TOMASZ ORŁOWSKI, KIEROWNIK DZIAŁU PRODUKTÓW ICT, NETIA SA

NA CZYM POLEGA KONCEPCJA ZERO TRUST

I DLACZEGO STAWIAJĄ NA NIĄ SPECJALIŚCI OD BEZPIECZEŃSTWA IT?

W świecie bezpieczeństwa IT nieustannie trwają poszukiwania skutecznych mechanizmów chroniących przed wyciekami danych. Tradycyjny model koncentrowania zabezpieczeń na brzegu sieci (filozofia budowania tzw. „zamku i fosy") po prostu się nie sprawdza. Mimo coraz większych wydatków na bezpieczeństwo IT, koszty firm, w związku z działalnością cyberprzestępców, dynamicznie rosną. Coraz większą popularność wśród ekspertów IT security zyskują technologie w modelu Zero Trust.

Model Zero Trust Network został stworzony w 2010 roku przez Johna Kindervaga. W ciągu kilku lat nieustannej walki z cyberprzestępczością i coraz bardziej wyrafinowanymi atakami, wielu CIO i CISO zdecydowało się na zmianę sposobu działania, a model Zero Trust dynamicznie zyskuje na popularności.

Zero Trust to koncepcja bezpieczeństwa skupiająca się na przekonaniu, że organizacje nie powinny automatycznie ufać czemukolwiek i komukolwiek wewnątrz lub na zewnątrz sieci. Zamiast tego muszą weryfikować wszelkie próby połączenia się z systemami przed udzieleniem do nich dostępu. Strategia wokół Zero Trust sprowadza się do tego, aby nikomu nie ufać. Mowa tu o odcięciu całego dostępu do adresów IP, maszyn, systemów, zasobów itp., dopóki sieć nie będzie wiedzieć, kim jest użytkownik (lub system) i czy posiada odpowiednie uprawnienia.

Model Zero Trust całkowicie dyskredytuje filozofię „zamku i fosy", w której organizacja skupiona jest na obronie brzegu sieci (perimeter) i zakłada, że wszystko, co znajduje się w środku, nie stanowi zagrożenia i nie podlega kontroli dostępu. Eksperci ds. bezpieczeństwa IT twierdzą, że podejście „zamek i fosa" nie działa, wskazując na fakt, że wiele wycieków danych ma miejsce w sytuacji, kiedy intruz, gdy tylko uzyska dostęp do korporacyjnego firewalla, jest w stanie poruszać się po systemach wewnętrznych bez większego oporu. Ale nie jest to jedyny powód coraz większego zainteresowania Zero Trust. Obecnie w większości przypadków sam „zamek" nie funkcjonuje w izolacji od pozostałej części świata IT. Firmowe centra danych nie obsługują wyłącznie zamkniętych sieci, ale utrzymują również aplikacje w publicznej chmurze, dostępne w modelu anytime, anywhere, również z publicznego Internetu.

Podejście Zero Trust opiera się na różnych istniejących technologiach i procesach zarządzania w celu zabezpieczenia środowiska informatycznego. Model zakłada wykorzystanie informacji o użytkownikach, ich lokalizacji i innych powiązanych danych, aby określić, czy można zaufać użytkownikowi, maszynie lub aplikacji żądającej dostępu do określonego systemu lub zasobu. Korzysta się przy tym z metod i rozwiązań, takich jak: uwierzytelnianie wieloskładnikowe, IAM, orkiestracja, analityka, szyfrowanie, scoring i uprawnienia systemu plików. Zero Trust wymaga również określenia zasad zarządzania dostępem, np. zapewnienie użytkownikom najniższego poziomu uprawnień, niezbędnego do wykonania potrzebnego zadania. Bezpieczeństwo sieci projektuje się więc od wewnątrz (poziom użytkownika), a nie od zewnątrz (zamek i fosa).

Zero Trust to ciągły proces i sposób myślenia o bezpieczeństwie, wymagający wkładania stałego wysiłku w rewizję stanu zabezpieczeń oraz wprowadzanie niezbędnych zmian i ulepszeń. Nie można przy tym zapomnieć, że w fundamentach bezpieczeństwa informacji najważniejsze miejsce zawsze zajmuje człowiek, wspomagamy przez technologię i procesy. Brak szkoleń w tematyce cyberbezpieczeństwa i ciągłego uświadamiania pracowników o czyhających zagrożeniach w przestrzeni cyfrowej, może zniweczyć wszelki trud oraz zmarnotrawić każde środki przeznaczone na zabezpieczenia, procesy oraz dokumentację formalną. Przejście na model Zero Trust powinno być integralną częścią strategii transformacji cyfrowej każdej firmy.

Dostępna na rynku oferta rozwiązań bezpieczeństwa IT daje dziś szeroki wybór spośród rozwiązań w formie usługi (as a service), bez konieczności inwestycji w dedykowane systemy. Ochrona może się rozciągać począwszy od zabezpieczenia łącza internetowego przez ISP, który może automatycznie oczyścić ruch internetowy, blokując szereg zagrożeń zanim dotrą one do klienta. Istnieje również szeroki wachlarz usług i rozwiązań chroniących sieć wewnętrzną firmy we wszystkich jej warstwach i na różnych potencjalnych wektorach ataku – od brzegu sieci, poprzez LAN, infrastrukturę serwerową, na komputerach i aplikacjach biznesowych kończąc.