76,2 proc. organizacji potwierdza incydent, a luki w monitoringu i procedurach nadal są powszechne

Cyberincydent przestał być rzadkością: 3 na 4 firmy (76,2 proc.) mówią wprost, że zetknęły się z cyberatakiem - wynika z raportu VECTO „Cyberbezpieczeństwo w polskich firmach 2025", opublikowanego przy okazji tegorocznego Dnia Bezpiecznego Internetu. Mimo to tylko 35,4 proc. organizacji monitoruje zagrożenia, a zaledwie 30,8 proc. ma gotowy scenariusz działania na wypadek incydentu. Gdy dojdzie do ransomware i zaszyfrowania danych, 81,5 proc. respondentów uważa, że firma zapłaciłaby okup.

Raport VECTO powstaje cyklicznie i - dzięki stałemu rdzeniowi pytań - daje rzadką na polskim rynku możliwość porównywania wyników między edycjami oraz obserwowania zmian w czasie: od świadomości ryzyka, przez gotowość organizacyjną, po realne praktyki bezpieczeństwa w firmach. Dziś jest to zatem jedno z najbardziej użytecznych opracowań trendowych dla zarządów oraz menedżerów IT i osób odpowiedzialnych za ryzyko i ochronę danych - pozwala nie tylko „zmierzyć deklaracje", ale też zobaczyć, gdzie rynek realnie przyspiesza, a gdzie kumulują się najsłabsze punkty.

„Najnowsza edycja Raportu powstała w momencie szczególnym. Polska znajduje się w regionie, w którym cyberprzestrzeń stała się jednym z narzędzi oddziaływania geopolitycznego wrogich państw. Oprócz klasycznej cyberprzestępczości nastawionej na zysk obserwujemy incydenty o charakterze zakłócającym i destrukcyjnym, wymierzone w instytucje, sektory strategiczne oraz elementy infrastruktury krytycznej. Dla biznesu oznacza to wzrost ryzyka bezpośredniego oraz pośredniego - poprzez łańcuchy dostaw i zależności od dostawców usług cyfrowych" - mówi **Jakub Wychowański**, prezes zarządu VECTO.

Jednym z najbardziej niepokojących wniosków, poza wspomnianą skalą cyberincydentów, pozostaje postrzeganie ransomware jako sytuacji bez wyjścia.

W scenariuszu skutecznego ataku i zaszyfrowania wszystkich danych 81,5 proc.

respondentów uważa, że firma zapłaciłaby okup - co może być sygnałem ograniczonej pewności co do skuteczności kopii zapasowych, testów odtworzeniowych i planów ciągłości działania.

Wyniki wskazują także, że obok „klasycznych" braków - takich jak monitoring czy gotowość proceduralna - na pierwszy plan coraz mocniej wchodzą dwa obszary, które będą determinować ryzyko w 2026 roku: tożsamość oraz nadzór nad narzędziami GenAI. W kluczowych usługach (m.in. poczta, VPN, ERP/CRM, chmura) MFA w większości

systemów deklaruje jedynie 23 proc. firm, co potwierdza, że rynek jest w fazie wdrożeń, ale bez pełnej standaryzacji.

Jednocześnie, po raz pierwszy w badaniu sprawdzono dojrzałość organizacji w zakresie zasad korzystania z AI/GenAI (np. ChatGPT, Copilot) w kontekście ochrony danych i oceny ryzyk. Wyniki są jednoznaczne: zaledwie 5 proc. firm deklaruje pełny model obejmujący politykę wraz ze szkoleniami i egzekwowaniem zasad, a duża część rynku pozostaje bez spójnych reguł lub nie potrafi ocenić, czy takie zasady w ogóle istnieją.

„Rynek ma dziś wysoką świadomość zagrożeń i rosnącą zależność od usług cyfrowych, ale różnice między deklarowaną troską o bezpieczeństwo a dojrzałością procesów nadal są wyraźne. Jak pokazujemy w raporcie, monitoring zagrożeń i scenariusze postępowania po incydencie wciąż nie są standardem - a to wprost przekłada się na decyzje podejmowane pod presją, także w scenariuszu ransomware. W 2026 roku przewagę zyskają organizacje, które zbudują spójny system ochrony: połączą technologię z procesami, zapewnią widoczność i uporządkują zarządzanie tożsamością oraz użyciem GenAI” - dodaje Jakub Wychowański.

Edycja Raportu 2025 koncentruje się również na obszarach, które w ostatnich miesiącach najsilniej zmieniły krajobraz ryzyka: ochronie tożsamości (MFA), detekcji i reakcji, odporności na ransomware, bezpieczeństwie łańcucha dostaw oraz przygotowaniu regulacyjnym. Część z nich pojawia się w raporcie po raz pierwszy, co - w kolejnych edycjach - może pozwoli ocenić tempo tych zmian i to, czy rynek nadąża za rosnącą presją technologiczną i regulacyjną.

Raport „Cyberbezpieczeństwo w polskich firmach 2025” jest dostępny online: https://vecto.pl/raport-2025

VECTO