Praca hybrydowa. Jest wygodnie, a musi być bezpiecznie

Patronat Business Insider Polska
6 maja 2022, 16:11

Według raportu Accenture liczba cyberataków w 2021 r. wzrosła o 31 proc. w porównaniu do 2020. W tym roku – w czasach niepewności gospodarczej i geopolitycznej – nic nie wskazuje na to, aby ataki miały się uspokoić.

Przewiduje się, że do 2025 r. koszty wywołane cyberprzestępczością osiągną 10,5 biliona dolarów rocznie. Dla porównania, w 2015 r. było to 3 biliony. I chodzi o biliony, nie miliardy. Już teraz, jak podają raporty branżowe, cyberprzestępczość kosztuje firmy na całym świecie blisko 2 miliony dolarów na minutę.

Firmy, pracownicy i klienci są atakowani każdego dnia, a same cyberzagrożenia są bardzo zróżnicowane. Ryzyko rośnie, tym bardziej że mamy obecnie trend pracy hybrydowej. Coraz więcej osób pracuje zdalnie z domu, korzystając na co dzień z urządzeń prywatnych, albo nie stosując się do polityki bezpieczeństwa rekomendowanej przez pracodawcę.

- **Pracownicy powinni być świadomi zagrożeń, jakie wynikają z cyberataków**
- **Szyfrowanie danych i stosowanie uwierzytelniania dwu- lub wieloskładnikowego to podstawa**
- **Firmy dopuszczające pracę zdalną powinny rozważyć wdrożenia systemów EMM do zarządzania urządzeniami mobilnymi**
- **Bardzo wskazane jest także podejście zero-trust**

Podczas pierwszego cyklu Business Insider TRENDS 2022 - Cybersecurity poprosiliśmy ekspertów o porady dla firm, które dopuszczają pracę zdalną i chcą zadbać o wysoki poziom bezpieczeństwa. Marek Psiuk, dyrektor ds. technologii w No Fluff Jobs, zauważył, że są co najmniej dwa aspekty, o które powinniśmy zadbać, gdy chodzi o bezpieczeństwo. — Po pierwsze, nasi pracownicy powinni być świadomi zagrożeń, jakie wynikają z cyberataków — powiedział. I dodał: — Po drugie, **musimy pokazywać, jak spełnianie poszczególnych elementów polityki bezpieczeństwa naszej firmy wpływa na ich bezpieczeństwo, i co się stanie, jeśli te elementy nie będą spełnianie.**

Praca zdalna zapewnia wysoki komfort, ale sprawia też, że zespoły IT muszą odpowiedzieć na wiele nowych wyzwań i wymagań, by zapewnić bezpieczeństwo. **Eksperci zalecają, aby stosować szyfrowanie danych oraz protokoły bezpieczeństwa takie jak uwierzytelnianie dwu- lub wieloskładnikowe** (multi-factor authentication - MFA). Do tego wskazana jest szczegółowa kontrola dostępu oraz stosowna polityka bezpieczeństwa, z konkretnymi procesami i procedurami operacyjnymi.

Wszelkie dane chronione hasłem lub aplikacje wymagające nazwy użytkownika i hasła w celu uzyskania dostępu nie są tak bezpieczne, jak mogłyby być. Poziom bezpieczeństwa na pewno znacznie wzrośnie, gdy zaczniemy stosować uwierzytelnianie MFA, które pomoże w ochronie danych firmy, do których pracownicy uzyskują dostęp za pośrednictwem dowolnej sieci. Skonfigurowanie tych protokołów – zwłaszcza dla pracowników zdalnych i podróżujących – jest konieczne, jeśli chcemy zapewnić sobie ochronę.

Poza tym, zespoły IT powinny też zatroszczyć się o stosowanie odpowiednich uprawnień. **Chodzi o możliwość udostępniania danych w zależności od potrzeb i tylko dla tych osób, które faktycznie ich potrzebują**. To konieczne, jeśli chcemy zapewnić bezpieczeństwo w dzisiejszym, rozproszonym świecie biznesu. Ograniczanie dostępu powinno być możliwe na podstawie klasyfikacji takiej jak użytkownik, grupa, adres IP, czy adres MAC.

Strategie dla hybrydowego modelu pracy

W przypadku gdy członkowie zespołu często pracują na home office, a w dodatku używają prywatnych urządzeń do realizacji zadań, utrzymanie bezpiecznego środowiska jest bardziej złożone. Wiele organizacji dopuszcza jednak takie możliwości, oferując program BYOD (bring your own device - przynieś własne urządzenie).

Niezależnie od stosowanych aplikacji i usług online, warto stworzyć własną politykę bezpieczeństwa, obejmującą aspekt BYOD. Jakich reguł powinniśmy przestrzegać? Ważne jest, aby nie pominąć rdzenia sieci, gdzie możemy określić reguły ochrony i dostępu, czy też zablokować ruch związany ze szkodliwym oprogramowaniem. **Reguły ochrony i dostępu powinny opierać się na rozpoznawaniu i powstrzymywaniu prób ataków, blokowaniu złośliwego oprogramowania, a także kontroli ruchu charakterystycznego dla poszczególnych aplikacji.**

Polityka powinna też obejmować konkretne poziomy dostępu, np. z urządzenia prywatnego pracownik nie będzie mógł zalogować się do intranetu. Jednocześnie dokument ten powinien jasno informować pracowników o tym, na co mogą liczyć, gdy korzystają z danego urządzenia.

Bardzo dobrym sposobem na poprawę bezpieczeństwa jest również wdrożenie systemu EMM (Enterprise Mobile Management), który służy do zarządzania urządzeniami mobilnymi. Systemy EMM pozwalają na tworzenie m.in. indywidualnych polityk użytkowania, zgodnie z rekomendacjami specjalistów IT naszej firmy. Dla przykładu możemy zabronić korzystania z konkretnych aplikacji, czy też wymuszać aktualizacje zabezpieczeń.

Jednocześnie w przypadku pracy zdalnej ważna jest dobra higiena bezpieczeństwa. Poza wspomnianymi rozwiązaniami **powinniśmy zapewnić również dostęp do zasobów firmowych za pośrednictwem sieci VPN, a także cykliczne szkolenia z cyberzagrożeń**.

Bartosz Kozłowski, współzałożyciel Sagenso, wyjaśnia, o czym firmy najczęściej zapominają, jeśli chodzi o cyberbezpieczeństwo:

Zero-trust, czyli zaufanie na warunkowym

"Nie ufaj w ciemno, zawsze weryfikuj" - tak można podsumować zasadę zero-trust, której przestrzega coraz więcej firm. **Podejście zero-trust ogranicza dostęp do zasobów cyfrowych za pomocą ściśle wymuszonych procesów weryfikacji tożsamości i urządzeń**. Mamy tutaj do czynienia z zabezpieczeniem tożsamości ZTI (zero-trust identity), a także dostępu ZTA (zero-trust access). Tego typu rozwiązania zapewniają, że żadne urządzenie lub użytkownik nie jest "domyślnie zaufany", niezależnie od tego, gdzie przebywa i jakie zajmuje stanowisko w firmie.

Jeśli wprowadzimy strategię zero-trust, ograniczymy dostęp do zasobów wyłącznie zweryfikowanym użytkownikom i urządzeniom. To z kolei **znacznie podniesie poziom bezpieczeństwa**. Co więcej, po domyślnej weryfikacji dana osoba uzyska dostęp tylko do tych zasobów czy segmentów sieci, które są jej niezbędne. To również minimalizuje ryzyko, że mogłoby dojść do jakichś naruszeń danych.

Marek Szustak, ekspert ds. cyberbezpieczeństwa w eSky, wyjaśnia, z jakimi cyberzagrożeniami firmy nie radzą sobie najbardziej:

Praca zdalna niesie ze sobą wiele zagrożeń, które mogą mieć poważne konsekwencje. Ekspozycja na potencjalne cyberzagrożenia jest wysoka i musimy mierzyć się z takimi wyzwaniami jak:

· **Phishing:** wysyłanie wiadomości e-mail lub innych komunikatów w celu zachęcenia pracowników do pobrania złośliwego oprogramowania, które zbiera poufne dane

· **Ransomware:** złośliwe oprogramowanie, które infekuje systemy przed zażądaniem zapłaty (okupu)

· **Spyware:** oprogramowanie szpiegujące przeznaczone do gromadzenia danych, z których mogli następnie korzystać oszuści lub konkurenci

· **Ataki dnia zerowego (zero-day):** ataki skupiające się w szczególności na niezałatanych systemach operacyjnych i aplikacjach, które mogą być trudne do zdalnego monitorowania

· **Kradzież danych:** najczęściej kradzież danych logowania, w celu uzyskania dostępu do baz danych klientów i pracowników

· **Sabotaż:** nienadzorowani pracownicy celowo lub nieświadomie niszczą aktywa firmy

Cyberatak wcześniej czy później nastąpi – to niemal pewne. Starajmy się przestrzegać zasad bezpieczeństwa i wdrożyć praktyki polecane przez ekspertów.

Inne źródła:

BI: Co jest niezbędne, kiedy pracownicy pracuja zdalnie a chcemy firmie zapewnić wysoki poziom bezpieczeństwa?

BI: Z jakimi cyberzagrożeniami firmy nie radzą sobie najbardziej?

BI: O czym firmy najczęściej zapominają, jeśli chodzi o cyberbezpieczeństwo?

Czy można "przesadzić" z cyberbezpieczeństwem?