Microsoft

# Scenariusze i rozwiązania z zakresu cyberbezpieczeństwa w prostych słowach

# Wstęp

**W ostatnich latach bezpieczeństwo informacji stało się jednym z głównych tematów, o jakich dyskutuje się w branży IT. Rosnąca liczba ataków hakerskich i wirusów oraz głośne historie dotyczące naruszenia bezpieczeństwa danych wzbudzają poruszenie w świecie technologii informatycznych.**

Dyrektorzy często nie rozumieją w pełni kwestii bezpieczeństwa informacji, ryzyka i bieżących zagrożeń. Zwykle mają pewne pojęcie o dwóch lub trzech zagrożeniach, którymi się ogólnie interesują, i nie chcą zagłębiać się w niuanse IT. Kiedy zatwierdzają budżet, ważne jest dla nich, aby inwestycje w nowe oprogramowanie były zoptymalizowane pod względem kosztów i miały korzystny wpływ na firmę.

W tym e-booku znajdziesz informacje, które możesz wykorzystać w rozmowach z osobami decyzyjnymi, używając ich języka — języka biznesu. Opisano w nim, w jaki sposób rozwiązania firmy Microsoft, takie jak Microsoft 365 i Microsoft Azure, pozwalają zmniejszyć ryzyko zagrożeń dla firmy i zapobiegać stratom powodowanym przez ataki hakerskie lub wirusy.

Niniejszy e-book stanowi zaktualizowane wydanie wersji z 2018 r. i zawiera informacje o nowych technologiach i wyzwaniach.

## Jak korzystać z tego e-booka

W e-booku znajdziesz przykłady różnego rodzaju ataków i ochrony przed nimi. Opisy są podane zarówno z użyciem języka technicznego, jak i języka zrozumiałego dla osób decyzyjnych.

## Sposób prowadzenia rozmów na temat bezpieczeństwa informacji

Rozmowy z osobami podejmującymi decyzje dotyczące bezpieczeństwa informacji mają zwykle pewne wyjątkowe cechy. Na bezpieczeństwo zwykle nie zwraca się zbyt wiele uwagi, o ile „wszystko jest w porządku". Firmy, które doświadczyły dużych trudności w związku z utratą danych z powodu wirusów szyfrujących, zwracają znacznie większą uwagę na bezpieczeństwo niż te, które jeszcze nie napotkały problemów. Z drugiej strony bezpieczeństwa nie da się zapewnić na 100%. Każdy system, dopóki funkcjonuje, jest narażony na ryzyko. Naszym zadaniem jest wykazanie obecności ryzyka i zmniejszenie go do akceptowalnego poziomu. Ponieważ zmniejszenie ryzyka zależy od zakupu oprogramowania, ważne jest, aby znaleźć równowagę w miejscu, w którym bardziej opłaca się płacić za bezpieczeństwo niż za jego brak.

# Główne wyzwania dla firm związane z bezpieczeństwem informacji

01 **Ludzie są najsłabszym ogniwem.**
Często nie znają wartości informacji, z którymi pracują, i są dość nieostrożni, jeśli chodzi o ich ochronę.

Wraz z przejściem na pracę zdalną sytuacja pogorszyła się z kilku powodów: urządzenia domowe są mniej bezpieczne niż firmowe, użytkownicy mają do nich nieograniczony dostęp i nie ma potrzeby hakowania hasła do Wi-Fi, ponieważ można po prostu o nie poprosić.

02 **Dostępność narzędzi.**
W dzisiejszych czasach stosunkowo łatwo jest zostać hakerem. Opracowano już tysiące narzędzi, które każdy początkujący może pobrać za darmo. Dlatego liczba tak zwanych „hakerów" jest w dzisiejszych czasach dość wysoka. Tacy „hakerzy" raczej nie włamią się do dobrze chronionej infrastruktury. W grupie ryzyka natomiast są firmy, które nie poświęcają bezpieczeństwu informacji wystarczającej uwagi.
Działania początkujących hakerów stały się skuteczniejsze, odkąd firmy zaczęły przechodzić na pracę zdalną.

03 **Nasza firma jest tak mała — kto by się nami interesował?**
Jest to szeroko rozpowszechniona opinia w wielu firmach. Nawet małe firmy mogą być celem ataku, ale problem polega przede wszystkim na tym, że atakujący nie wybierają swoich celów. Ataki są zautomatyzowane i ukierunkowane na wszystko, co może zostać zaatakowane. Gdy atak zakończy się pomyślnie, osoba atakująca sprawdza, w jaki sposób można wykorzystać uzyskane informacje. W praktyce znane są przypadki prób włamań do serwerów instytucji rządowych z przejętego przez hakerów serwera firmy.

04 **Przestarzałe technologie.**
Problem z przestarzałymi technologiami polega na tym, że zostały one zaprojektowane z myślą o ochronie przed zagrożeniami, które były aktualne w czasie tworzenia danego oprogramowania. Im dłużej oprogramowanie funkcjonuje w swojej pierwotnej postaci, tym więcej pojawia się ataków, przed którymi nie zapewnia ono ochrony. Nie wszystkim atakom można zapobiec przez „łatanie" przestarzałej technologii.

05 **Brak specjalistów ds. bezpieczeństwa informacji i niewystarczająca dbałość specjalistów IT o bezpieczeństwo informacji.**
W niektórych firmach nawet nie ma specjalistów ds. bezpieczeństwa informacji. Ich funkcje pełnią specjaliści IT. Problem polega na tym, że zadaniem takiej osoby jest zapewnienie funkcjonowania usług informatycznych, a bezpieczeństwo może to utrudnić. Na przykład starannie skonfigurowana zapora może blokować uruchamianie legalnych aplikacji. Specjalista IT ma do wyboru monitorowanie portów używanych przez aplikację lub wyłączenie zapory. Druga opcja jest łatwiejsza, więc niektórzy ją wybierają.

# Scenariusze i rozwiązania

Zagrożenie

# Hasło do poczty e-mail można ustalić, można o nie poprosić lub uzyskać je z pamięci przeglądarki internetowej

Rozwiązanie

Microsoft 365: uwierzytelnianie wieloskładnikowe

Konfiguracja uwierzytelniania dwuskładnikowego w usłudze Microsoft 365

Prawdopodobnie wiesz, że dla wielu użytkowników hasła nie mają na celu przede wszystkim ochrony przed nieautoryzowanym dostępem, lecz są pewnego rodzaju „schematem administratora". Osoby takie traktują hasła w sposób nieodpowiedzialny, jednocześnie domagając się odpowiedzialności za bezpieczeństwo informacji od działu IT.

Uwierzytelnianie wieloskładnikowe wymaga, aby użytkownicy nie tylko znali swoje hasło, ale także byli odpowiedzialni za swoje urządzenia osobiste. Jest to rozwiązanie proste do skonfigurowania dla usług online i rozwiązuje szereg problemów z bezpieczeństwem.

Może obejmować połączenie telefoniczne, wiadomość SMS, potwierdzenie w aplikacji mobilnej lub wprowadzanie cyfr z aplikacji mobilnej. Możliwe jest też elastyczne ustawianie wyjątków. Na przykład można nie wymagać drugiego składnika, gdy użytkownik pracuje z firmowego adresu IP, ale można wymagać go podczas pracy z domu.

Nawet jeśli nastąpi naruszenie zabezpieczeń, odpowiedzialność spoczywa na użytkownikach, ponieważ nie pilnują oni swoich haseł i urządzeń osobistych.

Zapewnij sobie pomoc techniczną w zakresie zarządzania, gdyż w przeciwnym razie uwierzytelnianie wieloskładnikowe będzie postrzegane jako kolejny „schemat administratora".

Językiem biznesowym

Samo hasło już nie wystarcza. Hasła są zapisywane na karteczkach samoprzylepnych lub w plikach, przekazywane innym osobom i zapisywane w przeglądarkach. Często są bardzo proste, dzięki czemu łatwo je zapamiętać. Ponadto użytkownicy używają tych samych loginów i haseł do rejestracji na różnych stronach i forach z wątpliwymi ustawieniami bezpieczeństwa.

Gdy łączysz się z bankiem online, oprócz hasła musisz wprowadzić kod z wiadomości SMS. Czy dokumenty biznesowe nie powinny być chronione tak samo?

Wyjaśnij swoim pracownikom, że dodatkowe 15 sekund spędzonych na wprowadzeniu tekstu to rozsądna cena, jaką trzeba zapłacić za ochronę dostępu do ważnych informacji.

Zagrożenie

# Zapomniane hasło

Rozwiązanie

## Microsoft 365: resetowanie hasła przez użytkowników

Poranki w działach IT zawsze wyglądają tak samo: użytkownicy dzwonią, aby uzyskać pomoc w zresetowaniu zapomnianych haseł. Umożliwienie użytkownikom resetowania haseł przy użyciu alternatywnych metod logowania znacznie zmniejsza liczbę próśb o pomoc.

Metody resetowania, które będą dostępne dla użytkowników, ustalamy samodzielnie. Może to być na przykład SMS, aplikacja mobilna, pytania zabezpieczające lub osobisty adres e-mail. Można wymagać jednej opcji lub kombinacji dwóch.

Tę funkcję można zintegrować z lokalną usługą Active Directory. Hasło zresetowane w chmurze zostanie zsynchronizowane z lokalną usługą Active Directory w ciągu jednej minuty.

Jak w przypadku każdego nowego rozwiązania, użytkownicy będą potrzebować czasu, aby się do niego dostosować. Twoim zadaniem będzie nie tylko wdrożenie funkcji resetowania hasła, lecz także poinformowanie o niej użytkowników za pomocą odpowiednich instrukcji.

Językiem biznesowym

Czy kiedykolwiek zdarzyło Ci się zapomnieć hasło do firmowej poczty e-mail lub komputera? Tak samo często zdarza się to również Twoim pracownikom.

Oprócz niedogodności i konieczności poświęcenia czasu na połączenie z działem IT może to również stwarzać dodatkowe zagrożenia bezpieczeństwa. W przypadku pracy zdalnej trudno jest sprawdzić, czy osoba dzwoniąca jest tą, za którą się podaje.

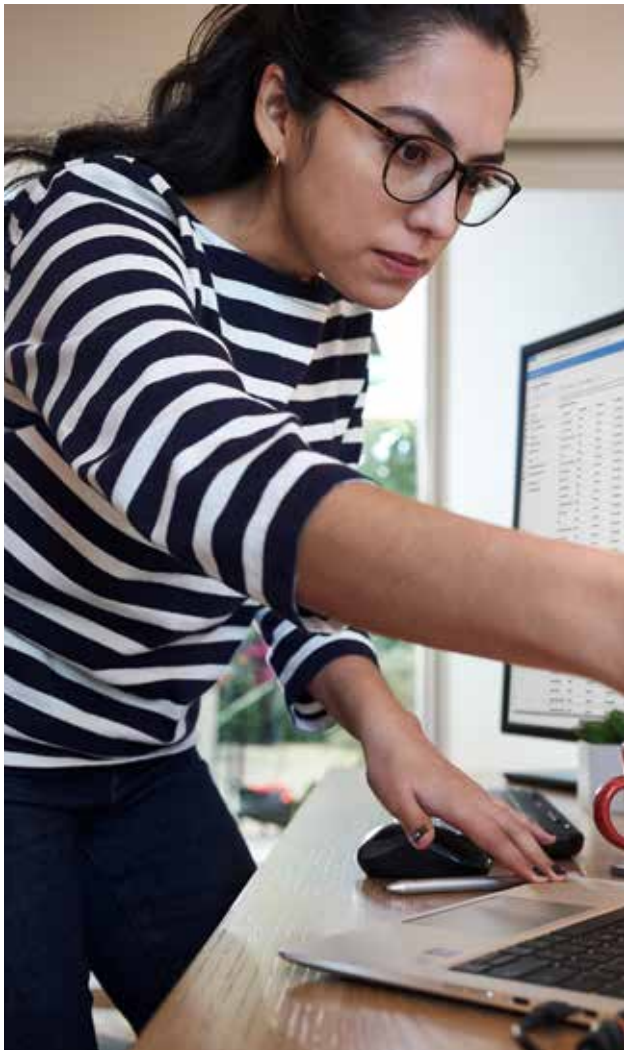
Prostym i skutecznym rozwiązaniem byłoby umożliwienie użytkownikowi zresetowania hasła za pomocą wiadomości SMS, pytań zabezpieczających lub specjalnego kodu w aplikacji mobilnej.

Zagrożenie

# Używanie słabych haseł

Rozwiązanie

## Microsoft 365: uwierzytelnianie bez hasła



Usługa Azure AD, która wykonuje uwierzytelnianie w Microsoft 365, udostępnia opcję rezygnacji z ustawiania haseł. Wachlarz możliwości jest dość szeroki:

01 Urządzenie mobilne jest rejestrowane jako urządzenie użytkownika. Podczas próby uwierzytelnienia na ekranie wyświetla się kod, a aplikacja Microsoft Authenticator wyświetla kilka liczb do wyboru. Użytkownik wybiera właściwą i, co ważne, potwierdza swoją tożsamość na urządzeniu mobilnym za pomocą odcisku palca.

02 Klucz sprzętowy. Używany jest zgodny klucz sprzętowy i dodatkowe dane.

03 Dane biometryczne.

04 Atrybuty nie są obsługiwane w usłudze Azure AD. Dzięki konfiguracji federacji między lokalną usługą AD a Azure AD można rozszerzyć opcje uwierzytelniania. Do uwierzytelniania można używać na przykład kart inteligentnych.

Każda opcja ma swoje własne funkcje, wymagania i zakresy. Dostępne możliwości są opisane na stronie https://docs.microsoft.com/pl-pl/azure/active-directory/authentication/concept-authentication-passwordless

Większość firm dopiero zaczyna wdrażać uwierzytelnianie bez hasła, więc metoda ta nie wygląda jeszcze znajomo. Proces przejścia na uwierzytelnianie bez hasła powinien odbywać się stopniowo, a ochrona hasłem nie powinna być zaniedbywana, dopóki proces nie zostanie ukończony.

### Językiem biznesowym

Wyobraź sobie jedną z następujących sytuacji:

01 Co najmniej jeden z Twoich pracowników otrzymał wiadomość e-mail w postaci dokumentu programu Word lub w formacie PDF od jednej z firm, z którymi współpracujesz. Po otwarciu dokumentu pracownik widzi dużą ilość zaszyfrowanego tekstu i komunikat „Ten dokument zawiera dane osobowe i został zaszyfrowany w celu zapewnienia zgodności z przepisami. Wprowadź swój adres e-mail i hasło, aby go odszyfrować".

02 Pracownik działu księgowości otrzymuje wiadomość z urzędu skarbowego o długu i prośbę o skorzystanie z linku w celu wyświetlenia szczegółowych informacji na temat tego długu. Po kliknięciu linku wyświetla się monit o podanie adresu e-mail i hasła.

Są to dwa przykłady phishingu, którego celem jest uzyskanie haseł pracowników.

Hasło jest jednym z najsłabszych ogniw i prędzej czy później będzie musiało zostać wyeliminowane.

Jak odblokowujesz swoje urządzenie mobilne? Prawdopodobnie odciskiem palca. Jest to jeden ze sposobów uwierzytelniania bez hasła, który już stał się bardzo powszechny wśród użytkowników urządzeń mobilnych. Jest bezpieczniejszy, ponieważ bardzo trudno jest z niego skorzystać bez fizycznej obecności właściciela urządzenia. Jest też wygodniejszy, ponieważ nie trzeba zmieniać hasła co określoną liczbę dni.

Teraz ta sama zasada jest wdrażana w systemach biznesowych, aby zapewnić bezpieczeństwo i wygodę, do których już przyzwyczailiśmy się podczas pracy z urządzeniem mobilnym. Jeśli pracownik zobaczy monit o wprowadzenie hasła, wzbudzi to podejrzenia, ponieważ jego firma nie używa haseł.

Zagrożenie

# Używanie haseł, których bezpieczeństwo zostało naruszone

Rozwiązanie

## Microsoft 365: ochrona hasłem

Zablokuj słowa, które nie powinny być używane jako hasło, takie jak nazwa firmy. Zablokowane zostanie nie tylko dane słowo, lecz także wyrazy pochodne.

Aby uzyskać więcej informacji, zobacz https://docs.microsoft.com/pl-pl/azure/active-directory/authentication/concept-password-ban-bad

Ta funkcja działa dla kont w chmurze, a także integruje się z lokalną usługą Active Directory.

Językiem biznesowym

Jakich słów spróbuje użyć haker, próbując odgadnąć hasło? Prawdopodobnie związanych z imieniem i nazwiskiem użytkownika oraz nazwą firmy.

Twoi pracownicy nie będą mogli używać słów, które mogłyby zostać łatwo odgadnięte, a dział IT utworzy listę takich słów.

Zagrożenie

# Nieautoryzowany dostęp z niezaufanych lokalizacji

Rozwiązanie

## Microsoft 365: ograniczenia dostępu przy użyciu geolokalizacji

Azure AD udostępnia opcję dostępu warunkowego, która jest jedną z kluczowych funkcji. Można go używać do włączania MFA, wymagania od użytkowników zmiany haseł, uniemożliwienia im logowania się z urządzeń osobistych itp.

Jednym z atrybutów, które należy wziąć pod uwagę w pierwszej kolejności, jest ograniczenie logowania z niezaufanych geolokalizacji.

Należy utworzyć listy lokalizacji na podstawie publicznych adresów IP lub odpowiadających im geolokalizacji. Mogą to być „białe" lub „czarne" listy.

Językiem biznesowym

Prawdopodobnie wiesz o tym, że hakerzy ukrywają swoje lokalizacje, aby zachować anonimowość. Nawet jeśli haker jest Twoim sąsiadem, kraj, z którego próbuje się połączyć, będzie inny.

Na świecie jest ponad 200 krajów. Dlaczego mielibyśmy zezwalać na dostęp do swoich danych ze wszystkich istniejących krajów?

Prostym rozwiązaniem jest umożliwienie połączenia tylko z niektórych krajów, których lista zostanie przygotowana przez dział IT.

Zagrożenie

# Zgodność z przepisami

Rozwiązanie

## Microsoft 365: zasady przechowywania

Wymogi dotyczące przechowywania danych stają się coraz bardziej rygorystyczne z roku na rok. Pojawiają się wymogi eksterytorialne, takie jak RODO. Zgodnością z nimi zarządza się zarówno za pomocą środków „biurokratycznych", jak i technicznych.

Zapewnienie zgodności jest złożonym procesem, który wykracza poza zakres niniejszego przewodnika, jak również poza kompetencje działu IT.

Istnieje jednak jeden ważny wymóg, który ma znaczenie dla większości przedsiębiorstw: zabezpieczanie informacji przed przypadkowym lub zamierzonym usunięciem.

Zasady przechowywania pozwalają:

01 Zagwarantować, że dokumenty będą przechowywane przez określony czas.

02 Automatycznie usuwać dokumenty po upływie określonego czasu.

03 Po upływie danego okresu wysyłać wiadomość do osoby odpowiedzialnej za podjęcie decyzji o usunięciu dokumentu lub jego dalszym przechowywaniu.

Językiem biznesowym

Ważne dokumenty mogą zostać usunięte lub zmodyfikowane.

Może to nie tylko doprowadzić do utraty ważnych informacji, lecz także skutkować nakładaniem grzywien.

Działy IT przechowują kopie dokumentów, by móc szybko je odzyskać, ale co zrobić, jeśli dokument został utworzony trzy lata temu? Zgodnie z prawem niektóre dokumenty muszą być przechowywane przez wiele lat.

Zasady przechowywania chronią ważne dokumenty, wiadomości e-mail, a nawet konwersacje przed przypadkowym lub zamierzonym usunięciem w wybranym okresie.

Zagrożenie

# Złośliwe załączniki wiadomości e-mail

Rozwiązanie

Microsoft 365: bezpieczne załączniki

Profil i konfiguracja bezpiecznych załączników zaawansowanej ochrony przed zagrożeniami usługi Office 365

Każdy załącznik znajduje się we własnej piaskownicy sprzętowej w centrum danych firmy Microsoft. Dopóki system nie sprawdzi, czy załącznik jest bezpieczny, nie jest dostarczany do użytkownika. Przeprowadzana jest analiza zachowania załącznika.

Administrator może otrzymywać kopie oryginalnych wiadomości e-mail z załącznikami.

Językiem biznesowym

Wyobraź sobie dwie sytuacje, kiedy otwierasz dokument z załącznika wiadomości e-mail, który:

01 Po prostu się otwiera.

02 Uruchamia makro, które wysyła dane z komputera lub szyfruje inne dokumenty.

Oba dokumenty mogą z zewnątrz wyglądać identycznie, ale zachowują się inaczej.

Usługa poczty e-mail firmy Microsoft testuje zachowanie dokumentu, zanim wiadomość dotrze do skrzynki. Jeśli jego zachowanie jest podobne do tego z drugiego scenariusza, wiadomość zostanie dostarczona bez załącznika.

Żaden szyfrator nie przeniknie przez firmową pocztę e-mail. System, w przeciwieństwie do pracowników, nie ufa atrakcyjnym wiadomościom e-mail i natychmiast je usuwa.

Zagrożenie

# Złośliwe linki w wiadomościach e-mail

Rozwiązanie

Microsoft 365: bezpieczne linki

Profil i konfiguracja bezpiecznych linków zaawansowanej ochrony przed zagrożeniami przy użyciu Office 365

Każde kliknięcie w wiadomości e-mail lub dokumencie pakietu Office jest sprawdzane. Jeśli link prowadzi do złośliwej witryny, zostanie zablokowany.

Administrator może ręcznie dodawać witryny do list złośliwych witryn.

Językiem biznesowym

Osoby, które dziś nazywamy hakerami, już dawno temu zostały ekspertami w dziedzinie marketingu.

Wysyłają atrakcyjne e-maile, tworzą prawdziwe kopie witryn bankowych i wykorzystują ludzkie emocje.

Kliknięcie linku w wiadomości e-mail może spowodować epidemię wirusa lub utratę dostępu do banku, rynku itp.

Informacje o takich linkach docierają do firmy Microsoft w ciągu kilku minut. Próby otwierania witryn z wirusami lub witryn podszywających się pod banki internetowe są blokowane.

Zagrożenie

# Ataki wirusów szyfrujących

Rozwiązanie

Windows 10: kontrolowany dostęp do folderu

Konfiguracja kontrolowanego dostępu do folderów

Funkcja kontrolowanego dostępu do folderów pozwala zapobiegać zapisywaniu danych w określonych folderach przez niezaufane procesy. Nie ma ona wpływu na procesy takie jak Eksplorator Windows lub MS Word, natomiast zmiany wprowadzone przez nieznane procesy są blokowane.

Ta funkcja nie działa, jeśli zainstalowany jest program antywirusowy innej firmy.

Językiem biznesowym

Szyfratory stanowią poważny problem i często omijają ochronę antywirusową. Nawet jeśli system zostanie zaszyfrowany, pliki w folderach chronionych pozostają nietknięte.

Nawet jeśli program antywirusowy nie poradzi sobie z wirusem szyfrującym, dokumenty pozostaną całkowicie bezpieczne.

Zagrożenie

# Ataki wirusów szyfrujących

Rozwiązanie

Microsoft 365: OneDrive dla Firm

Konfiguracja usługi OneDrive dla Firm w systemie Windows 10

Gdy szyfratory infiltrują system, szyfrują nie tylko dokumenty, lecz także archiwa. Usuwają też kopie w tle.

Wystarczy skonfigurować synchronizację dokumentów w Windows 10 z magazynem OneDrive dla Firm w chmurze, a wszystko będzie można odzyskać. Pliki synchronizują się natychmiast po zapisaniu ich w specjalnym katalogu.

Klient do synchronizacji jest zintegrowany z systemem Windows 10. Można też zainstalować go w systemie Windows 7.

Minimalna dostępna pojemność pamięci masowej wynosi 1 TB na użytkownika.

Wbudowana funkcja przechowywania wersji pozwala odzyskać nie tylko bieżącą wersję pliku, lecz także wersje wcześniejsze.

Językiem biznesowym

Czy kiedykolwiek zdarzyło Ci się bardzo żałować przypadkowego usunięcia dokumentu lub przekonać się, na czym polega atak wirusem szyfrującym? Albo usunąć fragment dokumentu bez możliwości jego odzyskania?

Oprócz wirusów szyfrujących istnieją też użytkownicy, którzy usuwają ważne dane i niekoniecznie robią to celowo.

Możesz automatycznie zapisywać kopie w chmurze. Wszystkie poprzednie wersje dokumentów również są zapisywane.

Jeśli pliki zostały zaszyfrowane, usunięte lub zmodyfikowane, zostaną przywrócone bez względu na to, ile zmian w nich wprowadzono.

Zagrożenie

# Pobieranie informacji z dysku bez hasła

Rozwiązanie

Windows 10: szyfrowanie funkcją Bitlocker

Dokumentacja funkcji BitLocker

Wiesz bardzo dobrze, że dysk twardy można wyjąć i połączyć z innym komputerem.

Można też uruchomić komputer z dysku DVD i uzyskać dostęp do systemu plików. W obu przypadkach nie trzeba znać hasła logowania.

Nośnik wymienny można także łatwo zgubić, a wartość zawartych na nim informacji wielokrotnie przewyższa koszt samego nośnika.

Dyski powinny być szyfrowane. Jak w przypadku każdego środka bezpieczeństwa, zwiększa to niedogodności i ryzyko.

Właściwa konfiguracja funkcji Bitlocker minimalizuje ryzyko.

Klucze odzyskiwania można przechowywać w lokalnej usłudze Active Directory lub w usłudze Azure Active Directory, by zapewnić sobie możliwość odzyskania danych, nawet jeśli dysk będzie fizycznie uszkodzony.

W celu zwiększenia niezawodności warto archiwizować dane.

Językiem biznesowym

W dzisiejszych czasach najprostszym sposobem na utratę informacji jest zgubienie ich wraz z urządzeniem.

Laptop pozostawiony w roztargnieniu na lotnisku lub dysk flash, który wypadł z torby. Takie sytuacje wiążą się nie tylko z koniecznością wydania pieniędzy na zakup nowego urządzenia, lecz również stwarzają poważne ryzyko nieautoryzowanego dostępu do informacji.

Nawet jeśli laptop jest chroniony hasłem, nie uniemożliwi to specjaliście IT uzyskania z niego informacji. Nierzadko zdarza się, że na laptopach znajdują się dokumenty z listą haseł lub hasła zapisane w przeglądarce.

Szyfruj dyski i dyski flash z ważnymi danymi. Jeśli urządzenie zostanie zgubione lub skradzione, nadal będziesz mieć problem, ale nikt nie będzie mógł uzyskać dostępu do danych.

Nawet utrata komputera lub dysku flash z ważnymi danymi nie spowoduje katastrofalnego wycieku danych. Dane będą bezpiecznie zaszyfrowane i niedostępne dla ciekawskich oczu.

Zagrożenie

# Ataki na urządzenia mobilne

Rozwiązanie

Microsoft Endpoint Manager (dawniej Microsoft Intune)

Dokumentacja usługi Microsoft Intune

Usługa Microsoft Endpoint Manager (dawniej Microsoft Intune) obsługuje urządzenia z chmury, dzięki czemu można zarządzać nimi niezależnie od lokalizacji użytkownika.

Urządzenia można skonfigurować tak, aby działały zgodnie z zasadami zabezpieczeń, a także usuwały określone lub wszystkie dane po rozwiązaniu umowy o pracę.

Językiem biznesowym

Firma Symantec przeprowadziła następujący eksperyment: kilka telefonów zostało „zostawionych przez pomyłkę" w miejscach publicznych w USA i Kanadzie. Oprogramowanie zainstalowane w tych telefonach zapisywało wszystkie działania wykonywane przy ich użyciu.

60% osób, które znalazły telefony, nie próbowało ich zwrócić. W ciągu kilku godzin nowy właściciel zaczynał przeglądać dokumenty i zdjęcia oraz otwierać aplikacje.

Największym zagrożeniem związanym z urządzeniami mobilnymi jest fakt, że są to urządzenia osobiste, natomiast informacje, które zawierają, mogą należeć do firmy. Dostępne opcje zarządzania urządzeniami osobistymi są raczej ograniczone.

Użytkownicy urządzeń osobistych bywają dość nieostrożni: urządzenia nie są szyfrowane, często nie są chronione kodami PIN, mają zainstalowane nie zawsze bezpieczne aplikacje i mogą zostać zgubione. Ponadto były pracownik firmy może zapisać archiwum poczty lub kontakty do klientów na smartfonie.

Jeśli pracownicy firmy obsługują pocztę firmową lub dokumenty z własnych telefonów, należy zapewnić sobie możliwość ochrony danych firmowych.

Połączenie telefonów z usługą MEM umożliwi ich bezpieczniejszą konfigurację, a także usunięcie danych biznesowych (lub wszystkich) w momencie rozwiązania stosunku pracy.

Poczta firmowa i dokumenty biznesowe zapisane na osobistym smartfonie nie „odejdą" wraz z byłym pracownikiem. W przypadku kradzieży lub utraty urządzenia dane można usunąć zdalnie.

Zagrożenie

# Wirusy

Rozwiązanie

## Windows 10: Microsoft Defender AV

### Językiem IT

Program antywirusowy wbudowany w platformę Windows 10. Poprzednie wersje Microsoft Security Essentials były dość proste. Microsoft Defender AV, następca Security Essentials, radykalnie różni się od swojego poprzednika.

Jego kluczową zaletą jest integracja z systemem Windows 10 i lepszy sposób działania z każdą nową kompilacją tego systemu.

Postępy w rozwoju oprogramowania antywirusowego zaskakują nawet niezależnych testerów. Niespodzianka! W najnowszych testach oprogramowania antywirusowego Windows Defender nie wypada słabo https://www.tomsguide.com/us/windows-defender-av-test,news-25524.html

Program jest całkowicie bezpłatny do użytku biznesowego i może być zarządzany za pomocą zasad grupy.

Niektóre funkcje, takie jak scentralizowane raportowanie, wymagają narzędzi komercyjnych.

### Językiem biznesowym

Program antywirusowy nie jest lekarstwem na wszystko. Kwestii bezpieczeństwa nie wolno zaniedbywać, ale należy też posiadać program antywirusowy. Jest on wbudowany i jest bezpłatny.

Komputery Mac były kiedyś uważane za bezpieczniejsze środowisko pracy niż komputery z systemem Windows, ponieważ były atakowane przez mniej wirusów. Głównym powodem takiego stanu rzeczy był udział tych urządzeń w rynku — 88% w przypadku komputerów z Windows i 9% w przypadku komputerów Mac (https://netmarketshare.com/operating-system-market-share.aspx )

Oczywiste jest, że Ci, którzy zarabiają na hakowaniu, skupiają swoje wysiłki na największej grupie docelowej. Korzystanie z systemu Windows 10 oznacza pozostanie w grupie 88% z ochroną na poziomie 9%.

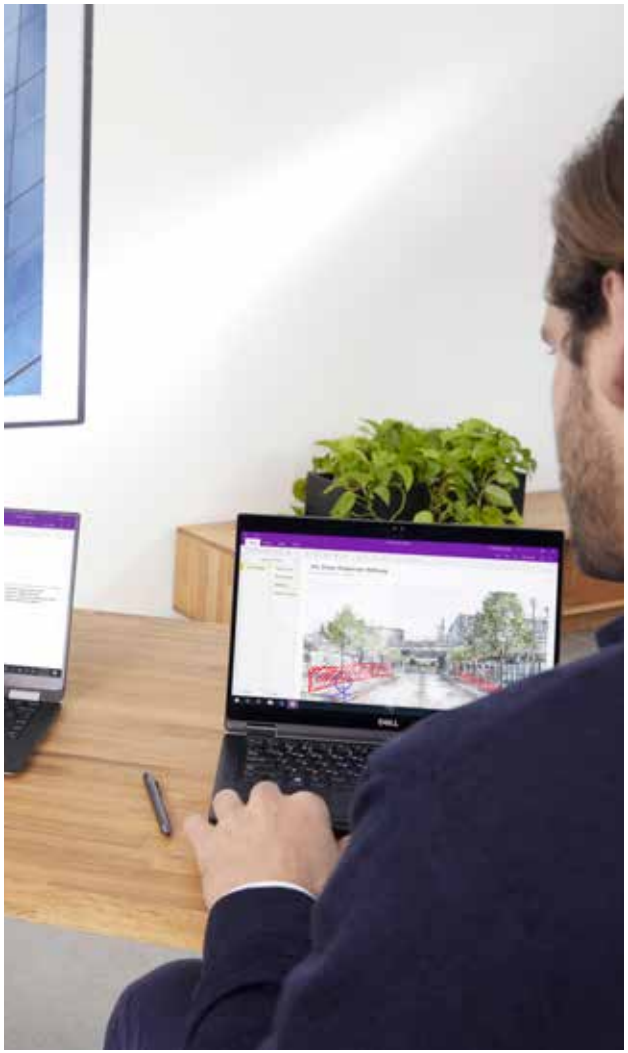
Zagrożenie

# Wyciek dokumentów

Rozwiązanie

Azure Information Protection

Dokumentacja usługi Azure Information Protection



Technologia ta chroni dokumenty poprzez szyfrowanie i przypisywanie praw dostępu innym użytkownikom, co umożliwia zachowanie skonfigurowanych ograniczeń, nawet jeśli dokumenty wydostaną się poza firmę.

Rozwiązanie to pomaga chronić poufne informacje w firmie i zapobiegać wyciekom danych.

Integruje się z aplikacjami pakietu Office, co pozwala użytkownikom szyfrować pliki bezpośrednio z programu Microsoft Word i za pomocą poczty Microsoft Exchange. Można zatem korzystać z niego zarówno ręcznie, jak i automatycznie, zgodnie z określonymi zasadami. Na przykład jeśli pracownik wysyła wiadomość z załącznikiem poza firmę / do określonych adresatów / zawierającą określone pliki itp., załącznik może być automatycznie szyfrowany.

Technologię tę można wykorzystywać zarówno w prostym scenariuszu, w którym wymagana jest tylko instalacja oprogramowania do ochrony dokumentów, jak i w przypadku bardziej zaawansowanych zadań, gdy trzeba wstępnie klasyfikować dokumenty w celu spełnienia wymagań określonych przepisami, a następnie zapewnić ochronę.

Językiem biznesowym

Biorąc pod uwagę wartość danych korporacyjnych, które wymagają ochrony, z pewnością warto w takie rozwiązanie zainwestować. Nawet gdy ktoś spróbuje wyprowadzić poufne informacje poza firmę, po prostu nie będzie mógł otworzyć dokumentu.

Jeśli menedżer postanowi wysłać pocztą e-mail bazę danych klientów do konkurencji, nikt w firmie konkurencyjnej nie odczyta takiej wiadomości, niezależnie od tego, jak bardzo będzie się starać.

Można także ograniczyć dostęp do dokumentów, tak aby żadne osoby postronne nie mogły zobaczyć informacji, które nie są dla nich przeznaczone.

Zagrożenie

# Więcej o wyciekach danych

Rozwiązanie

Microsoft 365 DLP

Szczegółowy przegląd usługi Microsoft 365 DLP

Zestaw zasad ochrony informacji poufnych dla usług Exchange Online, SharePoint Online, OneDrive dla Firm i Teams.

Zasady mogą nie zezwalać na różne operacje związane z informacjami poufnymi, takie jak przekazywanie poza firmę lub pobieranie do lokalnego komputera.

Administratorzy mogą otrzymywać powiadomienia o próbach wykonywania przez użytkowników zakazanych operacji.

System przechowuje szablony informacji poufnych do wykrywania danych z rosyjskich paszportów krajowych i międzynarodowych. Można także tworzyć szablony niestandardowe na podstawie słów kluczowych, wyrażeń regularnych, układów dokumentów lub klasyfikatorów z możliwością szkolenia.

Językiem biznesowym

Firmy mają obowiązek chronić dane osobowe przed wyciekami.

Co by się stało, gdyby pracownik przez pomyłkę wysłał dokument z danymi paszportowymi?

To zdarzyło się naprawdę: podczas przygotowań do szczytu G20 w Brisbane w 2015 r. pracownik Australijskiego Departamentu Imigracji przez pomyłkę wysłał do organizatorów Pucharu Azji w piłce nożnej dokument z danymi paszportowymi przywódców państw G20 (w tym Władimira Putina, Baracka Obamy, Angeli Merkel i Xi Jinpinga). Podczas wprowadzania adresu współpracownika w Outlooku pracownik ten nie sprawdził przed wysłaniem wiadomości adresu sugerowanego przez funkcję automatycznego wypełniania.

Administrator może skonfigurować zasady blokowania wychodzących wiadomości e-mail zawierających dane paszportowe lub inne dane osobowe.

Zagrożenie

# Jak przedstawia się kwestia wycieku danych przez Teams?

Rozwiązanie

## Microsoft 365 DLP dla Teams

Funkcja DLP jest dostępna dla poczty e-mail, magazynów dla programu SharePoint / OneDrive dla Firm i Microsoft Teams.

Istnieją jednak duże różnice w zakresie jej licencjonowania i stosowania.

W przypadku Microsoft Teams zasady dotyczą wiadomości w konwersacjach i kanałach prywatnych.

Dokumenty publikowane za pomocą Microsoft Teams znajdują się w usłudze OneDrive dla Firm i programie SharePoint. W związku z tym dokumenty takie są objęte zakresem zasad DLP dla usługi OneDrive dla Firm i programu SharePoint.

Językiem biznesowym

Popularność i wszechstronność Microsoft Teams niesie ze sobą zarówno szereg korzyści, jak i kilka nowych wyzwań. Na przykład:

01 Jeden z Twoich pracowników zaprosił przedstawiciela firmy partnerskiej do kanału Teams i przypadkowo wysłał w wiadomości dane poufne.

02 Pracownik opublikował dokument zawierający dane poufne w tym kanale Teams.

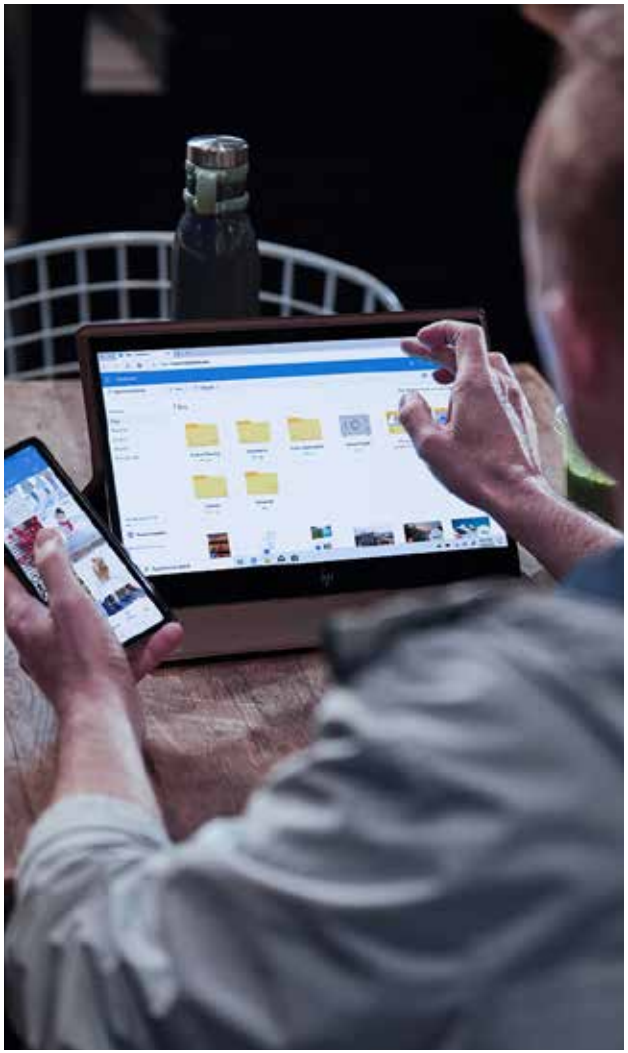
W obu przypadkach wiadomość i dokument nie będą dostępne dla przedstawiciela firmy partnerskiej, a informacje poufne nie opuszczą firmy.

Zagrożenie

# Trochę więcej o przeciekach i niezatwierdzonych zasobach IT (shadow IT)

Rozwiązanie

## Office 365 Cloud App Security



Usługa Microsoft Cloud App Security należy do rodziny brokerów zabezpieczeń dostępu do chmury. Funkcjonalność Microsoft CAS jest tak ogromna, że można jej poświęcić osobną publikację. Ma jednak „młodszego brata", Office 365 CAS, który jest odpowiedzialny tylko za aplikacje Office 365 i im podobne.

Office 365 CAS może śledzić działania użytkowników w Exchange Online, SharePoint Online i OneDrive dla Firm. Przykładowo umożliwia sprawdzenie, który pracownik pobrał określony plik, utworzył anonimowy link, usunął wiadomość e-mail itd.

Działania administratorów są rejestrowane i również mogą być wykrywane.

Zasady mogą służyć do powiadamiania o niektórych działaniach, a nawet ich blokowania.

Językiem biznesowym

Wyobraź sobie, że pracownik rozstający się z firmą postanowił pobrać pewne dokumenty, które są ważne dla firmy (i jej konkurentów).

Jeśli ten zamiar zostanie wykryty w odpowiednim czasie, można zapobiec dalszym problemom. W tym celu można skorzystać z polityk. Na przykład:

01 Pracownik pobrał 30 dokumentów w ciągu minuty.

02 Pracownik pobrał 10 dokumentów oznaczonych jako poufne.

03 Pracownik utworzył anonimowy link do pobierania poufnych dokumentów... I tak dalej.

Zagrożenie

# Bezpieczeństwo fizyczne

Rozwiązanie

## Korzystanie z centrum danych

Na bezpieczeństwo infrastruktury składa się szereg różnych czynników, w tym bezpieczeństwo fizyczne. Gdy sprzęt znajduje się na terenie firmy, zapewnienie bezpieczeństwa fizycznego może okazać się sporym przedsięwzięciem.

Oto aspekty, które należy wziąć pod uwagę:

01 Serwerownia musi znajdować się w odpowiedniej lokalizacji. W szczególności ściany serwerowni nie mogą przylegać do ścian zewnętrznych ani mieć okien.

02 Aby utrzymać parametry temperatury i wilgotności w określonych granicach, należy zadbać o odpowiednią instalację.

03 Drzwi muszą być wyposażone w zamki elektroniczne.

04 Podłogi w centrum danych muszą być podniesione.

05 W centrum danych muszą znajdować się gaśnice.

06 Systemy sprzętowe i magazynowe muszą być szyfrowane.

07 Należy zadbać o ogólne bezpieczeństwo fizyczne budynków.

Właściciele centrów danych już zadbali o możliwość spełnienia wszystkich powyższych warunków. Z punktu widzenia bezpieczeństwa Twoje dane będą znacznie lepiej chronione w miejscu, w którym jest wszystko, czego potrzeba.

### Językiem biznesowym

Gdy wszystkie dane znajdują się w pobliżu, jesteśmy naturalnie bardziej spokojni. Jednak osoby, które mogą legalnie lub nielegalnie dostać się na teren firmy, mogą również wejść w posiadanie Twoich danych. Nie muszą one nawet być hakerami — wystarczy, że ukradną sprzęt.

Centra danych wyposażone są w systemy kontroli dostępu, kontroli wejść i wyjść oraz całodobowego monitoringu wideo. Są również pilnowane przez pracowników ochrony. Dostęp osób trzecich jest skomplikowany lub prawie niemożliwy, zwłaszcza jeśli centrum danych, w którym dane są przechowywane, znajduje się w innym kraju.

Mniejsze firmy zwykle nie mogą sobie pozwolić na taki poziom bezpieczeństwa, ochronę serwerów lokalnych, kontrolę dostępu i nadzór wideo we własnym zakresie.

Zagrożenie

# Archiwizacja danych

Rozwiązanie

Kopia zapasowa w centrum danych

Dokumentacja usługi Kopia zapasowa Azure

Narzędzie do tworzenia kopii zapasowych danych w Microsoft Azure to podstawowe rozwiązanie do archiwizacji i odzyskiwania danych, które stanowi uzupełnienie dla istniejących narzędzi do archiwizacji.

Nawet w przypadku utraty lub uszkodzenia archiwum lokalnego kopia zapasowa w centrum danych Azure będzie przechowywana tak długo, jak chcesz.

Językiem biznesowym

Sprzęt bywa zawodny, a dane mogą zostać przypadkowo lub celowo usunięte. W tego typu sytuacji kopia zapasowa może okazać się ratunkiem.

A jeśli kopia również ulegnie zniszczeniu? Może tak się zdarzyć w przypadku pożaru, rozboju lub po prostu nieostrożnego przechowywania nośników.

Prawdopodobnie znasz film animowany „Toy Story 2". Czy wiesz, że większość materiału została przypadkowo zniszczona, a archiwum nie udało się przywrócić z powodu niewłaściwego przechowywania? Na szczęście film został uratowany, ponieważ członek zespołu skopiował materiał tuż przed tym zdarzeniem i zabrał go ze sobą, by pracować nad nim domu.

Zapewnienie niezawodnego archiwum jest dość kosztowne. Co więcej, nawet dobre rozwiązania do przechowywania mogą się nie sprawdzić z powodu ludzkich błędów.
W dużym szpitalu w Utah przechowywano archiwa z dokumentacją pacjentów w bezpiecznym miejscu. Każdego dnia kurier zawoził tam nośniki z danymi. Pewnego dnia, przed weekendem, kurier postanowił nie dostarczyć danych i zostawił pudełko na noc w samochodzie. W nocy ktoś włamał się do samochodu i nośniki z danymi zostały skradzione. Skończyło się to wypłacaniem pacjentom odszkodowań liczonych w milionach dolarów.

Pamięć masowa oparta na chmurze jest niezawodna z technologicznego punktu widzenia i niezależna od ludzkich słabości.

Wszelkie dane, w tym roczny raport księgowy czy listę płac, można odzyskać nawet po celowym usunięciu lub wykasowaniu.

Zagrożenie

# Jeśli dojdzie do ataku hakerskiego

Rozwiązanie

Advanced Threat Analytics (rozwiązanie lokalne)
Microsoft Defender for Identity (dawniej Azure Advanced Threat Protection) (rozwiązanie oparte na chmurze)
Dokumentacja usługi Microsoft Defender for Identity

Nie istnieją rozwiązania gwarantujące 100% ochrony. Problem polega na tym, że ataki hakerskie są często wykrywane dopiero po kilku miesiącach, gdy dane już zostały skradzione. Aby zapobiegać takim sytuacjom, wymagana jest zarówno ochrona, jak i monitorowanie.

Zwykle funkcję tę pełniły systemy IDSs (Intrusion Detection Systems). Ich najnowszą wersją są systemy UBA (User Behavior Analysis).

Systemy UBA nieustannie monitorują określone zachowania pracowników: kiedy pracują, do jakich urządzeń się logują, do jakich plików mają dostęp, do jakich grup należą itp. Po stworzeniu profilu behawioralnego użytkownika system zgłasza wszelkie anomalie, które mogą być spowodowane działaniami pracownika lub kogoś z zewnątrz, kto włamał się na konto użytkownika.

System UBA można wdrożyć na dwa sposoby:

01 Może być zainstalowany lokalnie i analizować ruch usługi Active Directory. Opcja ta nazywa się Microsoft ATA.

02 Może też być oparty na chmurze, z agentami zainstalowanymi lokalnie na kontrolerach domeny. Opcja ta nosi nazwę Microsoft Defender for Identity.

Językiem biznesowym

Nie istnieją rozwiązania gwarantujące 100% ochrony. Szczególnie trudno jest chronić przed tymi, których z natury uważamy za godnych zaufania: pracownikami. Nikt nie może zagwarantować, że pracownik pozbawiony premii nie dokona sabotażu lub nie skopiuje danych. System analizy zachowań pracowników pomaga wykrywać nietypowe zachowania.

Jeśli pracownik zostanie dłużej w pracy, aby wydrukować dane poufne, system nas o tym powiadomi.

Ponadto system poinformuje nas, gdy pracownik spróbuje uzyskać dostęp do dokumentów, których zwykle nie potrzebuje do wykonywania swoich obowiązków.

Zagrożenie

# Jeśli dojdzie do ataku hakerskiego. Lub jeśli jeszcze się to nie zdarzyło

Rozwiązanie

## Microsoft Defender for Endpoint

Większość złośliwych działań jest wykonywana przez osoby atakujące na komputerach użytkowników i serwerach. Na przykład jeśli udało się wyłudzić informacje od użytkownika za pomocą wiadomości e-mail, osoba atakująca może uzyskać dostęp do jego komputera i połączyć się z innymi osobami.

Komputery są domyślnie chronione przez oprogramowanie antywirusowe, ale możliwości programów antywirusowych są ograniczone. Oprogramowanie to opiera się na zasobach komputera użytkownika, a wykrycie zaawansowanych ataków może poważnie ograniczyć poprawne działanie komputera.

Wykrywanie i blokowanie można przenieść do chmury. W takim przypadku wbudowana usługa przesyła zdarzenia z komputera do usługi w chmurze, gdzie są one analizowane przy użyciu sztucznej inteligencji i bazy wiedzy firmy Microsoft.

Jeśli w firmie funkcjonuje centrum operacji bezpieczeństwa (SOC), znacznie łatwiej jest badać wszelkie zdarzenia.

Zagrożenie

# Włamanie na konto użytkownika mającego specjalne uprawnienia

Rozwiązanie

## Azure AD Privileged Identity Management

Jedną z podstawowych zasad bezpiecznego delegowania uprawnień w lokalnej usłudze Active Directory jest posiadanie przez administratora kilku kont z różnymi uprawnieniami. Na przykład:

01 Konto bez uprawnień do korzystania z Internetu

02 Konto do zarządzania komputerami użytkowników

03 Konto do zarządzania serwerami

04 Konto do zarządzania domeną

05 Itd.

Nawet jeśli ktoś włamie się na jedno z tych kont, nie uzyska wszystkich uprawnień.
Jednak ze względu na niedogodności związane z przełączaniem się między wieloma kontami niektóre firmy niestety zaniedbują to zalecenie.

W przypadku chmury korzystanie z jednego konta z dużą liczbą uprawnień może spowodować podobne problemy.

Funkcja Azure AD PIM służy do bezpiecznego delegowania i jednocześnie pozwala uniknąć konieczności korzystania z wielu kont.
Dzięki niej administrator ma tylko prawa zwykłego użytkownika, a wszystkie inne uprawnienia są aktywowane w razie potrzeby.

Oto przykład: inżynier pomocy technicznej musi zresetować hasło użytkownika. Proces ten może wyglądać następująco:

01 Inżynier loguje się i lokalizuje funkcję usługi Azure AD PIM. Następnie klika przycisk „Aktywuj rolę administratora pomocy technicznej”.

02 Następuje dodatkowa weryfikacja za pomocą uwierzytelniania wieloskładnikowego.

03 Inżynier wskazuje, przez ile godzin uprawnienie to ma pozostać aktywne.

04 Otrzymuje zgodę od odpowiedniej osoby zatwierdzającej.

05 Następnie może korzystać z uprawnień administracyjnych przez określoną liczbę godzin.
Nawet jeśli konto zostanie naruszone, osoba atakująca nie uzyska dostępu do specjalnych uprawnień.

Ta funkcja jest również częściowo zaimplementowana dla lokalnej usługi Active Directory i nosi nazwę Privileged Access Management (PAM).

# Podsumowanie

Biorąc pod uwagę zagrożenia i metody ochrony opisane powyżej, uważamy, że zintegrowane podejście do kwestii zabezpieczeń jest koniecznością. Nie istnieje magiczny przycisk, który jednym kliknięciem zapewni uniwersalną ochronę. Nie istnieje również jeden program, który zapewnia zabezpieczenia na wszystkich poziomach. Microsoft dla wygody i oszczędności oferuje oprogramowanie zarówno w postaci pojedynczych składników, jak i pakietów. Pakiet obejmujący większość funkcji opisanych w tym dokumencie nosi nazwę Microsoft 365. Więcej informacji na temat aktualnej oferty Microsoft 365 można znaleźć w oficjalnej witrynie: https://www.microsoft.com/pl-pl/microsoft-365


Microsoft