Bitdefender

Jak poprawić cyberbezpieczeństwo w firmie – 10 rad od zespołu Bitdefender

28.09.2023

Współczesna era technologiczna wprowadziła ekscytujące zmiany, które zapoczątkowały wiele nowych możliwości na przyszłość, ale wraz z nimi istnieją czynniki ryzyka, które mogą stanowić zagrożenie dla aktywów, operacji i zasobów firm oraz organizacji. Nawet przy pomocy elitarnych służb bezpieczeństwa poruszanie się po zmieniającym się krajobrazie zagrożeń nie jest prostym zadaniem. Każda organizacja, niezależnie od wielkości i rynku, na którym działa, jest narażona na ryzyko stania się ofiarą cyberataku. Mając to na uwadze, Zespół Bitdefender przygotował listę 10 skutecznych metod zwiększania bezpieczeństwa w firmach, organizacjach i instytutach rządowych.

10 rad, dzięki którym poprawisz cyberbezpieczeństwo w swojej firmie

Stosuj najlepsze praktyki dotyczące bezpieczeństwa w Internecie

Trojany dołączane do wiadomości e-mail, fałszywe strony logowania typu phishing i gromadzenie informacji za pomocą socjotechniki, to tylko niektóre z popularnych sposobów wykorzystywanych przez cyberprzestępców do tego, aby wykraść dane Twojej firmy. Jednak pamiętajmy o tym, że wiele z najbardziej niszczycielskich naruszeń bezpieczeństwa wynika z lekceważenia prostych, najlepszych praktyk, które mogą pomóc chronić środowisko komputerowe organizacji i użytkowników, którzy w niej działają.

Zalecenia Bitdefender:

- Uświadamiaj o ryzyku jakie niesie za sobą klikanie do łączy do nieznanych źródeł? Przypominaj im, aby nigdy nie pobierali oprogramowania z niezaufanych źródeł.

- Wydaj wytyczne dotyczące mediów społecznościowych, aby żadne wrażliwe informacje organizacji nie były udostępniane kanałami niezaszyfrowanymi.

Wykonuj rutynowe testy na wypadek kampanii phishingowej

Nawet zagrożenia tak znane, jak dawny trojan bankowy „EMOTET”, w celu dystrybucji wykorzystują taktykę poczty elektronicznej i phishingu. Dobrze spreparowane e-maile phishingowe stają się coraz trudniejsze w wykryciu dzięki przyjęciu narzędzi i technik, w tym generowania treści AI, a także załączników plików zawierających makra. Wciąż jednak powszechne, ukierunkowane i nieukierunkowane kampanie phishingowe

pozostają podstawową taktyką dla grup hakerskich, które wykorzystują dezinformację oraz oszustwo, aby nakłonić niczego niepodejrzewających użytkowników do zapewnienia dostępu do informacji i infrastruktury firm.

Zalecenia Bitdefender:

- Organizuj wewnętrzne symulacje kampanii phishingowych, które będą szerzyć świadomość o cyberzagrożeniach tego typu i wyposażają Twoich pracowników w praktyczną wiedzę i doświadczenie, jak sobie z nimi radzić.

- Rozważ wdrożenie dodatkowego oprogramowania i usług do ochrony poczty e-mail.

Prowadź bieżącą listę zatwierdzonych aplikacji

Pod koniec 2020 roku odkryto, że twórca powszechnie używanej platformy oprogramowania – SolarWinds Orion – został ofiarą cyberataku. Każdy użytkownik oprogramowania z kilku branż był potencjalnie podatny na ataki typu backdoor o nazwie SUNBURST. Organizacje musiały włożyć wiele wysiłku w sprawdzenie swoich systemów pod kątem obecności wersji oprogramowania, które zostało zhakowane.

Ograniczając liczbę unikalnych aplikacji w środowisku organizacji, można uniknąć niepotrzebnych komplikacji wynikających z podobnych potencjalnych luk w oprogramowaniu. Warto określić także oczekiwania

co do tego, jaki rodzaj funkcjonalności aplikacji jest akceptowany w miejscu pracy, co pomaga w dalszym ograniczaniu innych nieoczekiwanych aktywności w środowisku.

Zalecenia Bitdefender:

- Rozważ prowadzenie repozytorium aplikacji zawierającego wyłącznie oprogramowanie aplikacyjne firmy lub organizacji niezbędne do codziennego działania.

- Monitoruj nieautoryzowane oprogramowanie i ustalaj wytyczne dotyczące „Zasad dopuszczalnego użytkowania", aby wzmocnić jedność organizacji.

- Unikaj polegania na przestarzałym oprogramowaniu, które może narazić organizację na ryzyko.

Aktualizuj swoje środowisko

Niezależnie od tego, czy Twoja organizacja korzysta tylko ze stacji roboczych, serwerów, laptopów, czy też urządzeń mobilnych, aktualizowanie systemów operacyjnych wszystkich urządzeń i powszechnie używanego oprogramowania organizacyjnego za pomocą najnowszych poprawek zabezpieczeń to jeden z najprostszych sposobów wzmocnienia ochrony przed złośliwym oprogramowaniem, włamaniami do sieci i innymi niepożądanymi problemami związanymi z cyberbezpieczeństwem.

Zalecenia Bitdefneder:

- Zalecaj pracownikom regularne przeprowadzanie aktualizacji oprogramowania.

- Rozważ automatyczne zarządzanie poprawkami za pomocą skryptów Active Directory i PowerShell.

- Korzystaj z aplikacji zapewniających zgodność z zasadami, takich jak Microsoft Intune, aby mieć pewność, że użytkownicy przestrzegają procedur aktualizacji organizacji i wymagań dotyczących wersji.

Nadawaj uprawnienia administratora tylko dla wykwalifikowanych pracowników

Nie każdy pracownik w organizacji potrzebuje funkcjonalności dla zaawansowanych użytkowników. Weźmy na przykład skromnych przedstawicieli handlowych; prawie każda firma ich ma i zwykle działają podobnie na każdym rynku pionowym. Rola sprzedawcy zazwyczaj wiąże się z potrzebą komunikacji z dostawcami lub klientami spoza organizacji, często przy użyciu korespondencji e-mailowej i załączników plików. Jest to idealna droga dla zagrożeń, takich jak dokumenty biurowe zawierające makra, które mogą pobierać i wykonywać skrypty PowerShell.

Biorąc pod uwagę, że większość przedstawicieli handlowych nie potrzebuje dostępu do programu PowerShell, jest to jeden przypadek, w

którym można łatwo uniknąć zagrożenia. Jest to doskonały przykład tego, jak ograniczenie dostępu do określonych ról w organizacji może pomóc zmniejszyć ryzyko skutecznego naruszenia.

Zalecenia Bitdefender:

- Użyj ustawień zasad grupy, aby ograniczyć lub wyeliminować nieograniczone uprawnienia użytkowników i, jeśli to możliwe, używaj zasad najmniejszych uprawnień.

- Jeśli to możliwe, rozważ również utworzenie lokalnych użytkowników niebędących administratorami.

- Staraj się oddzielać role w organizacji, aby ograniczyć dostęp do narzędzi i informacji.

Zadbaj o podstawowe zasady cyberbezpieczeństwa, a jeśli to koniecznie wdrąż dodatkowe warstwy ochrony

Działanie w ramach centrum operacji bezpieczeństwa (SOC) zapewnia cenny wgląd w trendy, które mogą przynieść korzyści klientom pragnącym większego bezpieczeństwa. Jeden z najpowszechniejszych trendów przyjmuje formę ruchu bocznego, czyli taktyki, zgodnie z którą osoba atakująca – która uzyskała już dostęp do pojedynczego zaatakowanego punktu końcowego – wykorzystuje wyrafinowane techniki w celu uzyskania dalszego dostępu i poruszania się po całym środowisku.

Jeśli w środowisku znajduje się choćby kilka niemonitorowanych punktów końcowych, stanowi to punkt wejścia dla zaawansowanego, trwałego zagrożenia, a zanim SOC zda sobie sprawę z zagrożenia, to może ono rozpowszechnić się już w całej infrastrukturze firmy.. Ochrona punktów końcowych za pomocą skutecznego systemu antywirusowego to doskonały punkt wyjścia do ochrony organizacji, ale dodanie dodatkowych rozwiązań bezpieczeństwa, takich jak zarządzane wykrywanie i reagowanie, EDR i XDR może zwiększyć szanse na ochronę przed zagrożeniami bezpieczeństwa.

Zalecenia Bitdefender:

- Wdrażaj okresowe wewnętrzne kontrole środowiska, aby mieć pewność, że urządzenia są monitorowane i chronione przez oprogramowanie do wykrywania i reagowania na punkty końcowe (EDR).

- Sprawdź obecność kluczowych modułów i upewnij się, że na punktach końcowych zainstalowana jest najnowsza wersja.

- Rozważ zaporę obwodową dla publicznie dostępnych punktów końcowych serwerów lub zaporę aplikacji internetowej dla aplikacji zewnętrznych, które mogą obejmować portale logowania.

„Oprogramowanie i usługi zapobiegające phishingowi mogą pomóc w ograniczeniu niepożądanych próśb zewnętrznych o informacje i dostęp. Wymagaj połączenia VPN w przypadku dowolnej formy pracy zdalnej i

odradzaj korzystanie z niezabezpieczonych protokołów dostępu zdalnego, takich jak Secure Shell (SSH), protokołów przesyłania plików (FTP), protokołów pulpitu zdalnego (RDP) i bloków komunikatów serwera (SMB), które mogłyby zostać ujawnione w publicznym Internecie" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Egzekwuj rygorystyczne wymagania dotyczące haseł i wdrażaj uwierzytelnianie wieloskładnikowe

Może to być najbardziej banalne z wymienionych przez nas zagrożeń bezpieczeństwa, ale raporty firmy Bitdefender wskazują, że brak zunifikowanej, rygorystycznej polityki dotyczącej haseł jest bardzo częstą przyczyną skutecznych cyberataków na przedsiębiorstwa. Niestety większość pracowników podczas tworzenia swoich haseł przedkłada wygodę nad bezpieczeństwo oraz wykorzystują proste i krótkie kody. Wymagając rygorystycznych wymagań dotyczących haseł, można zmniejszyć ryzyko włamania się na konto użytkownika.

Uwierzytelnianie wieloskładnikowe (MFA) stało się nieocenionym, jeśli nie prawie niezbędnym dodatkiem do procedury bezpiecznego logowania do konta. W połączeniu z wymaganiami dotyczącymi silnych haseł można znacznie zmniejszyć ryzyko włamania się na konto użytkownika.

Zalecenia Bitdefender:

- Za każdym razem, gdy tworzone jest nowe konto, wymagaj

obowiązkowego resetowania hasła, aby wyeliminować używanie haseł domyślnych.
- Zniechęcaj użytkowników do używania tych samych haseł do wielu kont, usług lub oprogramowania.

- Ustaw wymagania dotyczące wielkości liter, znaków alfanumerycznych, długości i znaków specjalnych, aby zwiększyć złożoność haseł.

- Ustaw wymagania dotyczące wygaśnięcia haseł, aby mieć pewność, że użytkownicy resetują swoje hasła w regularnych i częstych odstępach czasu oraz sprawdzają podobieństwo do poprzednich haseł.

- W razie potrzeby zresetuj hasła, jeśli w wyniku wcześniejszego naruszenia zostanie wykryte naruszenie bezpieczeństwa konta.

- Rozważ wymagania usługi MFA dla swojej organizacji.

- Rozważ wdrożenie menadżera haseł dla pracowników Twojej firmy.

Stwórz politykę dotyczącą używania wymiennych urządzeń pamięci masowej

Wymienne urządzenia pamięci masowej stały się czymś w rodzaju współczesnego konia trojańskiego. Dlatego czasami najlepszym

podejściem jest ich całkowite unikanie. W przypadkach, gdy nie jest to możliwe, rozważ ich odkażanie po każdym użyciu.

Zalecenia Bitdefender:

- Rozważ udostępnienie alternatyw, takich jak firmowa witryna SharePoint lub rozwiązanie do przechowywania danych w chmurze.

- Po każdym użyciu należy odkażać wymienne urządzenia pamięci masowej.

- Rozważ zakazanie używania wymiennych urządzeń pamięci.

- Nie instaluj ani nie podłączaj wymiennych urządzeń pamięci masowej pochodzących z nieznanych lub niezaufanych źródeł.

Wdróż strategię tworzenia kopii zapasowych

Redundancja ma kluczowe znaczenie podczas odzyskiwania danych po każdej awarii, czy to związanej z IT, czy z cyberbezpieczeństwem. Podjęcie niezbędnych kroków w celu wdrożenia rozwiązania do tworzenia kopii zapasowych już dziś może pomóc uratować Twoją organizację w przyszłości. Zastanów się, jak i gdzie przechowywane są kopie zapasowe oraz w jaki sposób można je wdrożyć w przypadku incydentu bezpieczeństwa lub katastrofy.

Zalecenia Bitdefender:

- Rozważ skorzystanie z usługi tworzenia kopii zapasowych w chmurze.

- Regularnie wykonuj plany reagowania na cyberataki i katastrofy naturalne lub budowlane, aby zapewnić znajomość kluczowych interesariuszy, a także walidację procesów i procedur.

Nie zostawiaj urządzeń odblokowanych bez nadzoru

Może to również wydawać się oczywiste, ale dobre bezpieczeństwo fizyczne pomaga zapewnić dobre bezpieczeństwo cybernetyczne.

Zalecenia Bitdefender:

- Rozważ wyposażenie członków swojej organizacji w fizyczne zamki w celu zabezpieczenia urządzeń w dużych środowiskach korporacyjnych.

- Przypomnij członkom organizacji, aby przy wyjściu z biura zabezpieczyli swoje telefony służbowe lub niezależne mobilne stacje robocze.

- Rozważ funkcję BitLocker lub podobne szyfrowanie, aby chronić dane w spoczynku.

Wdrożenie 10 konkretnych kroków opisanych w tym artykule ma fundamentalne znaczenie dla wzmocnienia wysiłków Twojej organizacji w zakresie cyberbezpieczeństwa. Proaktywne podejście, obejmujące ciągłe monitorowanie i szybką reakcję, zapewnia ochronę cennych aktywów i płynną kontynuację pracy Twojej firmy.

Źródło: https://bitdefender.pl/jak-poprawic-cyberbezpieczenstwo-w-firmie/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 28.09.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.