Bezpieczne dane, bezpieczny biznes.

Ubezpieczenie cyber i OC IT w praktyce

Szkolenie IDD

Paulina Borowiec
Marcin Jarosz

Czego dziś się dowiesz?

Kluczowe zagadnienia szkolenia

1. **Czym są ryzyka cybernetyczne?**
   Definicja ryzyk cybernetycznych, typowe zagrożenia, przykłady szkód oraz wpływ cyberataków na działalność firm w różnych branżach.
2. **Ryzyka cyber w Polsce**
   Dane statystyczne oraz skala cyberataków w Polsce, poziomu narażenia firm, najczęściej atakowanych sektorów oraz rosnącej świadomości
3. **Oferta PZU - ubezpieczenia ryzyk cybernetycznych**
   Zakres ochrony, zdarzenia objęte ubezpieczeniem, szybka ocena ryzyka i dostępność online.
4. **Ocena ryzyka, czyli underwriting w praktyce**
   Jak wygląda proces oceny ryzyka w praktyce – jakie są wymagania techniczne i organizacyjne dla firm, jakie kryteria wpływają na decyzję underwritingową oraz jak uproszczono proces.
5. **Ubezpieczenie OC zawodowe IT - dedykowane dla branży technologicznej**
   Założenia i zakres ochrony polisy OC dla firm IT, typowe szkody (np. naruszenie praw autorskich, błędy w kodzie, niewłaściwa konfiguracja systemów).

Czym są ryzyka cybernetyczne?

Typowe zagrożenia cybernetyczne

Czym są ryzyka cybernetyczne?

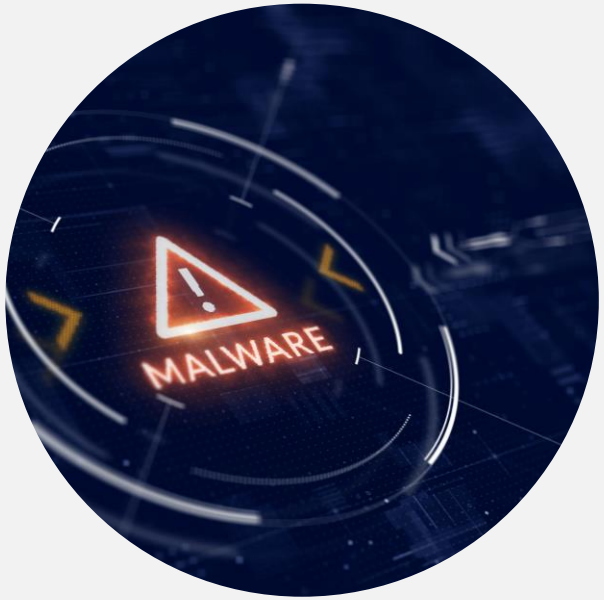
Ryzyko wystąpienia u ubezpieczonego lub u osób trzecich szkód związanych z eksploatacją sieci komputerowej.

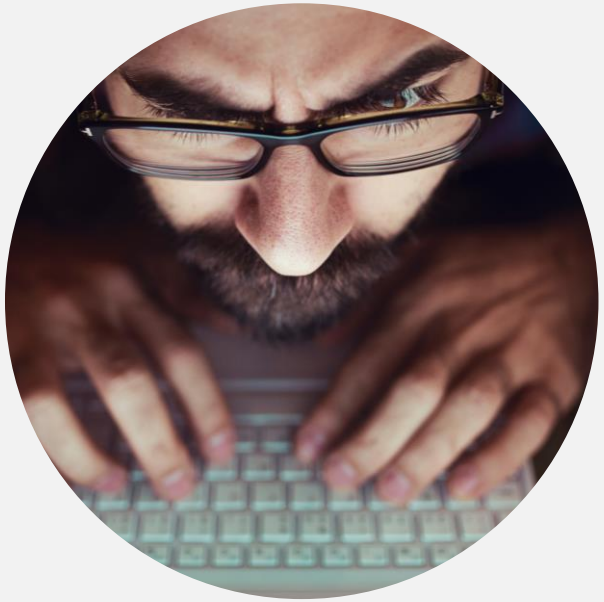
Szkody – straty finansowe, reputacyjny, operacyjne.

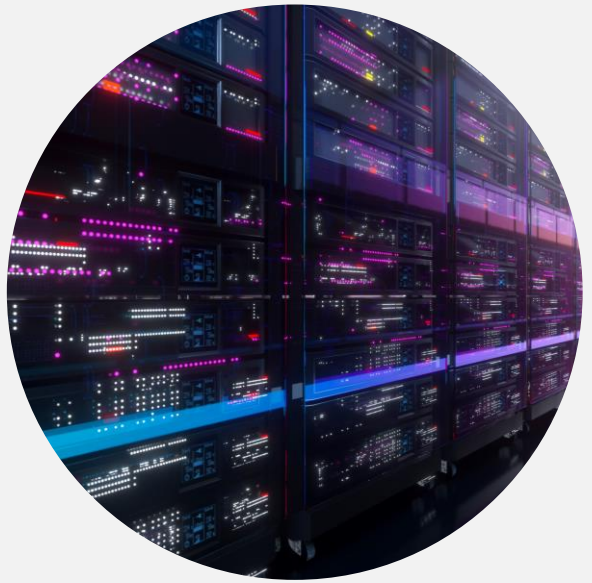
Do najczęstszych zagrożeń należą:
DoS/DDoS, ransomware, phishing

Krytyczne sektory, np. transport, zdrowie, energetyka, media czy finanse.
Jednocześnie to właśnie te firmy są najbardziej scyfryzowane.

Cyfrowe pułapki







#Ransomware
#Malware

#Phishing

#DDoS

Przykłady szkód

Tło

Colonial Pipeline to jedna z największych sieci rurociągów paliwowych w USA

Przebieg ataku

- **Data ataku:** 7 maja 2021 r.
- **Rodzaj ataku:** Ransomware
- **Sprawcy:** Grupa hakerska **DarkSide**, powiązana z rosyjskim cyberpodziemiem.
- **Metoda:** Zainfekowanie systemów IT ransomwarem, który zaszyfrował dane i zażądał okupu.

#Ransomware
#Malware

Reakcja i konsekwencje

- FBI i inne agencje federalne rozpoczęły śledztwo.
- Rząd USA ogłosił ransomware jako zagrożenie dla bezpieczeństwa narodowego.
- Colonial Pipeline wdrożyło nowe procedury bezpieczeństwa.
- Wzrost inwestycji w cyberbezpieczeństwo infrastruktury krytycznej.

Przykłady szkód

Tło

British Airways największy brytyjski przewoźnik lotniczy

Przebieg ataku

- **Data Ataku:** 2018
- **Rodzaj malware:** Złośliwy JavaScript (skrypt Magecart)
- **Szkody:**

→ Wykradziono dane 380 000–500 000 klientów (imiona, adresy, numery kart, CVV)

→ Kara: £183 mln (ostatecznie obniżona do £20 mln)

- **Mechanizm:** Atak na zewnętrzny system płatności przez wstrzyknięcie kodu na stronie BA

#Ransomware
#Malware

Ostatecznie British Airways zapłaciło znacznie niższą kwotę – **20 milionów funtów (26 milionów dolarów)** – za niedostateczną ochronę danych osobowych i finansowych klientów.

Przykłady szkód

Tło

Wanna Cry – globalny atak ransomware

Przebieg ataku:

- **Data ataku:** 2017r.
- **Rodzaj ataku:** Ransomware
- **Sprawcy:** grupa Lazarus, powiązana z Koreą Północną
- **Metoda:** Zainfekowanie systemów IT ransomwarem, który wykorzystał lukę w systemie Windows.

#Ransomware
#Malware

Skutki:

- Szacowane straty: **od 4 do 8 miliardów dolarów**.
- Pokazał, jak nieaktualne systemy operacyjne mogą być podatne na masowe ataki.
- Microsoft wypuścił **nadzwyczajną aktualizację** nawet dla nieobsługiwanych wersji Windows (XP, 8).

Przykłady szkód

Google i Facebook (2013–2015)

- **Sprawca:** Evaldas Rimasauskas – litewski cyberprzestępca.
- **Metoda:** Podszywanie się pod zaufanego dostawcę (Quanta Computer).
- **Mechanizm ataku:**
  → Wysyłał fałszywe faktury i e-maile do działów finansowych Google i Facebooka.
  → Używał podrobionych domen i kont bankowych.
  → Skutek: Obie firmy przelały łącznie ponad 100 milionów dolarów na konta kontrolowane przez przestępcę.

#Phishing

Cechy charakterystyczne:

- Adres e-mail nadawcy wygląda na autentyczny (np. inpost@dostawa24.pl).
- Strona phishingowa ma certyfikat SSL (https), co może uśpić czujność.
- Często stosowane są presja czasu i groźba utraty przesyłki.

Źródło: DDoS Attack Examples (2024): The 7 Worst Attacks Ever

Przykłady szkód

Metoda „na przesyłkę” (podszywanie się pod Inpost)

- **Forma ataku:** E-mail z informacją o konieczności dopłaty do przesyłki lub potwierdzenia danych.
- **Treść wiadomości:** Zawiera link prowadzący do fałszywej strony logowania, łudząco podobnej do oryginalnej.
- **Cel:** Wyłudzenie danych logowania, numerów kart płatniczych lub danych osobowych.

#Phishing

Cechy charakterystyczne:

- Adres e-mail nadawcy wygląda na autentyczny (np. inpost@dostawa24.pl).
- Strona phishingowa ma certyfikat SSL (https), co może uśpić czujność.
- Często stosowane są presja czasu i groźba utraty przesyłki.

Źródło: Niebezpiecznik.pl

Przykłady szkód

Dyn DNS Attack (2016)

- **Typ:** DDoS z użyciem botnetu Mirai
- **Cel:** Dyn – dostawca DNS obsługujący m.in. Twitter, Netflix, Reddit
- **Skutek:**
  - → Przerwy w dostępie do wielu popularnych serwisów
  - → Zakłócenie działania internetu na wschodnim wybrzeżu USA

#DDoS

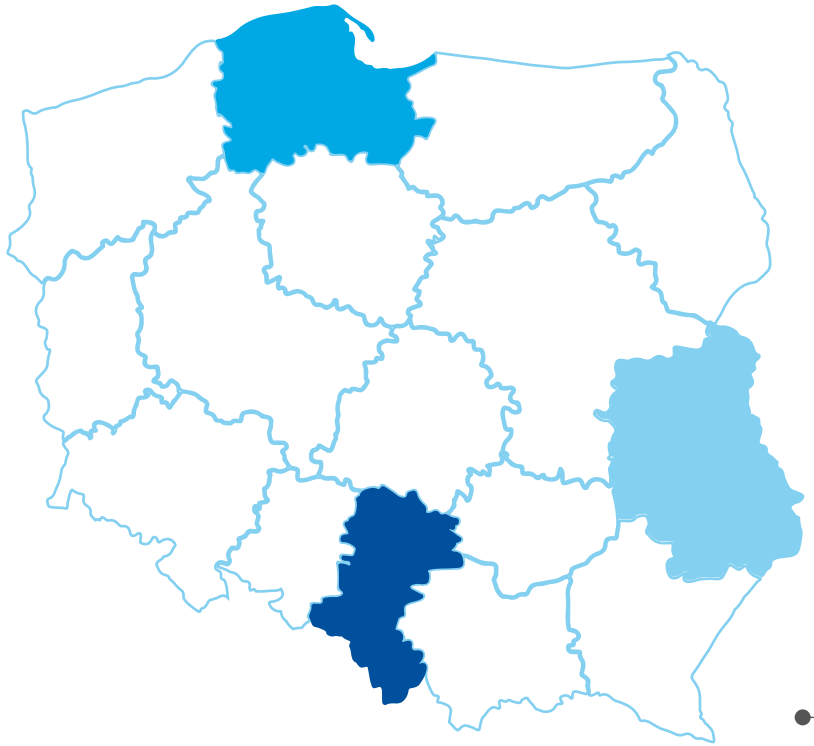
Koszty:
- Szacowane straty: ok. 100 mln USD
- Utrata reputacji i zaufania klientów

Źródło: DDoS Attack Examples (2024): The 7 Worst Attacks Ever

Ryzyka cyber w Polsce

Cyberzagrożenia w Polsce – skala, ryzyko, odpowiedzialność

Rekordowa liczba ataków w 2024 roku – czy firmy są odpowiednio zabezpieczone?



30%

Wzrost liczby ataków w sektorze finansowym.

1 800

W sektorze finansowym dochodzi do ponad 1 800 ataków tygodniowo.

2.miejsce

W Indeksie Cyberbezpieczeństwa Narodowego (NCSI).

Cyberbezpieczeństwo pod presją – 100 tysięcy ataków w 2024 roku

W Polsce obserwujemy dynamiczny wzrost zagrożeń cybernetycznych.

W 2024 – ponad 100 tysięcy ataków wymierzonych w firmy i instytucje.

Wzrost liczby ataków w sektorze finansowym, który wyniósł aż 30%.

Polska liderem cyberataków – najwyższy poziom narażenia w UE i na świecie

Polska - wysoki poziom narażenia – w 2024 roku odnotowaliśmy największą liczbę cyberataków na świecie.

Sektor finansowy - ponad 1 800 ataków tygodniowo.

Polska w czołówce cyberbezpieczeństwa

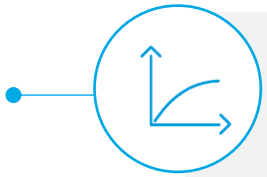
Polska zajmuje drugie miejsce w Indeksie Cyberbezpieczeństwa Narodowego (NCSI)

Cyberstatystyki 2023–2024

W ciągu zaledwie roku obserwujemy znaczący wzrost liczby zarejestrowanych incydentów cybernetycznych - aż o 23%.

CSIRT poziomu krajowego:	2023	2024	Zmiana procentowa
CSIRT NASK	80 267	103 449	▲+29%
CSIRT GOV	4 676	3 991	▼-15%
CSIRT MON	4 676	3 991	▼-28%
Sumaryczna roczna liczba zarejestrowanych incydentów:	90 784	111 660	▲+23%

+29% CSIRT NASK



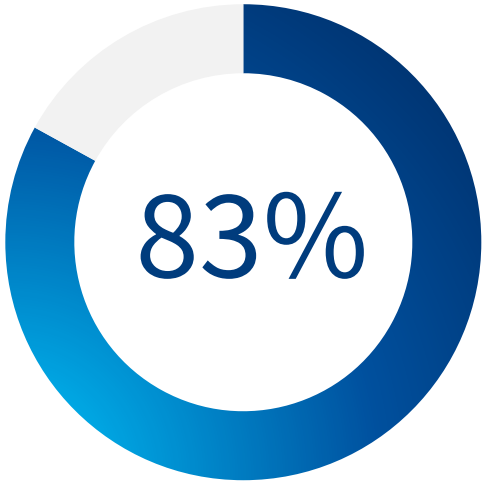
-15% CSIRT GOV

-28% CSIRT MON

CSIRT poziomu krajowego:	Zgłoszenia	Średnia dzienna	Incydenty	Średnia dzienna
2023	371 089	1 017	80 267	220
2024	609 900	1 671	103 449	283
Zmiana	▲+64%		▲+29%	

Czy ubezpieczenie cyberryzyk to dziś konieczność?

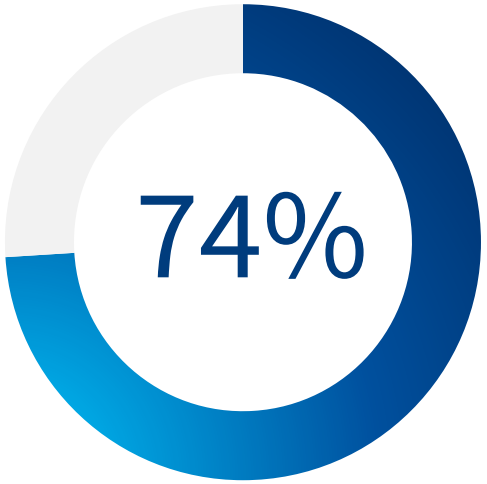
Dane nie pozostawiają wątpliwości - **ubezpieczenie od ryzyk cybernetycznych przestaje być opcją, a staje się koniecznością**.



Skala incydentów cyberbezpieczeństwa w polskich firmach

83% firm w Polsce zarejestrowało co najmniej jeden incydent cyberbezpieczeństwa w 2024 roku (wzrost o 16 p.p. względem 2023)

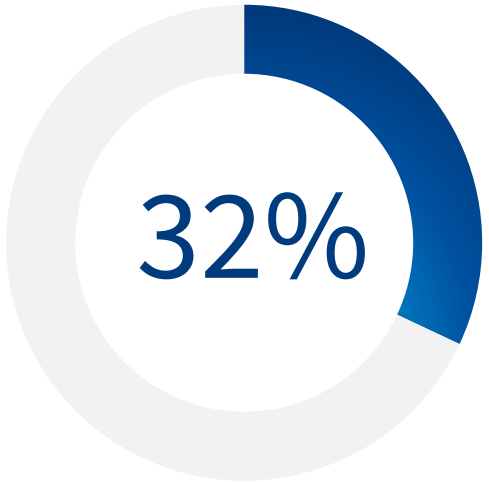
Źródło: Barometr cyberbezpieczeństwa 2025 - KPMG Poland



Gotowość firm do zapłaty okupu - realne zagrożenie ransomware

74% firm doświadczyło cyberataku, a 80% zadeklarowało gotowość zapłaty okupu w przypadku ransomware

Źródło: Raport Cyberbezpieczeństwo w polskich firmach - 2024 - BPC GUIDE



Polska na 2. miejscu w UE - skala ofiar cyberataków

32% przedsiębiorstw w Polsce padło ofiarą cyberataku - 2. miejsce w UE według Eurostatu.

Źródło: Raport EY: Oto najważniejsze wyzwania cyberbezpieczeństwa firm w Polsce | EY - Polska

Skala zagrożeń cybernetycznych w Polsce rośnie

Polska znajduje się na **2. miejscu w Unii Europejskiej** pod względem liczby przedsiębiorstw, które padły ofiarą cyberataku

Średnia liczba ataków tygodniowo na jedną firmę wzrosła z **1150 do 1848** - to niemal **60% wzrost** w ciągu kilku miesięcy.

Źródło: Cyberataki: trzy atakowane sektory w Polsce - CRN

Cyberataki kosztują – **ile tracą polskie firmy?**

Koszty cyberataków w Polsce w 2025 roku

Aż 88% organizacji w Polsce doświadczyło incydentu związanego z cyberbezpieczeństwem.

Polska znalazła się na 1 miejscu na świecie pod względem liczby wykrytych ataków ransomware w I połowie 2025 roku, wyprzedzając nawet Stany Zjednoczone i Słowację.

88%

organizacji w Polsce doświadczyło cyberataku lub wycieku danych w ostatnich latach

23%

wszystkich globalnych incydentów

Polska była **liderem światowym pod względem liczby wykrytych ataków ransomware** w I połowie 2025 roku, wyprzedzając USA (5,74%) i Słowację (5,45%)

Średni koszt ataku ransomware dla polskiej firmy:

~1 500 000 zł

Koszt usunięcia skutków ataku (np. zaszyfrowanie danych):

~ 500 000 zł dla firm zatrudniających powyżej 100 pracowników

Źródło: Polska najczęściej na świecie atakowana ransomware w 2025 roku | | ESET

Finansowe skutki cyberataków – jak wygląda sytuacja na świecie?

Cyberataki to dziś jedno z najdroższych zagrożeń dla biznes.

Średni koszt pojedynczego naruszenia danych w 2024 r. - 4,88 miliona dolarów (wzrost o 10% względem 2023).

Ataki z udziałem złośliwego insidera – koszt niemal 5 milionów dolarów.

Ataki phishingowe, przejęcia skrzynek e-mail, kradzież danych uwierzytelniających.

Finansowe skutki cyberataków są nie tylko wysokie, ale też rosną z roku na rok.

292 dni
do wykrycia i opanowania

koszt ataku z kradzieżą danych uwierzytelniających

4,99 mln USD
koszt ataku z udziałem złośliwego insidera

~ 4,88 mln USD
koszt ataku phishingowego

4,88 mln USD
koszt ataku z przejęciem skrzynki e-mail

Średni koszt pojedynczego naruszenia danych w 2024:

~4,88 mln USD

(wzrost o 10% względem 2023)

Źródło: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

Pośrednie koszty incydentów cybernetycznych

Przestoje operacyjne - utrata przychodów z powodu niedostępności systemów.

Koszty przywracania danych i systemów - informatyka śledcza, odzyskiwanie danych, nowe zabezpieczenia.

Koszty prawne i regulacyjne – grzywny, odszkodowania, postępowania sądowe.

Koszty reputacyjne – utrata klientów, spadek zaufania, konieczność działań PR.

Koszty notyfikacji - informowanie klientów o wycieku danych (wymóg RODO).

Firmy coraz bardziej świadome - cyberubezpieczenia zyskują na znaczeniu

Zwiększa się liczba zapytań
Coraz większa świadomość - zadbać należy również o cyberbezpieczeństwo swojej firmy.

Poprawia się poziom podstawowych zabezpieczeń
Stale rosnąca świadomość zagrożeń w zakresie bezpieczeństwa cybernetycznego i związane z tym działania dotyczące poprawy zabezpieczeń. Poziom zabezpieczeń - zależny od branży.

Wzrost świadomości zagrożeń
Stały wzrost świadomości zagrożeń ze strony cyberprzestępców, ataki są coraz częstsze i coraz częściej o nich słyszymy.

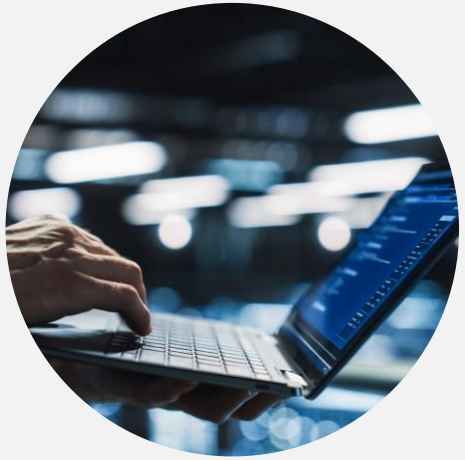
Nowe regulacje
Coraz większy nadzór nad cyberbezpieczeństwem - DORA czy NIS2

Bezpieczna firma zaczyna się od **świadomego pracownika**

Szkolenia i świadomość - fundament skutecznej ochrony przed cyberatakami

Szyfrowanie danych

Kopie zapasowe



Aktualizacje

Zabezpieczenie zdalnego dostępu

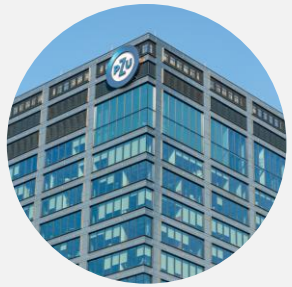
Segmentacja sieci

Bezpieczeństwo to proces – ludzie, systemy i… **dobre ubezpieczenie**

Oferta PZU - ubezpieczenia ryzyk cybernetycznych

Oferta PZU w zakresie **ubezpieczenia ryzyk cybernetycznych**

Zakres, odbiorcy, wyłączenia



Z ubezpieczenia mogą skorzystać:

→ klienci korporacyjni,

→ mali i średni przedsiębiorcy,

→ odpowiedzialni prawnie za rekordy danych osobowych lub wykorzystujący w swojej działalności infrastrukturę informatyczną.

Branże trudne:

- przemysł rozrywkowy dla dorosłych
- gry hazardowe on-line
- produkcja gier komputerowych
- wytwarzanie i przetwarzanie walut wirtualnych
- obsługa płatności
- agregacja i analityka danych
- linie lotnicze
- instytucje kościelne
- wydobycie i przetwarzanie paliw kopalnych

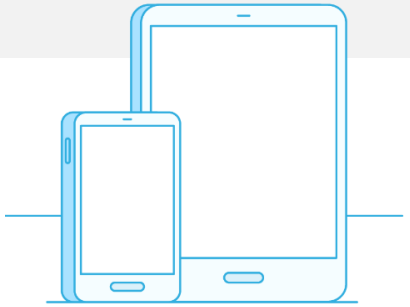
Rodzaje zdarzeń ubezpieczeniowych m. in:

- ujawnienie danych
- błąd operatora, pracownika
- włamania do baz danych, ransomware
- blokada usług
- cyberterroryzm

Skutki zdarzeń:

- spowolnienie działania lub zablokowanie sieci komputerowej
- utrata danych: klientów, pracowników, kontrahentów
- zaszyfrowanie danych i żądanie okupu za ich odzyskanie
- dostęp do danych wrażliwych przez osoby nieuprawnione
- nieplanowane przestoje i straty produkcji, utrata zysku
- utrata klientów

Ubezpiecznie ryzyk cybernetycznych to **ochrona przed stratami finansowymi (kosztami, odszkodowaniami), spowodowanymi naruszeniem danych**.



Oferta PZU w zakresie **ubezpieczenia ryzyk cybernetycznych**

Jak dobrać ubezpieczenie cybernetyczne do wielkości firmy?

OWU od ryzyk cybernetycznych

- klienci z przychodami **do 800 000 000 zł**

PZU Firma Pakiet Doradca

- klienci z przychodami **do 20 000 000 zł**

- Klauzula CYBER - zakres jak OWU
- Klauzula RODO - odpowiedzialność cywilna i administracyjna

SWU ryzyk cybernetycznych

- klienci z przychodami **powyżej 800 000 000 zł**

Dzięki takiej konstrukcji oferty, PZU może skutecznie chronić firmy każdej wielkości, niezależnie od branży czy poziomu ekspozycji na ryzyko cybernetyczne.

Konstrukcja ubezpieczenia ryzyk cybernetycznych

Kompleksowa konstrukcja polisy cyber – co obejmuje ochrona?

odpowiedzialność cywilna, administracyjna

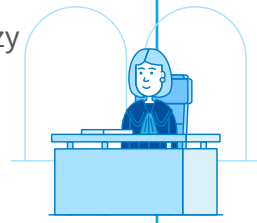
- np. odpowiedzialność z tytułu naruszenia prywatności: utrata danych klientów, pracowników
- naruszenie regulacji dotyczących ochrony danych osobowy

szkody własne, koszty

- np. koszty naruszenia koszty odtworzenia danych i programów
- utrata zysku
- utrata klientów

zarządzanie incydentem, panel specjalistów, assistance

- incydent menedżer
- biegli księgowi
- prawnicy
- agencja PR
- specjaliści IT, informatycy śledczy



Kluczowe przewagi oferty PZU

Lista ubezpieczanych działalności

Szybka i prosta ocena ryzyka

Brak podlimitów sumy ubezpieczenia

Niskie Udziały własne

Brak udziału własnego dla Kosztów Naprawienia

Odpowiedź na incydent

- Call Center - 24/7/365

Ocena ryzyka, czyli underwriting w praktyce

Ocena ryzyka

przychody do 100 000 000 zł	przychody do 300 000 000 zł
Zapora sieciowa (firewall) przeznaczona do użytku komercyjnego na wszystkich zewnętrznych bramach sieciowych oraz antywirus przeznaczonego do użytku komercyjnego w całej sieci	Wszystkie dane osobowe osób fizycznych są szyfrowane w sieci i podczas transmisji
Tworzenie kopii zapasowych istotnych danych co najmniej raz na 7 dni, przechowywanie ich w środowisku oddzielonym od pozostałej sieci oraz testowanie co najmniej co 365 dni	Wyłączono protokół RDP (Remote Desktop Protocol) na wszystkich punktach końcowych sieci, w tym na serwerach, chyba że są one chronione przez MFA
Poprawki krytyczne oprogramowania instalowane w ciągu 30 dni od ich wydania	Wdrożono protokoły SPF, DKIM lub DMARC
Zdalny dostęp do sieci zabezpieczony MFA (multifactor authentication, uwierzytelnianie wieloskładnikowe	Nie posiadasz sprzętu lub oprogramowania wycofanego z eksploatacji, a jeśli tak, to są one odizolowane od sieci
Brak szkód w okresie ostatnich 3 lat	Środowisko technologii operacyjnej (OT) jest oddzielone od systemów IT
	Roczny przychód z transakcji online nie przekracza 25% całości przychodów

Ubezpieczenia od ryzyk cybernetycznych – dostępne online

Od 1 października 2025 r. na platformie **mojaFirma.pzu.pl** udostępniliśmy nowa funkcjonalność - **możliwość samodzielnego przygotowania oferty i wystawienia polisy od ryzyk cybernetycznych dla klientów.**

1

Dla kogo:

dla firm z przychodami do **100 000 000 PLN**

2

Warunki:

Suma ubezpieczenia w **3 wariantach**, w zależności od poziomu przychodów.

Pełen zakres ubezpieczenia zgodnie z OWU.

3

Co zyskujecie dzięki nowemu rozwiązaniu?

Prosta ocena ryzyka, propozycja ubezpieczenia I polisa „od ręki”.

Minimum formalności, maksimum oszczędności czasu.

Tylko 3 kroki do wystawienia polisy.

Jak uzyskać dostęp do platformy **mojaFirma.pzu.pl** – krok po kroku

W celu uzyskania dostępu do Platformy mojaFirma.pzu.pl oraz skorzystania z funkcjonalności dedykowanej obsłudze ubezpieczenia od ryzyk cybernetycznych, należy przejść przez kilka kroków:

Cyfrowy ekosystem z myślą o efektywności

Cyber na **mojaFirma.pzu.pl** to kolejny krok w rozwoju kompleksowego ekosystemu narzędzi dla brokerów, który PZU tworzy w ramach **pakietu „PZU dla Brokera”**. Celem jest nie tylko uproszczenie procesów, ale także realne wsparcie w codziennej pracy i wspólne budowaniu przewagi konkurencyjnej.

Krok 1: Wniosek o rejestrację

Formularz „Wniosek o zarejestrowanie nowego użytkownika na platformie mojaFirma.pzu.pl” można pobrać bezpośrednio ze strony internetowej **pzu.pl/korpo/materialy-do-pobrania** w zakładce **ubezpieczenie od ryzyk cybernetycznych**

Krok 2: Kontakt z doradcą

Wypełniony i podpisany wniosek prosimy o przesłanie doradcy, z którym dotychczas Państwo współpracowaliście. Jeśli nie mają Państwo przypisanego doradcy, można go znaleźć poprzez stronę **pzu.pl/oddzialy-sprzedazy-korporacyjnej**.

Krok 3: Weryfikacja i dostęp

Po pozytywnej weryfikacji dokumentów otrzymacie Państwo e-maila aktywacyjnego z adresu **mojafirma@pzu.pl**. Następnie należy postępować zgodnie z instrukcją widoczną na ekranie.

Krok 4: Logowanie i korzystanie

Platforma dostępna jest pod adresem: **mojafirma.pzu.pl**. Znajdą tam Państwo również wymagania techniczne oraz regulamin korzystania z systemu.

Ubezpieczenie odpowiedzialności zawodowej z tytułu działalności technologicznej. OC zawodowe IT

PZU dla IT – kompleksowa ochrona dla cyfrowego biznesu

Ubezpieczenie **skierowane do przedsiębiorców z branży technologii informatycznej**, w szczególności wykonujących działalność związaną z oprogramowaniem i doradztwem w zakresie informatyki oraz działalność powiązaną.

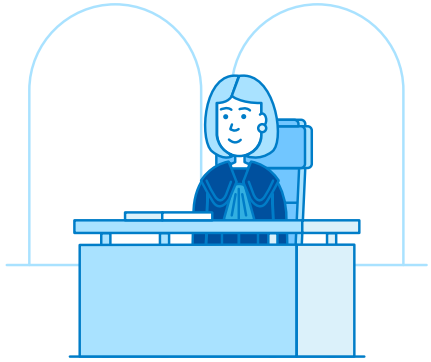
Adresaci produktu

- Software House'y (firmy tworzące dedykowane oprogramowanie)
- Dostawcy usług chmurowych
- Usługi hostingowe / tworzenie stron internetowych
- Sprzedaż, instalacja i konserwacja oprogramowania firm trzecich
- Oprogramowanie i usługi związane z bezpieczeństwem
- Usługi zarządzane (umowy SLA - Service Level Agreement)
- Producent lub projektanci sprzętu IT
- wiele innych…

Zakres ochrony

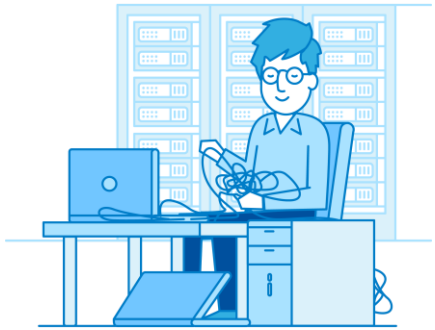
- Szkody wyrządzone osobie trzeciej z tytułu naruszenia dotyczącego usług technicznych i profesjonalnych
- Szkody wyrządzone osobie trzeciej z tytułu naruszenia dotyczącego produktów technicznych
- Koszty

Jakie szkody chroni ubezpieczenie OC zawodowe IT?



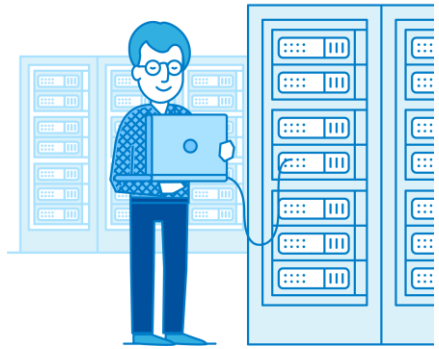
Naruszenie praw autorskich

- Ubezpieczony instaluje oprogramowanie na urządzeniach technicznych (np. sterownikach PLC, komputerach przemysłowych) bez posiadania odpowiedniej liczby licencji.
- Ubezpieczony modyfikuje oprogramowanie dostarczone przez zewnętrznego dostawcę, naruszając warunki licencji (np. open source z ograniczeniami).
- Ubezpieczony integruje cudze oprogramowanie (np. bibliotekę do analizy danych) w swoim produkcie technicznym bez uzyskania licencji.
- Ubezpieczony instaluje oprogramowanie przeznaczone wyłącznie do użytku OEM na urządzeniach, które nie spełniają tych warunków (naruszenie licencji OEM).



Skasowanie danych / uszkodzenie danych

- Ubezpieczony kasuje przez przypadek bazę zdjęć firmy medialnej/ bazę danych klientów.
- Uszkodzenie bazy danych przy okazji aktualizacji systemów.
- Błędy podczas integracji różnych systemów.



Bezpieczeństwo

- Ubezpieczony administrujący systemami podmiotów trzecich nie reaguje na atak hakerski lub czyni to z naruszeniem wymaganych terminów reakcji.
- Ubezpieczony nie instaluje na czas wymaganych aktualizacji zabezpieczeń u klienta, którego infrastrukturą IT zarządza.
- Niewłaściwa konfiguracja dostępów do bazy danych obsługiwanej firmy – wrażliwe dane mogły trafić do niewłaściwych osób.

i wiele innych sytuacji związanych z programowaniem…


Kwestionariusz oceny ryzyka
Możliwość oparcia się na kwestionariuszu zewnętrznym

Oferta PZU

Okres ubezpieczenia: 12 miesięcy

Trigger: claims made

SG do 10 mln zł i przychody do 50 mln zł - dostępna „od ręki”

Apetyt na ryzyko

1. Outsourcing IT
2. Rozwiązania chmurowe
3. Cyberbezpieczeństwo
4. Sprzedaż i instalacja oprogramowania
5. Informatycy prowadzący działalność gospodarczą (B2B)
6. Integracja systemów IT

7. Szkolenia IT
8. Zarządzenie infrastrukturą IT/ usługi zarządzane
9. Dostawcy usług internetowych
10. Tworzenie i hosting stron internetowych, optymalizacja stron internetowych
11. Projektanci i producenci sprzętu IT
12. … i wiele innych

Zapraszamy do Oddziałów Sprzedaży Korporacyjnej PZU

pzu.pl/korpo

Bezpieczne dane, bezpieczny biznes.

Ubezpieczenie cyber i OC IT w praktyce

Szkolenie IDD

Paulina Borowiec
Marcin Jarosz

Ryzyka cybernetyczne na platformie mojaFirma.pzu.pl