Microsoft

Mówimy tym samym językiem: cyber-bezpieczeństwo w biznesie

Wprowadzenie

W ostatnich latach bezpieczeństwo informacji było jednym z najczęściej dyskutowanych tematów w branży IT.

Rosnąca liczba wirusów i ataków hakerskich oraz głośne przypadki poważnych naruszeń bezpieczeństwa danych wywołują stanowcze reakcje środowiska IT.

Dyrektorzy małych i średnich firm często nie do końca zdają sobie sprawę z ryzyka i aktualnych zagrożeń związanych z bezpieczeństwem danych i nie chcą zagłębiać się w niuanse infrastruktury IT. Często mają niejasne pojęcie o dwóch lub trzech czynnikach ryzyka, które uważają za istotne. W procesie zatwierdzania budżetu ich priorytetem jest optymalizacja kosztów inwestycji w nowe oprogramowanie i ich pozytywny wpływ na rozwój działalności.

Ten przewodnik pomoże zrozumieć Ci, jakie są oczekiwania menadżerów patrzących z perspektywy biznesowej. Ponadto zawiera informacje o tym, w jaki sposób rozwiązania Microsoft (Microsoft 365 i Azure) pozwalają ograniczyć ryzyko związane z atakami hakerów i wirusami.

Jak korzystać z samouczka

Tekst zawiera przykłady różnego rodzaju ataków i odpowiednich środków ochrony. Opisy zostały podane w języku technicznym, jak również w formie bardziej zrozumiałej dla osób odpowiedzialnych za podejmowanie decyzji wdrożeniowych.

Jak rozmawiać na tematy dotyczące bezpieczeństwa informacji

Rozmowa z decydentami na temat bezpieczeństwa informacji powinna zawierać zasadnicze punkty. Ludzie zwykle pomijają kwestie zabezpieczeń, dopóki „wszystko działa prawidłowo". Firmy, które doświadczyły poważnych strat danych na skutek działania złośliwych programów szyfrujących, zwracają dużo większą uwagę na zabezpieczenia niż te, w których takie zdarzenia jeszcze nie wystąpiły. Z drugiej strony nie da się zabezpieczyć systemu w 100%. System, który działa, jest narażony na ryzyko. Naszym zadaniem jest identyfikacja czynników ryzyka i ograniczenie ich do akceptowalnego poziomu. Zminimalizowanie potencjalnych zagrożeń opiera się na zakupie oprogramowania. Z tego powodu ważne jest, by zrozumieć, że bardziej opłaca się zapłacić za zabezpieczenia, niż później ponosić koszty ich braku.

Główne problemy w obszarze bezpieczeństwa informacji w małych i średnich fimach

1) Najsłabszym ogniwem są ludzie. Często nie rozumieją wartości danych, z których korzystają, i nie zapewniają im odpowiedniej ochrony.

2) Dostępność narzędzi. W dzisiejszych czasach nic nie stoi na przeszkodzie, by zostać hakerem. Powstało tysiące narzędzi, z których każdy początkujący haker może bezpłatnie korzystać. To właśnie dlatego mamy dzisiaj tak wielu „hakerów". Raczej nie są oni w stanie spenetrować dobrze chronionej infrastruktury, ale firmy nieprzywiązujące wagi do bezpieczeństwa informacji mogą znaleźć się w grupie ryzyka.

3) „Nasza fima jest zbyt mała — kto się nami zainteresuje?" Takie podejście jest bardzo często spotykane w małych i średnich firmach. Nawet niewielka organizacja może stać się celem ukierunkowanego ataku. Jednak większym problemem jest fakt, że hakerzy nie wybierają swoich celów. Zdarzały się przypadki, gdy hakerzy próbowali włamać się na serwery agencji rządowych, wykorzystując w tym celu serwery firmowe z naruszonymi zabezpieczeniami. Firmy nie zdawały sobie sprawy z włamania, dopóki agenci służb wywiadowczych nie pojawili się u nich, by przesłuchać pracowników i skonfiskować sprzęt.

4) Przestarzałe technologie. Problemem przestarzałych technologii jest fakt, że zostały one zaprojektowane do ochrony przed zagrożeniami występującymi w czasie tworzenia danego oprogramowania. Im dłużej program funkcjonuje w niezmienionej wersji, tym więcej jest nowych ataków, których nie uwzględniają jego zasoby zabezpieczeń. „Poprawki" nie gwarantują ochrony przed wszystkimi atakami.

5) Brak wykwalifiowanych specjalistów ds. bezpieczeństwa informacji i deficyt zasobów zabezpieczeń dostępnych dla specjalistów IT. Małe i średnie firmy nie zawsze dysponują specjalistami ds. bezpieczeństwa informacji. Funkcje te realizują pracownicy działu IT odpowiedzialni za konfigurowanie i konserwację systemów, którym często brakuje czasu na te zadania. Jednak misją zespołu IT jest dostarczanie funkcjonalnych usług IT, a narzędzia zabezpieczeń mogą utrudniać świadczenie tych usług. Na przykład starannie skonfigurowana zapora ogniowa może wyłączyć prawidłowo działające aplikacje. Specjaliści IT stają wówczas przed dylematem: czy monitorować porty używane przez aplikację, czy też wyłączyć zaporę. Czasami wybierają tę drugą opcję, która zapewnia szybsze rezultaty.

Zagrożenie: Hasła poczty e-mail można zgadnąć, uzyskać w odpowiedzi na prośbę lub pobrać z pamięci przeglądarki

Rozwiązanie

Office 365: uwierzytelnianie wieloskładnikowe

Konfiguracja uwierzytelniania dwuskładnikowego w usłudze Office 365

W języku IT

Prawdopodobnie wiesz, że wielu użytkowników postrzega hasła jako „kaprys administratora", a nie środek ochrony przed nieautoryzowanym dostępem. Nie przykładają do ochrony haseł odpowiedniej wagi, a odpowiedzialność za bezpieczeństwo informacji przerzucają na dział IT.

Uwierzytelnianie wieloskładnikowe wymaga nie tylko znajomości hasła, ale także odpowiedzialności użytkownika za używane przez niego urządzenia.

Uwierzytelnianie wieloskładnikowe można łatwo skonfigurować w usługach online, rozwiązując w ten sposób szereg problemów związanych z bezpieczeństwem. Można wykorzystać połączenie telefoniczne, wiadomość SMS, potwierdzenie w aplikacji mobilnej lub cyfry wpisywane w aplikacji mobilnej. Możliwa jest także elastyczna konfiguracja wyjątków. Na przykład możesz zrezygnować z drugiego składnika w przypadku pracy z firmowego adresu IP, ale wymagać go, gdy użytkownik pracuje z domu. Możesz również łączyć się z lokalnymi usługami, takimi jak dostęp do sesji terminala, po wprowadzeniu kilku składników.

Nie da się w 100% zapobiec naruszeniom zabezpieczeń, ale można je znacznie utrudnić. Oprócz haseł atakujący musiałby uzyskać dostęp do osobistych urządzeń użytkowników, z którymi niechętnie się oni rozstają.

Uzyskaj wsparcie kadry zarządzającej. W przeciwnym razie uwierzytelnianie wieloskładnikowe będzie uważane za kolejny „wymysł administratorów".

W języku biznesu

Jedno zabezpieczenie w postaci hasła to dziś za mało. Użytkownicy przyklejają karteczki z hasłami lub zapisują hasła w plikach przechowywanych przez przeglądarki. Hasła są często bardzo proste, ponieważ tak jest wygodniej. Potem te same nazwy użytkowników są używane do rejestracji w witrynach internetowych lub na forach o wątpliwym poziomie zabezpieczeń.

Po nawiązaniu połączenia z bankiem internetowym oprócz hasła musisz podać kod otrzymany za pomocą SMS-a. Dlaczego dokumenty służbowe miałyby być słabiej zabezpieczone?

Wyjaśnij pracownikom, że dodatkowe 15 sekund potrzebne na wpisanie krótkiego tekstu to niewielka cena za bezpieczny dostęp do wrażliwych informacji.

Zagrożenie: Złośliwe załączniki do wiadomości e-mail

Rozwiązanie

Office 365: bezpieczne załączniki zaawansowanej ochrony przed zagrożeniami

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

W języku IT

Bezpieczne załączniki to funkcja usługi Microsoft 365 ATP, która otwiera załączniki w dedykowanym hiperwizorze, sprawdza je pod kątem złośliwego oprogramowania i podejmuje działania w celu wykrycia zagrożeń. Ta funkcja chroni korespondencję e-mail jeszcze przed pojawieniem się odpowiednich sygnatur antywirusowych.

Funkcja bezpiecznych załączników zaawansowanej ochrony przed zagrożeniami analizuje zawartość załączników. Współpracuje z najczęściej używanymi typami plików, takimi jak pliki programów Word, PowerPoint, Excel, pliki wykonywalne oraz pliki Flash i PDF.

Załączniki testuje się w środowisku wirtualnym z użyciem różnych wersji systemów operacyjnych i aplikacji. Zawartość załączników jest wykonywana pod nadzorem narzędzi sztucznej inteligencji w celu wykrycia złośliwych zachowań. Jeśli załącznik próbuje zainstalować konia trojańskiego, zaszyfrować pliki, delegować kontrolę do centrum sterowania lub wykonać podobne czynności, zostaje uznany za złośliwy.

Administrator może otrzymywać kopie początkowych wiadomości e-mail.

W języku biznesu

Wyobraź sobie dwie różne sytuacje — otwierasz dokument załączony do wiadomości e-mail, który:

1) po prostu się otwiera;
2) uruchamia proces przesyłania danych z Twojego laptopa lub szyfrowania innych dokumentów.

Z zewnątrz oba dokumenty mogą wyglądać identycznie, zachowują się jednak inaczej. Poczta e-mail Microsoft testuje zachowanie dokumentów, zanim wiadomości dotrą do skrzynki odbiorczej. Jeśli zachowanie jest zbliżone do opisu w drugim punkcie, wiadomość zostanie dostarczona bez załącznika. Żaden złośliwy kod nie przedostanie się do firmowej poczty e-mail. W odróżnieniu od ludzi system nie ufa „atrakcyjnym" wiadomościom i natychmiast je usuwa.

Zagrożenie: Złośliwe linki w wiadomościach e-mail

Rozwiązanie

Office 365: bezpieczne linki zaawansowanej ochrony przed zagrożeniami

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

W języku IT

Bezpieczne linki to funkcja usługi Microsoft 365 ATP, która chroni użytkowników przed złośliwymi linkami. Te linki często służą do wyłudzania ważnych informacji od użytkowników. W przypadku gdy odbiorca otrzymuje wiadomość z osadzonym linkiem, strona lub dokument otwierane przy jego użyciu mogą być bezpieczne w momencie otrzymania wiadomości, lecz stanowić zagrożenie po kliknięciu linka. Funkcja bezpiecznych linków chroni użytkownika, zastępując złośliwe linki.

Gdy użytkownicy klikają linki we wiadomościach e-mail lub w dokumentach, ich żądania są przekierowywane do serwera w środowisku Microsoft 365 w celu sprawdzenia adresów URL przy użyciu listy podejrzanych witryn. Jeśli zasób jest bezpieczny, przeglądarka przechodzi do żądanej witryny.

Jeśli witryna znajduje się na czarnej liście, przejście jest blokowane, a przeglądarka wyświetla stronę z ostrzeżeniem. Blokada obejmuje tylko złośliwe linki. Jeśli wiadomość e-mail zawiera kilka linków, zablokowane zostaną tylko te złośliwe.

Administratorzy mogą ręcznie dodawać witryny do list złośliwego oprogramowania.

W języku biznesu

Ludzie, których określaliśmy terminem „hakerzy", od dawna już działają jak marketerzy. Puszczają w obieg atrakcyjnie wyglądające wiadomości, projektują realistyczne kopie witryn bankowych i manipulują ludzkimi emocjami. Kliknięcie linka we wiadomości może spowodować epidemię wirusa, utratę dostępu do usług bankowych lub platformy handlowej itp.

Microsoft w kilka minut otrzymuje informacje o takich linkach. Wszelkie próby otwarcia zainfekowanych witryn lub fałszywych internetowych platform bankowych przy ich użyciu są blokowane.

Zagrożenie: Ataki z użyciem złośliwych programów szyfrujących

Rozwiązanie

Windows 10: kontrolowany dostęp do folderów

Konfiguracja kontrolowanego dostępu do folderów

W języku IT

Dzięki kontrolowanemu dostępowi do folderów możesz uniemożliwić niezaufanym procesom zapisywanie w określonych folderach.

W przypadku ataku z użyciem złośliwego programu szyfrującego system Windows zablokuje wszelkie próby zmodyfikowania plików w chronionych folderach. To oznacza, że pliki zawierające informacje wrażliwe pozostaną nietknięte. Konieczna będzie ponowna instalacja systemu operacyjnego, ale dane będą bezpieczne.

Pełne listy procesów nie są publikowane, ale aplikacje takie jak Powershell czy Cmd nie są zaufane, ponieważ mogą uruchamiać złośliwe skrypty. Procesy takie jak Windows Explorer lub MS Word pozostaną bez zmian. W razie potrzeby nieznany proces można dodać do białej listy. Kontrolowany dostęp do folderów bazuje na programie antywirusowym Windows Defender i nie będzie działać w przypadku zainstalowania oprogramowania antywirusowego innej firmy.

W języku biznesu

Złośliwe programy szyfrujące stanowią poważne zagrożenie i często omijają ochronę antywirusową. Dzięki kontrolowanemu dostępowi do folderów nawet w przypadku zaszyfrowania systemu pliki w chronionych folderach pozostaną nietknięte.

Jeśli oprogramowanie antywirusowe nie poradzi sobie z wirusem szyfrującym, Twoje dokumenty będą całkowicie bezpieczne.

Zagrożenie: Ataki z użyciem złośliwych programów szyfrujących

Rozwiązanie

Zmniejszanie obszaru podatnego na ataki

Konfiguracja zmniejszania obszaru podatnego na ataki

W języku IT

To zestaw reguł, który ogranicza prawdopodobieństwo włamania lub infekcji wirusowej.

Przykłady reguł:

Blokowanie zawartości wykonywalnej w kliencie poczty e-mail i poczcie w sieci Web. Użytkownicy, którzy pobiorą złośliwy kod w osobistej wiadomości e-mail, nie będą w stanie go wykonać.

Wyłączanie procesów pochodnych w aplikacjach Office. Źródłem infekcji są często złośliwe makra w pliku Office. Ta reguła powoduje, że makra nie mogą uruchamiać aplikacji innych firm (np. Powershell lub Cmd). Nie ma ona jednak wpływu na działania prawidłowych makr, na przykład służących do wykonywania obliczeń w programie Excel.

Wyłączanie procesów pochodnych w programie Adobe Reader. Podobna reguła dotycząca programu Adobe Reader.

Wyłączanie aplikacji opartych na USB. Nazwa mówi sama za siebie.

I tak dalej.

Lista reguł jest aktualizowana z każdą nową wersją systemu Windows 10. Może ona również działać w trybie inspekcji, w którym zamiast blokować działanie tworzy się wpis w logu. Funkcja zmniejszania obszaru podatnego na ataki działa w oparciu o program antywirusowy Windows Defender i nie będzie funkcjonować, jeśli zainstalowano program antywirusowy innej firmy.

Zagrożenie: Ataki z użyciem złośliwych programów szyfrujących

Rozwiązanie

Ochrona sieci

Konfiguracja ochrony sieci

W języku IT

Wszystkie sieci, stacje robocze i serwery są chronione przy użyciu zapory. Nawet jeśli jest ona prawidłowo skonfigurowana, najczęściej blokuje połączenia przychodzące i zezwala na niemal każde połączenie wychodzące.

Z jakimi zagrożeniami się to wiąże?

- Użytkownicy mogą uruchamiać oprogramowanie, które przekazuje kontrolę nad stacją roboczą do centrum sterowania.
- Hakerzy uzyskują pełny dostęp do stacji roboczych, a w rezultacie do wewnętrznej sieci firmowej.
- Użytkownicy mogą uruchamiać oprogramowanie, które przesyła dane na złośliwe adresy e-mail.
- Użytkownicy mogą otwierać linki do złośliwych witryn internetowych itp.

Funkcja ochrony sieci sprawdza każde połączenie wychodzące przy użyciu bazy wiedzy Microsoft. W przypadku znalezienia danego adresu i oznaczenia go jako złośliwego połączenie zostanie natychmiast zablokowane. Ta funkcja może również działać w trybie inspekcji, w którym zamiast blokować działanie tworzy się wpis w logu. Funkcja ochrony sieci działa w oparciu o program antywirusowy Windows Defender i nie będzie funkcjonować, jeśli zainstalowano program antywirusowy innej firmy.

Zagrożenie: Ataki z użyciem złośliwych programów szyfrujących

Rozwiązanie

Office 365: OneDrive dla Firm

Konfiguracja usługi OneDrive dla Firm w systemie Windows 10

W języku IT

Gdy złośliwe oprogramowanie szyfrujące infiltruje system, szyfruje dokumenty i archiwa oraz usuwa kopie w tle. Skonfiguruj system Windows 10 pod kątem synchronizacji dokumentów z usługą przechowywania w chmurze OneDrive dla Firm, by móc odzyskiwać dowolne elementy. Pliki będą synchronizowane natychmiast po zapisaniu we wskazanym katalogu. Klient synchronizacji jest wbudowany w Windows 10 lub opcjonalnie instalowany w Windows 7.

Minimalna dostępna pojemność magazynu wynosi 1 TB na użytkownika. Wbudowana funkcja przechowywania wersji umożliwia przywracanie zarówno bieżącej wersji pliku, jak i jego wcześniejszych kopii.

W języku biznesu

Czy zdarzyło Ci się krzyknąć ze złości z powodu przypadkowego usunięcia dokumentu lub ataku z użyciem złośliwego programu szyfrującego? Albo z powodu trwałej utraty części dokumentu?

Utrata ważnych danych zdarza się nie tylko z winy złośliwych programów szyfrujących użytkowników, ale także użytkowników, którzy mniej lub bardziej przypadkowo usuwają informacje.

System można skonfigurować w taki sposób, aby dokumenty przechowywane na komputerze PC lub laptopie były automatycznie synchronizowane z niezawodną usługą magazynu. Obsługa plików i folderów wygląda dokładnie tak samo.

W przypadku plików zaszyfrowanych, usuniętych lub zmodyfikowanych można przywrócić ich wcześniejsze wersje. Wszystkie są zapisywane niezależnie od liczby wprowadzonych zmian. Dzięki temu można przywrócić poprzednią wersję, która nie została zaszyfrowana przez złośliwy program szyfrujący lub w inny sposób utracona.

Zagrożenie: Pobieranie informacji z dysku bez hasła

Rozwiązanie

Windows 10: szyfrowanie funkcją BitLocker

Dokumentacja funkcji BitLocker

W języku IT

Na pewno wiesz o tym, że dysk twardy można wyjąć z jednego komputera i podłączyć do innego. Można też wykonać rozruch z dysku DVD i uzyskać dostęp do całego systemu plików. W obu przypadkach nie trzeba znać danych logowania. Nie zapominajmy również o nośnikach wymiennych, które łatwo zgubić. Koszt przechowywanych danych często wielokrotnie przewyższa koszt nośnika fizycznego.

Z tego powodu szyfrowanie dysków jest koniecznością. Jednak podobnie jak inne środki zabezpieczeń, często pociąga to za sobą pewne niedogodności. Właściwa konfiguracja funkcji BitLocker minimalizuje ryzyko. Klucze odzyskiwania można zapisywać w usłudze Active Directory. W przypadku fizycznego uszkodzenia dysku dane można przywrócić. Aby uzyskać jeszcze wyższy poziom niezawodności, zaleca się archiwizację kopii zapasowych danych.

W języku biznesu

W dzisiejszych czasach informacje giną razem z urządzeniami.

Laptop pozostawiony na lotnisku, dysk flash, który wypadł z torby... Wszystkie te wypadki wiążą się nie tylko z koniecznością poniesienia kosztów zakupu nowego sprzętu, ale także poważnym ryzykiem uzyskania dostępu do danych przez osoby nieuprawnione.

Nawet jeśli laptop jest chroniony hasłem, specjalista IT bez trudu wydobędzie informacje. Na laptopach często można znaleźć dokument zawierający listę haseł lub hasła zapisane w przeglądarce.

Szyfruj wszystkie dyski i dyski flash, które zawierają ważne dane. Utrata lub konfiskata urządzeń nadal pozostanie utrudnieniem, ale nikt nie uzyska dostępu do Twoich danych.

Informacje będą bezpiecznie zaszyfrowane i niedostępne dla tych, którzy znajdą Twoje urządzenie.

Zagrożenie: Pobieranie informacji z dysku niechronionych hasłem

Rozwiązanie

Microsoft Intune

[Dokumentacja usługi Microsoft Intune]

W języku IT

Microsoft Intune to system MDM, który kontroluje urządzenia z chmury i obsługuje kontrolę aplikacji niezależnie od lokalizacji użytkownika.

Kontrola jest dostępna dla wielu urządzeń, m.in. z systemami iOS, Mac OS X, Android, Windows 8.1 i Windows 10.

Główne funkcje:

- Dostęp do wiadomości e-mail i dokumentów mogą uzyskiwać jedynie urządzenia skonfigurowane przez firmę.
- Ustawienia zabezpieczeń: kod PIN, sprawdzanie zdjęcia zabezpieczeń systemu/katalogu głównego, blokowanie instalacji aplikacji niezakupionych w sklepie itp.
- Całkowite lub częściowe usuwanie danych z urządzeń.
- Wdrażanie sieci Wi-Fi, certyfikaty.
- Wdrażanie aplikacji, definiowanie ograniczeń specyficznych dla aplikacji. Na przykład kopiowanie tekstu z programu Outlook może być zabronione.

Nie możesz zmusić użytkowników do połączenia swoich urządzeń z MDM, ale możesz zablokować dostęp do zasobów firmowych z urządzeń niezarządzanych. Użytkownicy potrzebują dostępu do tych zasobów, więc będą musieli połączyć urządzenia przy użyciu konkretnych dozwolonych metod.

W języku biznesu

Firma zajmująca się badaniami w dziedzinie bezpieczeństwa informacji przeprowadziła kiedyś następujący eksperyment: pewną liczbę telefonów komórkowych z zainstalowanym oprogramowaniem do śledzenia aktywności „przypadkowo zgubiono" w miejscach publicznych w USA i Kanadzie. 60% osób, które znalazły te urządzenia, nie próbowało ich zwrócić. W ciągu 1–2 godzin nowi „właściciele" zaczęli przeglądać dokumenty i zdjęcia oraz uruchamiać aplikacje.

Głównym zagrożeniem związanym z urządzeniami mobilnymi jest fakt, że chociaż urządzenia są osobiste, mogą znajdować się na nich dane firmowe. Możliwości kontroli urządzeń osobistych są bardzo ograniczone.

Użytkownicy zwykle beztrosko korzystają ze swoich urządzeń osobistych — nie szyfrują danych, nie chronią dostępu kodem PIN, instalują niesprawdzone aplikacje i często gubią urządzenia. Ponadto zwolnieni pracownicy mogą przechowywać zarchiwizowane wiadomości lub kontakty do klientów na swoich smartfonach.

Jeśli pracownicy używają firmowej poczty lub dokumentów na urządzeniach mobilnych, musisz być stanie chronić informacje należące do firmy. Po połączeniu telefonów komórkowych z usługą Intune możesz je skonfigurować w bezpieczniejszy sposób, a także zyskujesz możliwość usunięcia danych firmowych (lub wszystkich) po zakończeniu okresu zatrudnienia.

To oznacza, że firmowe wiadomości e-mail czy służbowe dokumenty na osobistych smartfonach „nie odejdą" razem ze zwolnionymi pracownikami. Także w przypadku kradzieży lub utraty urządzenia będzie można zdalnie usunąć z niego dane.

Zagrożenie: Wirusy

Rozwiązanie

Windows 10: Windows Defender

Profil programu Windows Defender

W języku IT

Program Microsoft Security Essentials, używany we wcześniejszych wersjach systemu Windows jako rozwiązanie antywirusowe, był dość prosty. Windows Defender — jego następca — zasadniczo różni się od Security Essentials.

Jego główną zaletą jest integracja z Windows 10 oraz ulepszony aparat w każdej kolejnej wersji systemu.

To oprogramowanie antywirusowe jest całkowicie bezpłatne do użytku firmowego i można je kontrolować za pomocą zasad grupy.

Niektóre funkcje, takie jak centralne raportowanie, wymagają komercyjnych funkcji sterowania.

W języku biznesu

Oprogramowanie antywirusowe nie rozwiązuje wszystkich problemów związanych z bezpieczeństwem, ale jest kluczowym elementem systemu zabezpieczeń. Oprogramowanie antywirusowe jest wbudowane w system i bezpłatne. Windows to najpopularniejszy, a w związku z tym najczęściej atakowany system operacyjny.

Hakerzy próbują dotrzeć do możliwie najszerszej grupy potencjalnych odbiorców, dlatego środki ochrony powinny być wbudowanym elementem systemu i działać natychmiast. System Windows 10 oferuje takie wbudowane zabezpieczenia.

Zagrożenie: Wyciek dokumentów

Rozwiązanie

Azure Information Protection

[Dokumentacja usługi Azure Information Protection]

W języku IT

Technologia ochrony dokumentów oparta na szyfrowaniu i przydzielanie praw dostępu użytkownikom pozwalają narzucić określone ograniczenia nawet w sytuacji, gdy dokumenty wyciekną poza organizację.

Usługa Azure Information Protection pozwala zatrzymać informacje wrażliwe w środowisku firmowym i uniknąć wycieku danych.

Ta technologia integruje się z aplikacjami Office, obsługując szyfrowanie plików w programach Microsoft Word i Microsoft Exchange. Można ją stosować zarówno ręcznie, jak i automatycznie zgodnie z ustalonymi regułami. Na przykład gdy pracownik wysyła wiadomość e-mail z załącznikiem poza firmę lub na wskazany adres albo z załączonymi określonymi plikami, załącznik może być szyfrowany automatycznie.

W języku biznesu

Nawet jeśli ktoś podejmie próbę wyniesienia poufnych informacji poza firmę, nie będzie mógł otworzyć dokumentów.

Gdyby menedżer pocztą e-mail przesłał konkurencyjnej firmie bazę danych klientów, w żadnym wypadku nie byłaby ona w stanie odczytać tej wiadomości.

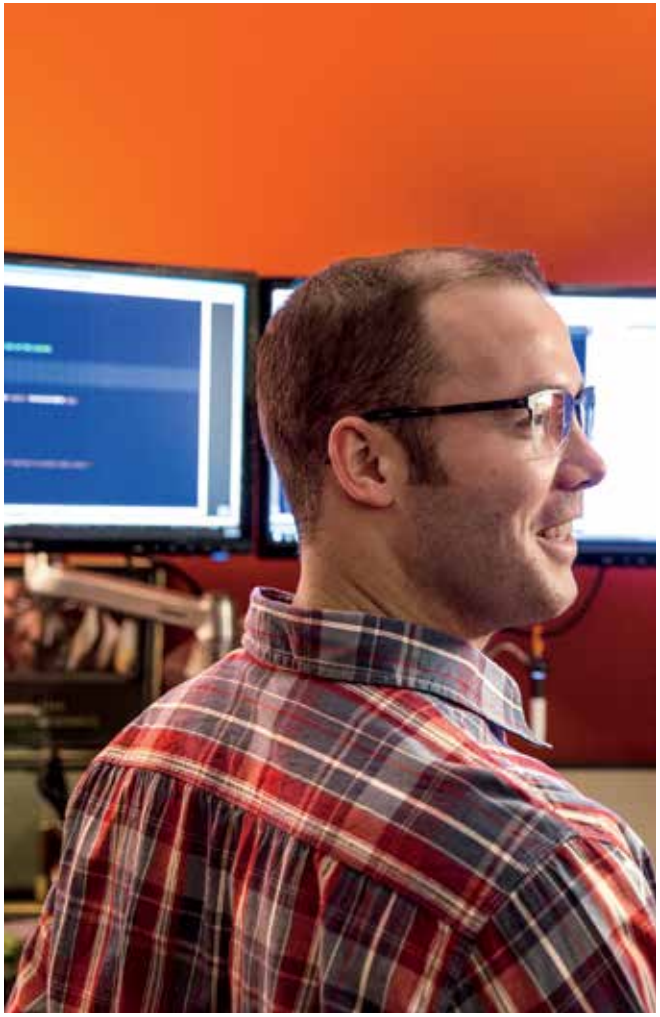
Można też zdefiniować ograniczenia dostępu do dokumentów, dzięki którym żadna osoba z zewnątrz nie wyświetli informacji przeznaczonych tylko dla pewnej grupy odbiorców.

Zagrożenie: Wyciek dokumentów (ciąg dalszy)

Rozwiązanie

Office 365 DLP (Ochrona przed utratą danych)

Szczegółowy przegląd usługi Office 365 DLP



W języku IT

Zbiór zasad usług Exchange Online, Sharepoint Online i OneDrive dla Firm służy do ochrony informacji wrażliwych. Zasady mogą zabraniać prowadzenia określonych działań z użyciem poufnych danych. Na przykład możesz uniemożliwić wysyłanie danych poza firmę lub pobranie ich na komputer lokalny.

Próby wykonania zabronionej operacji przez użytkownika są zgłaszane administratorowi.

Domyślnie system nie zawiera szablonu danych wrażliwych, który umożliwia wykrycie danych rosyjskiego paszportu. Należy zaprojektować go samodzielnie lub z pomocą integratorów systemów.

W języku biznesu

Państwo nie wymaga od firm zabezpieczenia przed wyciekiem danych osobistych.

Co się stanie, gdy pracownik przypadkowo wyśle pocztą e-mail dokument zawierający dane paszportowe?

Oto obrazowy przykład: podczas organizacji szczytu G20 w Brisbane w 2015 r. pracownik australijskiego departamentu ds. imigracji omyłkowo wysłał dokument zawierający dane paszportowe liderów G20 do pracowników administracji Pucharu Azji w piłce nożnej. Wpisując adres współpracownika w programie pocztowym, po prostu potwierdził on automatycznie sugerowany adres bez dokładnego sprawdzenia, po czym kliknął Wyślij.

Administrator może skonfigurować zasadę blokującą wychodzące wiadomości e-mail, w których wykryto dane paszportowe lub inne informacje osobiste.

Zagrożenie: Bezpieczeństwo fizczne — ryzyko włamania

Rozwiązanie

Korzystanie z centrów danych Microsoft

W języku IT

Bezpieczeństwo infrastruktury zależy od szeregu czynników, w tym zabezpieczeń fizycznych. Zapewnienie fizycznego bezpieczeństwa sprzętowi znajdującemu się w siedzibie firmy może być niełatwym zadaniem.

Oto kilka przydatnych wskazówek:

1) Serwerownia musi być odpowiednio umiejscowiona w siedzibie firmy. Ściany nie mogą być współdzielone z budynkami zewnętrznymi i nie mogą mieć okien.

2) Niezbędny jest system utrzymywania temperatury i wilgotności w określonym zakresie.

3) Drzwi muszą być wyposażone w zamki elektroniczne.

4) Podłogi w centrum danych muszą być podwyższone.

5) Centrum danych musi być wyposażone w system przeciwpożarowy.

6) Sprzęt i systemy przechowywania danych muszą być szyfrowane.

7) Cały budynek musi być wyposażony w zabezpieczenia fizyczne.

Firma Microsoft wszystkie te sprawy bierze na siebie. Z punktu widzenia zabezpieczeń Twoje dane będą chronione dużo lepiej w miejscu, które spełnia wszystkie te wymagania.

W języku biznesu

Gdy masz pod ręką wszystkie swoje dane, nie musisz się o nie martwić. Jednak każdy, kto uzyska dostęp do siedziby formy — legalnie lub nielegalnie — będzie mieć możliwość ich pozyskania. Intruz nie musi nawet być hakerem. Wystarczy, że po prostu wyniesie odpowiedni sprzęt.

Centra danych są wyposażone w systemy kontroli dostępu, punkty kontrolne i całodobowy nadzór wideo oraz dodatkowo chronione przez strażników. Uzyskanie dostępu do nich przez osoby nieupoważnione jest trudne lub prawie niemożliwe, szczególnie gdy centrum danych, w którym znajdują się Twoje dane, jest zlokalizowane w innym kraju.

Mniejsze firmy zwykle nie mogą sobie pozwolić na tak wysoki poziom zabezpieczeń, chronione serwery biurowe, kontrolę dostępu czy nadzór wideo.

Zagrożenie: Bezpieczeństwo fizczne — ryzyko włamania

Rozwiązanie

[Korzystanie z centrów danych Microsoft]

W języku IT

Wybierzmy się na wirtualną wycieczkę po centrach danych Microsoft.

Najpierw trzeba je odnaleźć. Adresy centrów danych są tajne, a wizyty w nich są możliwe jedynie w szczególnych okolicznościach (np. w celu przeprowadzenia audytu) i pod ścisłym nadzorem pracowników ochrony. Nawet, jeśli potencjalny przestępca zdobędzie w jakiś sposób adres jednego z centrów danych, ta informacja mu nie wystarczy. Musiałby jeszcze wiedzieć, w którym centrum są hostowane Twoje dane.

Aby dostać się do centrum danych, trzeba pokonać kilka warstw zabezpieczeń obejmujących m. in. uwierzytelnianie wieloskładnikowe, biometrię i szereg śluz bezpieczeństwa. Przez cały czas realizowany jest nadzór wideo.

W języku biznesu

Gdy w końcu znajdziemy się w centrum danych, zobaczymy wiele stojaków z serwerami, systemy przechowywania itp. Ani audytorzy, ani lokalny personel nie wiedzą, na którym stojaku z serwerami przechowuje się Twoje dane.

Cały sprzęt podlega określonym cyklom eksploatacji i regularnym uaktualnieniom prewencyjnym. Po zakończeniu cyklu życia systemy przechowywania danych utylizuje się przy użyciu niszczarek.

Sprzęt jest stale monitorowany w celu zapobiegania zdarzeniom związanym ze spadkiem wydajności lub utratą bezpieczeństwa.

Centra danych podlegają regularnym audytom i posiadają liczne certyfikaty potwierdzające ich niezawodność. Na taki poziom zabezpieczeń może sobie pozwolić tylko kilka firm na świecie.

Zagrożenie: Brak archiwizacji danych

Rozwiązanie

Przechowywanie kopii zapasowej w centrum danych

Dokumentacja usługi Kopia zapasowa Azure

W języku IT

Narzędzie do kopiowania danych Kopia zapasowa Azure firmy Microsoft to standardowe rozwiązanie do archiwizacji i przywracania danych, które stanowi uzupełnienie zestawu aktualnie dostępnych narzędzi.

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

Archiwizacja w chmurze jest alternatywą do stacji taśm. Dlaczego używa się taśm? Służą one jako niedrogi i niezawodny długoterminowy magazyn danych. Jednak stacje taśm nie mogą być jednocześnie tanie i niezawodne. Niską cenę nośników podnoszą koszty transportu, wynajmu bezpiecznej przestrzeni do ich przechowywania, księgowości i administracji. Jeśli te środki zostaną zaniedbane, w przypadku zdarzenia związanego z bezpieczeństwem nośniki mogą ulec zniszczeniu.

Magazyn oparty na chmurze oferuje porównywalne ceny i jest dużo prostszy pod względem obsługi administracyjnej i księgowej. Nie trzeba niczego nigdzie dostarczać ani wyszukiwać taśm na półkach. Wystarczy otworzyć portal internetowy, znaleźć żądane archiwum i jednym kliknięciem przywrócić dane.

Archiwizacja opiera się na agentach. Jeśli potrzebujesz zarchiwizować pliki, instalujesz agenta na serwerze plików i planujesz operację utworzenia kopii zapasowej. Jeśli chcesz zarchiwizować maszyny wirtualne lub bazy danych albo przywrócić dane na pustym urządzeniu, musisz zainstalować dedykowany składnik Serwer usługi Kopia zapasowa Azure, który Microsoft udostępnia bezpłatnie i który umożliwia centralne tworzenie kopii zapasowych.

W języku biznesu

Sprzęt lokalny może ulec awarii. Dane mogą zostać przypadkowo lub celowo wymazane. W takich sytuacjach ratunkiem są kopie zapasowe.

Co się jednak dzieje w przypadku utraty tych kopii, na przykład na skutek pożaru, kradzieży lub niedbałego przechowywania nośników?

W amerykańskim studio filmowym pracującym nad słynną kreskówką wystąpiła awaria techniczna, której skutkiem był utrata większości materiału filmowego. Z powodu nieodpowiedniego przechowywania archiwum nie udało się odzyskać danych. Łut szczęścia sprawił, że film ocalał — jeden z pracowników tuż przed wypadkiem zrobił kopię materiału, by popracować nad nią w domu.

Skonfigurowanie niezawodnego magazynu danych może być kosztowne. Ponadto nawet prawidłowo zorganizowany magazyn nie jest odporny na ludzkie błędy.

Duży szpital w stanie Utah przechowywał rejestry pacjentów w bezpiecznym magazynie. Kurier codziennie dostarczał nośniki z danymi do magazynu. Pewnego dnia, tuż przed weekendem, kurier nie dostarczył przesyłki tego samego dnia, lecz zostawił ją na noc w samochodzie. W nocy ktoś włamał się do samochodu i ukradł nośniki. W rezultacie firma musiała wypłacić swoim pacjentom milionowe odszkodowania.

Przechowywanie w chmurze jest bezpieczne pod względem technologicznym i wolne od ludzkich błędów.

Roczny raport księgowy, bazę danych płac czy jakiekolwiek inne dane można przywrócić nawet po ich celowym usunięciu lub konfiskacie.

Zagrożenie: Jeśli atak JUŻ nastąpił

Rozwiązanie

Usługa Advanced Threat Analytics (instalowana lokalnie)

Usługa Azure Advanced Threat Protection (w chmurze)

Dokumentacja usługi Advanced Threat Analytics

W języku IT

Żadna ochrona nie daje 100% gwarancji. Problem polega na tym, że firmy często wykrywają włamania kilka miesięcy po zdarzeniu, gdy haker zdążył już przejąć wszystkie dane. Aby zapobiec takim sytuacjom, nie wystarczy ochrona. Konieczny jest także monitoring.

Tę funkcję tradycyjnie pełnił system wykrywania nieautoryzowanego dostępu (IDS). Jego nowoczesnym odpowiednikiem jest analiza zachowania użytkowników (UBA).

Systemy UBA badają zestaw cech, jakimi charakteryzuje się zachowanie użytkownika: w jakich godzinach pracuje, na jakich urządzeniach się loguje, do jakich plików uzyskuje dostęp, do jakich społeczności należy itp. Po utworzeniu profilu behawioralnego użytkownika system będzie zgłaszać wszystkie zachowania odbiegające od normy. Można wyśledzić, czy dane zachowanie jest efektem działania użytkownika, czy intruza, który włamał się na jego konto.

System UBA można wdrożyć na dwa sposoby:

- System instalowany lokalnie w celu analizy ruchu w usłudze Active Directory. Takie rozwiązanie nosi nazwę Microsoft ATA.
- System w chmurze z agentami zainstalowanymi lokalnie w kontrolerach domeny. Takie rozwiązanie nosi nazwę Azure ATP.

W języku biznesu

Żadna ochrona nie daje 100% gwarancji.
Szczególnie trudne jest zapewnienie ochrony przed osobami, które należą już do strefy zaufania, takimi jak pracownicy. Nikt nie może być pewien, że pracownik, który nie otrzymał oczekiwanej premii, nie zdecyduje się na akt sabotażu i nie skopiuje wrażliwych danych. System analizy zachowania użytkowników pozwala wykrywać nietypowe działania.

System zgłosi np. fakt, że pracownik został po godzinach, by wydrukować poufne dane.

Analogicznie system zgłosi próbę uzyskania przez pracownika dostępu do dokumentów, które zwykle nie są mu potrzebne do wykonywania jego zadań.

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