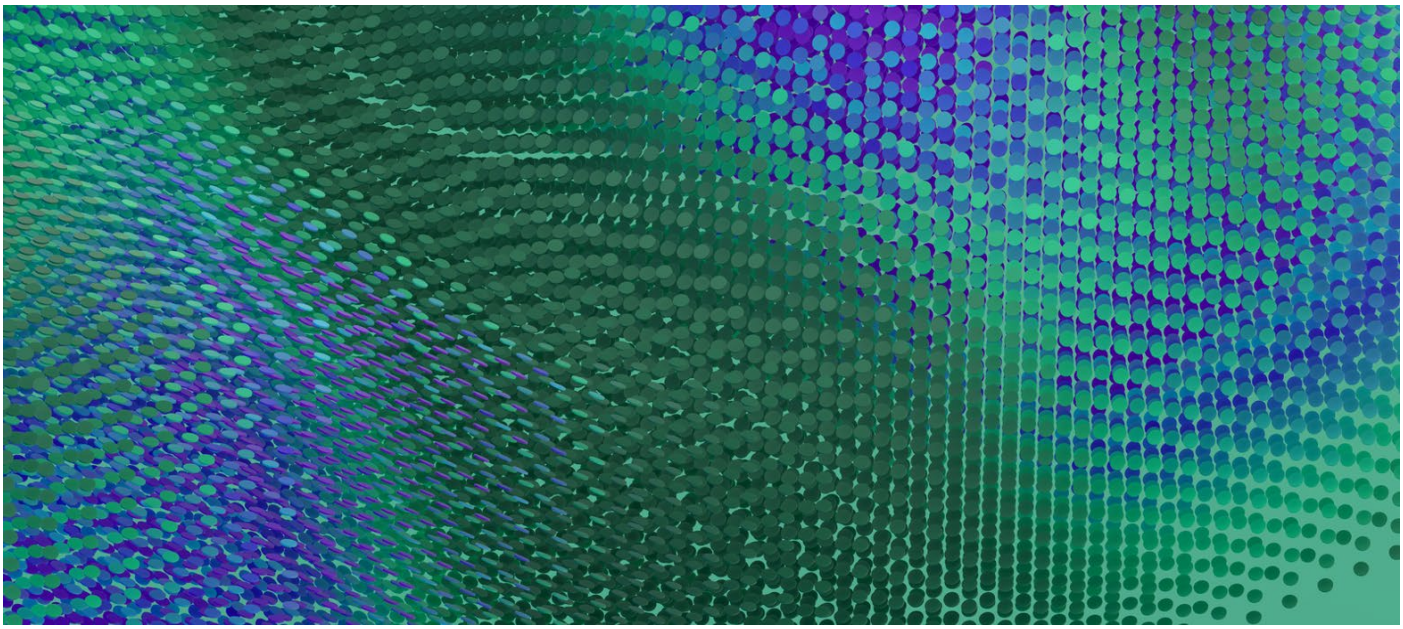
Hewlett Packard Enterprise



Bezpieczeństwo filarem zgodności

Podręcznik

Wydanie: 2024.02.05

Piotr Nogaś
Hewlett Packard Enterprise Polska

Projekt: HPECompliancePL CY24

Żądanie zmiany (Opl)	Wersja dokumentu	Data	Wykonał/ Zmodyfikował	Sprawdził	Zaaprobował	Rozdziały i zakres zmian
	2.0.8	2024.02.05	Piotr Nogaś	Michał Andruszkiewicz	Jaroslaw Mojsiejuk	

Spis treści

Przedmowa

Oddaję w Państwa ręce krótki podręcznik zawierający skondensowaną wiedzę i praktykę HPE w planowaniu, tworzeniu i rozwoju bezpiecznych środowisk informatycznych zapewniających inkorporację nowych/innowacyjnych technologii w zgodzie z trendami i regulacjami prawnymi oraz konsumowanym w dowolnym wybranym przez Państwa trybie – tradycyjnym i/lub chmurowym.

Podręcznik zawiera wytyczne dla procesu planowania i rozwoju oraz sygnalizuje niezbędne elementy procesów utrzymania dla kompletnych środowisk informatycznych.

W imieniu zespołu redakcyjnego zapraszam wszystkich zainteresowanych konkretnymi rozwiązaniami transformacji istniejących rozwiązań, przy uwzględnieniu nowych technologii i modeli przetwarzania do współpracy w transformacji środowisk zapewnianiającej wymaganą jakość, skalę, bezpieczeństwo i zgodność przetwarzania. HPE Polska posiada duże doświadczenie w dostarczaniu zgodnego z potrzebami, budżetem i regulacjami rozwiązań oraz planowania dróg dojścia do uzgodnionego/docelowego środowiska przetwarzania maksymalizując ochronę poczynionych inwestycji.

Niniejszy poradnik odzwierciedla stan wiedzy i aspektów prawnych na styczeń 2024 w zakresie obowiązujących regulacji, linii orzecznictwa oraz wytycznych podmiotów kontrolnych oraz zalecanych technologii oraz trendów rynkowych.

Poradnik nie jest źródłem regulacji, stanowi zestandaryzowany, zanonimizowany i uogólniony przykład rozwiązań, jak skutecznie, w prosty i ustandaryzowany sposób dochować należytej staranności w zapewnieniu zgodności z obowiązującymi regulacjami RP, EU oraz innymi międzynarodowymi regulacjami sektorowymi.

Rekomendujemy stosowanie najnowszej wersji podręcznika - aktualizacje podręcznika powinny być dostępne na:

https://www.gov.pl/web/baza-wiedzy/poradniki
http://www.hpe.com

W imieniu zespołu redakcyjnego

Piotr Nogaś.

Nowe regulacje

W Dzienniku Urzędowym UE z dnia 27.12.2022 zostały opublikowane niezwykle ważne akty prawne UE dot. m.in. sektora publicznego, ustanawiające nowe ramy cyberbezpieczeństwa w UE:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, zwana Dyrektywą CER.

Dyrektywy NIS 2 i CER pozostają w bezpośrednim związku - dyrektywa NIS 2 wymienia 11 stref ważnych dla zapewnienia funkcjonowania społeczeństw i państw UE w tym administracji publicznej oraz cyfryzacji. W sferze IT wdrożenie NIS 2 bezpośrednio wpływa na sposób wdrażania dyrektywy CER. Terminy na wdrożenie dyrektywy NIS 2 są jednocześnie krótsze niż terminy wdrożenia CER.

W tym samym dzienniku urzędowym znajdują się jeszcze dwa kluczowe akty dot. cyberbezpieczeństwa sektora finansowego: rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 - tzw. rozporządzenie DORA.

Wraz z obowiązującymi już RODO/GDPR, aktem o cyberbezpieczeństwie, aktem dotyczącym cyberodporności, oraz wciąż procedowanych aktach dotyczących sztucznej inteligencji, regulacje te stanowią podstawy i ramy unijnego systemu oceny zgodności (ang. Compliance) dla rozwiązań IT.

Administracja publiczna jak i dostawcy IT stoją przed zadaniem dostosowania się i swoich rozwiązań do nowych regulacji.

Wymaga to wdrożenia nowych/zmiany procesów organizacyjnych, nowych rozwiązań technicznych, a także przygotowania się od strony formalnej (udokumentowania procesów, zmian zapisów kontraktowych).

W 2024 roku i w latach kolejnych spodziewana jest intensyfikacja analiz, korekt i zmian w administracji publicznej oraz u dostawców IT w celu trwałego zapewnienia zgodności (Compliance IT).

Dyrektywa NIS 2 – zastępuje obowiązującą od 2016 r. dyrektywę NIS przez stworzenie ram prawnych dla zagadnień dotychczas nieuregulowanych. Najistotniejsze kwestie regulowane dyrektywą to zwiększenie odporności i eliminacji podatności podmiotów świadczących usługi kluczowe w zakresie cyberbezpieczeństwa; poszerzenie katalogu podmiotów, które należy uznać za dostawców usług

kluczowych o m.in. dostawców usług chmury obliczeniowej, firm kurierskich, podmiotów zajmujących się gospodarką śmieciami i odpadami, przedsiębiorstwa związane z przemysłem kosmicznym; administrację publiczną działającą na szczeblu centralnym i samorządowym. Wprowadzeniu kryterium wielkości – zgodnie z nowymi przepisami, każdy średni lub duży podmiot działający w sektorach uregulowanych w NIS 2 będzie podlegał przepisom dyrektywy, a dostawcy usług kluczowych zostali podzieleni na: niezbędnych (np. banki, administracja publiczna, cyfryzacja czy dostawcy żywności) oraz ważnych (np. dostawcy usług cyfrowych, firmy kurierskie).

Nowe przepisy nakładają obowiązki na dostawców usług kluczowych w zakresie wykrywania luk w systemach bezpieczeństwa, zarządzania incydentami, testowania poziomów bezpieczeństwa oraz zapewnienia poufności, w szczególności konieczność szyfrowania.

NIS 2 weszła w życie 16 stycznia 2023 r. Do dnia 17 października 2024 r. państwa członkowskie mają czas na implementację dyrektywy do krajowych porządków prawnych, a więc czasu pozostało niewiele. W związku z tym powinna zostać przyjęta w RP nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa lub opracowana i przyjęta zupełnie nowa ustawa. Dyrektywa NIS 2 obejmuje administrację centralną i samorządową/lokalną. W gestii Państw Członkowskich jest określenie czy dyrektywa ma być stosowanie do podmiotów administracji publicznej na poziomie lokalnym.

Kolejny istotny związek NIS 2 z Dyrektywą CER polega na tym, że dyrektywa NIS 2 ma zastosowanie do podmiotów zidentyfikowanych jako podmioty mające charakter krytyczny na mocy dyrektywy (UE) 2022/2557, niezależnie od ich wielkości.

Zgodnie z Dyrektywą CER każde państwo zobowiązane jest opracować ogólnopaństwową strategię jej wdrożenia, na podstawie analiz ryzyka w danym kraju, identyfikacji stref oraz podmiotów krytycznych. Wskazane podmioty krytyczne są zobowiązane m.in. do:

- utrzymania planów zwiększania odporności (równoważne),
- przeprowadzenia oceny ryzyka (12 miesięcy od identyfikacji uznana za podmiot IK),
- wprowadzenia odpowiednich i adekwatnych do oceny ryzyka środków technicznych, bezpieczeństwa i organizacyjnych dla zapewnienia wymaganej odporności.

Klient referencyjny

Podręcznik jest przeznaczony dla klienta, którego środowisko IT w znacznej części zostało lub może zostać zwirtualizowane, rozważa implementację nowych technologii w celu zwiększenia korzyści z posiadanych danych (Big Data/ML/DL/AI), wykorzystuje lub planuje wykorzystywać chmury publiczne oraz platformy konteneryzacji z zachowaniem pełnej kontroli na własnych zasadach i we własnym tempie (w trosce o zachowanie stabilności oraz ochronę poczynionych inwestycji).

HPE rekomenduje metodykę doboru optymalnego rozwiązania docelowego, charakteryzującego się elastycznymi opcjami dróg dojścia (ewolucja a nie rewolucja), zintegrowanego w celu zapewnienia zgodności (eliminacja ryzyka wysokich kar i utraty zaufania).

Analiza stanu obecnego, kierunków rozwoju i trendów rynkowych

Metodyka HPE obejmuje konfrontację planów rozwoju środowiska klienta z raportami i prognozami rynkowymi uznanych firm analitycznych w celu doboru niezbędnych technologii i funkcjonalności dla wymaganej skali, jakości oraz efektywności obsługi w planowanym czasie.

Przykładowe raporty wiodących firm analitycznych:

Strategiczne obszary zmian/inwestycji w najbliższych latach (IDC 2023):

- **Data Management**: Ochrona danych, bezpieczeństwo danych, usługi związane z danymi, mobilność danych, analityka, monetyzacja danych oraz tematy związane z pełnym cyklem życia danych. Obejmuje również europejski system regulacyjny i dynamikę danych, taką jak rosnąca ich ilość i fragmentacja.
- **Cloud data services**: DPaaS, DRaaS, cloud storage, object storage, cloud tiering, cloud backup, cloud gateways.
- **Market Shares**: Prognoza i analiza konkurencyjności technologii przechowywania i zarządzania danymi; prognoza usług związanych z przechowywaniem i zarządzaniem danymi.
- **End-User Data-Driven Strategies**: Plany inwestycyjne związane z danymi i strategie przekształcania danych w użyteczną wiedzę; trendy w zakresie przechowywania danych w chmurze.
- **DataOps**: Nowoczesne procesy łączące użytkowników i źródła danych.
- **Driving modernization and digital transformation with data-driven strategy**: Strategie związane z modernizacją i cyfrową transformacją.
- **Information Architecture for Future of Intelligence**: Platformy udostępniania danych, dostęp do danych, orkiestracja i integralność dla technologii platformowych, takich jak kontenery i PaaS.

Źródła i przydatne linki https://www.idc.com/getdoc.jsp?containerId=IDC_P269

Główne strategie i trendy technologiczne (Gartner 2022)

- **Generative Artificial Intelligence (AI)**
  - Jedną z najbardziej widocznych i potężnych technik sztucznej inteligencji wchodzących na rynek jest generatywna sztuczna inteligencja - metody uczenia maszynowego, które czerpią treści lub informacje z obiektów źródłowych i w celu tworzenia zupełnie nowych, całkowicie oryginalnych, realistycznych artefaktów.
  - Generatywna sztuczna inteligencja może być wykorzystywana do szeregu działań, takich jak tworzenie kodu oprogramowania, ułatwianie opracowywania leków i ukierunkowany marketing, ale także niewłaściwie wykorzystywana do oszustw, dezinformacji politycznej, fałszowania tożsamości i innych. Gartner przewiduje, że do 2025 r. generatywna sztuczna inteligencja będzie stanowić 10% wszystkich generowanych danych, w porównaniu z mniej niż 1% obecnie.
- **Data Fabric**
  - Liczba silosów danych i aplikacji wzrosła w ciągu ostatniej dekady, podczas gdy liczba wykwalifikowanych pracowników w zespołach zajmujących się danymi i analizą (D&A) pozostała na stałym poziomie lub spadła. Fabryki danych (ang. data fabrics) - elastyczna, odporna integracja danych między platformami i użytkownikami biznesowymi - pojawiły się w celu uproszczenia infrastruktury, integracji danych w organizacji i stworzenia skalowalnej architektury, która zmniejsza dług techniczny obserwowany w większości zespołów D&A z powodu rosnących wyzwań integracyjnych.
  - Prawdziwą wartością fabryki danych jest jej zdolność do dynamicznej optymalizacji wykorzystania danych dzięki wbudowanej analityce, zmniejszając wysiłki związane z zarządzaniem danymi nawet o 70% i przyspieszając czas uzyskania korzyści.
- **Distributed Enterprise**
  - Wraz ze wzrostem popularności pracy zdalnej i hybrydowej, tradycyjne organizacje skoncentrowane na biurach przekształcają się w rozproszone przedsiębiorstwa składające się z pracowników rozmieszczonych geograficznie.
  - "Wymaga to od CIO wprowadzenia poważnych zmian technicznych i usługowych w celu zapewnienia elastycznego środowiska pracy, ale jest też druga strona medalu: wpływ na modele biznesowe" - powiedział David Groombridge (analityk w firmie Gartner) "Dla każdej organizacji, od handlu detalicznego po edukację, ich model biznesowy musi zostać rekonfigurowany, obejmujący usługi rozproszone. Jeszcze dwa lata temu świat nie sądził, że będzie przymierzał ubrania w cyfrowej przymierzalni".
  - - Gartner przewiduje, że do 2023 roku 75% organizacji, które wykorzystują rozproszone rozwiązania dla przedsiębiorstw, osiągnie wzrost przychodów o 25% szybciej niż konkurencja.
- **Cloud-Native Platforms (CNPs)**
  - Aby naprawdę dostarczać cyfrowe możliwości w dowolnym miejscu i czasie, przedsiębiorstwa muszą odejść od znanych migracji typu "podnieś i przenieś" na rzecz CNP. CNP wykorzystują podstawowe możliwości przetwarzania w chmurze, aby zapewnić skalowalne i elastyczne możliwości związane z IT "jako usługi".
  - Gartner przewiduje, że platformy natywne dla chmury będą stanowić podstawę dla ponad 95% nowych inicjatyw cyfrowych do 2025 roku - w porównaniu z mniej niż 40% w 2021 roku.

- **Autonomic Systems**
    - W miarę rozwoju przedsiębiorstw tradycyjne programowanie lub prosta automatyzacja nie będą się skalować. Systemy autonomiczne to samozarządzające się systemy fizyczne lub programowe, które uczą się na podstawie swoich środowisk. W przeciwieństwie do systemów zautomatyzowanych, systemy autonomiczne mogą dynamicznie modyfikować własne algorytmy bez aktualizacji oprogramowania zewnętrznego, umożliwiając im szybkie dostosowanie się do nowych warunków w danym środowisku, podobnie jak robią to ludzie.
    - "Zachowanie autonomiczne stało się już znane dzięki niedawnym wdrożeniom w złożonych środowiskach bezpieczeństwa, ale w dłuższej perspektywie stanie się powszechne w systemach fizycznych, takich jak roboty, drony, maszyny produkcyjne i inteligentne przestrzenie" - twierdzi Groombridge.
- **Decision Intelligence (DI)**
    - Kompetencje decyzyjne organizacji mogą być istotnym źródłem przewagi konkurencyjnej, ale stają się coraz bardziej wymagające.
    - Systemy sztucznej inteligencji w procesach decyzyjnych to praktyczna dyscyplina wykorzystywana do poprawy procesu podejmowania decyzji poprzez wyraźne zrozumienie i inżynierię sposobu podejmowania decyzji oraz oceny wyników, zarządzania nimi i ich poprawy poprzez informacje zwrotne.
    - Gartner przewiduje, że w ciągu najbliższych dwóch lat jedna trzecia dużych organizacji będzie wykorzystywać sztuczną inteligencję do ustrukturyzowanego podejmowania decyzji w celu poprawy przewagi konkurencyjnej.
- **Composable Applications**
    - W stale zmieniającym się kontekście biznesowym, zapotrzebowanie na zdolność adaptacji biznesowej kieruje organizacje w stronę architektury technologicznej, która wspiera szybką, bezpieczną i wydajną zmianę aplikacji. Komponowalna architektura aplikacji umożliwia taką adaptację, a te, które przyjęły podejście komponowalne, wyprzedzą konkurencję o 80% pod względem szybkości wdrażania nowych funkcji.
    - "W burzliwych czasach, zasady biznesowe oparte na architekturze komponowalnej pomagają organizacjom opanować przyspieszone zmiany, które są niezbędne dla elastyczności i rozwoju biznesu. Bez tego nowoczesne organizacje ryzykują utratę dynamiki rynkowej i lojalność klientów" - powiedział Groombridge.
- **Hyperautomation**
    - Hiperautomatyzacja akceleruje wzrost i odporność biznesową dzięki natychmiastowej identyfikacji, weryfikacji i automatyzacji maksymalnej liczby procesów.
    - "Badania przeprowadzone przez firmę Gartner pokazują, że najlepsze zespoły zajmujące się hiperautomatyzacją koncentrują się na trzech kluczowych priorytetach: poprawie jakości pracy, przyspieszeniu procesów biznesowych i zwiększeniu elastyczności podejmowania decyzji" - powiedział Groombridge. "Technolodzy biznesowi wspierali średnio 4,2 inicjatywy związane z automatyzacją w ubiegłym roku".
- **Privacy-Enhancing Computation (PEC)**
    - Oprócz radzenia sobie z zaostrzającymi się międzynarodowymi przepisami dotyczącymi prywatności i ochrony danych, dyrektorzy ds. informatyki muszą unikać utraty zaufania klientów wynikającej z incydentów związanych z prywatnością. Dlatego też Gartner spodziewa się, że do 2025 roku 60% dużych organizacji będzie korzystać z jednej lub więcej technik przetwarzania zwiększających prywatność.
    - Techniki PEC - które chronią dane osobowe i wrażliwe informacje na poziomie danych, oprogramowania lub sprzętu - bezpiecznie udostępniają, łączą i analizują dane bez narażania poufności lub prywatności. Obecne przypadki użycia znajdują zastosowanie w wielu branżach, a także w infrastrukturach chmury publicznej (np. zaufane środowiska wykonawcze).
- **Cybersecurity Mesh**
    - "Dane to element wielu tegorocznych trendów, ale są one przydatne tylko wtedy, gdy przedsiębiorstwa mogą im zaufać" - powiedział Groombridge. "Obecnie zasoby i użytkownicy mogą znajdować się w dowolnym punkcie, co oznacza, że tradycyjne granice bezpieczeństwa odeszły do lamusa. Wymaga to stosowania architektury siatki bezpieczeństwa cybernetycznego (Cybersecurity Mesh Architecture – CSMA)".
    - CSMA pomaga zapewnić zintegrowaną strukturę bezpieczeństwa w celu zabezpieczenia wszystkich zasobów, niezależnie od lokalizacji. Do 2024 r. organizacje wdrażające CSMA w celu zintegrowania narzędzi bezpieczeństwa zmniejszą wpływ finansowy poszczególnych incydentów bezpieczeństwa średnio o 90%.
- **AI Engineering**
    - Liderzy IT zmagają się z integracją sztucznej inteligencji z aplikacjami, poświęcając czas i pieniądze na projekty AI, które nie są wdrażane do produkcji lub walcząc o zachowanie wartości z rozwiązań AI po ich uruchomieniu. Inżynieria AI to zintegrowane podejście do operacjonalizacji modeli AI.
    - "Dla zespołów pracujących nad sztuczną inteligencją, prawdziwym wyróżnikiem dla ich organizacji będzie zdolność do ciągłego zwiększania wartości poprzez szybką adaptację AI" - powiedział Groombridge. "Do 2025 r. 10% przedsiębiorstw, które ustanowią najlepsze praktyki inżynierii AI, wygeneruje co najmniej trzykrotnie większą korzyść ze swoich działań w zakresie AI niż 90% przedsiębiorstw, które tego nie zrobią".
- **Total Experience (TX)**
    - TX to strategia biznesowa, która łączy dyscypliny doświadczenia klienta (CX - Customer Experience), doświadczenia pracownika (EX - Employee Experience), doświadczenia użytkownika (UX - User Experience) i multi doświadczenia (MX - Multi-Experience). Celem TX jest zwiększenie zaufania klientów i pracowników, ich satysfakcji, lojalności i poparcia. Organizacje zwiększą przychody i zyski, osiągając dynamiczne i trwałe wyniki biznesowe TX.

Źródła i przydatne linki: Gartner's top strategic technology trends for 2022

Do 2025 r. 60% wszystkich przedsiębiorstw będzie wymagać od rozwiązań pamięci masowych **zintegrowanych mechanizmów ochrony przed oprogramowaniem ransomware**, w porównaniu z 10% w 2022 r.

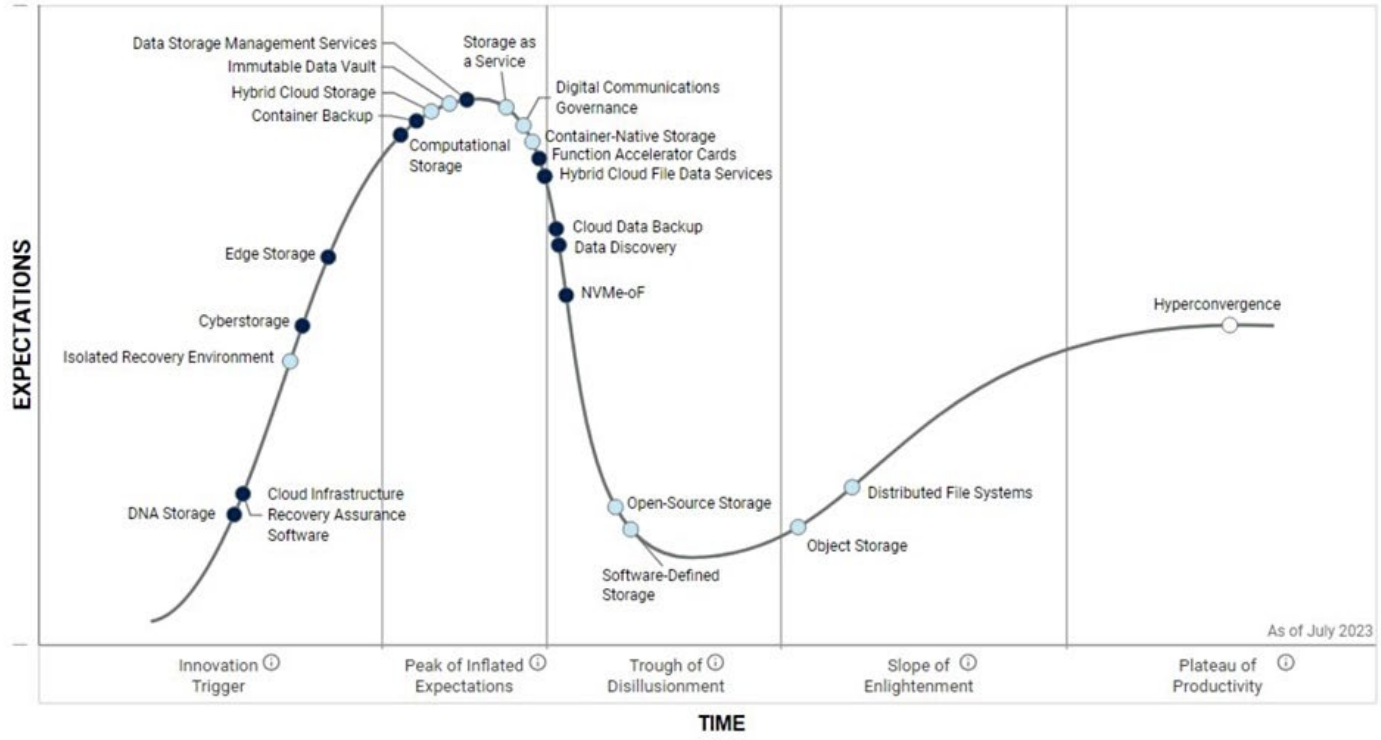
Do 2026 r. duże przedsiębiorstwa **potroją swoją pojemność nieustrukturyzowanych danych przechowywanych jako pliki lub obiekty lokalnie, na brzegu sieci lub w chmurze publicznej**, w porównaniu do 2022 r.

Do 2025 roku 60% liderów branży infrastruktury i operacji (I&O) **wdroży co najmniej jedną architekturę chmury hybrydowej**, w porównaniu z 15% w 2022 roku.

Do 2025 roku **ponad 40% pamięci masowych klasy korporacyjnych zostanie wdrożona na brzegu sieci,** w porównaniu z 15% w 2022 roku.

Źródła i przydatne linki: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf
https://www.gartner.com/en/documents/3987173

Krzywa technologii pamięci masowych i ochrony danych (Gartner 2023)



Źródła i przydatne linki: Gartner Hype Cycle for Storage and Data Protection Technologies, 2023

Cyberstorage – obszary stosowania

Według definicji firmy Gartner „Cyberstorage chroni dane systemu pamięci masowej przed atakami ransomware poprzez wczesne wykrywanie i blokowanie ataków oraz pomaga w odzyskiwaniu danych dzięki analizom pozwalającym określić, kiedy rozpoczął się atak. Rozwiązaniami mogą być czyste oprogramowanie, dedykowane urządzenie lub w pełni zintegrowane. Ataki ransomware stały się powszechne, co wymaga przyjęcia lub wdrożenia narzędzi cyberbezpieczeństwa do aktywnej obrony. Chociaż dostępnych jest wiele rozwiązań do ochrony punktów końcowych, brak jest zintegrowanych rozwiązań do ochrony kluczowych systemów głównych. Pamięć masowa (NAS) i skalowalne systemy plików nie zapewniają wystarczającej ochrony przed usunięciem lub zaszyfrowaniem danych przez oprogramowanie złośliwe. Cyberstorage zapewnia aktywną ochronę przed cyberatakiem na dane nieustrukturyzowane."

Implementacja Cyberstorage musi zapewniać zgodność z lokalnymi regulacjami, standardami i zaleceniami instytucji kontrolnych przez implementację modelu NIST Cybersecurity Framework w 5 głównych obszarach: Identyfikacja, Ochrona, Detekcja, Reakcja, Przywrócenie. Orkiestracja i ciągłe doskonalenie są jedyną słuszną strategią dla zapewnienia bezpieczeństwa oraz dochowania należytej staranności. Lokalne regulacje UE, RP oraz linia orzecznictwa doprecyzowują aktualną linię odniesienia – wskazując niezbędne, środki i procedury oraz określając wymagania jakościowe.

Należy pamiętać, że ogólna zasada zaleca, aby strategia bezpieczeństwa dostosowywała poziom zabezpieczeń do ekspozycji na zagrożenia, z minimalnym celem plasowania powyżej średniej bezpieczeństwa oraz metodami generowania kosztów po stronie atakujących – obecny hacking, to biznes zorientowany na efektywność kosztową.

Cyberstorage jest rozwinięciem lepiej lub gorzej znanych punktowych technologii, działających często w oderwaniu od usług bezpieczeństwa, ciągłości przetwarzania implementowanych w środowisku przetwarzania na innych warstwach/obszarach. Cyberstorage

to integracja kluczowych technologii w tym niezmiennych (immutability) repozytoriów, technologii szybkiej detekcji i remediacji zagrożeń w tym ransomware, wykorzystując AI, dedykowane środowiska przywracania (IRE/sandbox) w zintegrowanej, holistycznej formie z pozostałymi procesami zarządzania środowiskiem.

Cyberstorage to zunifikowana, holistyczna, a w niezbędnych obszarach nadmiarowa implementacja bezpieczeństwa mająca na celu zapewnienia zgodności – zastępuje punktowe rozwiązania typu Cyber-Bunker, Air-Gap polegające na periodycznym wyłączeniu komunikacji między ośrodkami – ich skuteczność jest niewystarczająca dla obecnych zagrożeń i regulacji.

Należy pamiętać, że zasady cyberbezpieczeństwa wymagają i zalecają skuteczne stosowanie izolacji, wielopoziomowego i zwielokrotnionego systemu zabezpieczeń.

Model Cyberbezpieczeństwa NIST – krótki opis

Większość nowych regulacji jest wzorowana na regulacjach NIST stąd przywołanie jej fundamentalnych zasad

Identyfikacja: Podstawą jest proces analizy usług przetwarzania, używający wielowymiarowej matrycy wymagań zgodności, typów zagrożeń z uwzględnieniem ryzyka wystąpienia, wpływu na przetwarzanie oraz bezpieczeństwo i integralność danych, w kontekście stosowanych w środowisku informatycznym technologii i rozwiązań. Jest procesem ciągłym/cyklicznym wyzwalanym zmianą poziomu zagrożenia lub rozpoznaniem nowych wektorów ataku.

Ochrona: Zintegrowane, zaimplementowane wielopoziomowo, zdublowane, tam gdzie niezbędne, mechanizmy bezpieczeństwa.

Detekcja: NGFW, IDS/IPS, detekcja zagrożeń typu „Dzień-Zero" oraz działania oprogramowania złośliwego w tym ransomware, honeypot, alerty CSIRT.

Reakcja: na zmianę poziomu zagrożenia, atak, nowe wektory ataku, zmian środowiska, wynikająca z analizy anomalii i/lub przeprowadzonych testów, audytu.

Przywrócenie: IaC (Infrastructure as Code), IRE - przywrócenie we wskazane miejsca w wielo-chmurze z niezbędnym SLA.

Mapowanie standardów i wytycznych

Podstawą zapewnienia zgodności Systemu informatycznego firmy jest wszechstronna analiza i klasyfikacja zagrożeń, rodzaju chronionej informacji oraz wymaganej dokumentacji formalno-prawnej w obszarach:

- wymogi dla SZBI ISO 27001,
- zalecenia najlepsze praktyki zarządzania bezpieczeństwem ISO 27002 (w chmurze ISO 27017),
- zarządzania bezpieczeństwem informacji i aplikacji (STIGs, PN-EN ISO/IEC 27001, ISO/IEC 27034, Mitre ATT&CK),
- zarządzania ciągłością działania (ISO 22301- wymagania, ISO 22313 - wytyczne),
- zarządzania obszarem technologii informacyjnej (ITIL, ISO/IEC 20000-20001, ISO/IEC 38500),
- zarządzania ryzykiem operacyjnym oraz audyt (ISO 31000, PN-ISO/IEC 27005, ISO/IEC 27002),
- centrów przetwarzania, bezpieczeństwa fizycznego i środowiskowego (PN/EN 50600, ISO/IEC TS 22237, ISO/IEC 27002),
- zarządzanie bezpieczeństwem informacji dla usług w chmurze (ISO/IEC 27002, ISO/IEC 27017 – praktyczne zasady, NSC),
- ochrona danych identyfikujących osobę w chmurach publicznych działających jako przetwarzający dane osobowe (ISO/IEC 27018),
- rozwiązań organizacyjnych i zasobów ludzkich w tym delegacji uprawnień, obowiązków, szkoleń dot. jakości i zgodności przetwarzania, przeprowadzona pod kątem spełnienia Unijnych i lokalnych regulacji i wytycznych oraz certyfikacji.
- Audyt i testy systemów bezpieczeństwa (ISO 19011, NIST 800-115, OWASP, OSSTMM, TIBER-EU, NSC)

Źródła i przydatne linki:
https://www.gov.pl/attachment/cda5a610-d275-4a9c-a6e8-6e04a236a934
https://public.cyber.mil/stigs/srg-stig-tools/
https://attack.mitre.org/
https://www.iso.org/standard/78550.htm

Narodowe standardy cyber-bezpieczeństwa:
https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

Certyfikacja przedsiębiorstw:
https://firmabezpiecznacyfrowo.pl/diagnoza/
https://uodo.gov.pl/pl/514/2300 normy ISO/IEC 17065.

Uwaga: HPE w planowaniu uwzględnia rekomendacje niezależnego audytora, w celu wykluczenia konfliktu interesów i potwierdzenie zgodności.

Należy pamiętać, że obecne i przyszłe regulacje przewidują certyfikację zarówno audytora jak i audytowanych podmiotów.

Źródła i przydatne linki:
https://www.kso3c.pl/
https://uodo.gov.pl/pl/427/2305
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pl.pdf
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_pl
https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl
https://firmabezpiecznacyfrowo.pl/poradnik/wstep/zakres-oceny/ (NASK)

Obszar zgodności

Analizy zgodności nie można ograniczać wyłącznie do samego przedsiębiorstwa. Należy objąć nią pełny ekosystem: obecni i spodziewani klienci oraz kontrahenci (kompletny łańcuch dostaw i zbytu).

Zapewnianie zgodności to proces ciągły. W przypadku braku lub anachroniczności obowiązujących regulacji/standardów branżowych zaleca się adaptację wymagań i zaleceń dla operatorów usług kluczowych lub krytycznych dla działania lub bezpieczeństwa państwa – będące naturalnym i na bieżąco aktualizowanym punktem odniesienia dla wszystkich innych podmiotów prowadzących działalność na terytorium Rzeczpospolitej Polskiej i Unii Europejskiej.

Źródła i przydatne linki
https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-
https://www.gov.pl/web/cyfryzacja/operatorzy-uslug-cyfrowych
https://www.gov.pl/web/rozwoj-technologia/cyberbezpieczenstwo-msp
https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber
https://www.gov.pl/web/cyfryzacja/akt-o-cyberbezpieczenstwie
https://uodo.gov.pl/pl/514/2300
https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych
Dyrektywa NIS 2
https://www.gov.pl/attachment/3c6d5be1-caf3-4a5b-a452-1fcc34d629c9
https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej
Dyrektywa i rekomendacje wdrażania CER
https://www.gov.pl/attachment/2e86d037-1149-48d3-8b17-fef86cc9eb6b
ttps://www.gov.pl/attachment/600219dc-e393-4cef-aca7-5e594054a6d0

Zgodność rozwiązań w świetle bieżącego orzecznictwa sądów powszechnych oraz decyzji Prezesa UODO

Rozdział ten wskazuje niezbędne funkcje platformy przetwarzania dla referencyjnego klienta – na podstawie rzeczywistych przypadków. Dla zobrazowania obecnej (2023r) linii orzecznictwa – oparto się na wybranych decyzjach reprezentatywnych dla większości firm i jednostek administracji publicznej.

Obecne orzecznictwo sądów powszechnych wskazuje na konieczność dostosowania polityk i procesów bezpieczeństwa do zmian poziomu i ewolucji zagrożeń – wymagają wprowadzenia adekwatnych rozwiązań w odpowiedzi na zmiany. Fakt, że podmiot NIE obserwuje działań wymierzonych bezpośrednio przeciwko niemu, nie zwalnia go z konieczności reakcji.

Obserwowana jest „radykalizacja" decyzji Prezesa UODO, kończącego okres przejściowy, w którym praktyką było upominanie (w szczególności) jednostek administracji publicznej oraz przedsiębiorstw państwowych (z uwagi na przepisy odrębne/szczegółowe). Obecnie orzecznictwo zrównało traktowanie podmiotów sektora publicznego i przedsiębiorstw prywatnych, w celu zapewnienia wyższych poziomów usług w sektorze publicznym począwszy od roku 2024.

Analizy orzecznictwa oraz zaleceń audytów wskazują, że zarzut niedochowania należytej staranności jest stawiany w przypadkach niewykorzystania lub braku odpowiednich funkcjonalności (technologii) w środowiskach informatycznych oraz zbyt niskich, zdaniem orzekających, poziomów usług, w tym przywrócenia przetwarzania także w wyniku działania ransomware. Mechanizmy zapewniające ochronę i przywrócenie danych muszą zapewniać zgodność z regulacjami UE, RP w tym RODO, NSC, ustawą o rachunkowości oraz tam, gdzie ma zastosowanie DORA, NIS 2 oraz pozostawać w zgodzie z dobrymi praktykami/regulacjami branżowymi (np. KNF).

Źródła i przydatne linki
https://uodo.gov.pl/pl/138/2764
https://uodo.gov.pl/pl/342/2703
https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52022PC0197
https://www.digital-operational-resilience-act.com

Regulacje NIS, DORA, ENISA, RODO wskazują i bazują na tych samych podstawowych zasadach i procesach niezbędnych dla zachowania należytej staranności. Zastosowanie najbardziej wymagającej regulacji dla podmiotu, prowadzi do uproszczenia, standaryzacji oraz redukcji kosztów i pracochłonności procesów utrzymania IT i wprowadzanych zmian.

Omówienie wybranych uzasadnień decyzji:

UODO opublikował 489 decyzji (w tym upomnienie 69 i umorzenie 17) z karami od 10tys do 1mln PLN w ciągu ostatnich 5 lat. Ogólna ilość kar za brak zgodności wg większości szacunków przekracza 1800. Najwyższe kary odnotowano w sektorach Mediów Społecznościowych, Finansowym, Telekomunikacyjnym oraz Sieci Sprzedaży.

Intensywność i dotkliwość kar znacząco wzrasta nie tylko w związku z NIS 2, CER, DORA, PSD 3 czy też aktualizacji PKE, ale także w miarę zacieśniania egzekwowalności sankcji nakładanych w ramach eskalacji sytuacji geopolitycznej (wojen militarnych i handlowych).

Przykłady orzeczonych kar:

Brak anonimizacji udostępnionych danych	1M €	https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020
Wyciek danych	644k €	https://uodo.gov.pl/decyzje/ZSPR.421.2.2019
Brak udokumentowanych testów	443k €	https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020
Ransomware	235k €	https://uodo.gov.pl/decyzje/DKN.5130.1354.2020
Niezgodności z ustawą o ochronie zdrowia	22k €	https://www.uodo.gov.pl/decyzje/DKN.5131.32.2023

- *W pierwszej kolejności istotnym jest określenie poziomu ryzyka, … a następnie należy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.*

  Pełna analiza zagrożeń zawierająca szacunki ryzyka i stopnia zagrożenia tworzy linię bazową w postaci wielowymiarowej matrycy, na podstawie której są dobierane i uzgadniane technologie, uprawnienia, procesy, procedury, obszary odpowiedzialności i ścieżki decyzyjne służące dochowaniu należytej staranności w zakresie zgodności. Obejmuje także zakres i harmonogram niezbędnych szkoleń. Kolejnym obszarem są aktualizacje wynikające z zaleceń okresowych audytów oraz wyników wykonywanych okresowo testów. Implementacja technologii i użyte środki nie powinny ograniczać możliwości rozwoju wskazanych, powinny zaś uwzględniać innowacyjne technologie i strategie rekomendowane w opracowaniach firm Gartner oraz IDC.

  <u>Kluczowe zagadnienia dla realizacji postulatu orzeczenia:</u>

  - *Uproszczona, zwięzła i granularna konstrukcja, redukcja pracochłonności przez automatyzację.*
  - *Samowystarczalność, samodzielność w zakresie obsługi i wprowadzania niezbędnych zmian w ramach utrzymania.*
  - *Rozwiązanie musi być otwarte i aktualizowane w zakresie nowych technologii/standardów.*
  - *Bezobsługowość procesów, akceleracja sprzętowa zadań zmniejszających jakość świadczonych procesów biznesowych.*

- *Z treści art. 32 ust. 1 rozporządzenia 2016/679 wynika, że **administrator jest zobowiązany do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku … decydując o środkach technicznych i organizacyjnych należy wziąć pod uwagę stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia** … Z przytoczonego przepisu wynika, że ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym.*

  <u>Kluczowe zagadnienia dla realizacji postulatu orzeczenia:</u>

  - *Dobór technologii na podstawie matrycy decyzyjnej. Dla klienta referencyjnego, następujące kluczowe środki techniczne (aka. technologie) są niezbędne w celu spełnienia wymagań jakościowych, wsparcia planów rozwoju oraz eliminacji ryzyka utraty danych/naruszenia przetwarzania:*

Cloud Infrastr. Recovery Assurance Software	*Container Native Storage*
Container Backup	*Hybrid Cloud File Data Svcs*
Cyber Storage	*Hybrid Cloud Storage*
Data Discovery	*HyperCovergence*
Data Storage Mgmnt Services	*Isolated Revcovery Environment*
Digital Communication Govern.	*Immutable Data Vault*

  - *Zintegrowane, automatyczne funkcje HA/DR/DP i provisioningu w jednym panelu zarządzania (doświadczenie chmury).*
  - *Provisioning na poziomie tenantów (dla platformy wirtualizacji, kontenerowej oraz w Data Fabric).*
  - *Doświadczenia analogiczne chmurowemu, usługi świadczone w siedzibie klienta przy konkurencyjności finansowej i jakościowej w stosunku do bieżącej oferty chmurowej.*
  - *Elastyczność i pełna swoboda przenoszenia usług do/z wielo-chmury oraz brzegu (ang. edge), eliminacja ryzyka poczynienia nietrafionych inwestycji.*
  - *Wysoki stopień automatyzacji oraz integracja usług, wsparcie procesów utrzymania algorytmami sztucznej inteligencji – zapewnienie informacji krytycznych dla podejmowania trafnych decyzji, podniesienie poziomu usług przy jednoczesnej redukcji pracochłonności utrzymania nowego środowiska.*
  - *Zerowy lub niski wpływ procesów zapewniających zgodność, na pracochłonność utrzymania, dostępność i wydajność procesów przetwarzania - preferowana akceleracja sprzętowa.*

- *Ustalenia te, w stosownym przypadku, powinny obejmować środki takie, jak pseudonimizacji i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

  Spełnienie tych wymagań wymaga holistycznego podejścia przez dobór zintegrowanego rozwiązania realizującego koncepcję Cyberstorage[1] wyposażonego w zestaw (najlepiej sprzętowo akcelerowanych) technologii wyszczególnionych powyżej dla ciągłego zapewnienia bezpieczeństwa, granularnego zarządzania na poziomie tenantów. Funkcje anonimizacji/maskowania danych muszą być zaimplementowane wszędzie tam, gdzie dostęp do danych rzeczywistych nie jest konieczny.

[1] Patrz: Cyberstorage

Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

- *DataFabric – wieloprotokołowa pamięć masowa - standard dla posiadanych i planowanych obciążeń (Big Data, Data Lake, przetwarzanie strumieniowe, ML/DL/AI, archiwa obiektowe) ze zintegrowanymi technologiami niezbędnymi dla skutecznej implementacji Cyberstorage.*
- *Dystrybuowane technologie EDR/XDR/NIDS/NIPS/StateFull FireWall akcelerowane sprzętowo.*
- *Elastyczna droga dojścia do konfiguracji docelowej na żądanie.*
- *Pełna automatyzacja scenariuszy testów – automatyczne powiadamianie Administratora o wykonaniu oraz indykacja problemów.*
- *Architektura zapewniająca ciągłość przetwarzania na poziomie co najmniej 99,999%.*
- *Czas przywrócenia przetwarzania RTO=0 w ośrodkach własnych (on-premises), oraz RTO=30min dla przywrócenia przetwarzania w chmurze.*
- *Przywrócenie danych RTO=30min lokalnie, RTO=1h w chmurze – akcelerowane sprzętowo.*
- *Technologie Immutable Data Vault dla archiwów oraz repozytoriów przywracania danych.*
- *Procedury reakcji na zmiany poziomów zagrożeń oraz wymagane przy detekcji specyficznego ataku (separacja i decommisioning zainfekowanych środowisk).*
- *Procedury i szablony zgłoszenia naruszeń.*
- *Procedury zabezpieczenia materiału dowodowego i trybu ich udostępniania instytucjom upoważnionym,*
- *Logi audytowe dla działań administracyjnych: 380 dni; dostępu użytkownika do danych: 30 dni.*

- *… Systemy antywirusowy i antyspamowy. Sewery proxy i bramki filtrujące: blokada ruchu na podstawie bazy reputacji, blokada dostępu do określonych stron (…).*

- *… wynika, **że Burmistrz był świadomy możliwości utraty dostępu do przetwarzanych danych osobowych na skutek ataku ransomware**. Przyczyną wystąpienia naruszenia ochrony danych osobowych była, po pierwsze, **nierzetelnie przeprowadzona analiza ryzyka** (szczególnie w zakresie wykonywania kopii zapasowych), po drugie**, niepełne wdrożenie środków technicznych i organizacyjnych gwarantujących bezpieczeństwo w procesie przetwarzania**.*

  Holistyczne rozwiązanie zawierające uzupełniające się, realizowane w wielu warstwach zabezpieczenia. Zaimplementowane rozwiązanie musi posiadać i integrować w sobie wszystkie wymienione powyżej środki techniczne i organizacyjne zorkiestrowane w celu realizacji Cyberstorage. Jakość utrzymania musi być weryfikowana okresowymi audytami. Wymagane pełne wdrożenie środków technicznych.

  Implementacja ciągłego procesu dostosowania zabezpieczeń do zmieniających się poziomów zagrożenia. Ciągły monitoring z opcją natychmiastowej reakcji na przykład dzięki zastosowaniu algorytmów decyzyjnych sztucznej inteligencji (patrz też AI TRiSM)[2].

  Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

  - *Dystrybuowane, redundantne technologie NIDS/NIPS/StateFull FireWall/XDR akcelerowane sprzętowo.*
  - *Centralne zarządzanie bezpieczeństwem wspierane sztuczną inteligencją; wysoki poziom automatyzacji.*
  - *Implementacja tzw. honeypot oraz bastion host*
  - *Gotowe zestawy reguł jako do zastosowania w odpowiedzi na zmiany poziomów zagrożeń lub detekcję ataku.*
  - *Ochrona wielowarstwowa/niezależne mechanizmy ochrony,*
  - *Zdublowane niezależne narzędzia przywrócenia danych.*
  - *Niezależne/odrębne mechanizmy i protokoły replikacji danych/repozytoriów pomiędzy ośrodkami i do chmury.*
  - *Ścisłe współdziałanie SOC z (nadrzędnymi) CSIRT.*

  Źródła i przydatne linki https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/four-steps-to-achieve-soc-2-compliance

- ***…system operacyjny**, zainstalowany przez administratora na serwerze, w czasie wystąpienia naruszenia ochrony danych osobowych, **nie miał wsparcia producenta**.*

  Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

  - *Oferowane rozwiązanie jest **w całości** wspierane przez producenta w zakresie poprawek bezpieczeństwa. Wsparcie musi obejmować w szczególności (nie ograniczając się do): wszystkich komponentów sprzętowych, programowych, usług oraz opcjonalnych usług wsparcia utrzymania w całym planowanym okresie użytkowania nie krótszym niż 60 miesięcy.*
  - *Szablony systemów operacyjnych dla platformy wirtualizacyjnej oraz kontenerowej muszą być utwardzone (ang. hardened).*

  Źródła i przydatne linki https://public.cyber.mil/stigs/srg-stig-tools/
  https://dl.dod.cyber.mil/wp-content/uploads/stigs/pdf/U_STIG_Viewer_3-x_User_Guide_V1R2.pdf
  https://www.vmware.com/security/certifications/stigs.html
  https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10
  https://www.hpe.com/psnow/doc/a00135108enw

[2] https://emt.gartnerweb.com/ngw/globalassets/en/publications/documents/2024-gartner-top-strategic-technology-trends-ebook.pdf

- *…należy zatem stwierdzić, że przed wystąpieniem przedmiotowego naruszenia ochrony danych osobowych obowiązujące u Administratora* ***zasady tworzenia kopii zapasowych nie zapewniały realizacji obowiązków*** *wynikających z art. 32 ust. 1 lit. b) i c) rozporządzenia 2016/679, tj.* ***zdolności do ciągłego zapewnienia dostępności systemów i usług przetwarzania oraz zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu*** *fizycznego lub technicznego.*

  Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

  - *Rozwiązanie musi zapewniać automatyczne usługi wysokiej dostępności, także dla scenariuszy utraty ośrodków przetwarzania, technologie natychmiastowego (minuty) przywrócenia aplikacyjnie koherentnych danych z protegowanych (immutable) repozytoriów oraz dedykowane środowiska przywracania (IRE/Sandbox). Proces przywracania musi być zautomatyzowany i obejmować wszystkie krytyczne usługi/aplikacje i zapewniać zachowanie bezpieczeństwa.*
  - *Rozwiązanie musi w prosty sposób pozwalać na objęcie wskazanych środowisk kwarantanną (izolacja) w tym blokadą dostępu przez użytkowników. Izolacja musi obejmować sieci zarządzającą i dostępową oraz izolację domeny użytkowników serwisowych.*
  - *RTO=1h.*
  - *Środowiska IRE.*
- ***…nie zastosował się do procedur, których był autorem****.*

  Rozwiązanie musi być zintegrowane w stopniu zapewniającym szeroką automatyzacją procesów, eliminując ryzyko pominięcia lub niewłaściwego wykonania procedur. Opcjonalne usługi utrzymania i/lub audytu dodatkowo adresują ten scenariusz.

  Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

  - *Proste przejrzyste,* ***zautomatyzowane*** *procedury.*
  - *Niezbędne Drzewa Decyzyjne.*

- ***nie były … testowane****, mierzone i oceniane* ***celem weryfikacji ich skuteczności****. W trakcie prowadzonego postępowania administrator* ***nie był w stanie wykazać****, że zastosowane* ***rozwiązania są wystarczające*** *dla zapewnienia bezpieczeństwa przetwarzanych danych. Ponadto administrator* ***nie przedstawił dowodu****, że po wystąpieniu naruszenia ochrony danych osobowych* ***dokonuje regularnego testowania****.*

  Wymaga dostarczenia w pełni zabezpieczonej platformy z udokumentowanymi, zintegrowanymi i automatycznymi procedurami utrzymania, testów oraz ich aktualizacji mających na celu zapewnienie zgodności. System audytowy, musi dokumentować prawidłowość wykonania procesów, testów i zmian konfiguracji. Procesy testowe muszą być zautomatyzowane i transparentne dla obciążeń produkcyjnych pozwalając na regularne, bezpieczne, nieuciążliwe przeprowadzania testów ze wskazaną przez administratora częstotliwością w standardowym oknie pracy.

  Kluczowe zagadnienia dla realizacji postulatu orzeczenia:

  - *Rozwiązanie musi automatycznie wykonywać i dokumentować działania w celu dochowania należytej staranności (np. przeprowadzenia testów).*

Źródła i przydatne linki
https://www.uodo.gov.pl/decyzje/DKN.5131.56.2022
https://uodo.gov.pl/decyzje/DKN.5131.8.2021
https://uodo.gov.pl/pl/138/2869

Dobór produktów zapewniający niezbędne technologie oraz integrację

Docelowe rozwiązanie musi:

- spełniać bieżące i planowane wymagania biznesowe klienta,
- pozostawać w zgodzie z trendami i przewidywaniami rynkowymi,
- zapewniać harmonijny rozwój środowisk klienta eliminując technologie nierozwojowe, których utrzymanie generuje zbędne rosnące z czasem koszty,
- zapobiega zbędnemu obciążeniu pracowników zadaniami o niskiej wartości.

Rozwiązanie zostało zbudowane za pomocą mapowania niezbędnych (wytłuszczone) technologii firmy Gartner na wybrane produkty oferty HPE.

Gartner Hype Cycle for Storage and Data protection 2023	PCBE	EDF	Scality	StoreOnce	CommVault / Veeam
Cloud Data backup		**X**	**X**	**X**	**X**
Cloud Infrastr. Recovery Assurance Software	X				

Gartner Hype Cycle for Storage and Data protection 2023	PCBE	EDF	Scality	StoreOnce	CommVault / Veeam
Computational Storage		X			
Container Backup	**X**				**X**
Container Native Storage	**X**	**X**			
Cyber Storage	**X**	**X**	**X**	**X**	**X**
Data Discovery		X			
Data Fabric		X			
Data Storage Mgmnt Services	**X**	**X**			
Digital Communication Govern.					
Distributed File Systems		X			
DNA Storage					
Edge Storage		X			
Functional Accelerator Cards	**X**				
Hybrid Cloud File Data Svcs		X			
Hybrid Cloud Storage		**X**	**X**		
HyperCovergence	**X**				
Immutable Data Vault	**X**	**X**	**X**	**X**	
Isolated Recovery Environment	**X**	**X**	**X**	**X**	**X**
NVME-oF	X				
Object Storage		X	X		
Open-Source Storage					
SaaS		X	X	X	X
SDS		X	X	X	X

gdzie: PCBE – HPE GreenLake for Private Cloud Business Edition
EDF – Ezmeral Data Fabric
Scality – Scality Ring/Artesca
StoreOnce – HPE Storeonce
Veeam/CommVault – Veeam Backup and Recovery/CommVault

Podsumowanie: Integracja 2-4 produktów HPE, dostarcza wszystkie niezbędne i kluczowe technologie infrastrukturalne/platformowe zapewniając klientowi, o każdych wymaganiach i wielkości, realizację każdego ze strategicznych celów w oparciu o sprawdzone, przyszłościowe technologie. Budowa rozwiązania stosując wzajemnie zintegrowanych technologiach zapewnia najwyższe: efektywność, automatyzację, prostotę procesów utrzymania, znacznie redukuje złożoność i pracochłonność implementacji Cybersecurity Mesh Architecture (CSMA) – tworząc solidną podstawę niezbędną dla dochowania należytej staranności w zakresie zgodności, przy jednoczesnym spełnieniu najbardziej rygorystycznych SLA i efektywności operacyjnej (eliminacja zbędnej pracochłonności).

Koncepcja Cyberstorage dla zapewnienia zgodności w rozwiązaniu HPE

Zgodnie ze wskazaniami stosowania technologii bazując na jej dojrzałości oraz trendach rynku IT kluczowe technologie niezbędne do budowy holistycznego rozwiązania dobraliśmy w oparciu o analizy firmy Gartner oraz IDC.

Należy zwrócić uwagę, że standaryzacja wraz z minimalizacją ilości narzędzi i technologii oraz jedna konsola zarządzania eliminuje złożoność zarządzania, upraszczają procesy klasyfikacji, analiz i zarządzania tenantami (aplikacjami, systemami, danymi) oraz ryzykiem, przy wykorzystaniu wielopoziomowej protekcji oraz dublowaniu krytycznych narzędzi.

Usługi ciągłości przetwarzania i wysokiej dostępności (BC/HA)

Usługi ciągłości przetwarzania i wysokiej dostępności oraz skalowalności rozwiązania są zaimplementowane na poziomie Vmware z wykorzystaniem (ale nie ograniczając się do) zaleceń STIG. W warstwie sieciowej za monitoring bezpieczeństwa sieciowego odpowiadają akcelerowane sprzętowo dystrybuowane rozwiązania firewall'a (realizowane na portach przełącznika lub kartach FACs). Konta serwisowe oraz użytkowników używają rozdzielnych domen autentykacji dedykowanych dla poszczególnych warstw stosu. Ciągły monitoring znanych wektorów ataku oraz anomalii zapewnia niezbędny poziom bezpieczeństwa. Opcjonalnie wykorzystanie algorytmów sztucznej inteligencji dla zapewniania natychmiastowej reakcji oraz wymiany informacji z CSIRT.

Usługi przeciwdziałania skutkom katastrof (DR)

Przeciwdziałanie skutkom katastrofy, w zależności od przyjętej architektury zapewnia, że utrata ośrodka przetwarzania skutkuje natychmiastowym automatycznym restartem zasobów w drugim ośrodku (RTO<5 min) bez utraty danych (RPO=0) lub przełączeniem automatycznym (opcja semi-automatycznym – wyzwalanym przez administratora) z RPO i RTO<1h w ośrodku zapasowym, który może być także w wielo-chmurze. Komunikacja pomiędzy ośrodkami przetwarzania musi być izolowana i zabezpieczona przed przechwyceniem. Rozwiązanie powinno umożliwiać przeprowadzenie testów DR bez wpływu na bieżące operacje.

Usługi ochrony danych (DP)

Rozwiązanie ***wyposażone jest w dwa niezależne mechanizmy ochrony danych działające równocześnie, wykorzystujące co najmniej dwa niezależne typy chronionych repozytoriów***. Zarządzanie retencją jest realizowane przez oprogramowanie backup'owe w pełni zintegrowane z funkcją „immutability" repozytoriów, eliminując ryzyko utraty danych spowodowane błędną konfiguracją.

Funkcje ***dwuskładnikowej autentykacji/autoryzacji*** (znane z systemów transakcji bankowych) wraz z opcjami szyfrowania transmisji oraz danych w miejscu przechowania, zapewniają spełnienie każdych wymagań zgodności.

Repozytorium powinno wspierać ***szyfrowanie danych w transmisji i składowaniu, blokady retencji (immutability)*** zarządzanej przez oprogramowanie kopii zapasowych.

Usługi ciągłego wykrywania skutków działania ransomware mają na celu natychmiastową detekcję jego i natychmiastowe wskazanie poprawnych (nieskażonych) punktów przywrócenia danych.

Efektywna ***opcja backupu do chmury*** zapewniająca, że między ośrodkami przetwarzania przesyłane są wyłącznie unikalne, skompresowane i zaszyfrowane w formie niejawnej dane.

Replikacja repozytoriów kopii zapasowych musi zapewniać ciągłą izolację środowisk przetwarzania pomiędzy lokalizacjami przetwarzania (głównego i zapasowych środowisk przetwarzania) i powinna ***stosować odrębne technologie niż wykorzystywana na potrzeby DR***. Rozwiązania ***czasowo blokujące komunikację obecnie są niewystarczające***.

Częścią przywrócenia danych jest przywrócenie niezbędnej infrastruktury – rekomendowane rozwiązania IaC.

Testy przywrócenia danych nie wpływają na przetwarzanie produkcyjne i są ***uruchamiane za pomocą kliknięcia lub wykonywane automatycznie***. Przywrócenie wskazanych zasobów, zachodzi we ***wskazanym środowisku IRE*** (Isolated Recovery Environments), w ośrodku przetwarzania/multi-chmurze, z wykorzystaniem koherentnego aplikacyjnie punktu przywrócenia, z dowolnego repozytorium typu Immutable Data Vault. Log z przywrócenia danych i poprawności działania przywróconych środowisk jest generowany automatycznie i przesyłany na wskazany adres celem udokumentowania procesu. Testy muszą być wykonane przy aktywnych najbardziej restrykcyjnych politykach bezpieczeństwa – dedykowanych dla krytycznych zagrożeń.

Źródła i przydatne linki:
https://helpcenter.veeam.com/docs/backup/vsphere/sandbox.html?ver=120
https://www.veeam.com/ransomware-protection.html
https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_appliance_storeonce.html?ver=120
Integracja Veeam immutability (ISV-DI)
https://helpcenter.veeam.com/docs/backup/vsphere/storeonce_supported_features.html?ver=120
https://community.veeam.com/blogs-and-podcasts-57/hpe-storeonce-immutability-with-v12-4273
https://www.hpe.com/psnow/doc/A00042003ENW.pdfhttps://www.hpe.com/psnow/doc/A00042003ENW.pdf
Integracja CommVault immutability
https://documentation.commvault.com/2023e/expert/data_immutability_feature.html
https://documentation.commvault.com/2023e/essential/supported_cloud_storage_products.html

Zabezpieczanie aplikacji z wykorzystaniem Web Application Firewall (WAF)

Rekomendowane „load balancer" posiada wbudowane funkcje WAF rozszerzające jego funkcjonalność o ochronę przed zagrożeniami nieobsługiwanymi w rozwiązaniach klasy UTM oraz NGFW. WAF to istotna linia obrony i mitygacji ataków:

1. typu "odmowa usługi" (DoS/DDoS), "brute-force" i "credential stuffing",
2. polegających na wstrzyknięciu skryptu i zniekształconych adresach URL (wbudowany SQL, JavaScript, ładowanie skryptu spoza witryny, próba zdalnego wykonania kodu (RCE) lub skryptów między witrynami (XSS)),
3. z określonych zakresów IP, blokada z wykorzystaniem geolokalizacji lub platformy używanej przez klienta,
4. specyficznych dla aplikacji ("ataki niszowe" lub ataki zużywające zasoby na przechowywanie obiektów w chmurze). Niezbędne, gdy sama aplikacja nie może zostać zmodyfikowana w celu załatania podatności,
5. dzięki funkcji „wirtualnego łatania" (wstępna naprawa znanych błędów przed dostępnością pełnej poprawki jako tymczasowy środka łagodzący do czasu dostępności łaty aplikacji źródłowej).

Zakres niezbędnych procedur i procesów dla zapewnienia zgodności

Przykładowe zakresy polityk, dla zapewnienia zgodności z dyrektywą NIS 2, artykuł 21, o środkach zarządzania ryzykiem:

1. Polityka analizy ryzyka i bezpieczeństwa systemów informatycznych:
    a. Wdrożenie polityk obejmujących analizę i ocenę ryzyka dla wszystkich aspektów systemów informatycznych, uwzględniającej ryzyka wewnętrzne i zewnętrzne.
    b. Regularna aktualizacja polityk w odpowiedzi na nowe zagrożenia i zmiany w środowisku technologicznym.
    c. Zastosowanie zaawansowanych technologicznie narzędzi do skanowania, identyfikacji luk w zabezpieczeniach oraz analizy ryzyka.
    d. Zastosowanie posiadanych technologii podnoszących poziom bezpieczeństwa, wskazanie technologii niezbędnych do pozyskania dla zapewnienia cyberbezpieczeństwa.
    e. Stosowanie bezpiecznych (certyfikowanych) produktów, bezpieczeństwo do fazy planowania
    f. Wdrażanie technik analitycznych takich jak analiza przyczynowo skutkowa, symulacje i modelowanie ryzyka.

2. Dostosowania strategii bezpieczeństwa fizycznego:
    a. Wdrożenie rygorystycznych procedur kontroli dostępu i uprawnień użytkowników, w tym zarządzanie kontami, hasłami i uprawnieniami w myśl zasady minimalnych niezbędnych uprawnień oraz izolacji/granularności.
    b. Regularne przeglądy i aktualizacje polityk dostępu, aby odpowiadały one zmieniającym się potrzebom i zagrożeniom zgodnie z zasadą Zero-Trust.
    c. Dokładna ewidencja i zarządzanie wszystkimi składnikami majątku IT, w tym oprogramowaniem, sprzętem i danymi (Configuration Management DataBase - CMDB).
    d. Wdrożenie procedur odpowiedzialności i kontroli zmian majątku (LifeCycle managemnt).
    e. Dwuskładnikowa kontrola dostępu, wykorzystanie biometrii.

3. Zapewnienia bezpieczeństwa w łańcuchu dostaw, w tym aspekty związane z bezpieczeństwem i zgodnością interakcji między podmiotami: Zamawiającym i kontrahentami (dostawcami, usługodawcami, odbiorcami):
    a. Systematyczne przeprowadzanie i wymiana wiedzy z zakresu audytów i ocen bezpieczeństwa kluczowych Kontrahentów.
    b. Zacieśnienie współpracy z kontrahentami w celu zwiększenia poziomu cyberbezpieczeństwa (wymiana wiedzy).
    c. Aktualizacja klauzul dotyczących zakresu i wymagań cyberbezpieczeństwa w umowach, zawierająca obowiązki jego ciągłego dostosowywania, w celu zachowania zgodności z NIS 2 oraz obowiązek informacyjny dotyczący incydentów (wystąpienie, ocena wpływu, sposób usunięcia i wdrożone aktualizacje) mających wpływ na świadczone usługi i wymianę informacji.
    d. Monitorowanie wykonania umów SLA, w szczególności w aspekcie bezpieczeństwa dostarczanych usług i produktów.

4. Zapewnienia ciągłości działania i zarządzanie kryzysowe:
    a. Wdrożenie strategii, opartej na kwantyfikowanych wskaźnikach SLI, SLO, KPI, SLA.
    b. Zapewnianie regularnych testów i procesów aktualizacji polityk na podstawie ich wyników (z zastosowaniem IaC IRE).
    c. Opracowanie szczegółowych planów przywracania przetwarzania w następstwie różnych scenariuszy – w odpowiedzi na serie incydentów (Rolling Disaster).
    d. Regularne ćwiczenia uwzględniające aktualizację planów w reakcji na nowe wektory ataku, zagrożenia i zmiany konfiguracji i technologii.

5. Dostosowania polityk i procedur oceny skuteczności zarządzania ryzykiem:
    a. Systematyczne przeprowadzanie testów i audytów bezpieczeństwa w zakresie skuteczności wdrożonych środków i zmian.
    b. Niezależne (zewnętrzne) audyty bezpieczeństwa w celu zapewnienia obiektywności.
    c. Definicja i monitorowanie miarodajnych wskaźników efektywności środków bezpieczeństwa (SLI/SLO/SLA).
    d. Regularna analiza KPI/SLI pod kątem optymalizacji efektywności zapewnienia cyberbezpieczeństwa.
    e. Usługi SOC/SOAR z wykorzystaniem XDR oraz dystrybuowanemu nauczaniu i współdzieleniu informacji CTI

6. Dostosowania procesów rozwojowych i utrzymania (inwestycji) systemów informatycznych, w tym postępowanie w przypadku ujawnienia nowych podatności:
    a. Wprowadzenie i przestrzeganie standardów bezpieczeństwa w procesie rozwoju oprogramowania, np. Secure Software Development Lifecycle (SSDLC), ISO/IEC 27034, STIG.
    b. Cykliczna ewaluacja standardów oraz jakości szyfrowania i zakresu ochrony danych przetwarzania i komunikacji.
    c. Stosowanie wieloskładnikowego uwierzytelniania i autoryzacji z wykorzystaniem technologii biometrycznych.
    d. Bezpieczne kanały łączności w sytuacjach nadzwyczajnych.
    e. Zapewnienie bezpiecznego i wysoko dostępnego zarządzania PKI.
    f. Implementacja polityk aktualizacji kluczy przed upłynięciem ich ważności.
    g. Regularna aktualizacja, przeglądy i testy bezpieczeństwa oprogramowania i infrastruktury w całym cyklu życia produktu.
    h. Stworzenie procesów identyfikacji, oceny ryzyka i remediacji na pojawiające się podatności w systemach informatycznych i oprogramowaniu.
    i. Ciągła aktualizacja i łatanie systemów w celu eliminacji znanych podatności.
    j. Uwzględnienie w procesie inwestycyjnym i transformacji niezbędnych dla cyberbezpieczeństwa produktów, technologii i usług i zmian konfiguracyjnych.

7. Dostosowania praktyk cyberhigieny i szkoleń w zakresie cyberbezpieczeństwa:
    a. Regularne szkolenia i warsztaty z cyberbezpieczeństwa dla zarządu i pracowników wszystkich poziomów organizacji.
    b. Rozwój świadomości i umiejętności niezbędnych do rozpoznawania i unikania zagrożeń cybernetycznych w tym phisingu.
    c. Przeprowadzenie cyklicznych testów (warsztaty/prowokacje) na bazie zachowania (oceny kultury informatycznej) użytkownika.
    d. Wdrożenie cyklicznego systemu szkoleń i aktualizacji wiedzy zespołu SOC i użytkowników środowiska informatycznego.

8. Obsługi incydentu:
    a. Opracowanie szybkich i skutecznych procedur identyfikacji, dokumentowania i reakcji na incydenty bezpieczeństwa.
    b. Wdrożenie procesów komunikacji i eskalacji, dla sprawnego zarządzania incydentem:
        i. CSIRT, instytucjami wskazanymi stosownymi regulacjami,
        ii. wewnątrz organizacji,
        iii. w łańcuchu dostaw (ISAC).

Źródła i przydatne linki:
https://cyberpolicy.nask.pl/poradnik-na-temat-tworzenia-isac-centra-wymiany-i-analizy-informacji/
https://attack.mitre.org/
https://oasis-open.github.io/cti-documentation/taxii/intro.html
https://oasis-open.github.io/cti-documentation/stix/intro
https://owasp.org/www-project-top-ten/

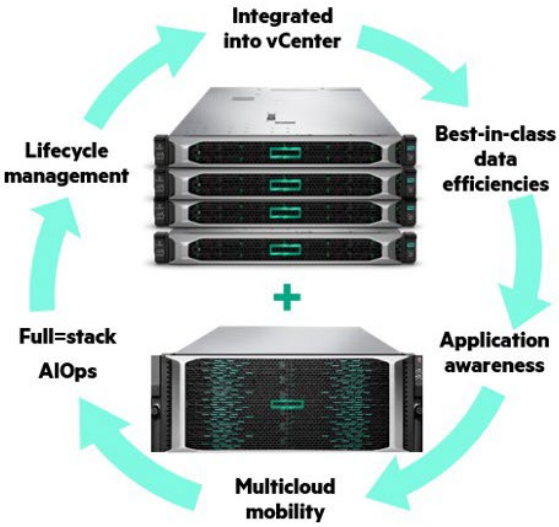
    c. Wykorzystanie centrum kompetencyjnego do analiz, reakcji na i zarządzania incydentem.

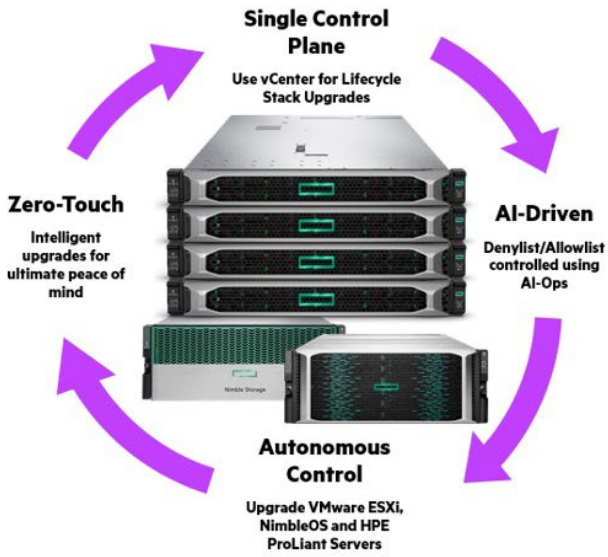
Załącznik 1 Referencyjne rozwiązanie HPE: kluczowe standardy, praktyki i technologie zapewniające zgodność.

Załącznik opisuje kompletne rozwiązanie. HPE dysponuje technologiami i praktyką dostosowania istniejących rozwiązań, wykorzystujących produkty firm trzecich, do stanu zgodnego z regulacjami w sposób zapewniający, że zasoby ludzkie nie będą przeciążone zadaniami o niskiej wartości. Wskazuje jak uniknąć zarzutu i kar za „…***niepełne wdrożenie środków technicznych i organizacyjnych gwarantujących bezpieczeństwo w procesie przetwarzania”.***

Technologie składowe rozwiązania

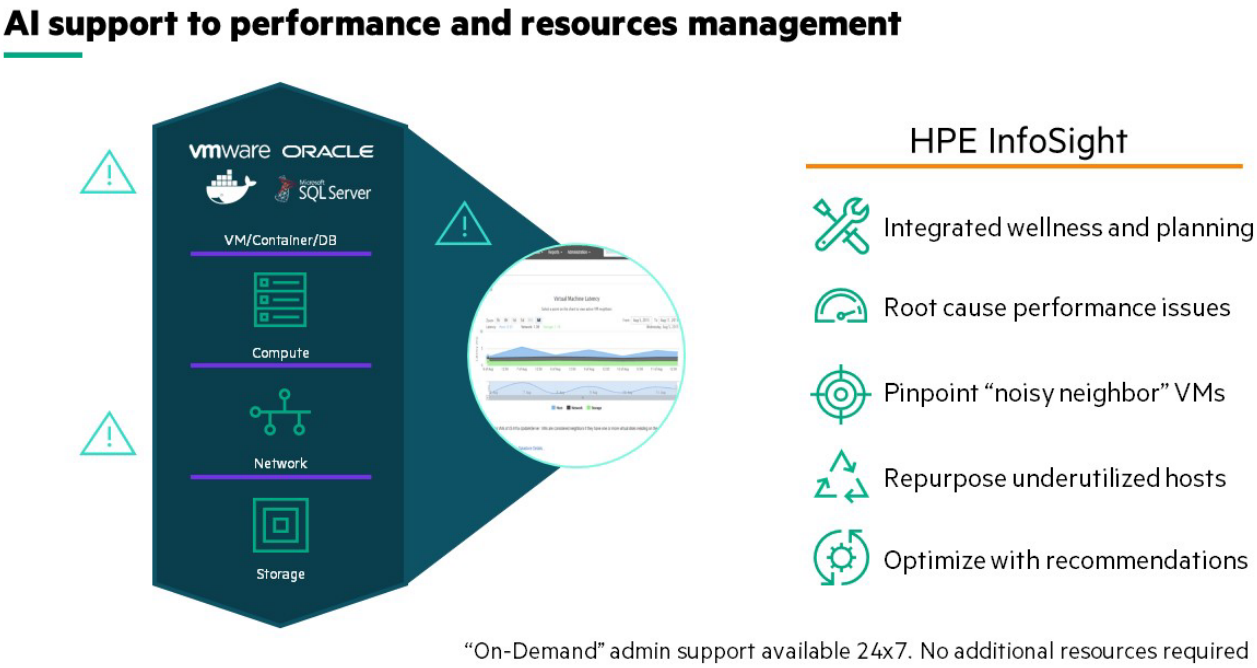
Podstawą rozwiązania jest HPE GreenLake for Private Cloud Business Edition (PCBE) zapewniające zintegrowaną w zakresie provisioningu (udostępniania zasobów), utrzymania, rozbudowy oraz monitoringu platformę wirtualizacyjną oraz kontenerową wspierającą rozbudowę w trybie scale-up oraz scale-out. Z punktu widzenia obsługi jest to jedno zintegrowane modularne urządzenie wspierające IaC.





Benefity: zautomatyzowany proces aktualizacji obejmuje całe środowisko (wszystkie komponenty rozwiązania), gwarantując poprawność doboru wszystkich komponentów składowych: firmware, sterowników, oprogramowania platformy wirtualizacyjnej w obrębie całego środowiska. Aktualizacja odbywa się w trybie na gorąco.

Algorytmy sztucznej inteligencji wykonują wszystkie okresowe, żmudne i czasochłonne zadania wspierając utrzymanie w zakresie zarządzania bezpieczeństwem, efektywności i jakości świadczonych usług.



Dodatkowe produkty dostępne jako oprogramowanie lub urządzenia zapewniają dostarczenie kluczowych technologii wraz ze zmieniającym się zapotrzebowaniem: HPE Ezmeral, Scality oraz HPE StoreOnce i Veeam są implementowane wraz z ewolucją potrzeb, wybraną strategią DR oraz zakresu korzystania z wielo-chmury.

Skalowalność rozwiązania HPE

Rozwiązanie skaluje się od 2 serwerów (100 SPECspeed2017_int) i 12 TB danych produkcyjnych (źródłowych) po środowiska o setkach tysięcy SPECspeed2017_int oraz dziesiątkami PB danych źródłowych. Klienci stają się beneficjentami skali już w początkowych fazach rozbudowy środowiska.

Bezpieczeństwo na poziomie aplikacji i platformy

Środowisko jest implementowane przy zachowaniu zasad Zero Trust w zgodzie ze STIG (baza dla ISO/IEC 27034), w szczególności, wszystkie konta typu administracyjnego i użytkowników uprzywilejowanych są tworzone zgodnie z zasadą separacji środowiskowej i minimalnych niezbędnych uprawnień. Autentykacja personelu z prawami Administratorów i PowerUser'ów wymaga zastosowania dwuskładnikowego uwierzytelnienia. Środowisko wykorzystuje mikrosegmentację, DMZ, Statefull Firewall, NAT akcelerowane sprzętowo oraz opcjonalnie Honeypot, wirtulane patchowanie oraz ochronę DDoS na poziomie WAF.

Kluczowe funkcje/technologie:

- Zweryfikowane metody tworzenia i holistycznego utrzymania bezpieczeństwa użytkowania aplikacji i usług biznesowych oraz komunikacji sieciowej zgodnej ze STIG/ISO 27034.
- Rozbudowa w trybie scale-up oraz scale-out z dystrybuowanymi usługami bezpieczeństwa.
- Wsparcie dla wielu tenantów w zakresie od zasobów infrastrukturalnych do aplikacji.
- Integracja z istniejącymi rozwiązaniami NGFW, IPS/IDS, WAF, CSM lub uzupełnienie tej funkcjonalności na poziomie platformy wirtualizacyjnej/kontenerowej w stopniu wymaganym przez Cyberstorage.
- Zintegrowane i bezpieczne usługi (oprogramowanie, narzędzia) i środowiska przywracania IRE/SandBox jako element Cyberstorage).
- Zdublowane, zintegrowane z aplikacjami usługi zabezpieczania danych z możliwością udostępnienia w trybie self service.
- Model autentykacji i szyfrowanie połączeń SPIFFE/SPIRE, WS Security lub analogiczna oparta z wykorzystaniem PKI.
- Komunikacja szyfrowana z wykorzystaniem TLS v1.3, lub algorytmów odpornych na łamanie z wykorzystaniem przetwarzania kwantowego.
- Opcjonalne zastosowanie WAF dla mitygacji specjalistycznych ataków DoS/DDoS, "brute-force", "credential stuffing", wstrzyknięcia skryptu lub zniekształconych adresaów URL (wbudowany SQL, JavaScript, ładowanie skryptu spoza witryny, próba zdalnego wykonania kodu (RCE) lub skryptów między witrynami (XSS)), blokady z wykorzystaniem geolokalizacji/platformy klienta, ataków niszowych na

aplikacje które nie mogą zostać zmodyfikowane w celu załatania podatności, (funkcja „wirtualnego łatania")- tymczasowy środek zstępczy do czasu dostępności łaty aplikacji źródłowej).

Źródła i przydatne linki:
https://public.cyber.mil/stigs/srg-stig-tools/
standard baseline for application security: ISO/IEC 27034
https://spiffe.io/
https://en.wikipedia.org/wiki/WS-Security_based_products_and_services

Bezpieczeństwo usług dostępowych i sieciowych

Bezpieczeństwo usług dostępowych jest realizowane na poziomie sieci dzięki zastosowaniu technologii SASE, SD-WAN, vLAN, mikrosegmentacji FACs (bezpośrednio na poziomie portów przełączników lub kart NIC). Integracja z platformą wirtualizacyjną jest realizowana z wykorzystaniem sprzętowo akcelerowanych OVSDB oraz funkcji distributed firewall. Integruje się z posiadanymi lub dostarcza (opcjonalnie) funkcje UTM/NGFW, IPS/IDS, WAF oraz load balancer.

Uwaga: zakres bezpieczeństwa IT obejmujący stosowanie technologii DLP, IDS/IPS, NGFW, SIEM, Decoy/HoneyPot są specyficzne dla klienta – rozwiązanie nie wnosi w tym zakresie żadnych istotnych ograniczeń, HPE dostosuje się do istniejącego lub zarekomenduje, dostarczy i zintegruje niezbędną funkcjonalność w tym zakresie.

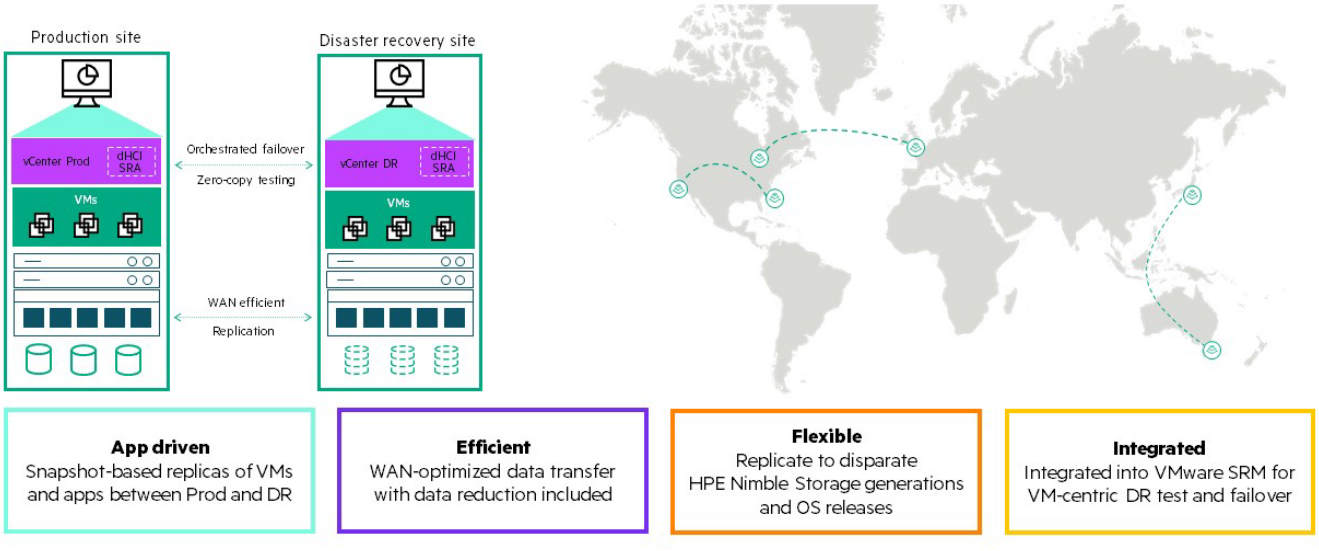
Kluczowe funkcje/technologie:

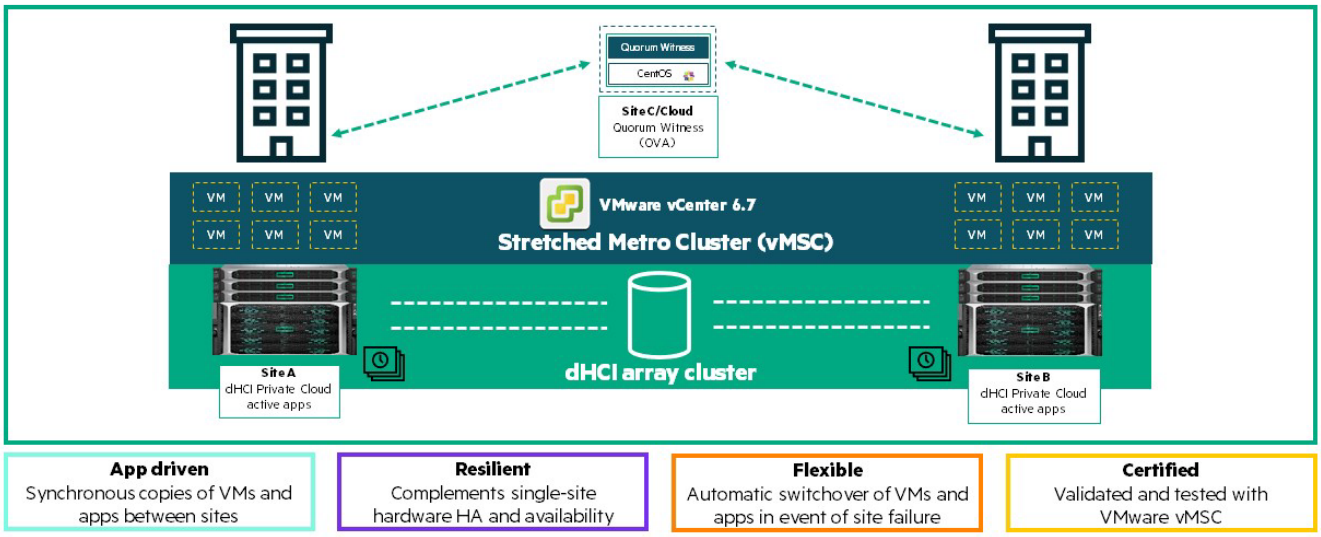
- Implementacja oparta o paradygmat Zero Trust.
- Separacja domen użytkowników serwisowych w ośrodkach.
- Zintegrowana z platformą wirtualizacyjną/kontenerową segmentacja i mikrosegmentacja.
- Niezależna i akcelerowana sprzętowo funkcjonalność zarządzania bezpieczeństwem połączeń na portach przełącznika lub FACs, zintegrowana z platformą wirtualizacyjną/kontenerową/Data Fabric.
- Aplikacyjnie koherentne migawki zabezpieczone dwuskładnikową autentykacją/autoryzacją jako repozytoria przywrócenia danych w środowisku produkcyjnym lub IRE/SandBox.
- Wykorzystanie sztucznej inteligencji do mitygacji ataków wykonanych przy użyciu sztucznej inteligencji.
- Metodyka autoryzacji i szyfrowanie połączeń SPIFFE/SPIRE, WS Security lub analogiczna oparta z wykorzystaniem PKI.
- Komunikacja szyfrowana z wykorzystaniem TLS v1.3, lub algorytmów odpornych na łamanie z wykorzystaniem przetwarzania kwantowego.

Źródła i przydatne linki:
https://www.hpe.com/psnow/doc/a50004267enw.pdf
https://www.arubanetworks.com/assets/wp/WP_Aruba-CX-10000.pdf
https://www.arubanetworks.com/resource/aruba-cx10000-guardicore-solution-overview/
https://www.gov.pl/web/cyfryzacja/akty-prawne

Ciągłość przetwarzania (BC/HA/DR)

Rozwiązanie wspiera dowolny tryb zapewniania ciągłości przetwarzania ang. Business Continuity (BC) z wykorzystaniem dostępnych technologii zapobiegania katastrofom ang. Disaster Recovery (DR) oraz technologii zapewniających wysoką dostępność ang. High Availability (HA) dzięki dowolności zastosowania trybu replikacji synchronicznej lub asynchronicznej do innego ośrodka/chmury. Chmura może być ośrodkiem podstawowym, zapasowym lub pełnić obie funkcje (tryb wszystkie ośrodki aktywne A/A). Rozwiązanie wspiera architektury o RPO=RTO=0 z wykorzystaniem replikacji synchronicznej i klastrów rozległych oraz RPO=RTO=1min+ dla replikacji asynchronicznej. Automatyczne przełączenie może być przeźroczyste dla aplikacji wykorzystujących kontenery lub wirtualizację.





Kluczowe funkcje/technologie:

- Wsparcie dla replikacji synchronicznej w trybie stretch cluster (RTT<5ms; BC=RPO=RTO=0).
- Wsparcie dla replikacji asynchronicznej - replikowane są wyłącznie unikalne skompresowane dane (BC/RPO/RTO>0).
- Przywrócenie danych/replikacji aplikacyjnie koherentnego punktu w czasie (immutable).
- Punkty przywracania chronione dwuskładnikową autentykacją.
- Metodyka autoryzacji i szyfrowanie połączeń SPIFFE/SPIRE lub analogiczna oparta z wykorzystaniem PKI/TLS V1.3, lub algorytmów odpornych na łamanie z wykorzystaniem przetwarzania kwantowego.
- Wsparcie dla procesów DR w trybie IaC.

Źródła i przydatne linki
https://www.hpe.com/psnow/doc/a50004267enw?jumpid=in_hpesitesearch
https://www.hpe.com/psnow/doc/PSN1014368376USEN?jumpid=in_hpesitesearch
https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
https://public.cyber.mil/stigs/srg-stig-tools/
standard baseline for application security: ISO/IEC 27034
https://spiffe.io/

Bezpieczeństwo usług ochrony danych (DP)

Rozwiązanie zapewnia zwielokrotniony mechanizm zabezpieczenia danych. Kopie zapasowe wykonywane przez oprogramowanie Veeam oraz wbudowany akcelerowanym sprzętowo workflow PCBE, skonfigurowane w sposób zapewniający koegzystencję, przy jednoczesnej niezależności – utrata jednego narzędzia i repozytorium danych nie dyskwalifikują użycia drugiego mechanizmu. Repozytoria danych są ***chronione dwuskładnikową autentykacją/autoryzacją w trybie Immutable Data Vault***. Żadne z oferowanych ***repozytoriów backupu nie są prezentowane jako lokalny bądź sieciowy system plików*** także w trakcie zadań tworzenia/przywracania kopii zapasowych. Funkcjonalność ***Immutable Data Vault jest zintegrowana z rozwiązaniem backupowym*** w celu eliminacji ryzyka utraty punktu przywracania przed upływem retencji. Istotną opcją jest możliwość ***stosowania uproszczonego zarządzania zgodnością z RODO*** na podstawie art. 6 i 11 dla przetwarzania (które nie daje bezpośredniego dostępu do danych wrażliwych).

Kluczowe funkcje/technologie:

- Implementacja zintegrowanych funkcji Immutable Data Vault dla repozytoriów danych w całym rozwiązaniu (oprogramowanie … sprzęt/chmura).
- Zabezpieczenie dwuskładnikową autentykacją/autoryzacją istotnych działań administracyjnych i zasobów.
- Repozytoria kopii zapasowych NIGDY NIE SĄ prezentowane jako lokalny bądź sieciowy system plików.
- Repozytoria danych są zabezpieczone przed modyfikacją.
- Pełna integracja funkcji Immutable Data Vault repozytorium danych z systemem kopii zapasowych (eliminacja ryzyka utraty punku przetwarzania z powodu niespójnej konfiguracji).
- Granularność uprawnień dla obsługi procesu przywracania danych.
- Delegacja/granulacja uprawnień w tym samoobsługa.
- Pełna integracja procesowa ze środowiskami IRE/Sandbox dla automatycznych, udokumentowanych testów przywracania danych i przetwarzania w tym w trybie IaC
- Technologie rozpoznawania wczesnych etapów działania ransomware.
- Metodyka autoryzacji i szyfrowanie połączeń SPIFFE/SPIRE, WS Security lub analogiczna oparta z wykorzystaniem PKI.
- Komunikacja szyfrowana z wykorzystaniem TLS V1.3, lub algorytmów odpornych na łamanie z wykorzystaniem przetwarzania kwantowego.
- Różne/niepowiązane mechanizmy klonowania repozytoriów backup (w pełni bezpieczna realizacja tzw. air-gap).

Źródła i przydatne linki
https://helpcenter.veeam.com/docs/backup/vsphere/sandbox.html?ver=120
https://www.veeam.com/ransomware-protection.html
https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_appliance_storeonce.html?ver=120
https://helpcenter.veeam.com/docs/backup/vsphere/storeonce_supported_features.html?ver=120
https://community.veeam.com/blogs-and-podcasts-57/hpe-storeonce-immutability-with-v12-4273
https://www.hpe.com/psnow/doc/A00042003ENW.pdfhttps://www.hpe.com/psnow/doc/A00042003ENW.pdf

Bezpieczeństwo i efektywność wykorzystania chmury prywatnej i/lub publicznej

Chmura publiczna jest coraz częściej wykorzystywana na równi z posiadanym ośrodkiem przetwarzania. Wykorzystanie jej w celach zachowania ciągłości przetwarzania wymaga technologii efektywnego wykorzystania jej zasobów w szczególności ograniczenie tzw. egresu (przesyłania danych z chmury). Pożądane są narzędzia optymalizacji kosztów utrzymania w chmurze.

Kluczowe funkcje/technologie:

- Redukcja (deduplikacja i kompresja) oraz szyfrowanie przesyłanych, oraz przechowywanych chmurze danych w sposób zapewniający wymagany dostęp (data Discovery/Data Insight).
- Zarządzanie własną PKI.
- Zarządzanie środowiskiem wielo-chmurowym (ang. multicloud).
- Dedykowane lub szyfrowane łącza komunikacyjne.
- Efektywność kosztowa zarządzania wielo-chmurą w tym eliminacja intensywnego egresu.
- Technologie zapewniające natychmiastowe przełączenie przetwarzania do/z wielo-chmury.
- Integracja technologii, w tym zabezpieczeń zapewniająca, że zasoby wielo-chmury są częścią Cyberstorage.
- Separacja domen kont serwisowych, wsparcie modelu domen zasobowych.
- Metodyka autoryzacji i szyfrowanie połączeń SPIFFE/SPIRE lub analogiczna oparta z wykorzystaniem PKI.
- Komunikacja szyfrowana z wykorzystaniem TLS v1.3, i/lub algorytmów odpornych na łamanie z wykorzystaniem przetwarzania kwantowego.
- Wsparcie szyfrowania danych na nośnikach.

Źródła i przydatne linki: https://www.gov.pl/attachment/f24aecca-8e81-4b30-becd-77da94a6b71c

Edukacja i szkolenia

Regulacje nakładają obowiązek na przeprowadzenie udokumentowanych adekwatnych szkoleń. HPE na potrzeby podmiotów i firm przygotowało specjalne pakiety szkoleń dostępnych w rocznej subskrypcji, w której znajdują się niezbędne szkolenia od zakresu sieci, bezpieczeństwa, usług (ITIL), Infrastruktury, chmury po DevOps, Sztuczną Inteligencję oraz zarządzanie produktami i projektami. Zakres szkoleń pozwala w łatwy i kompleksowy sposób dostosować pakiety wymaganych i rozszerzonych szkoleń dla każdej roli – od zarządu, specjalistów bezpieczeństwa w tym SOC, po użytkownika systemów informatycznych. Odbycie każdego szkolenia jest udokumentowane (na potrzeby zgodności) tzw. badge'm. Wśród szkoleń znajduje się 47 certyfikowanych programów organizacji w tym ISC, EC Council, Google, CompTIA, IIBA, Microsoft, PMI. Niektóre ze szkoleń w tym dot. Centrum Operacji Bezpieczeństwa są nieodpłatnie wykonywane w ramach programu współpracy PWCyber Ministerstwa Cyfryzacji RP w zakresie Cyberbezpieczeństwa.

Źródła i przydatne linki:
hpe.com/ww/digitallearnerSMB
https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen

Dochowanie należytej staranności dzięki efektywnej implementacji dostępnych technologii.

Lp	Technologia	PCBE	EDF	Store-Once	Veeam	Network	Wyjaśnienia
1.	Immutability	X	X	X	X		Zintegrowana retencja repozytoriów (Veeam ISV-DI) – eliminacja ryzyka błędu ludzkiego; akcelerowane sprzętowo. Repozytoria zabezpieczone przed skasowaniem (immutable)
2.	RTO (100TB)	<15 min	<4h*	<4h*	<4h*		RTO<15min niezbędne dla usług wymagających wysokiej dostępności. oraz dla mitygacji ransomware przy wykorzystaniu wielu IRE.
3.	2 składnikowa autentykacja	X	X	X	X	X	Specyfikowane w DORA, CER, NIS 2, NSC, zalecenia CeZ
4.	2 składnikowa autoryzacja	x		X			Dodatkowe zabezpieczenie przed błędem ludzkim i ransomware
5.	(mikro/dynamiczna) segmentacja	X	X	X		X	EDF z SPIFFE/SPIRE – mikrosegmentacja CX-10000 (mikro)segmentacja + dynamiczna segmentacja ze wsparciem XDR.

Lp	Technologia	PCBE	EDF	Store-Once	Veeam	Network	Wyjaśnienia
6.	Detekcja i mitygacja ransomware	X		X	X		Dzięki wbudowanym algorytmom detekcji, zdublowanym narzędziom przywrócenia w tym natychmiastowego, równoległego przywracania danych.
7.	szyfrowanie	X	X	X	X	X	W transmisji i składowaniu danych; ARUBA CX 10000 – 800Gbps sprzętowo szyfrowanych tuneli..
8.	Śluza dla backupu	X		X	X		Wszystkie repozytoria i systemy kopii zapasowych w każdym ośrodku są na stale odseparowane (okna synchronizacji są zbędne) i zapewniają tzw. Immutability.
9.	Ochrona danych (backup)	X			X		Zwielokrotnione narzędzia odzyskiwania danych (koegzystencja). Oraz Paradygmat 3-2-1 akcelerowany sprzętowo.
10.	Dystrybuowany FW L4-L5	X				X	(Dynamiczna) segmentacja oraz mikrosegmentacja akcelerowana sprzętowo w przełączniku ToR zintegrowanym z platformą.
11.	Izolowane środowiska przywracania (IRE)	X	X	X	X	X	Pełna automatyka, wsparcie dla Infrastructure as Code (IaC), ponad 10-krotne skrócenie testów przywracania/mitygacji skutków ransomware bez wpływu na produkcję. Równoległe przywracanie danych przy aktywnych najbardziej rygorystycznych politykach bezpieczeństwa.
12	Security Service Edge/SASE					X	Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) and Firewall as a Service (FWaaS) – SASE
13	Akceleracja sprzętowa	X	X	X		X	Sprzętowa akceleracja przetwarzania (CPU, GPU, FPGA, APU) i bezpieczeństwa (DPU, Immutability, remediacja ransomware, mikrosegmentacja, DDoS, NAT, dystrybuowany firewall, VPN).
14	Współdzielenie informacji CTI	X	X			X	Automatyczne współdzielenie i wykorzystanie informacji CTI w sektorach lub całej infosferze Polski trybie ciągłym - krytyczne dla predyktywnego zapewnienia bezpieczeństwa.

Wiele niezależnych linii zabezpieczeń to dobra praktyka SZBI. Wykorzystanie akcelerowanych sprzętowo technologii zapewnia efektywność kosztową i redukuje opóźnienia.

Załącznik 3 Słownik pojęć

AI TRiSM (Artificial Intelligence Trust, Risk, Security Management) – zarządzanie obszarami stosowania modeli sztucznej inteligencji.

Air-gap śluza – technologia pełnej separacji środowisk między ośrodkami DR (w tym chmura). Środowiska nie mają wzajemnie żadnego połączenia.

ANSI/TIA Norma infrastruktury telekomunikacyjnej dla centrów przetwarzania danych (TIA) zgodna z amerykańską normą krajową (ANS) - określa minimalne wymagania dotyczące infrastruktury centrum danych. https://en.wikipedia.org/wiki/TIA-942

BC (Business Continuity) – Ciągłość przetwarzania – zdefiniowane jako „procesy, procedury, decyzje i działania mające na celu zapewnienie organizacji możliwości funkcjonowania pomimo przerwy w działalności operacyjnej". Innymi słowy, chodzi o tworzenie proaktywnych i reaktywnych planów, eliminujących, przeciwdziałających i/lub minimalizujących wpływa awarii i katastrof zapewniający ich szybką remediację w celu przywrócenia normalnego funkcjonowania.

CER (Wykaz usług kluczowych świadczonych przez podmioty krytyczne) dyrektywa skorelowana ze dyrektywą w sprawie środków na rzecz wysokiego, wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (Dyrektywa NIS 2)

CI/CD Połączone praktyki ciągłej integracji (CI) i ciągłego dostarczania (CD) lub rzadziej, ciągłego rozwoju. Określane także mianem ciągłego rozwoju lub ciągłego rozwoju oprogramowania.

CMDB (Configuration Management DataBase). Baza danych zarządzania konfiguracją to termin ITIL określający bazę danych przechowującą informacje o zasobach sprzętu i oprogramowaniu (elementy konfiguracji) oraz informacje dotyczące relacji pomiędzy nimi. CMDB zapewnia sposób zrozumienia kluczowych aktywów organizacji i ich powiązań, takich jak systemy informacyjne, źródła wyższego szczebla lub zależności aktywów oraz dalsze cele aktywów

CommVault amerykańska firma zajmująca się oprogramowaniem do ochrony i zarządzania danymi.

CeZ Centrum e-Zdrowia. Odpowiada za realizację zadań z zakresu budowy społeczeństwa informacyjnego, które obejmują organizację i prawidłowe funkcjonowanie sektora ochrony zdrowia. Tworzy cyfrowe usługi i rozwiązania wspierające pracę profesjonalistów medycznych oraz ułatwiające obywatelom zarządzanie sprawami zdrowia. Operator sektorowego CSIRT.

CSIRT/SOC (Cyber Security Incident Response Team/Security Operations Center) CSIRT reaguje na incydenty związane z bezpieczeństwem, SOC zapobiegają ich wystąpieniu. Personel SOC jest odpowiedzialny za ciągły monitoring i analizę bezpieczeństwa organizacji w celu ochrony infrastruktury, danych i ciągłości przetwarzania.

CSMA (Cybersecurity Mesh Architecture). Zintegrowana struktura bezpieczeństwa w celu zabezpieczenia wszystkich zasobów, niezależnie od lokalizacji, w celu redukcji wpływu finansowego incydentów bezpieczeństwa oraz zachowania zgodności. Efektywnie integruje komponowalne, rozproszone narzędzia bezpieczeństwa w centralną płaszczyznę danych i kontroli

CTI (Cyber Threat Intelligence) ciągłe podnoszenie efektywności zarzadzania incydentami dzięki przetwarzaniu i analizie zgromadzonych danych w celu rozpoznania zagrożeń cyberprzestrzeni.

Data Fabric Konwergentna wieloprotokołowa pamięć masowa dla wszystkich posiadanych i planowanych obciążeń (Big Data, Data Lake, przetwarzania strumieniowego, ML/DL/AI, archiwa) ze zintegrowanymi technologiami niezbędnymi dla implementacji Cyberstorage Prawdziwą wartością fabryki danych jest jej zdolność do dynamicznej optymalizacji wykorzystania danych dzięki wbudowanej analityce, drastycznie redukując pracochłonność zarządzania danymi.

DLP (Data Loss Prevention). Detekcja potencjalnych naruszeń danych/transmisji eksfiltracji danych i ich remediacja poprzez ciągłe monitorowanie, wykrywanie i blokowanie wrażliwych danych podczas użytkowania (w miejscu przetwarzania), w ruchu (sieci) i w spoczynku (przechowywanie danych). Terminy „utrata danych" i „wyciek danych" są ze sobą powiązane i często są używane zamiennie. Incydenty związane z utratą danych zamieniają się w incydenty wycieku danych w przypadkach, gdy nośniki zawierające wrażliwe informacje zostaną utracone, a następnie przejęte przez osobę nieuprawnioną.

DORA (Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554). Rozporządzenie UE regulujące zarządzanie głównymi kategoriami ryzyka operacyjnego poprzez nie tylko alokację kapitału, ale przez zapewnienie odporności operacyjnej. DORA reguluje zasady dotyczące ochrony, detekcji, powstrzymywania, odzyskiwania i naprawy incydentów związanych z ICT. DORA ustanawia zasady dotyczące zarządzania ryzykiem ICT, zgłoszenia incydentów, testów odporności operacyjnej i monitorowania ryzyka stron trzecich ICT. Rozporządzenie wskazuje, że incydenty ICT i brak odporności operacyjnej zagrażają odporności całego systemu finansowego, nawet jeżeli istnieje „odpowiedni" kapitał na pokrycie tradycyjnych kategorii ryzyka.

DP (Data Protection). Ochrona danych - system zapobiegający utracie danych.

DR (Disaster Recovery) Odzyskiwanie po katastrofie to proces utrzymywania lub przywracania niezbędnej infrastruktury i systemów po katastrofie naturalnej lub spowodowanej przez człowieka, takiej jak powódź lub aktywność wojenna/terrorystyczna. Stosuje polityki, narzędzia, procesy i procedury. Odzyskiwanie po awarii koncentruje się na technologii informacyjnej (IT) lub systemach technologicznych wspierających krytyczne funkcje biznesowe, a nie na ciągłości biznesowej.

EDR (Endpoint Detection and Response) monitoring i ochrona indywidualnych urządzeń końcowych (w tym laptopy, stacje, serwery, urządzenia mobilne) w skali.

EHDS Europejska Przestrzeń Danych Medycznych. Określa zasady transgranicznej wymiany i dostępu do pierwotnych i wtórnych danych medycznych oraz ramy stosowania algorytmów Sztucznej Inteligencji.

ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa). Unijna agencja działającą na rzecz osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii Europejskiej.

HPE Ezmeral Modułowa platforma dla Big Data, środowisk kontenerowych oraz AI. Jednym z komponentów jest Ezmeral Data Fabric.

FAC/DPU/IPU (Function Accelerator Cards/Data Processing Units/Infrastructure Processing Unit) Karty sieciowe lub przełączniki oferujące zaawansowane technologie typu firewall, load balancer, tunneling, odciążające serwer od zadań ograniczania ruchu oraz detekcji niepożądanych połączeń.

GDPR patrz RODO

PCBE (HPE GreenLake for Private Cloud Business Edition). Zintegrowane platforma przetwarzania IT - rozwiązanie

HA (High Availability). Wysoka dostępność cecha systemu, której celem jest zapewnienie uzgodnionego poziomu wydajności i dostępności operacyjnej.

HoneyPot HoneyPot to mechanizm bezpieczeństwa IT, którego zadaniem jest detekcja i przeciwdziałanie próbom nieuprawnionego dostępu do systemów informatycznych z wykorzystaniem pułapki. HoneyPot składa się z danych (na przykład w witrynie sieciowej), które wydają się być częścią produkcyjnej witryny zawierającą informacje lub

	zasoby pożądane przez atakujących. W rzeczywistości jest izolowany, monitorowany zasób i zdolny do blokowania i analizy ataku w czasie zbliżonym do rzeczywistego.
HPE StoreOnce	Produkt HPE zapewniający implementację Immutable Data Vault dla repozytoriów rozwiązań ochrony danych. Oferowany jako urządzenie, SDS lub jako usługa.
IaC	(Infrastructure as Code). Zarządzanie infrastrukturą i jej udostępnianie poprzez kod, a nie procesami ręcznymi.
ICT	(Information and Communications Technology). Infrastruktura Informacyjno-komunikacyjna.
IPS/IDS	(Intrusion Prevention System/Intrusion Detection System). System protekcji/detekcji nieautoryzowanego dostępu.
IRE	(Isolated Recovery Environment). IRE zapewnia kompletny obszar przejściowy dla przywróconych maszyn wirtualnych, izolowany od innych sieci.
ISO/IEC	(International Organization for Standardization/International Electrotechnical Commission). Organizacje standaryzujące.
KPI	(Key Performance Indicators). Kluczowe wymierne wskaźniki postępu osiągniecia zamierzonego rezultatu. KPI skupiają się na doskonaleniu strategicznym i operacyjnym, tworzą podstawę analityczną do podejmowania decyzji i skupiając uwagę na tym, co najważniejsze.
Mikrosegmentacja	Proces segmentacji domeny kolizyjnej sieci na różne segmenty. Mikrosegmentacja jest wykorzystywana głównie w celu zwiększenia wydajności i/lub bezpieczeństwa sieci.
MITRE ATT&CK®	ogólnodostępna baza wiedzy z zakresu taktyk i technik przeciwnika, oparta na obserwacjach. Podstawa do opracowywania modeli zagrożeń i metodyki mitygacji w sektorach komercyjnym i administracji państwowej, oraz dostawców produktów i usług zapewniania cyberbezpieczeństwem.
NGFW	(Next-Generation FireWall). Zapora nowej generacji to rozwiązania zabezpieczające sieć, wykraczające poza tradycyjną zaporę połączeń stanowych. Podczas gdy tradycyjna zapora sieciowa zazwyczaj zapewnia stanową kontrolę przychodzącego i wychodzącego ruchu sieciowego, zapora nowej generacji zawiera dodatkowe funkcje, takie jak wykrywanie i kontrola aplikacji, zintegrowane zapobieganie włamaniom oraz chmurowa analiza zagrożeń.
NIPS/NIDS	(Network Intrusion Prevention System/Network Intrusion Detection System). System protekcji/detekcji nieautoryzowanego/niepożądanego dostępu, zaimplementowany w warstwie sieci.
NIS 2	(Dyrektywa NIS 2) to okołounijne prawodawstwo dotyczące cyberbezpieczeństwa. Zapewnia środki prawne mające na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa w UE. Wprowadzone w 2016 r. unijne przepisy dotyczące cyberbezpieczeństwa zostały zaktualizowane dyrektywą NIS 2, która weszła w życie w 2023 r.
NIST	(National Institute of Standards and Technology). Promuje innowacje i konkurencyjność przemysłu Stanów Zjednoczonych poprzez rozwój nauk pomiarowych, standardów i technologii w sposób zwiększający bezpieczeństwo ekonomiczne i jakość życia. https://nist.gov
NIST Cybersecurity Framework	zestaw wytycznych dotyczących remediacji zagrożeń cyberbezpieczeństwa organizacji, amerykańskiego Narodowego Instytutu Standardów i Technologii w oparciu o istniejące standardy, wytyczne i praktyki. https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf
NSC	(Narodowe Standardy Cyberbezpieczeństwa). Zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji, opracowane na podstawie standardów NIST, przyporządkowane obowiązującym w polskim systemie prawnym normom stosowanym w zarządzaniu.
OVSDB	(Open vSwitch Database), baza danych dostępna dla urządzeń sieciowych. Schematy w OVSDB określają tabele w bazie danych i typy ich kolumn oraz mogą obejmować ograniczenia dotyczące danych, unikalności i integralności referencyjnej. OVSDB oferuje atomowe, spójne, izolowane i trwałe transakcje.
PCBE	(HPE GreenLake for Private Cloud Business Edition). Rozwiązanie usprawniające i modernizujące wielogeneracyjne środowisko IT poprzez dostarczenie w pełni zintegrowanych usług chmurowych dla serwerów bare metal, kontenerów i maszyn wirtualnych w prywatnym środowisku klienta.
PKI	(Public Key Infrastructure). Zestaw ról, zasad, sprzętu, oprogramowania i procedur wymaganych do tworzenia, zarządzania, rozpowszechniania, używania, przechowywania i unieważniania certyfikatów cyfrowych oraz szyfrowania klucza publicznego.
RET	(Retention). Dla kopii zapasowych: okres rutynowego przechowywanie informacji. Dane powinny być przechowywane przez okres niezbędny do celów, w których dane te są przetwarzane.
RODO	(Rozporządzenie o Ochronie Danych Osobowych). Rozporządzenie Unii Europejskiej regulujące przetwarzanie danych osobowych. Ogólne rozporządzenie o ochronie danych, inaczej rozporządzenie o ochronie danych osobowych, OROD lub RODO (ang. General Data Protection Regulation, GDPR) – rozporządzenie unijne, zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu tych danych (normy ISO/IEC 27001, 27002, 27701)

RPO (Recovery Point Objective). Maksymalny akceptowalny okres, z którego dane są utracone (nie znajdują się w repozytorium backupu).

RTO (Recovery Time Obejctive). Maksymalny akceptowalny czas na przywrócenie przetwarzania po utracie danych.

RTT (Round-Trip Time). Czas od wysłania do potwierdzenie odbioru pakietu danych. Opóźnienie obejmuje czasy propagacji ścieżek pomiędzy dwoma punktami końcowymi komunikacji. RTT jest również nazywany czasem ping dla określonej wielkości pakietu i można go określić za pomocą polecenia ping.

Sandbox Izolowane środowisko testowe, umożliwiające uruchamianie aplikacji, programów lub otwieranie plików bez wpływu na aplikację, system lub środowisko produkcyjne. Twórcy oprogramowania używają piaskownic do testowania nowego kodu programowania, a działy bezpieczeństwa do bezpiecznej analizy podejrzanego kodu.

SDS (Software-Defined Storage). Oprogramowanie do przechowywania danych komputerowych, służące do udostępniania i zarządzania magazynowaniem danych w oparciu o zasady, niezależnie od sprzętu.

Scality Skalowalne rozwiązania pamięci obiektowej także w trybie chmury klasy korporacyjnej, z funkcją Immutable Data Vault.

SIEM (Security Information and Event Management). Dzięki analizie danych dokonuje rozpoznania, łączenia i priorytetyzację zdarzeń stanowiących zagrożenie bezpieczeństwa sieci, zanim wpłyną na operacje biznesowe.

SLA (Service-Level Agreement). Umowa określająca poziom jakości usług, jakie dostawca zapewnia klientowi.

SLI (Service-Level Indicator). Wskaźnik poziomu usługi. Metryka, kwantyfikująca jakość lub niezawodność usługi. Typowe wskaźniki SLI: dostępność, opóźnienie, przepływność i szybkość, procent błędów.

SLO (Service-Level Objective). Cele poziomu usług to mierzalne cele kluczowych wskaźników poziomu usług (SLI). Wskazują doświadczenie klienta aplikacji biznesowej lub infrastruktury. Wskazują, czy dostawca spełnia wymagania jakościowe dla świadczonych usług (SLA).

SOAR (Security Orchestration, Automation and Response) grupa technologii cyberbezpieczeństwa służących automatyzacji obsługi incydentów (remediacja), w zgodzie ze zdefiniowanymi priorytetami na podstawie alertów generowanych przez używane w SOC systemy SIEM/XDR/TIP.

SOC (Security Operations Center) scentralizowana funkcja lub zespół odpowiedzialny za poprawę cyberbezpieczeństwa organizacji oraz zapobieganie, wykrywanie i reagowanie na zagrożenia.

SPECspeed2017_Int (SPECspeed® 2017 Integer). Bieżąca wersja testów wydajności serwerów wyrażająca przepustowość i/lub pracę w jednostce czasu. Metodyka testów zabezpiecza przed niezharmoniowanymi produktami o niskiej wydajności.

SPiFFE/SPIRE (Secure Production Identity Framework for Everyone). SPIFFE/SPIRE zapewniają silnie potwierdzone tożsamości kryptograficzne dla obciążeń na wielu różnych platformach — projekty potwierdzone przez Cloud Native Computing Foundation. SPIRE – implementacja (ang. runtime) specyfikacji SPIFFE.

SSDLC (Secure Software Development Lifecycle). Integruje bezpieczeństwo z procesem zarządzania cyklem życiowym produktu. Wymagania dotyczące bezpieczeństwa są gromadzone wraz z wymaganiami funkcjonalnymi, na przykład przeprowadzana jest analiza ryzyka w fazie projektowania, a testy bezpieczeństwa odbywają się równolegle z rozwojem.

STIGs (Security Technical Implementation Guides). Kompleksowe wymagania dla urządzeń mobilnych, Systemów Operacyjnych, Sieci, Platform i Aplikacji. Wymagania obejmują wszystkie obszary konfiguracji urządzenia lub oprogramowania w celu osiągnięcia bezpiecznej integracji. Ma to na celu zapewnienie bezpieczeństwa systemów informatycznych i zapobieganie naruszeniom lub incydentom cyberbezpieczeństwa.

SZBI (System Zarządzania Bezpieczeństwem Informacji) holistyczny system bezpieczeństwa obejmujący procesy, infrastrukturę, systemy informatyczne oraz czynnik ludzki (uświadamianie, szkolenia i ćwiczenia).

TIP (Threat Intelligence Platform) skupiają w jednym miejscu czynności związane z obsługą źródeł CTI wielu uczestników. ENISA definiuje TIP-y poprzez 6 głównych funkcjonalności: analityka danych, wizualizacja, informatyka śledcza, przetwarzanie danych, raportowanie wyników i udostępnianie innym użytkownikom.

TLP (Traffic Light Protocol). System klasyfikacji informacji wrażliwych w celu udostępniania informacji wrażliwych. Podstawową koncepcją jest to, aby wytwórca zasygnalizował, jak szeroko informacje mogą być rozpowszechnione poza bezpośrednim odbiorcą.

UEBA (User Entity and Behavior Analytics) detekcja zagrożeń na podstawie anomalii wykorzystania środowiska informatycznego. Zapobiega niewłaściwemu wykorzystaniu uprzywilejowanego dostępu do kont w oparciu o analitykę behawioralną w celu identyfikacji ataku na wrażliwe obszary systemów informatycznych.

UODO (Urząd Ochrony Danych Osobowych). Organizacja nadzorująca w Polsce przestrzeganie RODO.

Veeam firma z siedzibą w USA, zajmująca się technologią informatyczną, dostarczająca oprogramowanie do tworzenia kopii zapasowych, odzyskiwania po awarii i nowoczesne oprogramowanie do ochrony danych dla obciążeń wirtualnych, natywnych w chmurze, SaaS, Kubernetes i serwerach fizycznych.

vLAN	(Virtual Local Area Network). Domena rozgłoszeniowa, która jest podzielona na partycje i izolowana w sieci komputerowej w warstwie łącza danych (warstwa 2 OSI). W tym kontekście wirtualny odnosi się do obiektu fizycznego odtworzonego i zmienionego przez dodatkową logikę w sieci lokalnej.
WAF	(Web Application Firewall). Zapora aplikacji internetowych chroni aplikacje internetowe przed różnymi atakami w warstwie aplikacji, takimi jak między innymi skrypty między-witrynowe (XSS), wstrzykiwanie SQL i zatruwanie plików cookie. Ataki na aplikacje są główną przyczyną włamań –są bramą do chronionych danych – WAF dba o ich bezpieczeństwo.
WS-Security	Web Services Security (WSS). Rozszerzenie protokołu SOAP dla zastosowania zabezpieczeń usług sieciowych, opublikowany przez firmę OASIS. Określa sposób egzekwowania integralności i poufności wiadomości i umożliwia komunikację w różnych formatach tokenów zabezpieczających, w tym SAML, Kerberos i X.509. Zapewnienia kompleksowe bezpieczeństwo dzięki stosowaniu podpisu XML i szyfrowania XML.
XDR	Ujednolicona platforma obsługi incydentów związanych z bezpieczeństwem, wykorzystująca sztuczną inteligencję i automatyzację, w celu remediacji zaawansowanych i złożonych zagrożeń cybernetycznych.
Zero Trust	Strategiczne podejście do cyberbezpieczeństwa, zabezpieczające organizację poprzez eliminację „ukrytego zaufania" i ciągłą weryfikację każdego etapu interakcji cyfrowej.

Załącznik 4 Źródła

Wybrane portale administracji publicznej dedykowane dla realizacji cyberbezpieczeństwa:

https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-
https://firmabezpiecznacyfrowo.pl/diagnoza/
https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa
https://www.gov.pl/web/rozwoj-technologia/cyberbezpieczenstwo-msp
https://www.gov.pl/web/baza-wiedzy/szkolenia
https://www.gov.pl/web/baza-wiedzy/cyberedukacja
https://www.gov.pl/web/baza-wiedzy/porozumienie-ws-listy-ostrzezen
https://www.cybsecurity.org/wp-content/uploads/2017/12/FBC_Wykorzystanie_modeli_cyber_threat_intelligence_jako_-element_skutecznego_reagowania_na_incydenty_komputerowe.pdf

Podmioty realizujące usługi krytyczne i ich łańcuch dostaw.

https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych
https://www.gov.pl/attachment/3c6d5be1-caf3-4a5b-a452-1fcc34d629c9 (Dyrektywa NIS 2)
https://www.gov.pl/attachment/2e86d037-1149-48d3-8b17-fef86cc9eb6b (Dyrektywa CER)
https://www.gov.pl/attachment/600219dc-e393-4cef-aca7-5e594054a6d0 (Rekomendacje wdrażania CER)
https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej
https://www.digital-operational-resilience-act.com/ Regulacja DORA
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017PC0477R(02) ENISA

Zespół redakcyjny:

Michal Andruszkiewicz	michal.andruszkiewicz@hpe.com
Katarzyna Jedlinska	katarzyna-danuta.jedlinska@hpe.com
Pawel Krakowian	pawel.krakowian@hpe.com
Jarosław Mojsiejuk	jaroslaw.mojsiejuk@hpe.com
Piotr Nogaś	piotr.nogas@hpe.com
Aneta Pękala	aneta.pekala@hpe.com

Więcej informacji

hpe.com