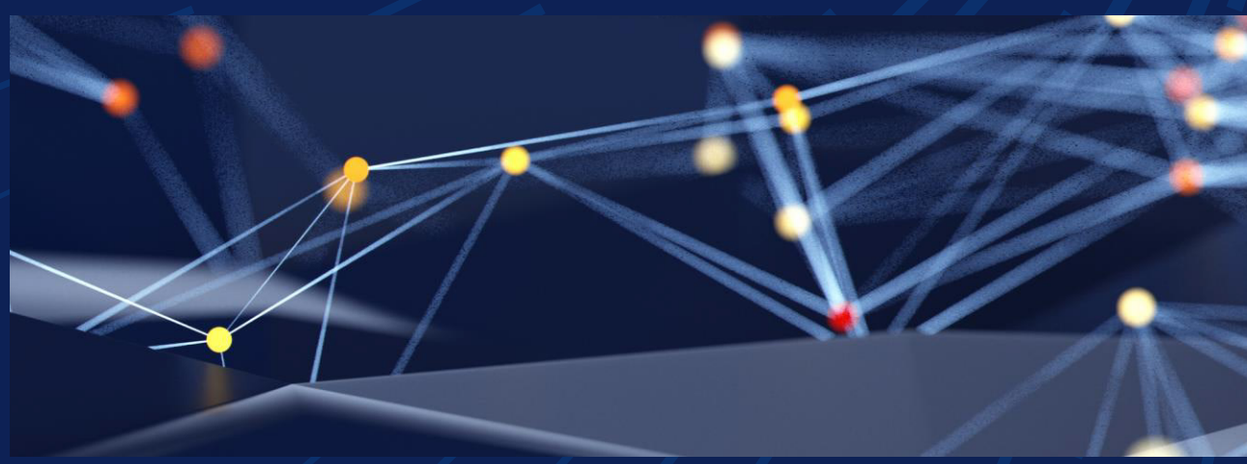
DELL Technologies

Przyszłość cyberbezpieczeństwa:

Adaptacja do nowej ery cyfrowej



Podczas gdy specjaliści ds. cyberbezpieczeństwa często skupiają się na zapobieganiu atakom i budowaniu planów odzyskiwania danych, ogólne środowisko bezpieczeństwa stale się rozwija. Dlatego ważne jest, aby planować przyszłość.

Patrząc w przyszłość, wyróżniają się trzy obszary: kryptografia postkwantowa, zmieniający się krajobraz regulacyjny i pojawiające się zagrożenia. Organizacje powinny działać teraz, planując i wdrażając rozwiązania w miarę ich dostępności.

Świt postkwantowej kryptografii

Komputery kwantowe obiecują transformację branż, oferując zdumiewającą moc obliczeniową zdolną do rozwiązywania problemów znacznie wykraczających poza możliwości komputerów klasycznych. Jednak ta sama moc może sprawić, że obecne metody kryptograficzne staną się przestarzałe. Algorytmy takie jak RSA i ECC, które stanowią podstawę wielu dzisiejszych bezpiecznych połączeń, mogą zostać złamane w ciągu kilku sekund przez odpowiednio zaawansowany komputer kwantowy. To rosnące zagrożenie zwiększyło pilność opracowania kryptografii postkwantowej.

Kryptografia postkwantowa (PQC) polega na opracowywaniu algorytmów kryptograficznych, które pozostaną bezpieczne w erze komputerów kwantowych. National Institute of Standards and Technology (NIST) uznał istnienie tego nadchodzącego ryzyka i przewodzi w standaryzacji algorytmów odpornych na kwanty.

W przypadku przedsiębiorstw przygotowanie się do tego przejścia nie podlega negocjacjom. Wczesne wdrożenie rozwiązań PQC zapewni bezpieczeństwo danych, gdy przeciwnicy uzyskają dostęp do funkcji obliczeniowych kwantowych.

Bobbie Stempfley, wiceprezes ds. cyberbezpieczeństwa i specjalista ds. bezpieczeństwa jednostki biznesowej w firmie Dell, podkreśla, że organizacje powinny rozpocząć ten proces, koncentrując się na dwóch kluczowych obszarach:

Identyfikacja i inwentaryzacja wszystkich obecnie używanych modeli kryptograficznych.

Należy wziąć pod uwagę dane w ruchu, a nie tylko dane w spoczynku.

Pomyśl o zarządzaniu kluczami, podpisywaniu kodu, identyfikacji urządzeń, bezpiecznym dostępie i telemetrii. Utwórz kompleksowy spis zasobów, a następnie stwórz plan działania.

Zrozumienie statusu dostawców.

Biorąc pod uwagę fakt, że nowoczesne przedsiębiorstwa mogą mieć tysiące dostawców, należy zdawać sobie sprawę z zagrożeń, jakie mogą z nich wynikać. Zadbaj o to, aby oni również planowali zmiany.

Poza tymi punktami wyjścia należy przeprowadzić ocenę ryzyka w celu identyfikacji podatnych systemów, rozważyć wdrożenie hybrydowych modeli kryptograficznych, aby zachować ciągłość działania w trakcie przejścia, oraz współpracować z dostawcami, którzy już pracują nad rozwiązaniami odpornymi na zagrożenia kwantowe, pamiętając jednak, że nie istnieje jeden dostawca ani technologia oferująca gotowe rozwiązanie.

Zmiany regulacyjne w zglobalizowanym świecie

Kolejnym kluczowym czynnikiem kształtującym przyszłość cyberbezpieczeństwa jest zmieniające się otoczenie regulacyjne. Obecnie przepisy mają znacznie szerszy zakres niż tylko zapewnienie zgodności — stają się kluczowym narzędziem do promowania odpowiedzialności, wprowadzania innowacji technologicznych i ochrony obywateli w świecie, w którym dane odgrywają kluczową rolę. Jednak szybko się rozwijają i są bardzo różne w zależności od regionu geograficznego, co zwiększa złożoność regulacyjną.

Mimo to przepisy te wykraczają poza zwykłe kary za naruszenia przepisów — służą jako katalizatory lepszych praktyk w zakresie cyberbezpieczeństwa. Firmy, które aktywnie dostosowują swoje zasady do wymogów prawnych, mogą osiągać nowy poziom zaufania i efektywności operacyjnej. W tym celu organizacje powinny ustanowić struktury zarządzania, które pozostają elastyczne w celu dostosowania się do zmian prawnych, przeprowadzania regularnych audytów zgodności z przepisami i inwestowania w szkolenia dla pracowników w zakresie postępowania z informacjami wrażliwymi zgodnie z najnowszymi standardami.

W miarę, jak osoby odpowiedzialne za bezpieczeństwo przygotowują się do spełnienia wymogów zgodności, ważne jest, aby pilnowały, by były zrozumiałe, a ich komunikaty powinny być właściwie odbierane. Zbyt często specjaliści ds. bezpieczeństwa posługują się językiem technicznym, który może nie być zrozumiały dla klientów, organów regulacyjnych i innych interesariuszy. To na profesjonalistach z branży bezpieczeństwa spoczywa odpowiedzialność za to, aby ich komunikaty były zrozumiałe, a nie na słuchaczach, którzy muszą je interpretować.

DELL Technologies

> Pomyśl o przejściu na kryptografię postkwantową jak o przeniesieniu w pełni umeblowanego domu. Będzie to proces tak skomplikowany, a wyzwaniem jest niepopsucie niczego w tym procesie”.
>
> ***Bobbie Stempfley***
> *Wiceprezes, dyrektor ds. cyberbezpieczeństwa i bezpieczeństwa jednostki biznesowej, Dell Technologies*

Ewolucja krajobrazu zagrożeń (i obrony)

Sztuczna inteligencja rewolucjonizuje biznes, zwiększa produktywność i odblokowuje nowe możliwości potencjału ludzkiego. Jeśli chodzi o cyberbezpieczeństwo, sztuczna inteligencja przynosi korzyści zarówno złośliwym podmiotom, jak i obrońcom:

Zastosowanie wrogie: sztuczna inteligencja umożliwia bardziej wyrafinowane ataki, takie jak wysoce przekonujące kampanie phishingowe i oszustwa typu deepfake.

Zastosowanie obronne: Sztuczna inteligencja pomaga obrońcom poprzez:

- Szybkie przetwarzanie ogromnych ilości danych związanych z bezpieczeństwem.
- Skuteczniejsze określanie priorytetów zagrożeń.
- Poprawianie zdolności do wykrywania i reagowania na zagrożenia

Zabezpieczenia będą jednak nadal się poprawiać, a przetwarzanie języka naturalnego umożliwi specjalistom ds. bezpieczeństwa bardziej bezpośredni kontakt z ich systemami i wyposażenie systemów w potencjał proaktywnego podejmowania działań naprawczych w zakresie cyberbezpieczeństwa.

Organizacje powinny pracować nad tym, aby korzystać z dostępnych możliwości, jednocześnie zapewniając aktualność ich szkoleń i innych mechanizmów obronnych. Najskuteczniejszym sposobem ochrony pracowników przed wyrafinowanymi atakami jest odpowiednie szkolenie.

Przejście na tryb bez hasła

Hasła nie są już najbezpieczniejszymi metodami zarządzania tożsamością i dostępem.

Tradycyjne systemy oparte na hasłach zawierają znaczne luki w zabezpieczeniach, co czyni je coraz bardziej nieodpowiednim rozwiązaniem dla nowoczesnych potrzeb w zakresie cyberbezpieczeństwa. Hasła są podatne na ataki, takie jak używanie skradzionych poświadczeń, phishing i ataki siłowe, często narażając organizacje na niepotrzebne ryzyko. Ponadto złe nawyki użytkowników, takie jak ponowne używanie haseł lub tworzenie słabych, pogłębiają te luki w zabezpieczeniach.

Metody uwierzytelniania bez hasła, takie jak dane biometryczne, certyfikaty i tokeny sprzętowe, zapewniają silniejszą, bezpieczniejszą alternatywę, eliminując całe klasy zagrożeń związanych z hasłami. Przejście na systemy bez hasła stanowi krytyczną ewolucję w zarządzaniu tożsamością i dostępem, dostosowując zabezpieczenia do rosnącej złożoności zagrożeń cybernetycznych.

Wdrożenie technologii bezhasłowych zapewnia również wiele korzyści, w tym zmniejszenie powierzchni ataku, poprawę komfortu użytkownika dzięki szybszemu, bezproblemowemu logowaniu oraz obniżenie kosztów IT poprzez zmniejszenie liczby incydentów związanych z hasłem. Zastosowanie zaawansowanych metod zapewnia lepszy stan bezpieczeństwa i pomaga organizacjom osiągnąć zgodność ze standardami regulacyjnymi. Przejście na systemy bez hasła to nie tylko trend — jest to niezbędny krok w kierunku zbudowania bezpieczniejszego, bardziej wydajnego ekosystemu cyfrowego zarówno dla osób indywidualnych, jak i organizacji.

Wnioski

Cyberbezpieczeństwo wchodzi w epokę transformacji, kształtowaną przez obliczenia kwantowe, zmieniające się przepisy i coraz bardziej zaawansowane zagrożenia. Aby utrzymać przewagę, organizacje muszą wdrożyć innowacje, takie jak kryptografia postkwantowa, zabezpieczenia oparte na sztucznej inteligencji i uwierzytelnianie bez hasła. Dzięki priorytetowi gotowości, współpracy i inwestycji strategicznych firmy mogą zbudować bezpieczniejsze i bardziej odporne środowisko cyfrowe. Czas na działanie jest teraz.

Produkty i rozwiązania firmy Dell, które mogą pomóc

Polecane rozwiązanie firmy Dell	Opis
Usługi doradztwa w zakresie cyberbezpieczeństwa	Specjalistyczne wskazówki, które mogą pomóc w planowaniu zmieniającego się środowiska zagrożeń, w tym bieżących i pojawiających się zagrożeń.
vCISO	Wirtualny dyrektor ds. bezpieczeństwa informacji i ekspert ds. cyberbezpieczeństwa, który może pomóc w identyfikacji ryzyka i zarządzaniu nim, a także kierować strategicznym podejmowaniem decyzji.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **dell.com/cybersecuritymonth**