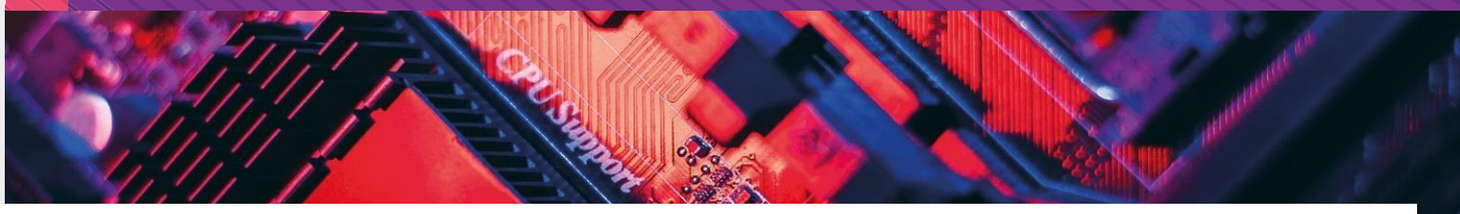

Ubezpieczenie ryzyk cybernetycznych

Dla członków Polskiej Izby Biegłych Rewidentów

Cyberatak nie musi zatrzymać działalności – pod warunkiem, że firma ma przygotowany plan reakcji i finansową ochronę na wypadek incydentu

Polska pozostaje jednym z głównych celów cyberprzestępców. Według ESET Threat Report H2 2025 Polska zajęła 3. miejsce na świecie pod względem ataków ransomware oraz 2. miejsce w kategorii zagrożeń rozsyłanych pocztą e-mail. Jednocześnie rozwój AI zwiększa skuteczność phishingu, scamów i kampanii socjotechnicznych.

Kluczowe trendy dla Polski – ESET H2 2025

2. miejsce
w kategorii zagrożeń rozsyłanych pocztą e-mail

3. miejsce
wśród najczęściej atakowanych państw pod względem ransomware

+40% r/r
prognozowany globalny wzrost liczby ofiar ransomware

Wniosek dla firm:

Ochrona techniczna jest niezbędna, ale nie eliminuje finansowych konsekwencji incydentu.

Ubezpieczenie cyber pomaga sfinansować reakcję kryzysową, odtworzenie danych, przerwę w działalności oraz potencjalne roszczenia.

Organizacje dzielą się na te, które zostały dotknięte cyberatakiem oraz te, które jeszcze o tym nie wiedzą.

Kto powinien mieć ubezpieczenia cyber?

Każda organizacja korzystająca z poczty e-mail, systemów IT, danych klientów lub dostawców cyfrowych jest potencjalnym celem cyberataku.

Wielkość firmy ani branża nie eliminują ryzyka – wpływają jedynie na jego charakter i potencjalną skalę strat.

wtw | Willis

Zakres ochrony ubezpieczeniowej

Zarządzanie zdarzeniem kryzysowym

- dostęp 24/7 do zespołu reagowania na incydent i pokrycie jego kosztów
- koordynacja działań po incydencie
- eksperci IT forensic, prawnicy i doradcy PR
- usługi call center i komunikacja z poszkodowanymi

Kary administracyjne

- kary i grzywny administracyjne – o ile są ubezpieczalne zgodnie z prawem
- koszty postępowania regulacyjnego
- wsparcie przy wykazaniu zgodności procedur z przepisami o ochronie danych

Straty własne firmy

- odtworzenie systemu IT oraz utraconych danych
- utrata zysku i dodatkowe koszty operacyjne
- koszty związane z próbą wymuszenia okupu (ransomware)
- koszty przywrócenia działalności po incydencie

Roszczenia osób trzecich

- koszty obrony i odszkodowania
- naruszenie prywatności lub informacji poufnych
- odpowiedzialność medialna za treści cyfrowe
- roszczenia związane z naruszeniem bezpieczeństwa sieci

Dlaczego WTW?

Pomagamy szybko przełożyć ryzyko cyber na konkretny program ochrony – od wstępnej analizy, przez kwotację, po wdrożenie rozwiązania.

program ochrony cyber dopasowany do specyfiki danej grupy zawodowej

wsparcie brokerów w dopasowaniu limitów ochrony

dostęp do rynku ubezpieczeniowego i aktualnych wymagań ubezpieczycieli

Zapraszamy do kontaktu

Opiekun Programu Ubezpieczeniowego
Karol Jędrzejewski
Broker Ubezpieczeniowy
Dział Grup Zawodowych
Departament FINEX
+48 723 330 343
karol.jedrzejewski@wtwco.com

Lider Ubezpieczeń Cyber
Magdalena Domańska
Starszy Broker
Dział Linii Finansowych
Departament FINEX
+48 887 043 353
magdalena.domanska@wtwco.com

wtw | Willis