POSPIESZNA CYFRYZACJA ZWIĘKSZA RYZYKO CYBERATAKÓW. 4-KROTNY WZROST LICZBY INCYDENTÓW

4-krotny wzrost liczby cyberataków w czasie wiosennego lockdownu w odniesieniu do okresu przed pandemią to efekt m.in. pospiesznej cyfryzacji oraz konieczności przejścia na tryb pracy zdalnej w skali masowej - wskazano w raporcie „2020 Cyber Threatscape", którego autorem są specjaliści Accenture.

Jak zauważono w raporcie, pandemia przyspieszyła transformację cyfrową firm, które dostrzegły, że cyfryzacja środowiska pracy jest niezbędna dla utrzymania ciągłości operacyjnej. Jednak ze względu na ekspresowe tempo wdrożeń nowych rozwiązań, wzrosła podatność infrastruktury firm na próby ataków cyberprzestępców. Także praca zdalna z domu sprawia, że prywatne urządzenia IT takie jak np. routery, stały się de facto częścią sieci korporacyjnej i jednocześnie jej słabym ogniwem. Co więcej, jak wskazało Accenture - w związku z kryzysem wiele firm ograniczyło wydatki, również te na IT, w tym zapewnienie cyberbezpieczeństwa. Według szacunków podanych w raporcie wydatki na cyberbezpieczeństwo zmniejszyły się o ok. 8 proc. w 2020 roku i ten trend może się utrzymać w kolejnym roku.

Jak wynika z raportu, sytuację tę szybko wykorzystali cyberprzestępcy: liczba kampanii phishigowych istotnie wzrosła, tylko Google blokował dziennie w kwietniu ok. 18 mln e-maili phishingowych i malware'owych, wykorzystujących motyw COVID-19. Równocześnie wiele organizacji i osób prywatnych padło ofiarami ransomware.

„2020 Cyber Threatscape" podaje, że podwoiła się również liczba bardzo niebezpiecznych ataków na aplikacje webowe, które stanowią już ponad 40 proc. wszystkich ataków. Może to skutkować wyciekami dużych wolumenów danych (np. klientów) lub też rozciągniętą w czasie inwigilacją systemów firm. Autorzy raportu zwracają uwagę, że nie wszyscy cyberprzestępcy realizują swoje cele od razu po przełamaniu zabezpieczeń. Wielu z nich zostawia otwartą furtkę lub kradnie dane z zamiarem ich wykorzystania w przyszłości, nawet po wielu latach.

Według eksperta Accenture Artura Józefiaka, uzależnienie od technologii wzrasta obecnie o wiele szybciej niż zdolność do odpierania cyberataków. „Bardzo ważne jest, aby organizacje zrozumiały, dlaczego i przez kogo są atakowane. Powinny także przemyśleć model zagrożeń w sytuacji pracy zdalnej, kwestie bezpieczeństwa przy korzystaniu z rozwiązań chmurowych czy dużego uzależnienia od firm zewnętrznych, które niekoniecznie mają ten sam poziom zabezpieczeń" – uważa Józefiak.

W raporcie podkreślono, że choć odpowiednie technologie są istotne w zapobieganiu cyberatakom, to stanowią tylko jeden z elementów skutecznej ochrony przed cyberzagrożeniami. Jego autorzy radzą, by zwrócić uwagę na odpowiednie przeszkolenie pracowników wszystkich działów i szczebli oraz uwrażliwienie ich na cyberzagrożenia, z którymi stykają się w codziennej pracy (tzw. secure mindset). Ponadto, firmy powinny przełączać się na podejście tzw. zero trust, zakładające że urządzenia czy aplikacje nie są w pełni zaufane oraz aktywnie je monitorować w celu identyfikowania zagrożeń.

Według ekspertów Accenture konieczne jest także odpowiednie zabezpieczenie pod kątem pracy zdalnej, gdyż pracownicy, którzy przed pandemią pracowali w zespołach, korzystają często z prywatnych komunikatorów, które nie zapewniają odpowiedniego poziomu bezpieczeństwa korporacyjnym informacjom i dokumentom.

Czytaj też: Pełnomocnik ds. GovTech: chcemy przyspieszyć transformację cyfrową całej administracji