Miesięcznik
Ubezpieczeniowy

ISSN 1732-2413 • WSZYSTKO, CO TRZEBA WIEDZIEĆ O RYNKU UBEZPIECZEŃ • TOM 23 I NUMER 7/8 I LIPIEC/SIERPIEŃ 2026 • 16 LIPCA 2026

W NUMERZE:

Ubezpieczenia cyber

Likwidacja szkód: współczesne wyzwania

Zarządzanie ryzykiem / Finanse 2.0 / Wycena przedsiębiorstw

JUSTYNA SZARANIEC
zastępca kierownika Zespołu Ubezpieczeń Specjalistycznych EIB

Ubezpieczenie od ryzyk cybernetycznych

Współczesne organizacje, niezależnie od branży, coraz częściej stają się celem ataków cybernetycznych. Ich skutkiem mogą być przerwy w działalności, utrata danych oraz znaczące straty finansowe i reputacyjne. Dlatego cyberbezpieczeństwo i odpowiednie zarządzanie ryzykiem – w tym poprzez ubezpieczenia – stają się jednym z kluczowych wyzwań organizacji. – Justyna Szaraniec

Ryzyka cybernetyczne niezmiennie należą do czołowych globalnych obaw – w „*Global Risks Report 2026*" Światowego Forum Ekonomicznego zajmują 6. miejsce w perspektywie krótkoterminowej i 8. w długofalowej. O samej dynamice wzrostu świadczą jednak również twarde dane: według CERT Polska i CSIRT NASK liczba zarejestrowanych incydentów w marcu 2026 r. była o 178% wyższa niż rok wcześniej.

Jak wynika z raportów *„Cyberportret polskiego biznesu 2025"* (ESET i DAGMA Bezpieczeństwo IT) oraz *„Barometr cyberbezpieczeństwa. Cyberodporność w erze zmian"* (KPMG w Polsce), zdecydowana większość przedsiębiorstw doświadczyła w ostatnim roku co najmniej jednego incydentu cyberbezpieczeństwa.

Na cyberzagrożenia narażone są dziś organizacje niezależnie od branży i skali – zarówno MŚP, jak i duże przedsiębiorstwa, których funkcjonowanie zależy od infrastruktury IT i systemów cyfrowych.

Szczególnie eksponowane na skutki incydentów są branże, w których kluczowe znaczenie mają ciągłość działania, przetwarzanie dużych wolumenów danych i wysoki poziom cyfryzacji procesów. Z kolei statystyki *Raportu rocznego CERT Polska za 2025 r. – Krajobraz bezpieczeństwa polskiego internetu* pokazują, że – poza osobami fizycznymi i administracją publiczną – najwięcej obsłużonych zgłoszeń dotyczyło handlu, oświaty, ochrony zdrowia, infrastruktury cyfrowej, usług, bankowości oraz transportu.

UBEZPIECZENIE CYBER JAKO ELEMENT ZARZĄDZANIA RYZYKIEM

Wobec rosnącej liczby incydentów i ich wpływu na działalność firm, ubezpieczenie na wypadek ryzyk cybernetycznych staje się istotnym elementem zarządzania ryzykiem. Z naszego doświadczenia wynika, że ubezpieczenie cybernetyczne coraz częściej staje się standardowym elementem programu ubezpieczeniowego organizacji, a zainteresowanie tym produktem wyraźnie rośnie wśród wszystkich podmiotów, niezależnie od branży.

Ochrona obejmuje przede wszystkim koszty przywrócenia systemów IT do pełnej sprawności po ataku – w tym pracę ekspertów informatyki śledczej, wsparcie prawne i doradztwo przy odbudowie infrastruktury. Polisa może też pokrywać odzyskanie danych zaszyfrowanych przez ransomware, naprawę uszkodzonych zasobów IT oraz zarządzanie kryzysowe i komunikację zewnętrzną, ograniczającą wpływ incydentu na wizerunek organizacji.

Istotnym elementem ochrony są także koszty zobowiązań regulacyjnych – powiadomienia osób, których dane dotyczą oraz organów nadzorczych, a w granicach dozwolonych prawem także potencjalne kary administracyjne za naruszenie przepisów o ochronie danych. Możliwe jest również pokrycie roszczeń cywilnoprawnych osób, których dane ujawniono w wyniku incydentu.

Dodatkowo polisa może zabezpieczać przedsiębiorstwo przed skutkami finansowymi przerw w działalności, obejmując utracony zysk oraz koszty niezbędne do kontynuowania operacji w ograniczonym zakresie. Ma to szczególne znaczenie w przypadku organizacji, dla których niedostępność systemów IT bezpośrednio przekłada się na zdolność świadczenia usług i generowanie przychodów.

NA CO ZWRÓCIĆ UWAGĘ PRZY ZAWIERANIU POLISY

Kluczowym elementem ubezpieczenia cybernetycznego jest natychmiastowy dostęp do wyspecjalizowanego wsparcia w trybie 24/7. W przypadku incydentu uruchamiany jest proces zarządzania kryzysowego, w ramach którego wyznaczany jest dedykowany *cyber incident manager*, odpowiedzialny za koordynację wszystkich działań naprawczych. Jego rolą jest szybkie dobranie i zaangażowanie odpowiednich ekspertów – w tym specjalistów z zakresu *cyber forensics*, doradców prawnych czy firm zajmujących się komunikacją kryzysową. Takie skoordynowane podejście pozwala na natychmiastową reakcję, ograniczenie skutków incydentu oraz sprawne przeprowadzenie organizacji przez cały proces.

W rozmowach z klientami regularnie pojawia się pytanie o to, jak taka pomoc wygląda w praktyce i czy mogą na nią

liczyć niezależnie od momentu wystąpienia incydentu. Ma to szczególne znaczenie, ponieważ zdarzenia cybernetyczne często mają miejsce poza standardowymi godzinami pracy – np. w weekendy czy w okresach świątecznych – a możliwość natychmiastowego zgłoszenia szkody i uruchomienia wsparcia jest wówczas kluczowa.
Równie istotnym elementem, który należy przeanalizować już na etapie zawierania umowy, jest tzw. data retroaktywna. Określa ona moment, od którego ubezpieczyciel obejmuje ochroną zdarzenia prowadzące do szkody. W praktyce oznacza to, że polisa pokrywa incydenty zapoczątkowane nie wcześniej niż w tej dacie – nawet jeśli ich skutki ujawnią się znacznie później. W wielu przypadkach moment naruszenia bezpieczeństwa infrastruktury IT może nastąpić na długo przed ujawnieniem jego skutków – takich jak zaszyfrowanie danych czy paraliż systemów, które pojawiają się dopiero na późniejszym etapie ataku. Jeśli początek zdarzenia miał miejsce przed datą retroaktywną wskazaną w polisie, jego skutki mogą nie być objęte ochroną, nawet jeśli ujawniły się już w okresie ubezpieczenia.
Dlatego w kontekście decyzji o zawarciu polisy każdy dzień zwłoki zwiększa ryzyko powstania luki w ochronie, w której może dojść do incydentów niewidocznych na pierwszy rzut oka, a wyłączonych z zakresu ubezpieczenia ze względu na datę ich powstania.

KRYTERIA UNDERWRITINGOWE W UBEZPIECZENIACH CYBER

Ubezpieczyciele zwracają szczególną uwagę na kilka kluczowych obszarów, które mają bezpośredni wpływ na ocenę ryzyka oraz warunki oferowanej ochrony. Z naszej praktyki wynika, że właśnie te obszary są najczęściej przedmiotem szczegółowych pytań ubezpieczycieli na etapie underwritingowym i w największym stopniu wpływają na ocenę ryzyka oraz warunki oferty. Jednym z najważniejszych jest poziom świadomości pracowników w zakresie cyberbezpieczeństwa. Wynika to z faktu, że jedną z najczęstszych przyczyn incydentów cybernetycznych pozostaje czynnik ludzki oraz związane z nim ataki socjotechniczne, w szczególności phishing.
W związku z tym ubezpieczyciele wymagają wdrożenia regularnych szkoleń dla pracowników mających styczność z systemami informatycznymi. Standardowo obejmuje to co najmniej jedno szkolenie rocznie, podczas którego uczestnicy uczą się rozpoznawania podejrzanych wiadomości e-mail, identyfikacji fałszywych linków oraz podstawowych technik wykorzystywanych w atakach socjotechnicznych, a także poznają przyjęte w organizacji procedury zgłaszania incydentów.
Kolejne kryterium to korzystanie wyłącznie z aktualnych, wspieranych rozwiązań i eliminowanie systemów przestarzałych, dla których zakończono wsparcie techniczne. Brak aktualizacji zwiększa podatność na znane luki, a więc i ryzyko incydentu. W konsekwencji ubezpieczyciel może wyłączyć z zakresu ochrony incydenty wynikające z korzystania z systemów niewspieranych przez producenta lub – na etapie oceny ryzyka – odmówić przedstawienia oferty ubezpieczenia.
Coraz częściej warunkiem koniecznym jest uwierzytelnianie wieloskładnikowe (MFA) przy zdalnym dostępie. MFA istotnie ogranicza ryzyko nieautoryzowanego dostępu – nawet po przejęciu danych logowania wymaga dodatkowego potwierdzenia tożsamości, np. kodem SMS czy aplikacją uwierzytelniającą. Jego brak może oznaczać nie tylko gorsze warunki oferty, ale i odmowę ochrony.
Istotnym elementem oceny ryzyka jest również sposób zarządzania kopiami zapasowymi danych. Ubezpieczyciele oczekują, aby backupy były tworzone regularnie oraz przechowywane w sposób zapewniający ich odseparowanie od głównych systemów – w szczególności w środowiskach offline lub w wydzielonych, zabezpieczonych lokalizacjach.
Dużą wagę ma również aktualny plan ciągłości działania (BCP) – dokument określający funkcjonowanie organizacji podczas zakłóceń (w tym incydentów) i umożliwiający szybkie przywrócenie kluczowych procesów. W praktyce dobrze przygotowany i przetestowany BCP stanowi jeden z kluczowych elementów ograniczania skutków incydentu i jest istotnym kryterium oceny dojrzałości organizacji w obszarze zarządzania ryzykiem.
Ubezpieczyciele analizują także historię incydentów cybernetycznych danej organizacji. Wystąpienie ataku nie musi jednak działać na jej niekorzyść – kluczowe znaczenie ma sposób reakcji oraz działania wdrożone po zdarzeniu. Organizacje, które wyciągnęły wnioski, wzmocniły zabezpieczenia i uporządkowały procedury, są często oceniane jako bardziej dojrzałe i lepiej przygotowane na przyszłe zagrożenia, co może pozytywnie wpływać na warunki oferty.
Nasza praktyka wskazuje również, że doświadczenie incydentu – nawet relatywnie niewielkiego – często skłania organizacje do zakupu ubezpieczenia cyber, ponieważ koszty obsługi takiego zdarzenia mogą łatwo przekroczyć koszt składki ubezpieczeniowej.

NOWE OBOWIĄZKI WYNIKAJĄCE Z REGULACJI – KSC/NIS2

Istotne są też zmiany regulacyjne – zwłaszcza nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC), wdrażająca dyrektywę NIS2. Rozszerza ona katalog podmiotów objętych obowiązkami i podnosi wymagania w zarządzaniu ryzykiem: wdrożenia środków technicznych i organizacyjnych, analizy ryzyka, raportowania incydentów oraz zapewnienia ciągłości działania. Niewywiązanie się grozi dotkliwymi sankcjami finansowymi i konsekwencjami regulacyjnymi.
Szczególnie ważne jest wprowadzenie osobistej odpowiedzialności kierowników podmiotów zaklasyfikowanych jako kluczowe lub ważne. Za niewykonanie obowiązków ustawowych mogą oni odpowiadać finansowo – do 300% miesięcznego wynagrodzenia w sektorze prywatnym oraz do 100% w sektorze publicznym.
Coraz częściej w związku z tymi zmianami członkowie zarządów pytają, w jaki sposób mogą ograniczyć swoją osobistą ekspozycję na ryzyko. W tym kontekście pomocne jest również ubezpieczenie D&O. Może ono obejmować roszczenia regresowe wobec osób pełniących funkcje zarządcze lub kierownicze, powiązane z karą administracyjną nałożoną na podmiot, jeśli wynikała ona z błędów w zarządzaniu lub nadzorze (np. braku odpowiednich procedur), a także kary administracyjne nałożone bezpośrednio na osoby ubezpieczone.

PODSUMOWANIE

Rosnąca skala cyberzagrożeń i zaostrzające się wymagania regulacyjne sprawiają, że zarządzanie ryzykiem cybernetycznym staje się jednym z kluczowych obszarów odpowiedzialności organizacji. Ubezpieczenie cyber pełni tu rolę nie tylko finansowej ochrony, ale i narzędzia wspierającego reagowanie na incydenty oraz utrzymanie ciągłości działania.
Warunki ubezpieczenia są dziś ściśle powiązane z poziomem wdrożonych zabezpieczeń. Firmy inwestujące w cyberbezpieczeństwo, budujące świadomość pracowników i dostosowujące się do wymogów regulacyjnych mogą liczyć nie tylko na mniejsze ryzyko incydentów, ale i na korzystniejsze warunki ochrony.
Skuteczne zarządzanie ryzykiem cyber wymaga więc dziś podejścia kompleksowego – łączącego rozwiązania technologiczne, organizacyjne oraz odpowiednio dobraną ochronę ubezpieczeniową. ❑