Cyberhigiena – nie dajmy się hakerom!

Funkcjonujemy w czasach, gdy nasze życie online i offline stale się przeplata, co chętnie wykorzystują cyberprzestępcy. Jak chronić swoje dane oraz poufne informacje firmy? Czy działania, które podejmujemy w tym celu, są skuteczne? Warto to przeanalizować, mając z tyłu głowy stwierdzenie, że każdy system jest tak bezpieczny, jak jego najsłabsze ogniwo.

Cyberhigiena to zbiór dobrych praktyk, których celem jest zabezpieczenie użytkowników, urządzeń, sieci i danych przed zagrożeniami, jakie niosą ze sobą cyberataki. Organizacje i specjaliści IT przestrzegają zasad cyberhigieny, by zapobiec naruszeniom danych oraz innym niepożądanym sytuacjom związanym z bezpieczeństwem. Koncepcję można porównać do higieny osobistej. Tyle że w trosce o dobre zdrowie i nienaganny wygląd nierzadko z aptekarską dokładnością liczymy kalorie, wybieramy produkty spożywcze, wylewamy siódme poty na siłowni czy przyjmujemy suplementy na piękne włosy i mocne paznokcie. Wszystko po to, by uchronić się przed przykrymi dolegliwościami. A ile czasu i energii jesteśmy w stanie poświęcić, by zadbać o swoje bezpieczeństwo w cyberprzestrzeni, która obecnie jest przecież nie mniej istotna?

Chroń swoją cyfrową tożsamość

Największym zagrożeniem dla cyfrowego bezpieczeństwa są użytkownicy, czyli my sami. Jak to możliwe? Ponieważ nie przestrzegamy podstawowych zasad, które mogłyby nas uchronić przed atakami hakerskimi. Istotnym elementem jest tworzenie silnych haseł, które będą trudne do złamania (składających się z małych i wielkich liter oraz znaków specjalnych). Internauci notorycznie używają również jednego hasła do logowania na różnych portalach, co sprawia, że jeśli dojdzie do włamania na jedno konto, zagrożone są także pozostałe. Można temu łatwo przeciwdziałać poprzez wykorzystywanie np. menedżera haseł. Za każdym razem, gdy zarejestrujemy się na innej platformie, automatycznie wygeneruje ono nowe hasło i przechowa je w swoich formularzach. Dostępne są również mechanizmy uwierzytelniania wieloskładnikowego w postaci weryfikacji tekstowej lub SMS-owej.

Najskuteczniejszą bronią przed cyberatakami jest stosowanie systemów antywirusowych ze sprawdzonych źródeł. Dodatkowo należy pamiętać o tym, aby aktualizować oprogramowania na komputerze i w telefonach. Warto logować się do wszystkich urządzeń za pomocą biometrii. Kod PIN również jest zabezpieczeniem, ale odcisk palca czy skanowanie twarzy ma wyższą skuteczność.

Dawniej i dziś

Praca zdalna i hybrydowa na dobre zagościły w polskich domach. Firmy coraz częściej mają świadomość, że oferowanie elastycznej formy zatrudnienia jest najważniejszym czynnikiem, który pozwala zatrzymać najlepszych pracowników i przyciągnąć nowych. Tymczasem jak wynika z badań[1], tylko 39% ankietowanych firm ma odpowiednią infrastrukturę (opartą na

[1] https://info.zscaler.com/resources-industry-reports-state-of-zero-trust-transformation-2023

Zero Trust lub VPN) do obsługi bezpiecznego hybrydowego środowiska pracy, a kolejne 41% albo nie rozpoczęło jej wdrażania, albo nie ma tego w planach. Podłączanie do firmowej sieci urządzeń używanych w pracy zdalnej należy wykonywać z dużą ostrożnością i zachowaniem zasad bezpieczeństwa.

Tradycyjna praca biurowa sprawiała, że szczególną uwagę przywiązywano do zabezpieczania wewnętrznych systemów i informacji przed atakami z zewnątrz. Firma odgrywała swego rodzaju rolę twierdzy z pracownikami i urządzeniami odgrodzonymi murem od reszty zewnętrznych zagrożeń. W ostatnich latach takie podejście już nie zdaje egzaminu, ponieważ w modelach hybrydowych pracownicy wykonują swoje obowiązku z domu, kawiarni, plaży czy biura. Użytkownicy oczekują dostępu do zasobów firmy z dowolnego miejsca w dowolnym czasie. Przedsiębiorstwa z kolei przechowują dane w chmurze i korzystają z platform dostępnych w publicznym internecie.

Zero Trust podstawą nowego środowiska pracy

We współczesnym świecie pełnym cyberzagrożeń zasada „ufaj, ale sprawdzaj" okazuje się już niewystarczająca. Nowy standard w zarządzaniu IT to model Zero Trust, czyli zero zaufania. Opiera się na założeniu, że bezpieczeństwo sieci już zostało naruszone, a wszyscy użytkownicy stanowią zagrożenie. Zatem nie ma tu miejsca na automatyczne zaufanie w stosunku do jakichkolwiek systemów lub użytkowników, bez względu na to, czy są oni wewnątrz sieci organizacji, czy poza nią.

Celem modelu Zero Trust jest ograniczenie ryzyka naruszenia danych poprzez eliminację zaufania jako punktu odniesienia dla strategii bezpieczeństwa. To oznacza, że każdy użytkownik, urządzenie lub system musi potwierdzić swoje uprawnienia za każdym razem, gdy próbuje uzyskać dostęp do zasobów. To zupełnie inne podejście w porównaniu do konwencjonalnych modeli bezpieczeństwa, które przyjmują, że wszystko wewnątrz sieci jest zaufane.

W modelu Zero Trust obowiązują następujące zasady bezpieczeństwa:

1. **Każdorazowa weryfikacja**: Każda próba dostępu do systemów, aplikacji lub danych musi być uwierzytelniona i autoryzowana.
2. **Minimalne uprawnienia**: Użytkownikom i systemom powinny być przydzielane tylko te uprawnienia, które są niezbędne do wykonania ich zadań. Gdy te zadania się kończą, uprawnienia powinny być cofane.
3. **Mikrosegmentacja sieci**: Sieć powinna być podzielona na małe segmenty, które mogą być kontrolowane i monitorowane oddzielnie. W przypadku ataku mikrosegmentacja może pomóc ograniczyć jego rozprzestrzenianie się na inne części sieci.
4. **Założenie stanu ciągłego zagrożenia**: Model Zero Trust zakłada, że atak może wystąpić w dowolnym momencie, a więc systemy bezpieczeństwa powinny być zawsze czujne i gotowe do reagowania.