Miesięcznik

Ubezpieczeniowy

ISSN 1732-2413 • WSZYSTKO, CO TRZEBA WIEDZIEĆ O RYNKU UBEZPIECZEŃ • TOM 23 I NUMER 1 I STYCZEŃ 2026 • 7 STYCZNIA 2026

W NUMERZE:

Ubezpieczenia OC

HR: nowa rola i nowe wyzwania

Zarządzanie ryzykiem / Ubezpieczenia na życie / Nadużycia

Prenumerata – patrz str. 2

MARCIN OGNIEWSKI
dyrektor Biura Rozwoju Biznesu Korporacyjnego, PZU

PIOTR NETTIK
dyrektor ds. Underwritingu Ubezpieczeń Pozakomunikacyjnych, PZU

Bezpieczne dane, bezpieczny biznes – od prewencji do transferu ryzyka

Cyfryzacja naszego życia, poza licznymi korzyściami, przynosi także różne zagrożenia i wyzwania. Jednym z nich są cyberataki, które mogą skutkować naruszeniem danych czy utratą pieniędzy. Liczba cyberataków na całym świecie, w tym w Europie i Polsce, konsekwentnie rośnie. – Marcin Ogniewski, Piotr Nettik

Według danych Rady Unii Europejskiej roczne globalne straty wynikające z cyberprzestępczości to 5,5 biliona euro[1]. Ataki są szybsze, tańsze i częściej wykorzystują słabe punkty naszych ekosystemów: pracowników, dostawców, urządzenia brzegowe oraz niespójne procedury. To już nie jest problem „informatyków", lecz centralny temat zarządzania ryzykiem i odporności operacyjnej.

KRAJOBRAZ ZAGROŻEŃ: EUROPA I ŚWIAT

Europejski raport ENISA Threat Landscape 2025[2] pokazuje dojrzewający ekosystem zagrożeń: phishing pozostaje głównym wektorem (ok. 60% prób wejścia), rośnie tempo „uzbrajania" świeżych luk (ok. 21% incydentów bazuje na exploitacji podatności), a ransomware utrzymuje pozycję najbardziej zakłócającego ataku dla ciągłości działania. Od strony „szumu" w przestrzeni publicznej uwagę przyciągają kampanie hacktywistyczne – licznie rejestrowane, lecz zwykle o niskim wpływie operacyjnym – podczas gdy prawdziwe koszty biznesowe generują operacje przestępcze i szpiegowskie wymierzone w łańcuchy dostaw, telekomunikację czy logistykę. Do tego dochodzi AI: coraz częściej wspiera masowe i personalizowane kampanie socjotechniczne, podnosząc wskaźniki skuteczności, choć równolegle poprawia się jakość narzędzi defensywnych.

POLSKA NA CELOWNIKU CYBERPRZESTĘPCÓW

W 2024 roku Polska znalazła się w centrum globalnej uwagi w kontekście cyberzagrożeń. Odnotowano ponad 100 tysięcy ataków wymierzonych w firmy i instytucje, co oznacza rekordowy wzrost w porównaniu z poprzednimi latami. Szczególnie narażony był sektor finansowy – liczba incydentów wzrosła aż o 30%, osiągając poziom ponad 1 800 ataków tygodniowo. Według danych CSIRT NASK, liczba zarejestrowanych incydentów w Polsce wzrosła o 29% rok do roku, a zgłoszeń cyberataków aż o 64%.

POLSKA – WYSOKA EKSPOZYCJA I WYSOKA GOTOWOŚĆ

Paradoks polskiego krajobrazu cyberbezpieczeństwa polega na jednoczesnym wysokim poziomie narażenia oraz relatywnie dobrej gotowości. Z jednej strony Polska znajduje się w gronie krajów o największej liczbie ataków na świecie, a firmy finansowe stały się jednym z głównych celów ze względu na wartość przetwarzanych danych, rozbudowane systemy transakcyjne i ścisłą integrację z globalnymi rynkami. Z drugiej – drugie miejsce w Indeksie Cyberbezpieczeństwa Narodowego (NCSI) potwierdza, że krajowy system ochrony – szczególnie w sektorze publicznym i finansowym – jest dojrzały i systematycznie wzmacniany. To ważna informacja dla przedsiębiorstw: regulatorzy podnoszą poprzeczkę, ale presja atakujących rośnie jeszcze szybciej.
Wzrost ekspozycji to wypadkowa trzech megatrendów:

- → Przyspieszona cyfryzacja – coraz więcej procesów biznesowych przenosi się do chmury, a łańcuchy dostaw zależą od rozwiązań IT i integracji systemów partnerów. Każda nowa integracja to potencjalny punkt podatności.
- → Profesjonalizacja przestępczości – grupy cyberprzestępcze oferują „usługi" Ransomware-as-a-Service, automatyzują skanowanie luk i łatwo skalują operacje. Atak nie jest już jednorazowym zdarzeniem, ale powtarzalnym „proceduralnym" procesem.

1 Zobacz: https://www.consilium.europa.eu/en/policies/a-cybersecure-society/.

2 Zobacz: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf.

→ AI jako akcelerator – generatywna sztuczna inteligencja ułatwia tworzenie wiarygodnych kampanii phishingowych (dobrej jakości język, personalizacja), a także automatyzuje rekonesans i obróbkę pozyskanych danych. W połączeniu z IoT zwiększa to powierzchnię ataku.

W efekcie phishing, ransomware, DDoS i malware pozostają najczęstszymi wektorami, lecz rośnie udział ataków wykorzystujących błędy konfiguracji, zaniedbane aktualizacje oraz luki u podwykonawców i dostawców usług chmurowych. Coraz częściej skuteczny atak jest rezultatem splotu czynników: słabej higieny bezpieczeństwa, presji czasu, niedoskonałych procedur reagowania oraz braku segmentacji sieci.

KOSZTY I KONSEKWENCJE: NIE TYLKO FINANSOWE

Cyberataki to dziś jedno z najdroższych zagrożeń dla biznesu. Średni koszt pojedynczego naruszenia danych w 2024 roku wyniósł aż 4,88 mln dolarów, co oznacza wzrost o 10% w porównaniu z rokiem 2023. Szczególnie kosztowne są ataki z udziałem złośliwego insidera, których skutki sięgają niemal 5 mln dolarów. Do najczęstszych metod należą phishing, przejęcia skrzynek e-mail oraz kradzież danych uwierzytelniających. Finansowe skutki cyberataków są nie tylko bardzo wysokie, ale też rosną z roku na rok, co czyni je jednym z kluczowych wyzwań dla współczesnych organizacji.

Średni koszt ataku ransomware dla polskiej firmy wynosi ok. 1 500 000 zł. Usunięcie skutków takiego incydentu, na przykład zaszyfrowania danych, to dodatkowy wydatek rzędu 500 000 zł w przypadku firm zatrudniających powyżej 100 pracowników. Ostateczny rachunek obejmuje również koszty modernizacji zabezpieczeń po incydencie i konieczność podniesienia standardów zgodności – co oznacza wielomiesięczny wysiłek organizacyjny, nie tylko finansowy.

Bezpośrednie koszty cyberincydentów – od odtworzenia danych, przez obsługę prawną i informatykę śledczą – to tylko wierzchołek góry lodowej. W praktyce przedsiębiorstwa mierzą się również z: przestojami operacyjnymi i utratą przychodów, karami administracyjnymi (np. za naruszenia przepisów o ochronie danych), odszkodowaniami dla poszkodowanych klientów lub partnerów, czy spadkiem zaufania i długotrwałymi kosztami reputacyjnymi.

UBEZPIECZENIE CYBER OD PZU – OD OPCJI DO KONIECZNOŚCI

W obliczu rosnącej częstotliwości i dotkliwości incydentów ubezpieczenie ryzyk cybernetycznych staje się jednym z filarów odporności organizacji. Produkt PZU Cyber nie ogranicza się do pokrycia szkód – obejmuje zarządzanie incydentem (24/7/365), wsparcie informatyków śledczych, prawników, biegłych księgowych i agencji PR, a także finansowanie odtworzenia danych i przywrócenia ciągłości działania. Kluczowa jest konstrukcja ochrony: segment odpowiedzialności (cywilnej i administracyjnej), segment szkód własnych oraz moduł reakcji na incydent. Dla firm oznacza to realne skrócenie czasu do przywrócenia normalnej pracy i ograniczenie strat.

W kontekście wzrostu wymagań (np. wynikających z europejskich regulacji) oraz presji ubezpieczycieli na minimalne standardy ochrony, warto podkreślić, że prostota i szybkość oceny ryzyka to dziś przewagi, które mają wymierne znaczenie dla klienta. Dodatkowym elementem odporności jest właściwie dobrana suma ubezpieczenia – adekwatna do skali działalności i profilu ekspozycji (liczba rekordów danych, przychody online, zależność od dostawców IT).

NOWE POTRZEBY BRANŻY IT: OC ZAWODOWE DLA FIRM TECHNOLOGICZNYCH

Drugim filarem ochrony cyfrowego biznesu jest oferowane przez PZU ubezpieczenie odpowiedzialności zawodowej dla branży IT. W praktyce chroni ono roszczenia osób trzecich wynikające z błędów w usługach technicznych (np. zarządzanie siecią klienta, konfiguracja systemów, outsourcing IT) lub produktach technicznych (np. instalacja i integracja oprogramowania, projektowanie rozwiązań). Istotnym elementem jest ochrona naruszeń praw autorskich (np. włączenie cudzej biblioteki bez właściwej licencji) oraz objęcie szkód powstałych wskutek rażącego niedbalstwa. Dla software house'ów, dostawców chmury, integratorów i jednoosobowych działalności B2B to rozwiązanie, które zamyka lukę między cyberpolisą a odpowiedzialnością za rezultat profesjonalnej usługi.

TRZY FILARY SKUTECZNEGO ZARZĄDZANIA RYZYKIEM CYBERNETYCZNYM

Współczesne podejście opiera się na trzech filarach:

1. Prewencja i higiena bezpieczeństwa – regularne aktualizacje, szyfrowanie danych, wieloskładnikowe uwierzytelnianie, segmentacja sieci oraz szkolenia pracowników to fundamenty, które minimalizują ryzyko ataku.
2. Procedury i gotowość operacyjna – jasne plany reagowania na incydenty, testy odtwarzania danych, monitoring i szybka eskalacja problemów pozwalają skrócić czas reakcji i ograniczyć straty.
3. Transfer ryzyka poprzez ubezpieczenie – nawet najlepsze zabezpieczenia nie eliminują ryzyka całkowicie. Dlatego ubezpieczenie cyber oraz OC zawodowe IT stają się kluczowym elementem strategii – zapewniają wsparcie ekspertów, pokrywają koszty odtworzenia danych, obsługi prawnej i działań PR, a także chronią przed roszczeniami osób trzecich.

Zarządzanie ryzykiem cybernetycznym to proces ciągły, wymagający integracji technologii, procedur i świadomości pracowników. PZU Cyber w tym układzie dostarcza operacyjny ekosystem pomocy i finansową tarczę, która ma znaczenie właśnie wtedy, gdy nadchodzi najtrudniejsza doba kryzysu. To różnica między chaosem a kontrolowanym incydentem, między długim przestojem a powrotem do biznesu. ❑

© Simple Line/stock.adobe.com