EXECUTIVE VIEWPOINT | TENABLE

ZARZĄDZANIE EKSPOZYCJĄ W CYBERBEZPIECZEŃSTWIE

Bernard Montel

ORGANIZACJE, ABY UCHWYCIĆ SENS I KRAJOBRAZ ZAGROŻEŃ MUSZĄ ZROZUMIEĆ GLOBALNY KONTEKST WOKÓŁ – POŁĄCZENIE ROZCHWIANEJ GOSPODARKI, AKTYWIZMU I NAPIĘĆ GEOPOLITYCZNYCH. HOLISTYCZNE SPOJRZENIE NA TE KWESTIE, WYKRACZAJĄCE DALEKO POZA OBSZAR TECHNOLOGII, JEST ABSOLUTNIE KLUCZOWE DLA POZYSKANIA WIEDZY, KTÓRE DRZWI I OKNA SĄ SZEROKO OTWARTE, A KTÓRE TRZEBA ZAMKNĄĆ W PIERWSZEJ KOLEJNOŚCI – mówi w rozmowie z Computerworld Bernard Montel, Dyrektor Techniczny EMEA i Strateg ds. Bezpieczeństwa w Tenable

Computerworld: Jak zmienił się krajobraz cyberbezpieczeństwa w ostatnich pięciu latach?

Bernard Montel: Globalna pandemia dramatycznie zmieniła sposób, w jaki pracujemy. Dla niektórych organizacji zmiana ta nastąpiła praktycznie z dnia na dzień. Zamiast podróżować do biur lub innych miejsc pracy, łączyliśmy się z systemami i zasobami zdalnie. Z punktu widzenia cyberbezpieczeństwa miało to ogromny wpływ na sposób myślenia o bezpieczeństwie.

Computerworld: Jakie były największe wyzwania związane z tą zmianą?

Bernard Montel: Sieć domowa, która nigdy wcześniej nie była zabezpieczona, nagle stała się przedłużeniem sieci korporacyjnej. Domowe routery stały się jedynym sposobem, w jaki pracownicy mogli uzyskać dostęp do zasobów, co znacznie rozszerzyło powierzchnię ataku. Korzystanie z sieci prywatnych (VPN) i uwierzytelniania wieloskładnikowego (MFA) było jedynym sposobem na zabezpieczenie tych połączeń. Przeniesienie zasobów do chmury wyeliminowało konieczność zestawiania łączy VPN, co bardzo ułatwiło życie pracownikom zdalnym, zapewniając jednocześnie dodatkową warstwę zabezpieczenia firmowych systemów i danych.

„Twierdza" reprezentowana przez sieć korporacyjną jest teraz rozproszona, co powoduje, że powierzchnia ataku nigdy wcześniej nie była tak duża, ani bardziej dynamiczna, niż obecnie.

Computerworld: Jakie najważniejsze doświadczenie pozostawiła pandemia COVID-19?

Bernard Montel: Jeśli moglibyśmy zachować jedną zmianę po pandemii, byłoby to przyspieszenie wdrażania usług chmurowych w każdym z modeli: Software as a Service (SaaS),

Platform as a Service (PaaS) czy Infrastructure as a Service (IaaS). Chmura zmieniła sposób, w jaki dziś pracujemy, eliminując potrzebę fizycznych maszyn, które były dostępnie jedynie zdalnie. W mojej opinii nie ma potrzeby być bezpośrednio podłączonym do sieci korporacyjnej, aby pozostawać bezpiecznym. Oczywiście nadal mamy wdrożone i używane pewne rozwiązania on-premise, jednak większość organizacji działa w środowisku hybrydowym, łącząc publiczną chmurę z zasobami obsługiwanymi lokalnie. Dzisiejsza „nowa normalność" oznacza, że „twierdza" reprezentowana przez sieć korporacyjną jest teraz rozproszona, co powoduje, że powierzchnia ataku nigdy wcześniej nie była tak duża, ani bardziej dynamiczna, niż obecnie.

Computerworld: Zatem, jak w kontekście nowych płaszczyzn ataku kształtują się obecnie trendy w dziedzinie cyberbezpieczeństwa?

Bernard Montel: Największym zagrożeniem nadal pozostaje ransomware. Liczba ataków, z którymi borykają się organizacje wyraźnie rośnie. Każdego dnia padają kolejne rekordy pod względem liczby naruszonych rekordów lub ilości wykradzionych danych. Bezpieczeństwo chmury to dzisiaj realny problem dla wszystkich organizacji. Przejście na zasoby chmurowe zmusza zespoły bezpieczeństwa do przemyślenia sposobu, w jaki zarządzają bezpieczeństwem. Tradycyjne podejście perymetryczne z punktem końcowym i/lub serwerem jako głównym obiektem praktyk bezpieczeństwa jest prawie bezużyteczne w przypadku mikroserwisów i kontenerów.

Computerworld: Najsłabszym ogniwem w ekosystemie cyberbezpieczeństwa pozostaje człowiek. Wszystko zaczyna się od wykradzionych haseł...

Bernard Montel: Zarządzanie tożsamością zawsze było kluczowe w zapewnieniu bezpieczeństwa danych. W ostatnich dwóch dekadach wyzwania te adresowane były poprzez stosowanie systemów klasy Identity and Access Management (IAM). Dzisiaj problemy związane z zarządzaniem tożsamością są nadal widoczne, ale obszary i metody ochrony stały już znacznie bardziej złożone. Mam tutaj na myśli konieczność stosowania federacyjnych tożsamości, MFA, Active Directory i EntraID w połączeniu z tożsamościami chmurowymi (AWS, Azure, GCP).

Kolejnym obszarem zainteresowania w obszarze cyberbezpieczeństwa, podobnie jak w innych technologiach, staje się sztuczna inteligencja. Atakujący dopiero zaczynają zdawać sobie sprawę z możliwości jakie oferuje AI. Jednocześnie my jako obrońcy, atakowani musimy określić jak wykorzystać tę technologię do ochrony. Wykorzystanie mocy i szybkości generatywnej AI, takiej jak Google Virtex AI, OpenAI GPT-4 czy LangChain, umożliwia uzyskiwanie nowych, inteligentnych informacji w ciągu minut. Może to przyspieszyć cykle badań i rozwoju w dziedzinie cyberbezpieczeństwa, poszukiwanie wzorców i wyjaśnianie tego, co zostało znalezione, w możliwie najprostszy sposób. Wykorzystanie mocy AI pozwala zespołom bezpieczeństwa szybciej pracować, szukać i analizować, a ostatecznie podejmować właściwe decyzje.

Wykorzystanie mocy i szybkości generatywnej AI umożliwia uzyskiwanie nowych, inteligentnych informacji w ciągu minut. Może to przyspieszyć cykle badań i rozwoju w dziedzinie cyberbezpieczeństwa, poszukiwanie wzorców i wyjaśnianie tego, co zostało znalezione

Computerworld: Jaki tok myślowy powinny przyjąć organizacje w kwestii zagrożeń bezpieczeństwa?

Bernard Montel: W większości przypadków to znana, opublikowana luka (vulnerability) umożliwia cyberprzestępcom dostanie się do infrastruktury organizacji. Po uzyskaniu dostępu, atakujący dążą do dalszej infiltracji organizacji w celu kradzieży danych, szyfrowania systemów lub innych złowrogich działań. Otwarte drzwi dla atakujących stanowią również, z pozoru nieszkodliwe, błędy konfiguracyjne, czyli podstawowe błędy ludzkie - od pozostawionych „domyślnie" ustawień aż do błędów programistów, którzy przesyłają niesprawdzony kod w szybkim cyklu DevOps.

Computerworld: Czy mniejsze firmy również narażone są na te zagrożenia?

Bernard Montel: Często istnieje przekonanie, że małe firmy, z uwagi na swój rozmiar, nie stanowią atrakcyjnego celu dla atakujących. Nic bardziej mylnego. Oczywiście zgadzam się, że to zazwyczaj duże i znane firmy trafiają na nagłówki gazet. Cyberprzestępcy zdają sobie jednak sprawę, że mniejsze organizacje, będące częścią łańcucha dostaw, również mogą być celem, otwierając drzwi do większych firm.

EXECUTIVE VIEWPOINT | TENABLE

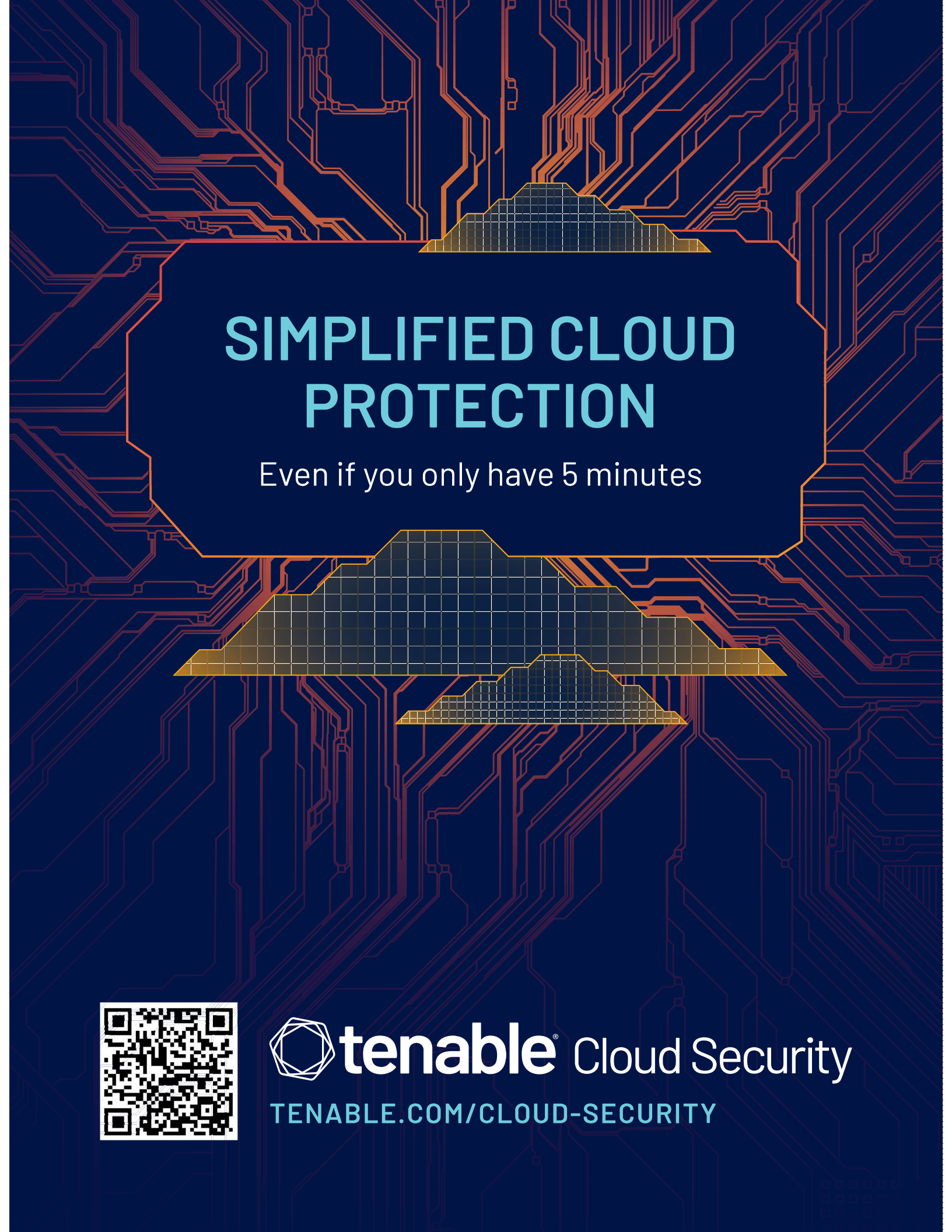
Computerworld: Wróćmy jeszcze na chwilę do ataków ransomware jako tych, których skutki mogą być naprawdę bolesne dla firmy. Jak ewoluowały ataki tego typu w ostatnich latach?

Bernard Montel: Dziesięć lat temu atak ransomware był łatwo zauważalny. Nikt nie miał wątpliwości co się stało, gdy komputer stawał się bezużyteczny po jego zablokowaniu komunikatem żądania okupu wyświetlanym na ekranie. Dzisiaj ataki stają się mniej oczywiste i mogą pozostawać niewykryte przez kilka tygodni. Cyberprzestępcy starają się ukryć swoją obecność, aby móc poruszać się po infrastrukturze w celu wykonywania innych złowrogich działań. Co więcej, grupy zajmujące się wymuszeniami przez ransomware stosują metodę podwójnego wymuszenia, która łączy taktykę szyfrowania z dodaniem kolejnego elementu. Jeszcze przed zaszyfrowaniem plików, przestępcy kradną je i grożą opublikowaniem ich w dark webie, jeśli okup nie zostanie zapłacony. Dodatkowa presja, wynikająca z tego rodzaju wymuszenia sprawia, że ataki ransomware są tak skuteczne.

Dzisiaj ataki ransomware stają się mniej oczywiste i mogą pozostawać niewykryte przez kilka tygodni. Cyberprzestępcy starają się ukryć swoją obecność, aby móc poruszać się po infrastrukturze w celu wykonywania innych złowrogich działań.

Computerworld: Na koniec spróbujmy zastanowić się jakie podejście powinny przyjąć organizacje, aby skutecznie zarządzać ryzykiem?

Bernard Montel: Przedsiębiorstwa i instytucje publiczne, aby uchwycić sens i krajobraz zagrożeń, muszą zrozumieć globalny kontekst wokół — połączenie rozchwianej gospodarki, aktywizmu i napięć geopolitycznych. Skupienie się tylko na „technologicznym" aspekcie cyberzagrożeń nie wystarczy, aby zredukować ryzyko. Kluczowe dla jego ograniczenia jest proaktywne podejście prewencyjne. Holistyczne spojrzenie na kwestie zarządzania ryzykiem, wykraczające daleko poza obszar technologii, jest absolutnie kluczowe dla pozyskania wiedzy, które drzwi i okna są szeroko otwarte, a które trzeba zamknąć w pierwszej kolejności. Podejście to nazywamy zarządzaniem ekspozycją.


SIMPLIFIED CLOUD PROTECTION
Even if you only have 5 minutes
tenable Cloud Security
TENABLE.COM/CLOUD-SECURITY