Bitdefender

Dlaczego wszystkie firmy powinny inwestować w zabezpieczenia warstwowe

21.06.2023

Cyberataki mogą przytrafić się Twojej firmie na wiele różnych sposobów. W przeszłości zapewnienie odpowiedniego poziomu cyberbezpieczeństwa było prostsze. Przypominało to ochronę drzwi wejściowych do domu. Wystarczyło zainstalować skuteczny system antywirusowy, aby uniemożliwić intruzowi dostanie się do Twojej sieci. Aktualnie krajobraz cyberzagrożeń całkowicie się zmienił, a organizacje potrzebują więcej niż jednego rozwiązania, aby być w pełni zabezpieczone i móc zapobiegać cyberatakom, bronić się przed hakerami.

Zabezpieczenia wielowarstwowe

Najlepszym sposobem dla firm na zapewnienie skutecznej ochrony przed cyberzagrożeniami jest zastosowanie zabezpieczeń warstwowych. Oznacza to wiele narzędzi, systemów, a także procesów, które nakładają

się na siebie oraz zapewniają zapobiegawcze i proaktywne cyberbezpieczeństwo. Te narzędzia i systemy powinny się wzajemnie uzupełniać oraz informować, aby stworzyć bezpieczniejsze środowisko. Jednak dlaczego właściwie zabezpieczenia warstwowe są ważne i jak organizacje mogą je wdrożyć?

Firmy każdej wielkości muszą chronić się bardziej niż kiedykolwiek

Hakerzy często skupiają się na określonej części sieci firmy, aby ją skompromitować i potencjalnie włamać się do jej systemów. Obszar ten jest znany jako powierzchnia ataku. Im większa powierzchnia ataku, tym większe ryzyko ponosi firma, a także tym więcej musi zrobić, aby się obronić i zabezpieczyć.

W ciągu ostatnich kilku lat średnia powierzchnia ataku wzrosła w dużej mierze ze względu na zwiększenie zakresu cyfrowego środowiska przeciętnej firmy. Obecnie często zawiera ono między innymi:

- Punkty końcowe, takie jak laptopy, serwery, urządzenia biurowe oraz urządzenia zdalne i prywatne łączące się z siecią firmą (np. telefon komórkowy pracownika).
- Chmurę internetową. Podobnie jak dostawcy usług w chmurze, w tym narzędzia takie jak Office 365, Slack, Zoom i Dysk Google – mniejsze firmy najczęściej korzystają z usług opartych na chmurze i partnerów w celu usprawnienia usług i działów.
- Urządzenia Internetu Rzeczy (IoT), takie jak inteligentne ekrany, lodówki, drukarki, aparaty fotograficzne, które są podłączone do Internetu i mogą nie zapewniać najlepszych zabezpieczeń.

- Pracownicy. To nadal najsłabsze ogniwo, jeśli chodzi o obronę firmy przed cyberprzestępcami – każda osoba może stanowić potencjalne zagrożenie.
- Wiele lokalizacji (czy pracownicy zdalni lub hybrydowi) wymaga zwiększonych środków bezpieczeństwa, zwłaszcza jeśli dane są przechowywane i/lub przesyłane między tymi lokalizacjami.

Zaawansowane cyberataki wymagają czegoś więcej niż tylko zabezpieczenia punktów końcowych. Ze względu na wszystkie te obszary, które złoczyńcy mogą wykorzystać do włamań do firm, każdy rodzaj biznesu, zarówno duży, jak i mały, jest zagrożony bardziej zaawansowanymi atakami. Tego rodzaju cyberniebezpieczeństwa (poza tradycyjnymi punktami końcowymi) wykorzystują luki w zabezpieczeniach i często są przeprowadzane z większą precyzją. Hakerzy nierzadko atakują luki w zabezpieczeniach popularnych aplikacji opartych na chmurze lub infrastrukturę chmurową firmy, mając na celu bezpośredni dostęp do wrażliwych danych i zasobów.

Jak organizacje mogą budować kompleksowe zabezpieczenia za pomocą warstw?

Aby uwzględnić całą potencjalną powierzchnię ataku firmy, ważne jest zbudowanie kompleksowego bezpieczeństwa za pomocą warstwowej strategii cyberbezpieczeństwa, która obejmuje kontrole zapobiegawcze, proaktywne działania, wykrywanie i możliwości reagowania. Wiele z tych możliwości wykracza poza to, co oferują tradycyjne systemy antywirusowe. Do najważniejszych strategii należy zapewnienie:

Widoczności

Świadomość wszystkich komponentów tworzących środowisko cyfrowe może pomóc w jego ochronie. Pomyśl o tym jak o znajomości wszystkich punktów wejścia do domu i wiedzy, gdzie dokładnie znajdują się twoje bezpieczne i najważniejsze dokumenty.

Wykrycia

Gdy uzyskasz lepszy wgląd w swoje środowisko, możesz wdrożyć narzędzia, takie jak wykrywanie i reagowanie na punkty końcowe (EDR) oraz rozszerzone wykrywanie i reagowanie (XDR). Są to narzędzia analityczne, które obejmują całą Twoją sieć i dowolną infrastrukturę chmurową, aby właściwie identyfikować nieautoryzowanych użytkowników lub złośliwe ataki występujące w Twoim środowisku.

„EDR wykrywa incydenty bezpieczeństwa na poziomie punktu końcowego i dostarcza zespołowi informacji przydatnych w działaniu, umożliwiając im podjęcie odpowiednich kolejnych kroków w celu powstrzymania i usunięcia zagrożenia (lub pozostawienia go w spokoju, jeśli okaże się, że jest to łagodny alert). Z kolei XDR wykracza poza punkt końcowy i uwzględnia informacje dotyczące bezpieczeństwa z innych źródeł, w tym z chmury, co dodatkowo chroni infrastrukturę i zasoby firmy” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Hartowania

Hartowanie odnosi się do zestawu procesów, które zapewniają minimalizację ryzyka kompromisu lub ataku. Przykłady hartowania obejmują zarządzanie poprawkami — jest to proces dający pewność, że

wszystkie Twoje urządzenia, systemy, aplikacje i usługi działają z najnowszą wersją oprogramowania. Wzmocnienie obejmuje również ukierunkowane kontrole bezpieczeństwa oraz narzędzia, takie jak ochrona poczty e-mail, filtry antyspamowe, narzędzia antywirusowe, a także pełne szyfrowanie dysku, które chroni dane, nawet jeśli zostaną skradzione i wyjęte z sieci lub serwerów firmy.

Bezpieczeństwa w chmurze

Chmura stała się tak kluczowym elementem dla większości firm, że wymaga własnych środków bezpieczeństwa. Firmy muszą mieć sposoby na ochronę i zabezpieczenie oprogramowania takiego jak Office 365, One Drive, Google Apps i inne. Są to ukierunkowane narzędzia bezpieczeństwa, które mogą pomóc zabezpieczyć pliki, serwery oraz kontenery w chmurze.

Odpowiednich protokołów bezpieczeństwa w razie ataku

To, jak reagujesz na potencjalny atak, ma takie samo znaczenie, jak to, co robisz, aby mu zapobiec. Narzędzia do reagowania mogą pomóc w usunięciu dostępu hakera do sieci lub zminimalizowaniu szkód, jakie może on wyrządzić Twojej firmie. Są to narzędzia takie jak EDR, XDR, a także usługi reagowania od partnerów, którzy zapewniają zarządzane wykrywanie i reagowanie lub zarządzanych dostawców zabezpieczeń. Zlecając pracę zespołowi ekspertów dostępnych 24 godziny na dobę, 7 dni w tygodniu, będziesz w stanie reagować znacznie szybciej.

Firm zewnętrznych

Zbudowanie kompleksowego działu bezpieczeństwa jest trudne,

ponieważ wymaga wielu zasobów. Potrzebnych jest nie tylko wiele narzędzi i technologii bezpieczeństwa, ale także wykwalifikowany personel ds. cyberbezpieczeństwa, który mógłby zinterpretować wszystkie informacje, alerty i dane wysyłane do organizacji za pomocą tych narzędzi.

Znalezienie odpowiednich pracowników i narzędzi także jest zadaniem bardzo trudnym, dlatego warto rozważyć współpracę z kluczowym dostawcą cyberbezpieczeństwa. Wykorzystanie EDR i XDR w celu kompleksowego zrozumienia Twojego środowiska IT może pomóc w lepszej ochronie firmy przed zaawansowanymi atakami.

Firmy powinny również rozważyć współpracę z dostawcą zarządzanych usług bezpieczeństwa (MSSP), który może działać jako zewnętrzny dział bezpieczeństwa cybernetycznego. Dostawcy ci często korzystają z narzędzi i technologii oraz szybko reagować na zagrożenia, aby zapobiec wszelkim szkodom.

Chociaż zbudowanie kompleksowego cyberbezpieczeństwa może być trudne, organizacje mają do dyspozycji wiele opcji. Najważniejsze jest to, by nie poprzestać na jednym narzędziu zapobiegawczym, np. podstawowym antywirusie. W przeciwnym razie zostawiasz swój dom szeroko otwarty.

Źródło:https://bitdefender.pl/dlaczego-wszystkie-firmy-powinny-inwestowac-w-zabezpieczenia-warstwowe/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 21.06.2023

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.