Test pozwalającą symulować dowolną liczbę klientów aplikacji webowej.
- Azure Virtual Machines pozwalające odwzorować środowisko on-premise na potrzeby testów developerskich.

5.1.1.16. ŚRODOWISKO ODBIORU APLIKACJI OD WYKONAWCÓW, BEZ KONIECZNOŚCI BUDOWANIA FIZYCZNEJ INFRASTRUKTURY DO TESTÓW

W przypadku, gdy aplikacja dostarczana jest na zamówienie przez zewnętrznego dostawcę ważne jest by można było dokładnie sprawdzić, czy spełnia one założone kryteria przed zainstalowaniem ich we własnym centrum przetwarzania. Optymalnym rozwiązaniem jest stworzenie środowiska do testów partnerskiej aplikacji w chmurze. Zakładamy, że rozwiązanie podczas tworzenia udostępniane jest zleceniodawcy w chmurze, dzięki czemu może on na bieżąco monitorować postęp prac a także zgłaszać uwagi doprecyzowujące działanie rozwiązania.

Ważniejsze cechy:

- Możliwość testowania na bieżąco budowanego rozwiązania.
- Nie ma konieczności częstego modyfikowania środowiska we własnym centrum danych, ponieważ wersje developerskie wdrażane są w środowisku chmury publicznej.
- Łatwość dostępu do środowiska testowego dla partnera dostarczającego rozwiązanie.
- Zarządzanie procesem testowym co pozwala zapewnić powtarzalność wyników.
- Wykonywane testy można łatwo powtórzyć w sytuacji, gdy kolejna wersja rozwiązania ma dodatkowe funkcjonalności (aktualizacja rozwiązania, poprawki gwarancyjne itp.).

Używane narzędzia i technologie:

- Visual Studio Enterprise wraz z licencją MSDN pozwalającą właścicielowi na nieograniczone uruchamianie środowisk developerskich i testowych. w tym stawianie środowisk dla SharePoint Server czy SQL Server.
- Visual Studio Team Services zawierającą usługę testów funkcjonalnych (Functional Test) które pozwalają zautomatyzować przeprowadzone testy.
- Zarządzanie procesem testowym przy użyciu VSTS.
- Azure Virtual Machines pozwalające odwzorować środowisko on-premise na potrzeby testów developerskich.

5.1.1.17. ANALIZA LOGÓW I STANU BEZPIECZEŃSTWA

Microsoft oferuje gotowe narzędzia do wykrywania zagrożeń (ATA). Jednak każda firma ma swoją specyfikę (z punktu widzenia analizy bezpieczeństwa). Czasami zagrożeniem są także wewnętrzne rozwiązania zachowujące się w niestandardowy sposób.

Ciekawym podejściem jest rozwiązanie, w którym logi związane z bezpieczeństwem są analizowane w środowisku hostowanym Azure w sposób znacznie bardziej dokładny i znacznie mniejszym kosztem niż może mieć to miejsce we własnym centrum danych.

Ważniejsze cechy:

- Możliwość długoterminowego przechowywania logów do późniejszej analizy.
- Zastosowanie dowolnego typu algorytmów – analiz PCA, wykorzystanie sieci neuronowych, proste klasteryzacje itp. Niektóre z nich wymagają gigantycznej mocy obliczeniowej, która dzięki chmurze jest łatwo dostępna.
- Narzędzia do analizy danych NOSQL, które pozwalają analizować dane w niestandardowy sposób (bez ograniczeń narzucanych przez bazy relacyjne). Dzięki temu można wykryć problemy które inaczej pozostałyby niewidoczne.
- Centralne repozytorium skryptów, pomysłów i procesów co pozwala na łatwiejszą pracę grupową nad problemem.

Używane narzędzia i technologie:

- Azure Machine Learning.
- Azure Data Lake Store do przechowywania gigantycznych logów.

- Azure Data Lake Analysis – używane do analizy w stylu No-SQL.
- komponent wysyłający logi ze infrastruktury klienta.
- Visual Studio do pisania i testowania skryptów w języku R oraz do wspomagania analiz w Azure Machine Learning i Data Lake.
- zarządzanie procesem przy użyciu VSTS.

5.1.1.18. AZURE JAKO ŚRODOWISKO INTERAKCJI Z UŻYTKOWNIKAMI (PODMIOTAMI) ZEWNĘTRZNYMI Z FUNKCJĄ NIEZAPRZECZALNEGO UWIERZYTELNIANIA, W TYM ZA POŚREDNICTWEM PROFILU ZAUFANEGO

Funkcje pozwalające użytkownikom na wykorzystanie systemów i usług osadzonych w chmurze lub w środowiskach własnych udostępniającego usługę. Tego typu rozwiązanie pozwala na:

1. Stworzenie warstwy dostępowej odseparowanej od wewnętrznych środowisk chronionych.
2. Wykorzystanie zabezpieczeń Azure przed cyberatakami różnych typów.
3. Możliwość wykorzystania gotowych mechanizmów niezaprzeczalnego uwierzytelnienia, w tym uwierzytelnienia wieloskładnikowego.
4. Możliwość wykorzystania mechanizmów pozwalających na wdrożenie mechanizmu pojedynczego logowania do usług zewnętrznych.
5. Elastyczne skalowanie środowisk pozwalające uwzględnić aktualne potrzeby związane z liczbą użytkowników i generowanych przez nich ruchem.
6. Szybki i efektywny model wdrożenia niewymagający budowy i konfiguracji infrastruktury i mechanizmów bezpieczeństwa.

Wymagane produkty: Azure MC, Azure AD Premium

5.1.1.19. AZURE JAKO STANDARDOWEGO ROZSZERZENIA CHMURY PRYWATNEJ Z JEDNOLITYM ZARZĄDZANIEM W RAZ Z PROMOCJĄ WINDOWS SERVER 2022 I AZURE STACK

Organizacja własnych zasobów teleinformatycznych w postaci chmury prywatnej powoduje konieczność jej ciągłej rozbudowy z uwagi na rosnący wolumen danych i wdrażanie nowych

usług. Prostszym, szybszym we wdrażaniu i bezpiecznym modelem jest rozszerzanie własnych zasobów o wymagane zasoby (maszyny wirtualne, przestrzeń dyskowa, gotowe usługi) z chmury.

Usługa oferuje spójne zarządzanie i administrację zasobami własnymi i hostowanymi, wraz z możliwością przenoszenia zasobów pomiędzy tymi środowiskami i dynamicznego skalowania części hostowanej.

5.1.1.20. AZURE JAKO BEZPIECZNA I NIEZAWODNA USŁUGA BACKUP

To proste i tanie rozwiązanie typu kopia zapasowa jako usługa, która umożliwia ochronę danych bez względu na ich lokalizację: w centrum danych przedsiębiorstwa, w biurach zdalnych i oddziałach firmy, czy też w chmurze publicznej. Azure Backup wymaga minimalnej obsługi i oferuje spójne narzędzia umożliwiające tworzenie kopii zapasowej w trybie offline i odzyskiwanie danych.

Najważniejsze cechy:

- Rozwiązanie do wykonywania kopii zapasowych w chmurze stanowiące atrakcyjną alternatywę dla taśm. Usługa Backup to świetna alternatywa dla taśm zapewniająca znaczne obniżenie kosztów, krótszy czas odzyskiwania i możliwość przechowywania danych do 99 lat.
- Bezpieczne i niezawodne rozwiązanie do obsługi kopii zapasowych oferowane jako usługa. Dane kopii zapasowych są bezpieczne podczas przesyłania i przechowywania. Są one przechowywane w magazynie, który zawiera 6 kopii danych rozmieszczonych w dwóch centrach danych systemu Azure. Usługa Backup zapewnia dostępność na poziomie 99,9%.
- Wydajne i elastyczne usługi kopii zapasowych online. Po zakończeniu pierwszego backupu wysyłane są tylko zmiany przyrostowe co określony czas.

Więcej informacji na stronie: https://azure.microsoft.com/pl-pl/services/backup/

Wymagane usługi: Azure Backup, Azure Storage.

5.1.1.21. AUTOMATYZACJA ZARZĄDZANIA I MONITORING DZIĘKI ZAAWANSOWANYM MECHANIZMOM AZURE - OMS AUTOMATION & CONTROL

Gotowe mechanizmy automatyzacji zadań dostępne w formie usługi z chmury wzbogacone o możliwości kontroli konfiguracji. Dzięki temu IT otrzymuje działające narzędzia „as a service" do śledzenie zmian konfiguracji serwerów i desktopów, zarzadzania poprawkami, kontroli stanu konfiguracji i automatyzacji.

Najważniejsze funkcje:

- Azure Automation,
- Desired state configuration,
- Change tracking,
- Update management.

Wymagane usługi: OMS Automation & Control (w ramach usługi prawo do System Center Configuration Manager w wersji on-premise).

5.1.1.22. AZURE AD JAKO TOŻSAMOŚĆ CYFROWA UCZNIÓW W CAŁYM PROCESIE EDUKACYJNYM

Jednym z większych wyzwań powodujących nadmierne nakłady pracy w jednostkach edukacyjnych każdego szczebla jest konieczność „ręcznego" wpisywania danych ucznia do kilku różnych systemów. Osadzenie uzupełnialnego na poszczególnych etapach cyfrowego profilu danych ucznia w Azure AD umożliwiłoby automatyzację tego procesu i wprowadzenie zasad niezaprzeczalności.

Dodatkowo możliwe jest stosowanie usług Azure w niezliczonych scenariuszach, na przykład:

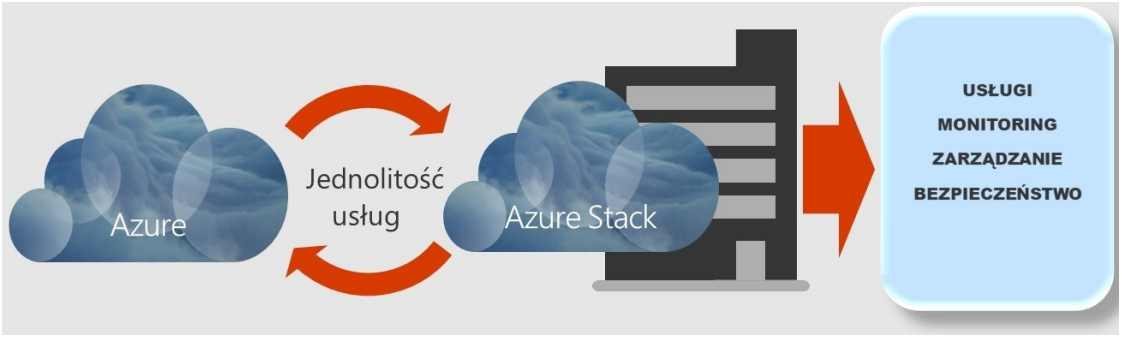
1. Azure i AAD jako standardowa platforma dla systemów informacyjnych typu tablice informacyjne lub kioski informacyjne.
2. Azure + SharePoint jako standardowa platforma dla baz danych publicznych i witryn publicznych w tym nowych lub migrowanych BIP.
3. Oferta Azure jako standardowego, bezpiecznego archiwum dokumentów z tworzeniem paczek dla archiwum centralnego.

6. PLATFORMA HYBRYDOWA AZURE STACK

Doświadczenia wypływające z obserwowanych obecnie projektów wskazują, że najbardziej rozpowszechnionym modelem implementacji usług informacyjnych będzie platforma hybrydowa, obejmująca zarówno zasoby własne jak i zasoby z chmury. Niesie to za sobą konieczność zastosowania jednorodnych i spójnych mechanizmów platformowych, zarządczych, monitorujących i zapewniających wymagany poziom bezpieczeństwa.

6.1. KONCEPCJA AZURE STACK

Dużym ułatwieniem w budowie takich rozwiązań jest Azure Stack, czyli zespół narzędzi pozwalających dostarczyć i uruchomić kluczowe usługi dostępne na platformie Azure we własnych centrach przetwarzania, tworząc jednorodny model budowy usług on-premise i w hybrydzie.



Usługa Azure Stack, dostarczana jako subskrypcja, jest rozwiązaniem sprzętowo-programowym, wyposażonym w precyzyjne wytyczne wdrożeniowe i utrzymaniowe. Jedną z najważniejszych jej zalet jest wielokrotne przyspieszenie wdrożenia nowoczesnego centrum przetwarzania przy znaczącym ograniczeniu ryzyk projektowych, poprzez wykorzystanie gotowych komponentów, metodyk i planów wdrożeniowo-utrzymaniowych.

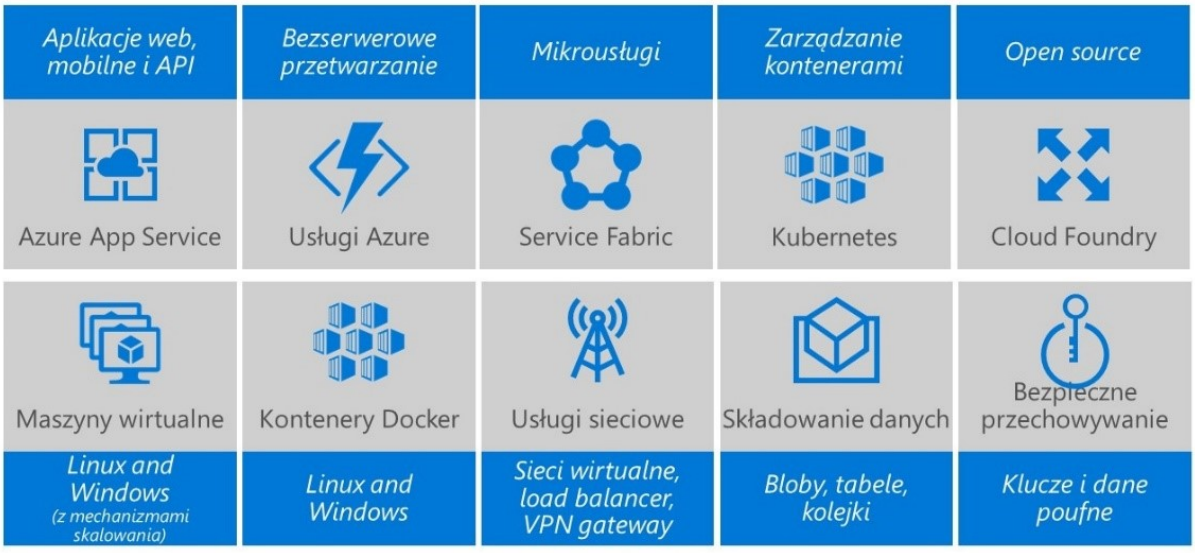
Dalszą zaletą hybrydowego rozwiązania jest elastyczność w podejmowaniu decyzji, gdzie przetwarzamy i przechowujemy dane – na przykład w wyniku decyzji na bazie klasyfikacji danych.

Dodatkowo w takim modelu możliwe jest tanie obsłużenie pików przetwarzania skalując je w Azure bez konieczności nadmiernej rozbudowy własnej infrastruktury.

Funkcje Azure Stack są stale rozwijane, a w chwili obecnej kluczowymi są:

- wdrażanie systemów Linux,
- wdrażanie systemów Windows,
- konfiguracja powyższych za pomocą *Desired State Configuration* (DSC),
- zarządzanie Azure Stack z poziomu Windows i Linux,
- wykorzystywanie własnych obrazów VHD systemów operacyjnych,
- powoływania do życia całych infrastruktur za pomocą szablonów,
- rozszerzenia,
- PaaS On-Premises,
- tworzenie Planów, Ofert i Subskrypcji.

Dzięki Azure Stack można obecnie udostępnić w środowisku hybrydowym następujące obszary usług:



Ważną cechą rozwiązania Microsoft jest ciągły rozwój wymienionych usług, to znaczy, że są one ciągle ulepszane i jest ich coraz więcej.

Podobnie jak we wszystkich usługach online Microsoft wykorzystywana jest usługa Azure Active Directory, pozwalająca przechowywać profile użytkowników, synchronizować je

z własnym Active Directory i wprowadzić mechanizm pojedynczego logowania. Alternatywą dla AAD jako źródła tożsamości jest konfiguracja Active Directory Federation Services (AD FS).

Rozpoczynając wdrożenie oparte o Azure Stack warto skorzystać z Azure Stack Development Kit, czyli zespołu narzędzi pozwalających prototypować rozwiązanie hybrydowe pozwalające wdrożyć on-premise architekturę zgodną z platformą Azure, podstawowe usługi i API. Rozwiązanie to pozwala na szybką ocenę przydatności funkcji Azure Stack i wstępne testy funkcjonalne, natomiast nie nadaje się do testów wydajnościowych.

W koncepcji wykorzystania Azure Stack występują dwie główne role:

- Administrator Chmury – mogący konfigurować, monitorować i udostępniać usługi.
- Użytkownik – mogący wykorzystywać usługi zgodnie z nadanymi uprawnieniami.

6.2. PORTAL AZURE STACK

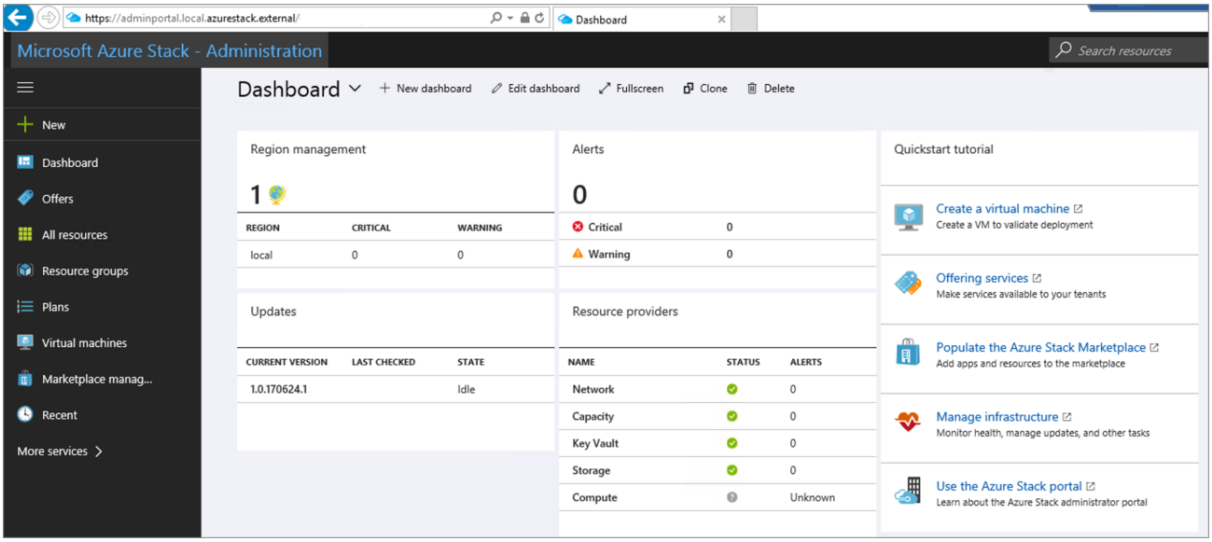
Klasycznym wykorzystaniem rozwiązania opartego o Azure Stack jest scenariusz „przezroczysty" dla użytkownika, a więc taki w którym uprawniony użytkownik ma dostęp do konkretnych aplikacji czy zasobów. Tym niemniej dla administrujących platformą wymagane są narzędzia pozwalające na konfigurację i zarządzanie. Tym zadaniom służy portal administratora Azure Stack[82] oraz Azure Stack PowerShell.

Portal ten pozwala na:

- zarządzanie infrastrukturą (w tym kondycja systemu, aktualizacje, zarządzanie siecią, maszynami, pojemnością itp.),
- konfiguracja dostępnych użytkownikom usług w marketplace,
- tworzenie planów i oferty,
- tworzenie kont i subskrypcji użytkowników wraz z określaniem ich uprawnień.

Zawartość portalu poddaje się bardzo elastycznej konfiguracji pozwalając na dostosowanie do potrzeb i typowego działania administratora.

[82] *https://docs.microsoft.com/pl-pl/azure/azure-stack/azure-stack-manage-portals*



6.3. APLIKACJE W AZURE STACK

Dzięki wykorzystaniu jednolitej opartej na standardach przemysłowych platformy możliwe jest znaczące przyspieszenie procesu implementacji aplikacji dla użytkowników. Po pierwsze, mamy do dyspozycji jednorodną platformę z ściśle zdefiniowanymi usługami i wymaganiami dla wszelkich aplikacji. Dodatkowo możemy wykorzystać kilka standardowych scenariuszy udostępniania aplikacji i przetwarzania danych na platformie z wykorzystaniem gotowych usług, serwisów aplikacyjnych, maszyn wirtualnych, kontenerów, narzędzi developerskich, itp. Mamy więc zachowany jednorodny, łatwy w rozwoju i utrzymaniu model aplikacji opartych o standardowe interfejsy API dostępne w Azure Resource Manager.

7. KOMPONENTY CHMURY PUBLICZNEJ W KONTEKŚCIE ZAMÓWIEŃ PUBLICZNYCH

Rozwiązania z chmury publicznej nie zostały uwzględnione jako odrębny przedmiot zamówienia w prawie zamówień publicznych. Doświadczenia ostatnich lat wskazują, że takie wyodrębnienie nie było potrzebne, a nawet mogłoby być szkodliwe z uwagi na mnogość potencjalnych scenariuszy działania, wykorzystania, czy też nabywania usług typu *cloud*. Odbyło się już kilkaset postępowań, w których przedmiotem zamówienia były usługi z chmury. Przeszły one pomyślnie procedurę zamówień publicznych oraz późniejszych audytów.

7.1. USTALENIA W ZAKRESIE PRZEDMIOTU ZAMÓWIENIA

Jak należy traktować przedmiot zamówienia zawierający komponenty chmury publicznej?

Praktyka wynikająca z ogłoszonych i rozstrzygniętych postępowań wskazuje, że najlepszym podejściem jest zdefiniowanie przedmiotu zamówienia jako **dostawy standardowych pakietów subskrypcji chmury publicznej**. Taki opis wynika między innymi z przytoczonej definicji chmury publicznej, czyli pakietów standardowych o precyzyjnie określonym zakresie funkcjonalności i sposobie działania.

Można więc podobnie jak w przypadku pakietów oprogramowania lub karty telefonicznej prepaid określić pakiety usług chmury publicznej jako **Produkty** podlegające dostawie, opisane kodem CPV 48900000-7 – różne pakiety oprogramowania i systemy komputerowe. Rozszerzając ten opis definiujemy opisywany komponent chmury publicznej jako produkt typu COTS (Commercial of the Shelf). Pola eksploatacji takich Produktów określone są zwykle przez Dostawcę w umowach typu adhezyjnego, które można przyjąć (jeżeli odpowiadają wymaganiom Zamawiającego) lub zrezygnować z zakupu produktu.

Podstawowym obowiązkiem organizatora przetargu publicznego jest ustalenie rodzaju zamówienia. Rodzaj zamówienia (kwalifikacji go do kategorii dostawy albo usługi) będzie determinował szereg konsekwencji prawnych. Aktualnie obowiązujące w Pzp definicje legalne dostaw i usług wskazują odpowiednio, że:

- Dostawą jest nabywanie rzeczy oraz innych dóbr, w szczególności na podstawie umowy sprzedaży, dostawy, najmu, dzierżawy oraz leasingu z opcją lub bez opcji zakupu, które może obejmować dodatkowo rozmieszczenie lub instalację.

zaś

- Usługą wszelkie świadczenia, których przedmiotem nie są roboty budowlane lub dostawy.

Co prawda nowelizacja Pzp z 2016 r. zmodyfikowała brzmienie definicji pojęcia dostawy usuwając z niej nabycie "praw" i pozostawiając w zakresie pojęciowym nabywanie „innych dóbr", jednak można ocenić, że zakres pojęcia dostawa w dalszym ciągu obejmuje również nabywanie praw. Tytułem przykładu nadal w art. 143 Pzp wskazuje się na możliwość zawarcia umowy na czas nieoznaczony w przypadku dostaw licencji na oprogramowanie komputerowe.

Zasadniczo uznać można, że w sytuacji, gdy w ramach świadczenia usług chmurowych zamawiający nabywa prawo do korzystania z oprogramowania, a więc mamy do czynienia z dostawami.

W przypadku tzw. zamówień rodzajowo mieszanych obejmujących jednocześnie dostawy oraz usługi, przepisy Pzp zawierają w art. 5c ust. 1 wytyczną, zgodnie z którą decyduje o kwalifikacji rodzajowej całego zamówienia jego główny przedmiot (aktualnie nie decyduje już przeważający udział wartościowy w całości zamówienia).

Jest to szczególnie ważne w sytuacji, gdy udział wykonawców jest ograniczony do zapewnienia zamawiającemu dostępu do usług chmurowych świadczonych przez podmiot trzeci - Dostawcę. Dodatkowo specyfika przedmiotowych usług polega na tym, że w zamówieniach tych nie ubiegają się zazwyczaj Dostawcy chmury obliczeniowej co oznacza, że wymóg, aby faktycznie to Wykonawca składający ofertę był dostawcą chmury - ogranicza konkurencyjność. Podobnie istotne znaczenie ma rodzaj zamówienia w przypadku kwestii ew. udostępniania potencjału podmiotów trzecich dla spełniania warunków udziału (art. 22a Pzp) w przypadku, gdy użyczanym potencjałem jest doświadczenie dla usług, podmiot udostępniający potencjał ma wykonać takie zamówienie zaś w przypadku dostaw takiego obowiązku brak (art. 22a ust 4 Pzp).

7.1.1. SZACOWANIE KOSZTU PRODUKTÓW Z CHMURY

Decydując się na wykorzystanie zasobów chmury publicznej należy przeprowadzić szacunki dotyczące przewidywanego poziomu ich wykorzystania w okresie, na który chcemy zawrzeć umowę. Większość Dostawców produktów typu cloud oferuje specjalne narzędzia

(kalkulatory) pozwalające na oszacowanie kosztu Produktu w czasie poprzez wprowadzenie danych o zakresie ich wykorzystania i danych wolumetrycznych takich jak liczba użytkowników, wymagana przestrzeń dyskowa, liczba rdzeni procesora czy wykorzystywane pasmo sieciowe.

Należy zwrócić uwagę na to, że Dostawcy oferują zwykle trzy modele płatności za produkty:

1. Model subskrypcji określający niezależnie od poziomu wykorzystania Produktu stałą cenę w jednostce czasu (zwykle na jednego użytkownika miesięcznie). Taki model jest zwykle stosowany dla Produktów typu SaaS (Software as a Service) gdzie ich funkcjonalność jest dokładnie sprecyzowana i występuję w postaci gotowego do użycia narzędzia.
2. Model subskrypcji pozwalającej na zakup zdefiniowanej puli zasobów na określoną jednostkę czasu. w takim modelu Zamawiający zużywa przedpłaconą pulę zasobów we własnym zakresie decydując o sposobie ich użycia, wybierając z szerokiego katalogu technologii Dostawcy. Jest to model stosowany zwykle dla rozwiązań platformowych typu IaaS (Infrastructure as a Service) lub PaaS (Platform as a Service).
3. Model płatności podążającym za fizycznym użyciem Produktu, często określanym jako model pay-as-you-go.

Konstrukcja zapisów SIWZ musi uwzględniać występowanie tych modeli płatności, a w szczególności możliwość uzupełniania zasobów w trakcie trwania umowy poprzez dodatkowe zakupy Produktów, co jest możliwe poprzez stosowanie prawa opcji, zamówień uzupełniających lub zawieranie umów ramowych.

Zamawiający powinien też określić, który z powyżej opisanych modeli najlepiej wpisuje się w jego potrzeby i wymagania.

7.1.2. ROZPOZNANIE RYNKU

Szczególnie ważnym elementem przygotowania postępowania na usługi chmurowe, między innymi pozwalające na oszacowanie kosztów ich eksploatacji, jest właściwe rozpoznanie rynku. Bez tej wiedzy Zamawiający nie jest w stanie ani ustalić swoich wymagań w zakresie zamawianych Produktów ani należycie ustalić ich wartości, która jest niezbędna dla wszczęcia postępowania.

Koniecznością staje się ustalenie możliwości rynkowych jak najbardziej aktualne względem daty wszczęcia przetargu. Niestety dynamika zmian rynku chmurowego może być poważnym problemem i wyzwaniem w trakcie realizacji umów o zamówienie publiczne. Konieczna staje się znajomość ścieżek rozwojowych zarówno w samych produktach jak i ich polach eksploatacji oraz wprowadzenia do SIWZ konkretnych i skutecznych narzędzi gwarantujących elastyczność takich jak dopuszczenie stosowania produktów następczych lub realizujących wymagania Zamawiającego w nowy, bardziej efektywny sposób. Bez takich zapisów w krótkim czasie umowy takie mogą stać się nieefektywne z punktu widzenia aktualnej ofert rynkowej. Rozpoznanie rynku w zakresie przygotowania postępowania i zaznajomienia się z dostępną ofertą Dostawców można przeprowadzić metodą dialogu technicznego, bądź trybów udzielania zamówień, które przewidują negocjacje/dialog z wykonawcami.

Procedura dialogu technicznego (określona w art. 31a-c Pzp) jest bardzo elastyczna i nie stanowi jeszcze wszczęcia postępowania o zamówienie publiczne, co powoduje, że może trwać stosunkowo krótko i dawać wymierne efekty. Pzp nie narzuca czasu trwania takiej procedury i nie ingeruje w techniczny sposób jej prowadzenia. Przedmiotem dialogu mogą być praktycznie wszystkie elementy przyszłego postępowania w szczególności: opis przedmiotu zamówienia, kryteria oceny ofert, warunki udziału, koszty realizacji zamówienia, warunki umowne itd.

Przykładowy harmonogram procedury z wykorzystaniem we wstępnej fazie dialogu technicznego może wyglądać następująco:

1. Ustalenie wymagań funkcjonalnych, technicznych, wydajnościowych oraz z zakresu zgodności z politykami bezpieczeństwa i prawem.
2. Przygotowanie zapytania i wszczęcie dialogu technicznego.
3. Przygotowanie zestawienia wniosków z dialogu technicznego.
4. Doprecyzowanie wymagań funkcjonalnych, technicznych, wydajnościowych oraz z zakresu zgodności z politykami bezpieczeństwa i prawem.
5. Wszczęcie postępowania publicznego.

Podsumowanie wniosków z przeprowadzonego dialogu technicznego lub innej formy rozpoznania rynku jest też dobrym momentem do oceny, jakie zmiany konieczne są

w posiadanej infrastrukturze lub wewnętrznych politykach – w szczególności politykach bezpieczeństwa, tak aby zastosowanie komponentów chmurowych było możliwe.

Jest to też okres, w którym można przeprowadzić analizę ryzyka w zakresie cyberbezpieczeństwa z uwzględnieniem planowanych komponentów.

7.1.3. REKOMENDACJE DOTYCZĄCE OPISU PRZEDMIOTU ZAMÓWIENIA

Ustawa Prawo Zamówień Publicznych (Pzp) zobowiązuje Zamawiającego do precyzyjnego opisu przedmiotu zamówienia, pozwalającego na jego wycenę przez Wykonawców, a jednocześnie nie naruszającego zasad uczciwej konkurencji i neutralności technologicznej.

Powoduje to, że opis zamawianych komponentów chmury publicznej (Produktów) powinien zawierać wymagania dotyczące ich funkcjonalności, cech użytkowych, zgodności z obowiązującym prawem, normatywami, standardami bezpieczeństwa, ochrony danych, dostępności, wsparcia technicznego czy też innych elementów chroniących interesy Zamawiających.

Opis przedmiotu zamówienia ma być opracowany przez Zamawiającego w sposób uwzględniający obiektywne potrzeby, z drugiej jednak strony musi zapewniać konkurencyjność.

7.1.3.1. WYMAGANIA STAWIANE WYKONAWCOM

Ponieważ przyjęliśmy, że przedmiotem zamówienia jest **dostawa Produktów**, a więc wymagania wobec Wykonawców powinny dotyczyć tylko i wyłącznie tego zakresu, np.:

- możliwości dostawy Produktów spełniających wymagania,
- doświadczenie w zakresie realizacji takich dostaw.

7.1.3.2. WYMAGANIA W ZAKRESIE PRODUKTÓW

Odnosząc się do koniecznych elementów opisu przedmiotu zamówienia należy wskazać na następujące konieczne minimalne wymagania odnośnie funkcjonalności, cech użytkowych Produktów, czy też ich zgodności z wymaganiami bezpieczeństwa i prawa, np.:

- Wymagania dotyczące czasu w jakim Produkt będzie dostępny dla Zamawiającego – na przykład w okresie 12 lub 36 miesięcy.

- Określenie parametrów dostępności usług w Produkcie – na przykład dostępność 24/7 z SLA[83] na poziomie minimum 99,9%.
- Listę wymaganych funkcji realizowanych przez Produkt, na przykład:
  - możliwość tworzenia maszyn wirtualnych,
  - analizy danych,
  - składowania danych,
  - obsługi poczty elektronicznej,
  - funkcji systemu finansowego,
  - specyficznych usług z zakresu bezpieczeństwa teleinformatycznego.
- Oprócz określenia głównych funkcji Produktu należy również opisać szczegółowe wymagania funkcjonalne czy techniczne, na przykład rodzaj systemu operacyjnego na maszynach wirtualnych, narzędzia monitorujące i zarządzające, sposób komunikacji, protokoły i wszystkie inne potrzebne Zamawiającemu cechy.
- Wymagania dotyczące parametrów poszczególnych komponentów Produktu i zakresu możliwych zmian tych parametrów przez uprawnionego użytkownika (konfiguracji), na przykład minimalna pojemność przestrzeni dyskowej, rdzeni procesora czy pamięci RAM, z określeniem możliwości i sposobu jej zmiany w trakcie eksploatacji, określenie wymaganego szyfrowania danych i transmisji danych czy też parametrów wydajnościowych.
- Wymagania dotyczące współpracy z posiadana przez Zamawiającego infrastrukturą, np.: mechanizmami zarządzania tożsamością cyfrową czy wymiany danych.
- Wymagania dotyczące narzędzi administracyjnych, konfiguracyjnych, monitorujących i raportujących umożliwiających administrowanie Produktem i jego użytkownikami.
- Wymagania dotyczące bezpieczeństwa systemów i danych, w tym:

[83] *Service Level Agreement - umowa o gwarantowanym poziomie świadczenia (dostępności) usług*

    - dostępność narzędzi pozwalających na uzyskanie rozliczalności działań w systemach opartych o Produkty,
    - monitorowania działań użytkowników,
    - monitorowania stanu systemów oraz usług,
    - dostępności logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
- Wymagania w zakresie niezaprzeczalności tych działań, w tym oparcia dostępu o niezaprzeczalne uwierzytelnienie wraz z uwierzytelnieniem wieloskładnikowym.
- Wymagania dotyczące zapewnienia mechanizmów umożliwiających w połączeniu z infrastrukturą Zamawiającego realizację pojedynczego logowania (single sign-on).
- Wymagania dotyczące dostępności wbudowanych mechanizmów bezpieczeństwa, takich jak:
    - Bramki VPN,
    - Obsługa IPSec,
    - Akceleracja SSL,
    - Firewall warstwy aplikacyjnej – WAF,
    - mechanizmy przeciwdziałania włamaniom – IPS,
    - mechanizmy zabezpieczające przez atakami DDoS.
- Określenie wymagań szczegółowych w zakresie zgodności z powszechnie uznanymi standardami, na przykład HTTP(S) – TLS, Docker, REST API, Java, .NET, PHP, Python czy Node.js.
- Określenie wymagań szczegółowych w zakresie dostępności typu Disaster Recovery i redundancji dla całości wdrożonego na komponentach chmurowych rozwiązania.

- Określenie wymagań szczegółowych dotyczących dostępności mechanizmów pozwalających na migrację danych (czy też aplikacji) do środowisk dostarczanych przez innych Dostawców lub własnej infrastruktury. Minimalnym wymaganiem w tym zakresie jest dostępność mechanizmów opartych o standardy przemysłowe umożliwiające wykonanie takiej operacji.
- Wymagania dotyczące redundancji usług oraz replikacji danych, na przykład przechowywanie danych w dwóch centrach przetwarzania rozproszonych geograficznie.
- Wymagania w zakresie zapewnienia udzielania licencji na używanie Produktu podmiotom trzecim wykorzystującym system Zamawiającego.
- Określenie wymagań szczegółowych w zakresie zgodności z prawem, na przykład zawarcie przez Dostawcę w umowie do Produktu zapisów o zgodności z RODO i określenia się Dostawcy jako podmiotu przetwarzającego w rozumieniu tego rozporządzenia czy też zawarcie przez Dostawcę w umowie do Produktu tzw. standardowych klauzul umownych opublikowanych przez Komisję Europejską.
- Możliwość zastrzeżenia miejsca składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego.
- Wymagania publikacji przez Dostawcę raportów na temat aktualnych cyberzagrożeń i znanych podatności Produktów.
- Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych danych po stronie Zamawiającego.
- Gwarancja usunięcia danych Zamawiającego przez Dostawcę po zakończeniu umowy.
- Gwarancja braku dostępu do danych Zamawiającego, z wyłączeniem działań serwisowych wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy.
- Określenie wymagań szczegółowych w zakresie zgodności z normami czy certyfikatami, na przykład posiadanie przez Produkt (lub jego Dostawcę) certyfikatów ISO 20000-1:2011, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO

27701, ISO-9001, PCI DSS, SOC 1/ISAE 3402, SOC 2, SOC 3 czy EN 301 549 zawierający WCAG. Certyfikacje takie pokrywają większość wymagań związanych z prawem pod warunkiem umieszczenia przez Dostawcę odpowiednich zapisów w umowie dołączonej do Produktu.

- Wymaganie dostępności potwierdzenia pozytywnego przejścia audytów wykonanych przez uznane podmioty trzecie, potwierdzających lub certyfikujących zgodność z wymienionymi normami. Przeprowadzenie własnych audytów przez Zamawiającego jest kosztowne i wymaga odpowiednich zasobów kadrowych, a czasem jest niemożliwe z uwagi na obowiązujące polityki bezpieczeństwa Dostawcy.
- Wymagania dotyczące przewidywalności kosztów eksploatacji Produktów zarówno w przypadku ryczałtowych płatności jak i płatności za fizyczne wykorzystanie zakupionych zasobów. Dostępność mechanizmów monitorowania użycia zasobów chmury i kosztów z tym związanych.

Należy zwrócić uwagę, że wszystkie przedstawione wyżej wymagania dotyczą Produktu i jego Dostawcy, natomiast błędem jest oczekiwanie wypełnienia ich przez Wykonawcę. Dojdzie bowiem wtedy do ograniczenia konkurencji, w której tylko ci Wykonawcy, którzy jednocześnie są Dostawcami mają możliwość przedstawienia oferty. Zamawiający powinien zatem wymagać przedstawienia przez wykonawców już wraz z ofertą dokumentów/dowodów dotyczących Dostawcy, potwierdzających spełnianie stawianych wymagań, w tym załączenia umowy oferowanej przez Dostawcę Produktu względnie innych źródeł informacji o Produkcie publikowanych przez Dostawcę. Informacje powyższe odnoszą się bowiem do sposobu realizacji zamówienia i stanowią potwierdzenie zgodności oferowanego świadczenia z wymaganiami Zamawiającego.

7.1.3.3. WYMAGANIA W ZAKRESIE WSPARCIA TECHNICZNEGO

Decydując się na oparcie kluczowych systemów na komponentach chmury publicznej należy zapewnić dla nich odpowiedni poziom wsparcia technicznego. z uwagi na to, że sposób działania Produktów jest zależny od działań Dostawcy, a nie Wykonawcy, należy przeprowadzić analizę czy cechy Produktu, a w szczególności zapisy umowy dostarczanej przez Dostawcę wraz z Produktem są wystarczające, czy należy wymagać dostawy

dodatkowego, płatnego pakietu wsparcia technicznego Dostawcy. Dostępność pakietów wsparcia technicznego Dostawcy, ich rodzaje, zakres i ceny powinny być elementem rozpoznania rynku.

7.1.3.4. WYMAGANIA W ZAKRESIE WDROŻENIA

Każdy z Produktów zamawianych w opisywanej procedurze wymaga wdrożenia produkcyjnego. w zależności od decyzji kto będzie dokonywał wdrożenia (Zamawiający, Wykonawca czy też Dostawca) można zawrzeć zakres usługi wdrożenia w zakresie przedmiotu zamówienia. Niestety takie podejście komplikuje znacząco opis przedmiotu zamówienia, zapisy projektu umowy oraz wydłuża zwykle całość procedury. Może też powodować ograniczenie konkurencyjności postępowania poprzez postawienie nowych, związanych z usługą wdrożenia, wymagań wobec Wykonawców.

Problemu tego można uniknąć, jeżeli Dostawcy dysponują w swojej ofercie pakietami godzin wdrożeniowych, co pozwala na ich zakup w formie dostawy, a więc rozszerzenie zakresu przedmiotu zamówienia o kolejny Produkt – pakiet godzin wdrożeniowych Dostawcy. w przypadku braku takiej możliwości lub występowaniu innych przyczyn, dla których taki pakiet nie spełnia oczekiwań Zamawiającego, optymalnym wydaje się wszczęcie oddzielnego postępowania na usługi wdrożeniowe.

7.1.4. REKOMENDACJE DOTYCZĄCE PROJEKTU UMOWY

Projekt umowy w kontekście opisanych rekomendacji definiować przedmiot zamówienia jako dostawę Produktów ze wszystkimi konsekwencjami takiej definicji – o czym była mowa na wstępie.

Umowa musi zawierać zobowiązania Wykonawcy w zakresie prawidłowego wykonania dostawy, a nie odpowiedzialności za pola eksploatacji czy sposób działania dostarczonych Produktów.

Najprostszą formą uszczegółowienia przedmiotu umowy jest powtórzenie istotnych zapisów z opisu przedmiotu zamówienia dotyczących pól eksploatacji i sposobu dostarczenia produktu.

W warunkach płatności warto uwzględnić typowe rozwiązania stosowane przez Dostawców, gdyż postawienie innych wymagań może spowodować zwiększenie ryzyka finansowego

Wykonawcy, a co za tym idzie może spowodować znaczący wzrost ceny oferty bez dodatkowych korzyści dla Zamawiającego.

Z uwagi na konieczność elastycznego podejścia do wykorzystania Produktów, ich skalowalnego użycia i dopasowania ich zużycia do aktualnych potrzeb Zamawiającego należy rozważyć możliwość wykorzystania instytucji umów ramowych. Postępowanie w celu zawarcia umowy ramowej może być prowadzone zarówno w procedurze podstawowej jak przetarg nieograniczony jak również stosując odpowiednio przepisy dotyczące udzielania zamówienia w trybach dwuetapowych. Umowy ramowe są coraz częściej stosowane w ramach centralnych zamówień czy też zamówień wspólnych. Atutem procedury umowy ramowej jest możliwość szybkiego i maksymalnie odformalizowanego trybu dokonywania zamówień wykonawczych, których przedmiotem są konkretne Produkty.

Inną możliwością skalowalnego wykorzystania produktów chmurowych jest wprowadzenie prawa opcji w opisie przedmiotu zamówienia i we wzorze umowy. Prawo opcji zakłada, że Zamawiający każdorazowo określa minimalny poziom zamówienia, który zostanie na pewno zrealizowany, co pozwala Wykonawcom na rzetelne i właściwe dokonanie wyceny oferty. Wskazuje jednocześnie dodatkowy zakres, którego realizacja jest uzależniona od wskazanych w kontrakcie okoliczności i stanowi uprawnienie Zamawiającego, z którego może, ale nie musi on skorzystać. Realizacja prawa opcji przez Zamawiającego nie skutkuje aneksowaniem umowy bowiem Wykonawca już składając ofertę wycenia także część opcjonalną i nie jest ona przedmiotem negocjacji.

Dodatkowo, w umowie na dostawy Produktów chmurowych wymagane są zwykle mechanizmy waloryzacji świadczeń w szczególności w związku z koniecznością uwzględnienia zmian ryzyka kursowego cen produktów.

8. ZAŁOŻENIA INTEROPERACYJNOŚCI

8.1. DOKUMENT ELEKTRONICZNY I DOKUMENT PAPIEROWY

Większość działań związanych z informatyzacją obiegu informacji opiera się na obowiązujących regulacjach dotyczących dokumentu elektronicznego w formacie XML. Tym niemniej, należy spodziewać się, że w ciągu najbliższych lat większość spraw będzie wnoszona w postaci dokumentów papierowych. Istnieje konieczność wypracowania metod przekształcania dokumentu papierowego na elektroniczny w sposób zgodny z obowiązującymi regulacjami w zakresie dokumentu elektronicznego, archiwizacji i podpisu elektronicznego oraz w zgodzie z możliwością użycia tej formy dokumentów w obiegach dokumentów elektronicznych.

Odpowiedzią na ten problem jest specyfikacja meta standardu dokumentów elektronicznych opracowanego w ramach projektu ePUAP. Przewiduje ona tworzenie szablonów (wzorów) dokumentów elektronicznych nie tylko w postaci pełnych formularzy, ale też nagłówków kopertujących. Użycie mechanizmu załączania skanu dokumentu papierowego do nagłówka XML zawierającego metadane i podstawowy opis sprawy umożliwia:

- Jednorodne procesowanie dokumentów elektronicznych i skanowanych.
- Zgodność z obowiązującymi regulacjami – między innymi w kontekście archiwizacji danych.
- Możliwość podpisania całości (nagłówek + załącznik) podpisem elektronicznym.
- Możliwość prostej realizacji mechanizmów wyszukiwania.
- Możliwość udostępniania urzędnikom podejmującym decyzję wglądu w kluczowe dla procesu informacje i status sprawy bez konieczności dostępu do pełnej treści załączników.
- Możliwość budowy brokerów usług pozwalających na automatyzację uprawnionego dostępu do niezbędnych informacji.

8.2. INTEROPERACYJNOŚĆ W PROJEKTOWANIU SYSTEMU

Projektując system należy także zwrócić uwagę na następujące zagadnienia:

8.2.1. PODSTAWOWA INTEROPERACYJNOŚĆ

Ze względu na to, że w systemach wykorzystywane są bardzo różne platformy i technologie, nowo wdrażane usługi Web Service muszą charakteryzować się interoperacyjnością niezależnie od tego, w jakiej technologii zostały utworzone. Specyfikacja *WS i Basic Profile* (na końcowym etapie prac, dostępna pod adresem http://www.ws-i.org/Profiles/BasicProfile-1.1.html) stanowi podstawy interoperacyjności usług *Web Service*, definiując zestaw standardów, na których oparte powinny być wszystkie implementacje usług *Web Service*. Specyfikacja ta precyzuje minimalny zestaw wymagań dla usług Web Service, których spełnienie gwarantuje interoperacyjność pomiędzy usługami działającymi na różnych platformach. Wymagane standardy to SOAP 1.1 (mimo że status rekomendacji W3C uzyskała już wersja 1.2 tego protokołu), XML 1.0 i HTTP 1.1 jako sposoby zapisu i przesyłania komunikatów, WSDL 1.1 i XML Schema 1.0 do opisu usług, UDDI v2 do publikowania i wyszukiwania usług oraz HTTPS (HTTP over TLS and SSL), X.509 *Public Key Infrastructure Certificate (PKI)* i CRL Profile jako standardy zapewniające bezpieczeństwo.

8.2.2. BEZPIECZEŃSTWO KOMUNIKATÓW

Po ustaleniu podstawowych specyfikacji, następnym krokiem jest zapewnienie bezpieczeństwa przesyłanych komunikatów. Zabezpieczanie komunikatów ma istotną przewagę nad zabezpieczaniem kanałów transmisji — ma znacznie szerszy zakres działania. Innymi słowy, zastosowanie mechanizmów zabezpieczeń na poziomie warstwy transportowej jest nieistotne, ponieważ zabezpieczenia dotyczą bezpośrednio samego komunikatu. Zastosowanie specyfikacji *WS-I Basic Security Profile* (obecny status *Working Group Draft*, dokument dostępny pod adresem http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html) do zapewnienia bezpieczeństwa na poziomie komunikatu gwarantuje interoperacyjność w zakresie zabezpieczeń pomiędzy wszystkimi stronami interakcji, które wiedzą, w jaki sposób komunikat jest zabezpieczony. Specyfikacja definiuje akceptowalne mechanizmy zabezpieczania komunikacji z usługami Web Service. Uwzględniono zabezpieczenia warstwy transportowej (SSL i TLS) oraz zabezpieczanie komunikatów SOAP zgodnie ze specyfikacją *WS Security* (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss) oraz określono wspierane typy tokenów bezpieczeństwa. Istnieją także dodatkowe specyfikacje, definiujące inne typy tokenów — na przykład REL (*Rights Expression Language*) czy SAML (*Security Assertion*

Markup Language). Pozostałych aspektów bezpieczeństwa komunikatów dotyczą inne specyfikacje z rodziny WS-*, na przykład *WS Trust* dotyczy wystawiania tokenów bezpieczeństwa, *WS SecureConversation* określa sposoby generowania kluczy sesji, używanych do zabezpieczania komunikacji na poziomie sesji, a *WS SecurityPolicy* uzupełnia specyfikację *WS Security* o możliwość definiowania wymagań w zakresie bezpieczeństwa komunikatów — typów obsługiwanych tokenów, algorytmów szyfrowania itp.

8.2.3. WYMAGANIA USŁUG

Z poszczególnymi usługami mogą być związane wymagania dotyczące konsumentów korzystających z tych usług. Wymagania te mogą precyzować typy obsługiwanych tokenów bezpieczeństwa czy algorytmów podpisywania komunikatów. Informacje o wymaganiach powinny być udostępniane w jednym, standardowym dla wszystkich usług formacie. Format taki został zdefiniowany w specyfikacji *WS Policy*. Specyfikacja ta pozwala na określanie wymagań i możliwości usług poprzez tworzenie odpowiednich zasad, pobieranych przez programistów podczas tworzenia aplikacji. Ponieważ w specyfikacji nie określono sposobu pobierania zasad czy też dołączania ich do usług *Web Service*, konieczne jest oparcie się na innych specyfikacjach, charakterystycznych dla wykorzystywanych technologii. Taką specyfikacją jest *WS PolicyAttachment*, która określa mechanizmy wiązania zasad z usługami *Web Service*.

8.2.4. ADRESOWANIE USŁUG WEB SERVICE

Aby móc rozpocząć korzystanie z usługi *Web Service*, niezbędne jest poznanie stosowanego przez tę usługę protokołu wymiany komunikatów oraz adresu, pod który komunikaty te należy wysyłać. Stosowanie specyfikacji *WS Addressing* (posiadającej obecnie status *Working Draft*; specyfikacja znajduje się pod adresem http://www.w3.org/TR/ws-addr-core/) do przesyłania komunikatów w sieci w sposób niezależny od warstwy transportowej gwarantuje, że każda ze stron kontraktu będzie rozumiała sposoby adresowania komunikatów stosowane przez drugą stronę i znała adres, pod który ma wysyłać komunikaty. Specyfikacja określa standardowe sposoby adresowania punktów końcowych usług Web Service za pomocą referencji punktu końcowego oraz przekazywania w nagłówkach informacyjnych komunikatu informacji na temat routingu komunikatu oraz sposobu wywołania usługi. Dzięki temu w nagłówkach komunikatu SOAP w standardowy

sposób można definiować przepływy zarówno synchroniczne, jak i asynchroniczne. Metoda ta jest całkowicie niezależna od warstwy transportowej, w przeciwieństwie do metod polegających na zawarciu opisu wywołania w nagłówkach warstwy transportowej. Przykładem może być stosowanie nagłówka SOAP ACTION w protokole HTTP do opisu operacji SOAP na poziomie warstwy transportowej, jak ma to dziś miejsce w większości usług Web Services. Przeniesienie tej informacji do nagłówka SOAP, dzięki czemu stanie się ona częścią komunikatu SOAP, pozwala zagwarantować pomyślne przesłanie komunikatu SOAP z wykorzystaniem dowolnego protokołu sieciowego i wykonanie właściwej operacji we właściwej usłudze.

8.2.5. NIEZAWODNE DOSTARCZANIE

W każdej rozproszonej architekturze opartej na wymianie komunikatów, niektóre komunikaty z pewnością uznawane są za krytyczne i ich poprawne dostarczenie jest wymaganiem stawianym całemu systemowi. Stosowanie specyfikacji *WS ReliableMessaging* (http://schemas.xmlsoap.org/ws/2005/02/rm/) pozwala na transmisję komunikatów z gwarancją dostarczenia. Przed przesłaniem komunikatu, nadawca i odbiorca wymieniają serię pakietów powitalnych (*handshake*), co gwarantuje niezawodność transmisji. Co więcej, specyfikacja *WS RealiableMessaging* definiuje także mechanizmy zachowania kolejności komunikatów — wywoływana usługa otrzymuje komunikaty w takiej kolejności, w jakiej zostały wysłane.

8.2.6. OBSŁUGA TRANSAKCJI

Czasami zachodzi konieczność, by wywołanie usługi *Web Service* było elementem transakcji wchodzącej w skład większej operacji. Zakres transakcji może być bardzo różny — od prostych transakcji bazodanowych (będących zwykle transakcjami zgodnymi z warunkami ACID) po długoterminowe transakcje biznesowe, których czas realizacji liczony jest w dniach, tygodniach i miesiącach, a nie w sekundach. Specyfikacje *WS Coordination, WS AtomicTransaction* oraz *WS BusinessActivity* zapewniają wsparcie dla transakcji, definiując sposób reprezentacji transakcji w komunikacie SOAP i pozwalając odbiorcy komunikatu na uczestnictwo w transakcji związanej z tym komunikatem.

8.2.7. ZAŁĄCZNIKI KOMUNIKATÓW

Stosowanie załączników jest dość powszechne, szczególnie w przypadku poczty elektronicznej. Może zaistnieć potrzeba dołączenia do komunikatu jakiegoś materiału w celu przesłania go do usługi oddziałowej. w takim wypadku protokół stosowany do komunikacji z usługą *Web Service* musi pozwalać na osadzanie załączników. Zarówno specyfikacja SOAP *Message Transmission Optimization Method* (MTOM) jak i XML-*binary Optimized Packaging* (XOP) pozwalają na osadzenie danych binarnych w kodzie XML w postaci wiadomości zakodowanej w MIME i dołączenie takiej treści do komunikatu SOAP.

8.2.8. METADANE USŁUG WEB SERVICE

Wraz z upowszechnieniem się usług Web Service nadejdzie konieczność Udostępnienia standardowego mechanizmu pobierania metadanych, dzięki któremu konsumenci w czasie projektowania aplikacji będą mogli pobrać metadane związane z usługą Web Service w sposób niezależny od wykorzystywanej warstwy transportowej. Dzięki temu konsument będzie mógł poznać wymagania i możliwości usługi Web Service. Metadane obejmują informacje takie jak zasady (WS Policy), kontrakt (WSDL) i schemat (XSD). Taki standardowy mechanizm pobierania metadanych związanych z usługą został zdefiniowany w specyfikacji *WS MetadataExchange*.

8.3. METASTANDARD DOKUMENTÓW ELEKTRONICZNYCH

W ramach planowanych projektów powinna zostać rozszerzona funkcjonalność opracowania „Metastandard dokumentów elektronicznych”, które powstało w ramach projektu ePUAP. w ramach istniejącego Meta standardu, zostały zdefiniowane podstawowe obiekty – składowe do budowania formularzy elektronicznych. Za pomocą formularzy elektronicznych zbudowanych z wykorzystaniem założeń Meta standardu mieszkańcy/przedsiębiorcy mogą kierować wnioski oraz podania.

Rozbudowa Meta standardu powinna być zrealizowana w trzech obszarach:

1. Rozszerzenie słownika o nowe obiekty podstawowe z zakresu zarządzania oświatą, zarządzania infrastrukturą.

2. Rozbudowa Meta standardu o elementy umożliwiające wykorzystanie formularzy wykorzystujących go do obsługi Wielokanałowej Platformy Świadczenia Usług Administracji Publicznej.
3. Rozbudowa Meta standardu o komponenty pomocne w budowania komunikatów służących do wymiany informacji i dokumentów pomiędzy jednostkami.

8.4. POWSZECHNE PROBLEMY DOTYCZĄCE ARCHITEKTURY

8.4.1. ZAPEWNIENIE DOSTĘPU DO STALE ROZSZERZAJĄCEGO SIĘ ZAKRESU FUNKCJI

Inicjatywy budowy systemów często powstają jako niewielkie projekty z ograniczonym zestawem funkcji, a następnie są stopniowo rozwijane i obejmują coraz szerszą funkcjonalność. Związanych jest z tym kilka specyficznych problemów, wynikających z różnorodności typów systemów i z rosnącej liczby tych systemów.

Systemy zaplecza (*back-end*) świadczące usługi publiczne pracują na wielu różnych platformach i korzystają z różnych technologii. Stopniowe wdrażanie różnorodnych usług jest scenariuszem typowym ze względu na stały rozwój i ewolucję inicjatyw w organizacjach. Zaprojektowanie i wdrożenie wspólnej infrastruktury, zdolnej do efektywnej obsługi rosnącej funkcjonalności systemu, jest dużym wyzwaniem, wykraczającym znacznie poza problemy spotykane w tradycyjnych systemach komercyjnych.

Efektywna platforma elektroniczna — wdrożona i działająca w warunkach produkcyjnych — powinna być dostatecznie elastyczna, by można było w łatwy sposób wprowadzać nowe usługi, nowe transakcje i dostosowywać platformę do zmieniających się wymagań — i to bez zmian w kodzie podstawowego rozwiązania, a najlepiej bez powodowania przestojów innych usług. Wdrażanie nowych usług powinno być standardową funkcją systemu, odpowiednio uwzględnioną w projekcie rozwiązania, a nie rzadkim, wymagającym specjalnego traktowania przypadkiem.

8.4.2. RÓŻNORODNOŚĆ KANAŁÓW DOSTĘPU

Istnieje wysokie prawdopodobieństwo, że nawet jeśli kanały dostępu do pierwotnego zestawu usług zostaną dobrze zdefiniowane w początkowym etapie projektu i właściwie przygotowane w pierwszej implementacji, to po pewnym czasie i tak pojawi się potrzeba

obsługi nowych kanałów dostępu, takich jak kioski multimedialne, interaktywna telewizja czy urządzenia przenośne.

Dobrze zaprojektowana platforma integracyjna, zapewniająca spójny sposób świadczenia usług, powinna umożliwiać dodawanie nowych kanałów dostępu poprzez jednorazowe zmodyfikowanie centralnego huba bez konieczności modyfikowania poszczególnych usług.

Szerokie wsparcie różnorodnych platform klienckich

Projekty teleinformatyczne związane z interakcją ze światem zewnętrznym są często przedmiotem znacznie bardziej ścisłych regulacji i ograniczeń niż typowe systemy komercyjne. Zapewnienie niedyskryminującego dostępu do usług z szerokiej gamy platform klienckich jest często wymaganiem jasno sprecyzowanym w przepisach prawnych, a przynajmniej pożądanym z politycznego punktu widzenia. Może się to wiązać z obsługą różnych typów i wersji sprzętu, systemów operacyjnych i oprogramowania przeglądarkowego.

Właściciel systemu komercyjnego może podjąć uzasadnioną ekonomicznie decyzję wykluczenia niewielkiej części potencjalnych klientów poprzez ograniczenie zakresu obsługiwanych platform. Takie postępowanie — niewiele zmniejszając potencjalny przychód — pozwala uzyskać znaczne oszczędności, wynikające z mniejszego zakresu prac projektowych i programistycznych nad systemem i mniejszej liczby niezbędnych do wykonania testów.

Dostawcy usług dla obywateli i przedsiębiorstw mają w tym zakresie mniejszą swobodę działania i często muszą ponosić znaczne koszty związane z uwzględnieniem różnych platform, by nie wykluczyć i nie dyskryminować nawet niewielkich grup społecznych.

Jest niezwykle istotne, by ograniczenia i wymagania związane z obsługą szerokiego spektrum platform klienckich zostały uwzględnione już na etapie projektowania architektury platformy integracyjnej — uwzględnienie tych warunków na dalszych etapach projektu może być bardzo kosztowne, a nawet niemożliwe.

8.4.3. OBSŁUGA WIELU JĘZYKÓW I WSZECHSTRONNY DOSTĘP

W wielu krajach zapewnienie wielojęzycznego dostępu do usług jest wymaganiem prawnym, a przynajmniej należy do dobrych zwyczajów. w przypadku komunikacji

z przedstawicielstwami Komisji Europejskiej jest to zwykle niezbędne. Uwzględnienie tego warunku już na początku realizacji projektu jest istotne, ponieważ wymaganie to ma duży wpływ na architekturę rozwiązania. Należy też mieć na uwadze:

- Zapewnienie różnych poziomów obsługi wielojęzyczności, w tym akceptowanie danych wielojęzycznych, zróżnicowanie skryptów i stron (na przykład do obsługi języków zapisywanych od prawej do lewej lub z użyciem znaków diakrytycznych).
- Problemy dotyczące przetwarzania i przechowywania danych, które mają wpływ na stosowany model danych i wymagają szczególnej uwagi podczas pisania kodu aplikacji.
- Wymagania zaprojektowania w pełni wielojęzycznego interfejsu użytkownika, w którym wszystkie łańcuchy tekstowe i komunikaty są odseparowane od kodu. w takim wypadku do pełnej obsługi języków znakowych pisanych od prawej do lewej niezbędne jest przygotowanie alternatywnych plików graficznych i innych treści. Należy także wziąć pod uwagę, że ten sam tekst w różnych językach może mieć różną długość.

Witryny i usługi elektroniczne są często objęte bardzo rygorystycznymi wymaganiami dotyczącymi przystępności (*accessibility*) dla osób o ograniczonej sprawności — znacznie większymi niż w przypadku zwykłych witryn komercyjnych, gdzie przystępność jest pożądana w celu poszerzenia grupy odbiorców, ale jej brak ma jedynie niewielki wpływ na komercyjny efekt przedsięwzięcia. Dla witryn i usług administracji publicznej przystępność jest zwykle wymagana prawem, a na dodatek jest ważnym problemem politycznym. Zajęcie się problemem przystępności już po zaprojektowaniu systemu jest trudne, drogie, a często niewykonalne. Przystępność już od samego początku powinna być podstawowym założeniem projektu.

W części Odsyłacze, listy kontrolne i dalsze informacje tego opracowania zamieszczono listy kontrolne dotyczące tworzenia aplikacji łatwych w lokalizacji oraz listę odsyłaczy do bieżących regulacji prawnych dotyczących przystępności, do inicjatyw (w tym także do wytycznych w zakresie przystępności, opracowanych przez organizację *World Wide Web Consortium* — W3C), do programów syntezy mowy odczytujących teksty z ekranu komputera

oraz do specjalnych przeglądarek, narzędzi do testowania przystępności aplikacji oraz do innych przydatnych zasobów.

8.4.4. OBSŁUGA WIELU RÓŻNYCH POŚWIADCZEŃ TOŻSAMOŚCI

Korzystanie z różnych usług elektronicznych zwykle wymaga podania specyficznego dla danej usługi identyfikatora użytkownika — na przykład numeru PESEL, identyfikatora NIP, identyfikatora dostawcy – REGON, itp. Gdy kontrola dostępu jest implementowana niezależnie dla każdej z usług, umożliwienie elektronicznego dostępu do wielu usług oznacza utworzenie odrębnych, niezależnych dla każdej usługi poświadczeń tożsamości. Użytkownicy muszą wtedy pamiętać wiele identyfikatorów i zarządzać wieloma hasłami.
Stanowi to problem nawet w przypadku często wykorzystywanych usług, takich jak bankowość elektroniczna. w przypadku usług administracji publicznej, próba przypomnienia sobie hasła czy identyfikatora do każdej z usług może sprawiać jeszcze większe trudności. Wprowadzenie platformy dla sektora publicznego, zapewniającej dostęp do wielu usług na podstawie pojedynczego zestawu poświadczeń tożsamości, jest niezwykle istotne dla upowszechnienia się usług dla tego sektora.

8.4.5. UDOSTĘPNIENIE KAŻDEJ Z USŁUG W SPÓJNY I BEZPIECZNY SPOSÓB

Udostępnienie dowolnej usługi za pomocą kanałów elektronicznych wymaga znacznych nakładów i wysiłków — konieczne jest spełnienie wszystkich wymagań w zakresie bezpieczeństwa, dostępności i niezawodności. w niektórych krajach obowiązują rygorystyczne uregulowania prawne i każdy system administracji publicznej przed podłączeniem do Internetu musi przejść obowiązkowy proces certyfikacji. Tworzenie dostępu elektronicznego dla każdej usługi z osobna prowadzi do powielenia tych wysiłków. Oznacza to stratę czasu, zasobów i niepotrzebne angażowanie specjalistów, którzy nie zawsze są dostępni w urzędach świadczących te usługi.

Problem staje się szczególnie istotny, gdy usługi elektroniczne zaczynają być tak popularne, że muszą być świadczone nie tylko przez początkową grupę dużych jednostek administracji, które mają odpowiednią wielkość, widoczność i wpływy polityczne potrzebne do zabezpieczenia sobie niezbędnych zasobów. Mniejsze organizacje, takie jak administracja samorządowa, nie są w stanie samodzielnie pokryć początkowych kosztów świadczenia usług w sposób elektroniczny.

Zidentyfikowanie najbardziej problematycznych elementów systemu i jednokrotne zaimplementowanie ich w powszechnej platformie, współdzielonej przez wszystkie usługi, pozwala zapewnić wysoką jakość, spójność i bezpieczeństwo tworzonych rozwiązań oraz uzyskać znaczące oszczędności.

8.4.6. ZARZĄDZANIE TOŻSAMOŚCIĄ

Zaprojektowanie i wdrożenie efektywnego i bezpiecznego systemu zarządzania tożsamością nie jest zadaniem trywialnym, zważywszy, że liczba potencjalnych użytkowników może sięgać setek tysięcy. Ze względu na koszty i złożoność problemu, jest oczywiste, że zarządzanie tożsamością powinno zostać zaimplementowane w postaci pojedynczego systemu, współdzielonego przez wszystkie usługi.

8.4.6.1. POJEDYNCZE POŚWIADCZENIA DO DOSTĘPU DO WIELU USŁUG

Wprowadzenie możliwości wykorzystania pojedynczego poświadczenia tożsamości do dostępu do wielu usług (jak zostało to opisane wcześniej w rozdziale Obsługa wielu różnych poświadczeń tożsamości) wymaga zbudowania powszechnej infrastruktury uwierzytelniania użytkowników, wspólnej dla wszystkich usług wchodzących w skład systemu.

Warto w tym miejscu zauważyć, że stosowanie jednego zestawu poświadczeń tożsamości do dostępu do wielu usług wcale nie oznacza, że do dostępu do wszystkich usług musi być stosowany jeden i ten sam zestaw poświadczeń. Mimo oczywistych zalet dostępu do wielu usług z wykorzystaniem jednego zestawu poświadczeń, platforma powinna pozostawiać użytkownikom swobodę wyboru usług, do których chcą uzyskiwać dostęp na podstawie określonego zestawu poświadczeń, i umożliwiać korzystanie z wielu niezależnych zestawów poświadczeń.

8.4.6.2. SPÓJNE LOGOWANIE A POJEDYNCZE LOGOWANIE

Gdy użytkownicy uzyskali już możliwość logowania się do rosnącej liczby usług za pomocą jednego zestawu poświadczeń, to zarówno dla użytkowników, jak i dostawców usług istotne staje się, by koszty i nakłady pracy, związane z umożliwieniem dostępu do każdej kolejnej usługi, utrzymać na jak najniższym poziomie.

Dostęp do poszczególnych usług na podstawie jednego zestawu poświadczeń może być realizowany na różnych poziomach — między innymi poprzez spójne logowanie lub

pojedyncze logowanie. Spójne logowanie to forma najprostsza — dostęp do poszczególnych usług realizowany jest na podstawie pojedynczego zestawu poświadczeń, ale użytkownik nadal musi meldować się do każdej usługi z osobna. Co prawda użytkownicy muszą pamiętać tylko jeden zestaw poświadczeń, ale za każdym razem, gdy chcą korzystać z innej usługi, muszą się ponownie zameldować (jednak w niektórych przypadkach taki dodatkowy etap logowania może okazać się pożądany).

Jednym ze sposobów implementacji spójnego logowania jest utrzymywanie przez każdą niezależną usługę własnej bazy danych uwierzytelniających. Bazy danych wzajemnie synchronizują swoją zawartość, dzięki czemu poszczególne kopie poświadczeń logowania są identyczne. Poszczególne usługi — zamiast implementować własne mechanizmy uwierzytelniania — mogą korzystać z pojedynczej, wspólnej usługi uwierzytelniania. Zakładana spójność uzyskiwana jest automatycznie, ponieważ poświadczenia użytkowników przechowywane są tylko w jednej lokalizacji.

Bardziej zaawansowane rozwiązanie umożliwia użytkownikom przezroczysty dostęp do wielu usług po jednokrotnym zalogowaniu. Oznacza to prostotę korzystania z systemu przez użytkowników i pozwala na agregowanie usług. Dobrymi przykładami takich rozwiązań są portale, które komunikując się w tle z różnymi usługami zapewniają użytkownikom możliwość korzystania z wielu usług jednocześnie.

8.4.6.3. ODWZOROWYWANIE TOŻSAMOŚCI

Zastosowanie pojedynczego zestawu poświadczeń do dostępu do wielu usług jest niewątpliwie użyteczne, ale rozwiązuje tylko jedną część problemu — ułatwia użytkownikowi korzystanie z systemu. Systemy docelowe nadal korzystają z własnych, specyficznych identyfikatorów, wyróżniających użytkownika w kontekście danego systemu. Identyfikatory te są niezbędne do prawidłowego rozpoznania użytkownika i poprawnej pracy systemu i zwykle nie mają żadnego znaczenia poza kontekstem określonej usługi. Większość obecnie wykorzystywanych systemów korzysta z takich specyficznych identyfikatorów, w związku z tym udostępnianie przez wspólną platformę funkcji odwzorowania pojedynczego zestawu poświadczeń na odpowiednie identyfikatory, specyficzne dla poszczególnych usług, jest niezwykle istotne dla zapewnienia efektywnego dostępu do rosnącej liczby usług.

W wielu krajach nie wprowadzono uniwersalnego krajowego identyfikatora dla obywateli, w związku z czym każda usługa wykorzystuje własne, specyficzne identyfikatory. Pewne ograniczenia istnieją nawet w krajach, w których wszyscy obywatele posiadają unikatowe identyfikatory i systemy mogą w oparciu o nie identyfikować użytkownika. Na przykład w sytuacji, gdy jedna osoba może mieć wiele relacji z daną usługą (np. kontakt z wieloma urzędami), identyfikator obywatela nie pozwala na rozróżnienie poszczególnych relacji, w związku z czym potrzebny jest identyfikator specyficzny dla danej usługi.

W przypadku bardziej złożonych relacji (na przykład takich jak opisane w następnym rozdziale Trudne przypadki) konieczność odwzorowania pojedynczego zestawu poświadczeń na odpowiedni, właściwy w danym kontekście identyfikator, jest jeszcze bardziej oczywista.

Nawet jeśli bezpośrednie zastosowanie numeru identyfikacyjnego obywatela jest technicznie możliwe, mogą pojawić się wątpliwości dotyczące poufności danych. Takie stosowanie numeru identyfikacyjnego stoi także w sprzeczności z podstawowymi zasadami zarządzania tożsamością. Chodzi głównie o zasady minimalnego zakresu ujawniania niezbędnych informacji oraz tożsamości ukierunkowanej.
W czasie obsługi interakcji użytkownika z usługą należy uwierzytelnić użytkownika (jeśli to możliwe — na podstawie pojedynczego zestawu poświadczeń), a następnie przekazać usłudze jedynie specyficzne dla niej identyfikatory dotyczące tej interakcji. Nie należy ujawniać głównego identyfikatora użytkownika, który mógłby zostać użyty do skorelowania tożsamości użytkownika w poszczególnych usługach. w przypadkach, gdy taka korelacja jest korzystna i potrzebna (na przykład w celu zapewnienia lepszej obsługi użytkowników i agregacji usług), musi ona zostać przeprowadzona jawnie i za zgodą użytkownika. Korelowanie informacji o użytkowniku bez uzyskania zgody tego użytkownika jest niedozwolone — raz ze względu na dobre praktyki, dwa — na uwarunkowania prawne. w niektórych krajach, takich jak Francja, Portugalia czy Wielka Brytania, tworzenie takich korelacji jest zabronione prawem.

Zapewnienie niezawodnego, bezpiecznego, jednokierunkowego odwzorowania tożsamości użytkownika na specyficzne dla usług i właściwe dla kontekstu interakcji identyfikatory to podstawowe zadanie, realizowane przez powszechną infrastrukturę, współdzieloną przez wszystkie usługi wchodzące w skład systemu.

8.4.6.4. POCZĄTKOWA IDENTYFIKACJA UŻYTKOWNIKÓW

Bezpieczne udostępnianie usług uzależnione jest od rozwiązania problemu identyfikacji początkowej, to jest od przydzielania poświadczeń tożsamości konkretnym osobom. Prawidłowa identyfikacja początkowa jest niezwykle istotna dla ogólnego bezpieczeństwa i udanego wdrożenia rozwiązania. w przypadku platformy, gdzie liczba użytkowników może sięgać wielu milionów, a każdy z użytkowników korzysta z rosnącej liczby usług, niezwykle istotne jest przeprowadzenie tej identyfikacji w sposób efektywny, skalowalny i wystarczająco elastyczny, by uwzględnić szeroki zakres wymagań.

Istnieje kilka sposobów początkowej identyfikacji użytkownika:

- Scentralizowany — pojedynczy, zunifikowany mechanizm początkowej identyfikacji użytkowników. Po początkowym zidentyfikowaniu użytkownika i przydzieleniu mu poświadczeń tożsamości, wszystkie kolejne relacje z różnymi usługami inicjowane są na podstawie tej jednokrotnej identyfikacji początkowej, co implikuje, że wszystkie usługi opierają się na zunifikowanej procedurze identyfikacji początkowej i ufają jej.
- Zdecentralizowany (związany z usługami) — relacje pomiędzy użytkownikiem a poszczególnymi usługami nawiązywane są indywidualnie i są niezależne od relacji z innymi usługami. w takim wypadku nie występują związki zaufania ani zależności pomiędzy usługami. Poszczególne usługi mogą definiować własne, odpowiednie i różne reguły i procedury identyfikacji początkowej.
- Zaufanie ukierunkowane — poszczególne usługi mogą opierać się na procedurach identyfikacyjnych innych usług. Inaczej mówiąc, mogą ufać tym usługom. Model ten jest podobny do modelu scentralizowanego, pozwala jednak na tworzenie wielu różnych związków zaufania.

Model scentralizowany może wydawać się atrakcyjny, prostszy i bardziej efektywny, istnieje jednak kilka przeszkód utrudniających udaną implementację tego modelu w rozwiązaniach:

- Model ten wymaga istnienia nadrzędnego organu, któremu ufają i będą ufać wszystkie inne usługi i który będzie prowadził scentralizowany proces identyfikacji. Nawet jeżeli dostawcy początkowego zestawu usług uzgodnią

odpowiadający im wspólny proces identyfikacji początkowej, to nie ma gwarancji, że powstające w przyszłości usługi będą pasowały do tego modelu.

- Wymagany poziom szczegółowości i niezawodności identyfikacji początkowej jest różny dla różnych kategorii usług, dlatego pojedyncza uniwersalna procedura identyfikacji musi gwarantować najwyższy poziom pewności, jaki może być wymagany przez dowolną z usług. Może to być zbyt uciążliwe dla użytkowników, którzy korzystają wyłącznie z usług o niższych wymaganiach co do identyfikacji początkowej.

Model zdecentralizowany (związany z usługami) daje większą elastyczność i pozwala na uwzględnienie szerszego zakresu wymagań, włącznie z wymaganiami zmiennymi w czasie i nieznanymi podczas pierwotnej implementacji systemu. Jeśli identyfikacja początkowa zostanie oparta na podstawowej, wspólnej strukturze, pozwalającej na stosowanie „wymiennych" reguł, definiowanych przez poszczególne usługi, rozwiązanie może łatwo ewoluować — można w nim wprowadzać dodatkowe wymagania dla nowych usług bez wpływu na działanie usług już istniejących. Jeśli liczba oferowanych przez system usług jest znaczna, taki zdecentralizowany, związany z usługami model jest jedynym realnym rozwiązaniem.

Model zdecentralizowany, dzięki elastyczności wymiennych modułów uwierzytelniania początkowego — pozwala także na implementację modelu zaufania ukierunkowanego, który może obejmować sprawdzenie, czy dany użytkownik został wcześniej zidentyfikowany przez inną usługę.

9. ZASADY PROWADZENIA PROJEKTU

9.1. PODSTAWOWE ZASADY

PLANOWANIE PRAC i JEDNOZNACZNE PRZYPISANIE ZADAŃ

Projekt realizowany jest w oparciu o szczegółowy plan, przygotowany przed rozpoczęciem prac przez doświadczonego menedżera. Plan służy do bieżącej kontroli postępów prac oraz stanowi narzędzie komunikacyjne dla zespołu projektowego i osób współpracujących z projektem. Plan może być modyfikowany w uzgodnieniu z Zamawiającym, aby odzwierciedlić zmieniające się warunki, status projektu i oczekiwania wobec projektu. Projekt ma jasno określoną strukturę organizacyjną, ścieżki raportowania i podział zadań.

RAPORTOWANIE STATUSU i NAPOTKANYCH TRUDNOŚCI

Zespoły oraz cały projekt raportują w cyklu tygodniowym w sposób formalny postęp prac w stosunku do planu oraz napotkane trudności. Kierownictwa zespołów oraz kierownictwo projektu reaguje natychmiast na opóźnienie i inne napotkane trudności udzielając zespołom wskazówek, przemieszczając zasoby, podejmując wymagane decyzje lub zwracając się o decyzje do właściwych osób.

W procesie tym biorą udział członkowie zespołu projektowego oraz jego kierownictwo ze strony Wykonawcy oraz Zamawiającego. Obydwie strony podlegają podobnej dyscyplinie.

ZAPEWNIENIE JAKOŚCI

Projekty są objęte programem zapewnienia jakości. Jakość jest zdefiniowana jako spełnienie lub przekroczenie oczekiwań Zamawiającego względem rezultatów i przebiegu projektu.

W skrócie, zapewnienie jakości projektu odbywa się w następującym cyklu:

- identyfikacja oczekiwań sponsorów projektu i stron zainteresowanych (np. w formie rozmów ze sponsorem i najważniejszymi odbiorcami rezultatów prac),
- planowanie działań projektowych w sposób, który pozwoli na spełnienie zidentyfikowanych oczekiwań,
- rygorystyczna realizacja planu projektu,
- ocena zgodności rezultatów pośrednich i końcowych z oczekiwaniami,

- podejmowanie działań korekcyjnych oraz dostrajanie procesów celem osiągnięcia oczekiwanych efektów i stałej poprawy.

Zgodnie z metodyką, w regularnych odstępach czasu wykonawca przeprowadza potwierdzenie zarządzania jakością u Zamawiającego (ang. Client Quality Management Assurance - CQMA), razem z zespołem zamawiającego. CQMA zostanie przeprowadzone przez niezależnego Partnera jakości z firmy Wykonawcy i będzie skoncentrowane na zapewnieniu i zweryfikowaniu, że Wykonawca dostarcza usługi na poziomie umożliwiającym zaspokojenie potrzeb i celów jednostki. Jednocześnie CQMA pozwoli na określenie możliwości ulepszenia realizacji projektu przez biorące w nim udział zespoły.

ZARZĄDZANIE RYZYKIEM PROJEKTU

Zarządzanie ryzykiem służy redukcji podatności przedsięwzięć na potencjalne zdarzenia, które mogą zagrozić osiągnięciu planowanych celów.

Powyższy cel jest osiągany za pomocą szeregu elementów:

- role i obowiązki uczestników projektu w zakresie zarządzania ryzykami,
- linie i częstotliwość raportowania ryzyk i działań z nimi związanych,
- proces zarządzania ryzykiem.

W szczególności proces zarządzania ryzykiem obejmuje:

- identyfikację ryzyk w dziedzinie projektu;
- klasyfikację ryzyk ze względu na rodzaj (finansowe, terminowe, techniczne, operacyjne i organizacyjne);
- oszacowanie poziomu wpływu każdego zidentyfikowanego ryzyka na projekt w wymiarze prawdopodobieństwa jego wystąpienia, zakresu zagrożenia, jakie niesie i poziomu kontroli nad ryzykiem;
- ustalenie strategii postępowania w kategoriach podjęcia działań redukujących ryzyko, przyjęcia innych rozwiązań dla uniknięcia ryzyka, transferu odpowiedzialności na inny podmiot, opóźnienia decyzji i podjęcia działań oraz akceptacji ryzyka na obecnym poziomie;

- podjęcie i monitorowanie działań redukujących ryzyko;
- Analiza i aktualizacja zbioru zidentyfikowanych ryzyk.

Na etapie planowania projektu powstaje plan zarządzania ryzykiem, który zawiera definicje powyższych elementów w kontekście rozważanego projektu i precyzuje sposób postępowania. Na tym etapie powstaje również rejestr ryzyk, gdzie na bieżąco w czasie trwania projektu aktualizowane są informacje o każdym ryzyku, zgodnie z procesem. Zazwyczaj właścicielem rejestru ryzyk jest kierownictwo przedsięwzięcia.

TESTOWANIE

W ramach procesu wdrożeniowego, prócz testów jednostkowych rozszerzeń, przeprowadzone będą dwukrotne testy systemu.

Zasady przeprowadzania testów

Zarówno testy wstępne jak i akceptacyjne, będą prowadzone przez uprzednio przeszkolonych członków zespołu wdrożeniowego ze strony Zamawiającego. Zamawiający jest odpowiedzialny za przygotowanie scenariuszy testowych i danych testowych, przeprowadzenie testów oraz przygotowanie wyników testów.

Procedura testów obejmuje następujące etapy:

- Opracowanie i akceptacja planu testów.
- Opracowanie i akceptacja scenariuszy (skryptów testowych).
- Przeprowadzenie testów.
- Opracowanie i akceptacja analizy uwag testowych.

Testy będą przeprowadzone przez Zamawiającego w terminie przewidzianym w harmonogramie, zgodnie z zaakceptowanym planem testów. Nieprzystąpienie do testów w tym terminie jest równoznaczne, z przeprowadzeniem testów bez uwag.

Testy zostaną przeprowadzone w oparciu o przygotowane wcześniej i zatwierdzone scenariusze (skrypty) testowe. Scenariusze (skrypty) testów zostaną przygotowywane dla każdego testu, zgodnie z planem testów i planem projektu przez administratorów biznesowych lub / i użytkowników kluczowych Zamawiającego. Testy zostaną wykonane z użyciem środowiska testowego, na bazie reprezentatywnej próbki danych

eksploatacyjnych. Dane testowe zostaną przygotowane przez administratorów biznesowych lub / i użytkowników kluczowych Zamawiającego. Testy będą przeprowadzone przez użytkowników kluczowych Zamawiającego, którzy uczestniczyli w procesie definiowania sposobu realizacji wymagań biznesowych.

Zakres testów nie może wykraczać poza merytoryczny zakres projektu.

Test może zostać przerwany, jeżeli z jakiejkolwiek przyczyny nie może być kontynuowany (np. poważny błąd w oprogramowaniu lub awaria systemu). Test taki może zostać powtórzony lub kontynuowany w innym terminie po obustronnym uzgodnieniu.

Scenariusze testów i dane testowe przygotowywane są dla każdego testu i obejmują:

- operacje do wykonania w aplikacji,
- oczekiwany rezultat,
- uwagi - wpisywane w czasie przeprowadzania testu, gdy wystąpią różnice pomiędzy rezultatami oczekiwanymi w czasie testu a uzyskanymi.

Po zakończeniu testowania każdego z obszarów, wyznaczona ze strony Zamawiającego osoba odpowiedzialna za przebieg testowania podpisuje i przekazuje kierownikowi projektu ze strony Wykonawcy protokół testów. Protokół testów zawiera uwagi rejestrowane w czasie przeprowadzania testów, gdy wystąpią różnice pomiędzy rezultatami oczekiwanymi, a uzyskanymi w czasie testu. Uwagi zapisane w czasie testów są następnie poddawane analizie podczas spotkania potestowego, w formie dokumentu „Analiza uwag potestowych”. Spotkanie potestowe musi odbyć się w ciągu 2 dni od momentu zakończenia testów. w spotkaniu uczestniczą użytkownicy kluczowi, konsultanci wiodący oraz kierownicy projektu.

Testy wstępne

Testy wstępne zostaną przeprowadzone po opracowaniu modelu systemu na podstawie odwzorowania na system docelowych procesów biznesowych.

Celem testów wstępnych nie jest finalny odbiór / akceptacja rozwiązania a sprawdzenie poprawności parametryzacji systemu w stosunku do zaakceptowanego modelu biznesowego.

Każda uwaga, zapisana w czasie testów wstępnych musi mieć nadany status. Działania podjęte w wyniku zgłoszenia uwagi będą zależały od nadanego statusu. Na spotkaniu potestowym mogą zostać uzgodnione następujące statusy zgłoszonych uwag:

Status	**Opis**
Nie dotyczy	Uwaga jest wycofana – np. mogła być nieuzasadniona lub nie odnosić się do istoty testu
Brak zmian	Funkcja jest zaakceptowana bez podejmowania żadnych akcji naprawczych
Zmiana	Funkcja zostanie zmieniona
Dodatkowa funkcjonalność	Funkcja jest zaakceptowana, jej zmiana wymaga realizacji procedury Żądania Zmiany

Uwagi o statusie „Zmiana" będą opatrzone sposobem realizacji zmiany.

Status uwag oraz sposób realizacji zostanie uzgodniony pomiędzy Zamawiającym a Wykonawcą.

Testy akceptacyjne

Testy akceptacyjne stanowią podstawę do odbioru systemu i rozpoczęcia eksploatacji produkcyjnej. Celem testów akceptacyjnych jest potwierdzenie działania systemu zgodnie z odwzorowaniem na system docelowych procesów biznesowych i uzgodnionym sposobem realizacji uwag z testów wstępnych.

Uwagi z testów akceptacyjnych zostaną opracowane w formie dokumentu „Analiza uwag potestowych". Dokument będzie zawierał status poszczególnych uwag testowych.

Każda uwaga, zapisana w czasie testów akceptacyjnych musi mieć nadany status. Działania podjęte w wyniku zgłoszenia uwagi będą zależały od nadanego statusu. Na spotkaniu potestowym mogą zostać uzgodnione następujące statusy zgłoszonych uwag:

Status	Opis
Nie dotyczy	Uwaga zostaje wycofana - np. mogła być nieuzasadniona lub nie odnosić się do istoty testu
Brak zmian	System zostanie zaakceptowany bez podejmowania żadnych akcji naprawczych
Zmiana natychmiastowa	Funkcja musi zostać poprawiona przed zaakceptowaniem systemu
Zmiana odroczona	System zostanie zaakceptowany, funkcja musi zostać poprawiona przed upływem uzgodnionego terminu
Dodatkowa funkcjonalność	System zostanie zaakceptowany, zmiana funkcji wymaga realizacji procedury żądania zmiany.

Uwagi o statusie „Zmiana natychmiastowa” i „Zmiana odroczona” będą opatrzone sposobem realizacji zmiany. Status „Zmiana natychmiastowa” lub „Zmiana odroczona” nie może zostać nadany funkcji, dla której nie zgłoszono uwag i nie uzgodniono zmiany podczas testów wstępnych. Status „Zmiana natychmiastowa” może zostać przypisany jedynie uwadze uniemożliwiającej działanie systemu, gdy nie istnieje sposób jego obejścia przy pomocy procedur ręcznych. Status uwag oraz sposób realizacji zostanie uzgodniony pomiędzy Zamawiającym, a Wykonawcy.

Odbiór całości lub części systemu nastąpi po przeprowadzeniu testów akceptacyjnych i realizacji uwag testowych opatrzonych statusem „Zmiana natychmiastowa”. Rozpoczęcie produkcyjnej eksploatacji systemu jest jednoznaczne z odbiorem całości lub części systemu i potwierdzeniem realizacji wszystkich zadań zmierzających do jego uruchomienia i umożliwia ich jednostronną akceptację przez Wykonawcy.

PROCEDURA ŻĄDANIA ZMIANY

Celem procedury jest kontrola integralności końcowego rozwiązania, jego zgodności z celami stawianymi wskazanymi w umowie, kontrolowanie podstawowych ograniczeń: zakresu, budżetu oraz harmonogramu.

Procedura umożliwia wprowadzenie zmian w stosunku do zakresu planowanych prac, zatwierdzonych produktów projektu, harmonogramu, budżetu lub jakości produktów projektu.

Potrzeba wprowadzenia zmian może wynikać między innymi z:

- Potrzeb, które zostały błędnie zdefiniowane, nie zostały zdefiniowane lub uległy zmianie w trakcie dotychczasowego przebiegu projektu.
- Zaakceptowanego sposobu neutralizacji ryzyk projektowych.
- Wprowadzenia w trakcie wdrożenia zmian organizacyjnych u Zamawiającego, które mają wpływ na zatwierdzony sposób realizacji procesów biznesowych.
- Konieczności wprowadzenia zmian w zatwierdzonych produktach projektu.

Każde żądanie zmiany ma jeden z poniższych stanów:

Stan	Opis
Zgłoszone	Żądanie zmiany nie zostało przypisane do szczegółowego rozpoznania
Rozpoznawane	Żądanie zmiany przekazano do rozpoznania
Zaprojektowane	Sposób realizacji żądania zmiany wraz z harmonogramem został zaprojektowany i oszacowany. Zdefiniowany został zakres żądanych zmian i wymagana jest aprobata dla przyjętego rozwiązania.
Zatwierdzone	Zaprojektowany sposób realizacji żądania zmiany, wraz ze zmianami w koszcie i harmonogramie projektu zostało zaakceptowane i jest gotowe do realizacji.
Zaniechane	Żadna akcja nie zostanie podjęta. Zaniechanie zmiany.

ZGŁOSZENIE ŻĄDANIA ZMIANY

Kierownik projektu każdej ze stron, ma prawo i obowiązek formalnego zgłoszenia żądania zmiany, jeżeli uzna, że dla zapewnienia sukcesu projektu konieczne jest podjęcie działań mających wpływ na ustalony zakres prac, harmonogram, budżet, jakość lub ryzyko projektu.

Zmiana zatwierdzonych produktów projektu, jeżeli ma wpływ na wyżej wymienione aspekty projektu, również winna być realizowana poprzez zgłoszenie żądania zmiany. Żądanie Zmiany może być też zainicjowane w ramach procedury zarządzania ryzykiem.

Żądanie zmiany jest dokumentowane przez zgłaszającego za pomocą formularza żądania zmiany. Żądanie otrzymuje stan „zgłoszone".

ROZPOZNANIE

Kierownictwo projektu przypisuje osobę z zespołu projektowego do szczegółowego rozpoznania zmiany. Zmienia stan żądania na „rozpoznawane" i wyznacza datę zakończenia rozpoznania, przy czym termin nie powinien być dłuższy od 5 dni od daty zgłoszenia.

W przypadku rozpoznania zmiany przeprowadzanego przez Wykonawcy, nakład pracy konsultantów Wykonawcy na rozpoznanie żądania zmiany oszacowany przez kierownika projektu Wykonawcy musi być zaakceptowany przez kierownika projektu Zamawiającego, przed przystąpieniem do rozpoznania. w przypadku decyzji o realizacji żądania zmiany, koszty przeprowadzenia analizy zwiększają koszt realizacji żądania.

Osoba wyznaczona do rozpoznania, dokonuje szczegółowej analizy wpływu zmian na zakres prac, harmonogram, pracochłonność, koszty, jakość i ryzyko projektu oraz przedstawia rekomendację sposobu realizacji żądania zmiany.

Jeśli kierownictwo projektu uzna, że analiza jest niewystarczająca rozpoznanie przeprowadzane jest ponownie.

SKIEROWANIE ŻĄDANIA DO KOMITETU STERUJĄCEGO

Kierownictwo projektu, w ciągu 3 dni od otrzymania sposobu realizacji zmiany, musi podjąć jedno z następujących działań:

- Zaniechać realizacji zmiany. Wraz z uzasadnieniem swej decyzji, zmienić stan żądania na „zaniechane".

- Przedstawić komitetowi sterującemu żądanie zmiany wraz ze szczegółowym planem i kosztem realizacji. Zmienić stan żądania na „zaprojektowane”.
- Przy bezskutecznym wyczerpaniu powyższej procedury, zmiana ma stan „zaniechane”.

ZATWIERDZENIE

- Na swym najbliższym posiedzeniu, komitet sterujący może podjąć jedno z następujących działań:
- jednogłośnie, pisemnie zatwierdzić na formularzu żądania zmiany sposób realizacji zmiany. Stan dokumentu zostanie zmieniony na „zatwierdzone”.
- zaniechać realizacji zmiany - stan „zaniechane”
- wyłącznie jeden raz skierować do ponownego rozpoznania w ciągu 5 dni roboczych wyznaczając osobę odpowiedzialną - stan „rozpoznawane”.
- wyłącznie jeden raz odroczyć datę podjęcia decyzji do określonego dnia, lecz nie później niż o 5 dni, podając ostateczny dzień podjęcia decyzji.

Zmiany skutkujące rozszerzeniem zakresu prac Wykonawcy zostaną skierowane do realizacji wyłącznie po zatwierdzeniu dodatkowego zamówienia na usługi.

Przy bezskutecznym wyczerpaniu powyższej procedury, zmiana ma stan „zaniechane”.

Po zatwierdzeniu żądania zmiany, kierownicy projektu są zobowiązani do wprowadzenia odpowiednich zmian w planie projektu w celu realizacji zmiany oraz o poinformowanie uczestników projektu o wprowadzeniu zmiany i jej skutkach na przebieg prac projektowych.

ODBIÓR FAZ i ETAPÓW

Akceptacja wszystkich wchodzących w skład fazy lub etapu produktów i zadań, za które odpowiedzialny jest wyłącznie Wykonawcy, jest jednoznaczny z odbiorem odpowiednio fazy lub etapu.

Procedura tworzenia i odbioru produktów

Celem procedury jest określenie zasad tworzenia, dokonywania przeglądów, nanoszenia zmian oraz zatwierdzania produktów projektu.

Przygotowanie

Kierownicy projektu wyznaczają osoby, które będą współtworzyły produkt. Zostaje wskazany właściciel produktu.

Opracowanie produktu może być poprzedzone spotkaniem, w którym uczestniczą osoby współtworzące produkt oraz kierownicy projektu. w trakcie spotkania ustala się: szczegółowy zakres zadania, kryteria poprawności oraz podział pracy przy jego realizacji.

OPRACOWANIE PRODUKTU

Przygotowanie produktu jest organizowane przez właściciela produktu. Jeśli przeprowadzane są spotkania służące ustaleniu cech produktu lub sposobu jego wykonania, powinny być one potwierdzane notatkami wg obowiązującego wzoru Wykonawcy.

Brak produktu wejściowego niezbędnego do realizacji zadania lub opracowania danego produktu może być przyczyną wstrzymania jego realizacji. Powoduje to automatyczne przesunięcie harmonogramu wszystkich zadań zależnych o czas opóźnienia.

Przygotowany produkt otrzymuje status „roboczy".

Jeżeli zadanie nie dostarcza produktu w postaci dokumentu, jego reprezentacją jest dokument „Potwierdzenie realizacji zadania". Przygotowuje go osoba odpowiedzialna za realizację tego zadania. w takim wypadku nie jest przygotowywana wersja robocza produktu, chyba że kierownicy projektu uzgodnią inaczej.

Produkt jest przekazywany do biblioteki projektu.

PRZEGLĄD i ODBIÓR PRODUKTU WYKONAWCY

Poniższy rozdział opisuje procedurę przeglądu i odbioru produktów, za których wykonanie odpowiedzialna jest strona Wykonawcy. Celem przeglądu jest kontrola formy i treści opracowanego produktu.

Kontrola formy obejmuje zagadnienia technicznej poprawności produktu, jego zgodności z obowiązującymi w projekcie standardami.

Kontrola treści obejmuje sprawdzenie produktów pod względem:

- KOMPLETNOŚCI – produkt powinien obejmować cały uzgodniony zakres.
- POPRAWNOŚCI – produkt powinien spełniać kryteria merytoryczne.

Produkty wykonane przez Wykonawcy są przekazywane do kierownika projektu ze strony Zamawiającego. Jest on odpowiedzialny za dokonanie przeglądu produktu w ciągu 2 dni od daty otrzymania. Jeśli produkt jest poprawny, kierownik projektu ze strony Zamawiającego akceptuje produkt.

Wyniki przeglądu dokumentuje „Formularz przeglądu produktu”. Uwagi zgłoszone w innej formie nie są rozpatrywane. Brak uwag w tym terminie oznacza, że produkt został zaakceptowany w formie przedstawionej do przeglądu i umożliwia jednostronną akceptację produktu przez Wykonawcy.

„Formularz przeglądu produktu” jest przekazywany przez kierownika projektu Zamawiającego do właściciela produktu. Lista uwag jest listą zamkniętą umieszczoną na jednym formularzu, nie może być aktualizowana bądź rozszerzana po jej przekazaniu, uwagi nie mogą być wzajemnie sprzeczne. Uwagi niespełniające powyższych kryteriów są automatycznie odrzucone.

Zgłoszone uwagi są analizowane przez właściciela produktu w ciągu 2 dni od otrzymania formularza przeglądu. Sposób uwzględnienia uwag w produkcie jest dokumentowany w formularzu przeglądu. w przypadku, gdy uwag nie można uwzględnić w sposób bezpośredni, dokonuje się ich wyjaśnienia. Po wprowadzeniu w produkcie zmian wynikających z przeglądu, produkt otrzymuje nowy numer wersji roboczej.

Zmieniony produkt wraz z uzupełnionym formularzem przeglądu jest przekazywany przez właściciela produktu do kierownika projektu ze strony Zamawiającego. Poprawność uwzględnienia uwag z przeglądu jest sprawdzana w okresie 1 dni od daty ponownego przekazania produktu. w trakcie sprawdzania poprawności zamieszczonych uwag nie zgłasza się nowych uwag, dotyczących nowych zagadnień ani uwag zgłoszonych poprzednio. Uwagi niespełniające powyższych kryteriów są automatycznie odrzucone.

Jeśli sposób uwzględnienia uwag jest poprawny, kierownik projektu ze strony Zamawiającego akceptuje produkt. Brak w tym terminie uzasadnionych zastrzeżeń co do sposobu uwzględnienia uwag oznacza, że produkt został zaakceptowany w nowej formie i umożliwia jednostronną akceptację produktu przez Wykonawcy.

Zaakceptowany produkt wraz z formularzem przeglądu trafia do biblioteki projektu.

Jeżeli pojawiły się jakichkolwiek rozbieżności, których nie można wyjaśnić, decyzję o sposobie uwzględnienia uwag podejmują kierownicy projektu. Każdy z kierowników w ciągu 2 dni od daty sprawdzenia poprawności uwzględnienia uwag przedstawi kierownikowi drugiej strony pisemną propozycję rozwiązania sporu. Jeśli w ciągu następnych 2 dni kierownicy nie uzgodnią sposobu rozwiązania, to ich wcześniejsze pisemne propozycje są przedkładane do rozstrzygnięcia komitetowi sterującemu.

PRZEGLĄD i ODBIÓR PRODUKTU ZAMAWIAJĄCEGO

Przegląd i odbiór produktu Zamawiającego są przeprowadzane i dokumentowane przez Kierownika projektu ze strony Zamawiającego.

Dodatkowo:

W odniesieniu do wdrożenia projektu należy m.in. określić: kto będzie odpowiedzialny za realizację projektu w całości i poszczególnych jego elementów, w jaki sposób zostaną wybrani członkowie zespołu projektowego, jakie wymagania formalne powinni spełniać, jak wyglądać będzie struktura organizacyjna i zależności służbowe zespołu projektowego, w jaki sposób finansowana będzie praca zespołu projektowego, jakiego rodzaju umowy będą podpisane z członkami zespołu projektowego oraz udzielić wszelkich istotnych informacji pozwalających na ocenę projektu pod kątem przygotowania organizacyjnego do wdrożenia. Jeśli już w momencie wykonywania studium wykonalności projektu wiadome jest, jakie osoby będą odpowiedzialne za realizację projektu lub jego istotnych części, można zamieścić curriculum vitae tych osób, jako świadectwo posiadania odpowiednich kwalifikacji przez osoby nadzorujące realizację projektu.

Ponadto należy określić, czy we wdrożeniu projektu będą brały udział podmioty zewnętrzne, a jeśli tak – jakie zadania będą spełniać, w jaki sposób zostaną wybrane i z jakich źródeł pochodzić będzie ich wynagrodzenie.

W przypadku prac budowlanych należy określić, kto będzie pełnić rolę inspektora nadzoru, inwestora zastępczego.

W odniesieniu do eksploatacji projektu należy określić: kto będzie odpowiedzialny za eksploatację projektu, czy eksploatacja zostanie zlecona podmiotom zewnętrznym, czy sam Beneficjent projektu będzie jego późniejszym operatorem. w przypadku eksploatacji

zewnętrznej należy udzielić wszelkich informacji na temat sposobu wyboru oraz wynagradzania operatora zewnętrznego.

9.2. HARMONOGRAM REALIZACJI PRZEDSIĘWZIĘCIA

Harmonogram realizacji przedsięwzięcia powinien obejmować wszystkie istotne działania podejmowane w ramach realizowanego projektu. Zaleca się sporządzenie harmonogramu w okresach miesięcznych, a jeśli z powodu specyfiki projektu nie jest to możliwe – co najmniej w okresach kwartalnych.

Harmonogram powinien ujmować odpowiednio długi okres przeznaczony na pozyskanie zezwoleń i decyzji, ich uprawomocnienie, przygotowanie i przeprowadzenie procedury przetargowej, łącznie z czasem na ewentualne oprotestowanie przetargów.

Proponuje się prezentację harmonogramu w formie tabelarycznej lub wykresu Gantta.