Microsoft

6 kroków opracowywania kompleksowej strategii zabezpieczeń

Ta publikacja jest przeznaczona dla

dyrektorów i kierowników ds. bezpieczeństwa informacji lub IT, którzy:

- Potrzebują krótkiego, konkretnego przewodnika po ogólnej strategii zabezpieczeń.
- Chcą być na bieżąco z najnowszymi praktykami bezpieczeństwa.

Szacowany czas czytania: 9 minut

Spis treści

Sprostać wyzwaniom

Zabezpieczanie danych i systemów stanowi priorytet dla organizacji. Jednak sprostanie temu wyzwaniu staje się coraz trudniejsze, ponieważ z każdym dniem ataki stają się bardziej wyrafinowane, pracownicy korzystają z większej liczby urządzeń i aplikacji, a dane są przesyłane na więcej sposobów. Wraz z masowym przejściem do pracy zdalnej bezpieczeństwo staje się jeszcze bardziej zagrożone.

Trzeba równoważyć działania mające na celu sprostanie tym wyzwaniom z potrzebą zapewniania efektywnej współpracy, wprowadzania innowacji i rozwijania firmy. Niezbędne jest wieloaspektowe podejście do bezpieczeństwa, które pozwoli zapewnić stałą ochronę wszystkich urządzeń klienckich, wykrywać wczesne oznaki naruszeń i podejmować odpowiednie działania, zanim powstaną szkody. Niezależnie od tego, jak silnymi zabezpieczeniami dysponujesz, środki prewencyjne przestają wystarczać — konieczne jest przyjęcie postawy zakładającej nieuniknioność naruszenia, która uwzględnia środki jego wykrywania i reakcji na nie.

Dyrektorzy ds. bezpieczeństwa informacji (CISO) potrzebują dzisiaj elastycznych platform zabezpieczeń umożliwiających transformację cyfrową i opartych na kompleksowych strategiach, które uwzględniają technologie, procesy i programy szkoleniowe. Chociaż wszystko to jest dostępne w przypadku rozwiązań lokalnych, prawda jest taka, że przejście do chmury natychmiast poprawia możliwości zabezpieczeń w całej organizacji.

W tym e-booku opisano sześć najlepszych praktyk przygotowanych przez CISO, którzy uczynili bezpieczeństwo podstawą sukcesu biznesowego. Mają one zastosowanie do rozwiązań lokalnych, ale nieporównanie łatwiej je zrealizować w chmurze.

1. Używaj zintegrowanych produktów zabezpieczających, aby umożliwić szybkie reagowanie

75

Liczba produktów zabezpieczających używanych przez przeciętną dużą organizację[1]

Hakerzy odchodzą od krótkich ataków. Teraz chcą zapewniać sobie długoterminową obecność w systemie ofiary. Współcześni przestępcy stosują coraz bardziej zaawansowane narzędzia i techniki. Ich przykłady to kradzież poświadczeń, instalacja złośliwego oprogramowania, które samoistnie usuwa się, by uniknąć wykrycia, modyfikowanie procesów wewnętrznych, przekierowywanie danych sieciowych, korzystanie z socjotechnik, a nawet atakowanie telefonów komórkowych czy urządzeń domowych pracowników.

Organizacje wdrażają coraz więcej narzędzi zabezpieczających przed tymi zagrożeniami. Rozwiązania te jednak powstają w odpowiedzi na konkretne zagrożenia i rzadko ze sobą współdziałają. Wiele firm korzysta ze swoich własnych pulpitów zarządczych, konsol i dzienników. Trudności z integracją utrudniają uzyskanie całościowego widoku i szybkie priorytetyzowanie zagrożeń. Staje się to jeszcze większym wyzwaniem, gdy jednocześnie są używane zasoby chmurowe i lokalne. W efekcie takie ataki mogą pozostać niewykryte przez ponad 140 dni[2].

[1] „Symantec Introduces New Era of Advanced Threat Protection" (Symantec przedstawia nową erę zaawansowanej ochrony przed zagrożeniami), Businesswire, październik 2015 r.

[2] „Threat Landscape: By the Numbers" (Krajobraz zagrożeń w liczbach), Mandiant, A FireEye Company, 2016 r.

Wypróbuj to

Wraz ze wzrostem znaczenia szybkiego wykrywania i reagowania wypracowano następujące najlepsze praktyki:

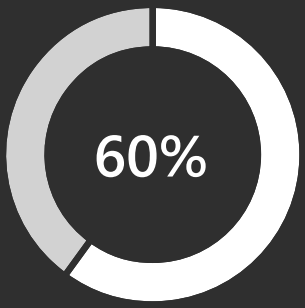
- Uzyskaj kompleksowy widok zabezpieczeń całej sieci, w tym środowisk chmurowych i hybrydowych.
- Zbuduj ekosystem produktów i platform zabezpieczających, które integrują się ze sobą i dostarczają analiz.
- Wybierz takich dostawców technologii, którzy współdziałają i wymieniają się informacjami w branży zabezpieczeń.

Najważniejsze wnioski

Brak integracji między produktami z obszaru zabezpieczeń utrudnia zespołom ds. zabezpieczeń szybkie wykrywanie zagrożeń oraz ich kompleksowe zwalczanie.

Szukaj produktów zaprojektowanych pod kątem ich wzajemnej integracji.

2. Zarządzaj dostępem na poziomie tożsamości, a nie urządzeń klienckich



naruszeń wynika ze złamania zabezpieczeń urządzeń klienckich[3].

Naruszenie bezpieczeństwa danych może wiązać się z ogromnymi kosztami. Jednym ze sposobów przeciwdziałania temu jest wprowadzenie odpowiednich mechanizmów zabezpieczeń pozwalających na uzyskanie wglądu w zagrożenia i ataki. Ale zespoły ds. bezpieczeństwa muszą również wspierać model konsumeryzacji IT oznaczający, że ludzie nie używają już wyłącznie ściśle kontrolowanych, firmowych urządzeń, ale chcą pracować w dowolnym miejscu, na dowolnych urządzeniach i platformach, niezależnie od tego, czy zostały one zatwierdzone przez firmowy dział IT.

To oznacza, że w ramach strategii zabezpieczeń opartych na tożsamości dostęp jest powiązany z tożsamością, a nie z urządzeniami. Zastosuj funkcje kontroli zabezpieczeń na podstawie roli i potrzeb — niezależnie od sposobu łączenia się przez użytkownika. Koncentrując się na odpowiednim uwierzytelnianiu użytkowników uzyskujących dostęp do zasobów firmowych oraz zarządzaniu nimi, organizacje mogą chronić dane niezależnie od tego, gdzie są one przechowywane, w jaki sposób uzyskuje się do nich dostęp i komu są one udostępniane.

[3] „Top Five Security Threats Facing Your Business and How To Respond" (Pięć największych zagrożeń dla bezpieczeństwa Twojej firmy oraz właściwe sposoby reagowania), blog Microsoft Secure, październik 2016 r.

Wypróbuj to

Odejście od strategii zabezpieczeń dotyczącej wyłącznie urządzeń klienckich zapewnia poprawienie bezpieczeństwa. Te narzędzia mogą pomóc:

- **Rozwiązania do zarządzania tożsamościami i dostępem (Identity and Access Management, IAM)** oraz **do zarządzania aplikacjami mobilnymi z funkcją ochrony przed utratą danych (Data Loss Prevention, DLP)**. Oba typy rozwiązań pozwalają ograniczyć ryzyko przez ochronę dostępu do aplikacji i danych w zasobach firmowych oraz w środowisku chmury. Rozwiązania do zarządzania tożsamościami i dostępem pozwalają wyeliminować potrzebę stosowania wielu poświadczeń, zapewniając pracownikom możliwość korzystania z jednej tożsamości do uzyskiwania dostępu do zasobów przechowywanych lokalnie i w chmurze. Systemy IAM oparte na chmurze mogą również używać funkcji analizy zagrożeń od dostawcy technologii, aby sprawniej wykrywać niestandardowe próby uzyskania dostępu i automatycznie odpowiednio reagować.
- **Uwierzytelnianie wieloskładnikowe** zapewnia kolejną warstwę ochrony, ponieważ użytkownik musi znać odpowiednie dane (hasło) oraz posiadać odpowiedni dostęp (uwierzytelnianie pomocnicze przy użyciu urządzenia, czytnika linii papilarnych lub funkcji rozpoznawania twarzy). Inne zaawansowane strategie mogą na przykład uzależniać przyznanie dostępu od ryzyka związanego z użytkownikiem, urządzeniem, aplikacją lub nawet lokalizacją. Te funkcje mogą automatycznie zezwalać na dostęp, blokować go lub wymagać od użytkownika uwierzytelnienia wieloskładnikowego w czasie rzeczywistym na podstawie ustawionych zasad, co pozwala organizacjom zwiększyć ochronę już podczas uzyskiwania dostępu do zasobów firmowych.

Najważniejsze wnioski

W przypadku strategii bezpieczeństwa opartej na tożsamości mniejszy nacisk kładzie się na śledzenie urządzeń klienckich, a większy na zarządzanie użytkownikami uzyskującymi dostęp do danych firmowych.

Jeśli naruszenia już wystąpią, to dzięki bardziej zaawansowanej ochronie urządzeń klienckich możliwe jest analizowanie technik przestępców.

3. Przyjmij model zerowego zaufania na potrzeby obrony przed zagrożeniami

17 000

alertów dotyczących złośliwego oprogramowania

To dotyka przeciętną dużą organizację co tydzień[4].

Hakerzy wiedzą, że każda organizacja ma wiele punktów wejścia. Wykorzystują oni różne taktyki, takie jak wyłudzanie informacji, zagubione i skradzione urządzenia, socjotechnika, złośliwe oprogramowanie i programy szpiegujące oraz programy wykorzystujące luki w zabezpieczeniach przeglądarek i oprogramowania. Aby radzić sobie ze znanymi zagrożeniami i mieć świadomość nowych, należy nieustannie zachowywać czujność.

Niektóre narzędzia zapewniają stale działające funkcje zabezpieczeń, jednak o większy sens ma spojrzenie z szerszej perspektywy. Tradycyjne narzędzia działają przede wszystkim zapobiegawczo, a to już nie wystarczy. Organizacje muszą zakładać, że już doszło do naruszenia lub że nastąpi ono wkrótce. Jest to nazywane „zerowym zaufaniem" (zero trust). Następnie muszą one znaleźć sposoby na znaczne skrócenie czasu wymaganego na wykrycie naruszeń i usuwanie ich skutków.

[4] „The Cost of Malware Containment" (Koszt powstrzymywania złośliwego oprogramowania), Ponemon Institute (na zlecenie Damballa), 2015 r.

Wypróbuj to

Wyspecjalizuj się w zakresie zabezpieczeń. Zapobieganie zagrożeniom może oznaczać analizę przeszłości — wyciąganie wniosków z incydentów i działań hakerów.

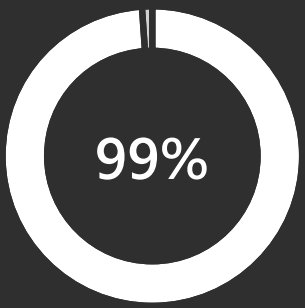
- Wiele aplikacji zabezpieczających korzysta z wbudowanych funkcji analitycznych i uczenia maszynowego, aby analizować, w jaki sposób haker uzyskał dostęp. Bardziej zaawansowane zabezpieczenia i rozwiązania do analizy wykorzystują te szczegółowe dane do automatycznego zapobiegania podobnym naruszeniom i reagowania na nie, co pozwala znacznie ograniczyć czas łagodzenia ich skutków.
- Ogromna rozległość i ilość wykorzystywanych danych w połączeniu z doświadczeniem i wiedzą ekspertów sprawiają, że rozwiązania te mogą okazać się potężnymi narzędziami, które pozwolą stawić czoła dynamicznie rozwijającym się zagrożeniom.

Najważniejsze wnioski

Aplikacje natywne dla chmury skuteczniej obsługują model zerowego zaufania niż starsze aplikacje.

Starsze aplikacje wymagają modernizacji, aby obsługiwały dostęp warunkowy oparty na tożsamości.

4. Przenieś się bezpiecznie do chmury



awarii zabezpieczeń w chmurze będzie winą klienta do 2025 r.[5]

Każda organizacja jest na innym etapie przenoszenia zasobów do chmury. Konieczność zachowania zgodności z wymogami i lokalnymi przepisami oraz inne wyzwania związane z migracją oznaczają, że nie każda organizacja jest gotowa na przeniesienie krytycznych obciążeń do chmury. Chmura hybrydowa to jeden ze sposobów, w jaki organizacje mogą wprowadzić rozwiązania chmurowe: pozostawiając niektóre obciążenia lokalnie, a inne przenosząc.

Modele usług w chmurze wpływają na sposób, w jaki odpowiedzialność jest dzielona pomiędzy dostawców usług i ich klientów. Dotyczy to CISO, którzy tracą część kontroli nad lokalnymi rozwiązaniami na rzecz dostawcy chmury, dzięki czemu zwiększa się ogólne bezpieczeństwo.

Najważniejszą regułą dotyczącą bezpieczeństwa w chmurze jest to, że odpowiedzialność jest wspólna. O ile dostawca usług w chmurze musi zapewnić nowoczesne zabezpieczenia oraz szyfrowanie, to będąc jego klientem, należy upewnić się, że zakupione od niego usługi są naprawdę bezpieczne i uwzględnić w polityce bezpieczeństwa także nowe zasoby w chmurze.

[5] „Is the Cloud Secure" (Czy chmura jest bezpieczna), Gartner, październik 2019 r.

Wypróbuj to

Zadawaj właściwe pytania. Ocena dostawców usług w chmurze nie sprowadza się tylko do wybrania konkretnej usługi. To wybór podmiotu, któremu powierzysz swoje dane. Oto najistotniejsze pytania dotyczące zabezpieczeń i kontroli dostępu, które należy sobie zadać:

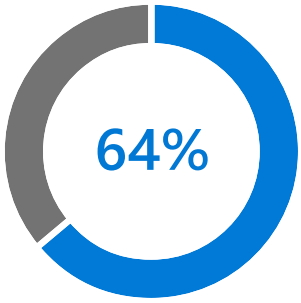
- Czy nasze dane są chronione przy użyciu silnych zabezpieczeń i nowoczesnych technologii?
- Czy ochronę prywatności rozważono już na etapie projektowania i czy zapewniono kontrolę nad danymi w naszej firmowej chmurze?
- W jakie skuteczne i innowacyjne procesy z zakresu zgodności z przepisami zainwestowano, aby zapewnić zgodność z przepisami naszej organizacji?
- Gdzie będą przechowywane nasze dane, kto ma do nich dostęp i dlaczego?
- Czy przeprowadzasz coroczne oceny zewnętrzne w celu zapewnienia przestrzegania standardów bezpieczeństwa i zgodności z przepisami?
- Czy odrzucisz wszelkie wnioski o ujawnienie danych osobowych klientów, które nie będą prawnie wiążące?
- Czy stosujesz się do norm regulacyjnych i dotyczących zgodności z przepisami obowiązujących w różnych krajach i regionach? Jeśli tak, to do których?

Najważniejsze wnioski

Oceniając dostawców usług w chmurze, należy wziąć pod uwagę, czy stosują się oni do międzynarodowych norm.

Należy szukać takich dostawców, którzy publikują szczegółowe informacje na temat sposobu prowadzenia przez nich działalności oraz przetwarzania danych.

5. Przyjrzyj się niezatwierdzonym zasobom IT



pracowników utworzyło co najmniej jedno konto (rejestracja w witrynie lub aplikacji związanej z pracą) bez angażowania działu IT[6].

„Shadow IT" występuje wtedy, gdy pracownik tworzy konto w chmurze bez autoryzacji lub świadomości firmy. Konta takie wydają się na pozór nieszkodliwe: będzie to na przykład narzędzie do sprawdzania gramatyki. Jednak te konta stwarzają luki w zabezpieczeniach nawet w najbardziej rygorystycznych konfiguracjach zabezpieczeń.

Ludzie często akceptują warunki korzystania z aplikacji bez ich wcześniejszego przeczytania i pełnego zrozumienia tego, jakie uprawnienia nadają. Tradycyjne rozwiązania z zakresu bezpieczeństwa sieci nie były opracowywane pod kątem ochrony danych w aplikacjach SaaS i nie zapewniają wglądu w to, w jaki sposób pracownicy korzystają z chmury.

Nie powinniśmy zwalczać motywacji stojących za tworzeniem niezatwierdzonych zasobów IT. Zapewnienie ludziom i zespołom możliwości korzystania z aplikacji w chmurze, które są najlepiej dostosowane do ich rodzaju pracy, pomoże wydajności i innowacyjności. Należy jednak zwiększyć widoczność, kontrolę oraz ochronę przed zagrożeniami tych niezatwierdzonych aplikacji SaaS. Będą to pierwsze kroki na drodze do zarządzania ryzykiem sprzyjające już rozpoczętej transformacji cyfrowej w Twojej firmie.

[6] „New research reveals risks of shadow IT" (Nowe badania ujawniają zagrożenia związane z niezatwierdzonymi zasobami IT), 1password, luty 2020 r.

Wypróbuj to

Uzyskaj potrzebne informacje. Broker zabezpieczeń dostępu do chmury (CASB, Cloud Access Security Broker) zapewnia organizacji szczegółowy obraz tego, w jaki sposób jej pracownicy korzystają z chmury:

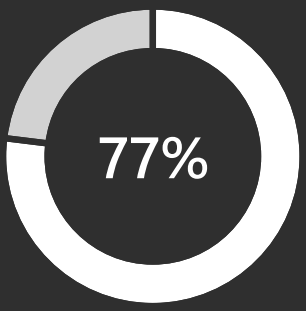
- Których aplikacji w chmurze używają pracownicy?
- Jakie ryzyko stwarzają te aplikacje dla organizacji?
- W jaki sposób jest uzyskiwany dostęp do tych aplikacji?
- Jakiego rodzaju dane są wysyłane do tych aplikacji i udostępniane za ich pośrednictwem?
- Jak wygląda ruch związany z pobieraniem/przesyłaniem?
- Czy istnieją jakiekolwiek nieprawidłowości w zachowaniu użytkowników, takie jak nieudane próby logowania, podejrzane adresy IP?

Najważniejsze wnioski

Brokerzy zabezpieczeń dostępu do chmury mogą dać Ci szczegółowy obraz tego, w jaki sposób pracownicy korzystają z chmury.

Dzięki zwiększeniu widoczności można ustalać zasady, które pozwolą śledzić i kontrolować sposób, w jaki pracownicy korzystają z tych aplikacji.

6. Zapewnij ochronę i wydajność



CISO twierdzi, że są zawieszeni pomiędzy umożliwianiem ludziom swobodnej pracy a zapewnianiem bezpieczeństwa w przedsiębiorstwie[7].

Obecnie dane wymykają się spod kontroli bardziej niż kiedykolwiek, ponieważ są udostępniane przez pracowników, partnerów biznesowych i klientów. Pomaga to zwiększyć wydajność i innowacyjność, ale może też nieść ze sobą poważne konsekwencje, jeśli dane wrażliwe znajdą się w niewłaściwych rękach. Specjaliści ds. bezpieczeństwa muszą w zgodzie z przepisami prawa chronić dane przechowywane w wielu miejscach i udostępniane na całym świecie.

Pracownicy tolerują utrudnienia, dopóki nie znajdą obejścia wymagań narzuconych przez zabezpieczenia. Najlepszą metodą dbania o bezpieczeństwo danych jest ich klasyfikowanie i szyfrowanie, które nie utrudnia produktywnego używania informacji ani ich udostępniania. Błędów ludzkich można uniknąć, automatyzując procesy klasyfikacji danych. Narzędzia potrafią rozumieć kontekst danych, na przykład numery kart kredytowych w pliku, czy stopień poufności danych, który jest związany z ich pochodzeniem. Po oznaczeniu odpowiednimi etykietami można automatycznie stosować do danych wrażliwych oznaczenia wizualne, takie jak nagłówki i stopki czy znaki wodne, oraz ochronę, na przykład szyfrowanie, uwierzytelnianie czy prawa do ich używania.

[7] „IT security hindering productivity and innovation, survey shows" (Badania pokazują, że zabezpieczenia IT ograniczają wydajność i innowacyjność), ComputerWeekly.com, październik 2017 r.

Wypróbuj to

Poznaj szczegóły. Zespoły ds. bezpieczeństwa powinny mieć możliwość monitorowania działań dotyczących udostępnianych plików, które są ściśle poufne lub mają strategiczne znaczenie dla firmy, a w razie potrzeby także odwoływania dostępu do nich.

- Takie stałe zabezpieczenia są powiązane z danymi i zapewniają ich nieustanną ochronę — niezależnie od tego, gdzie są przechowywane lub komu zostały udostępnione.
- System zarządzania dostępem bazujący na tożsamości ułatwia śledzenie wysoce poufnych plików.

Najważniejsze wnioski

Bezpieczeństwo na poziomie danych jest obowiązkiem każdego.

Klasyfikacja i oznaczanie danych powinny następować w momencie ich tworzenia. Zespoły zajmujące się bezpieczeństwem powinny mieć możliwość monitorowania działań na plikach oraz podejmowania szybkich akcji.

Microsoft

Podsumowanie

Wielowymiarowy charakter cyberzagrożeń sprawia, że rozwiązywanie tylko wybranych problemów związanych bezpieczeństwem to za mało. Potrzeby każdej firmy w zakresie bezpieczeństwa są wyjątkowe, ale wszystkie firmy stoją przed takimi samymi wyzwaniami i ponoszą taką samą odpowiedzialność za ochronę swoich danych, ludzi i systemów, a także za wprowadzanie innowacji i rozwój. Obecnie firmy potrzebują elastycznych platform zabezpieczeń wspierających cyfrową transformację i opartych na kompleksowych strategiach bezpieczeństwa, które uwzględniają technologie, procesy i programy szkoleniowe.

Jeśli jeszcze nie masz danych w chmurze, nadszedł czas, aby poznać jej zalety w zakresie bezpieczeństwa. Microsoft 365 to kompletne i inteligentne rozwiązanie dla firm różnych wielkości, które wspiera cyfrową transformację, zapewniając bezpieczeństwo i zgodność z przepisami na każdym poziomie.

Dowiedz się więcej z tej bezpłatnej, kompleksowej serii webinarów.

Obejrzyj serię >