



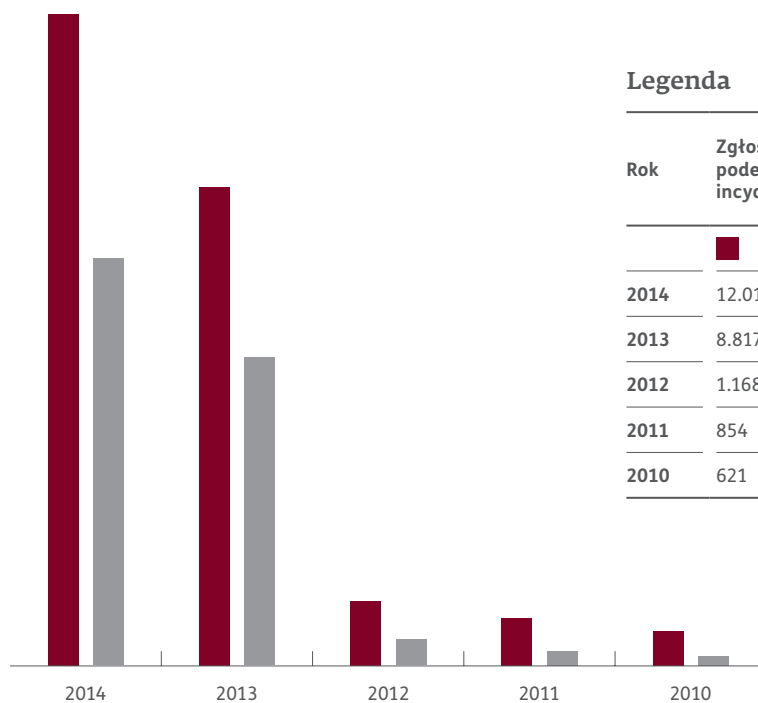
# Ryzyka cybernetyczne



W dobie technologicznego rozwoju i danych elektronicznych zabezpieczenie się przed szkodami cybernetycznymi staje się konieczne. Według ekspertów ryzyka cybernetyczne będą w najbliższych latach jednym z głównych zagrożeń dla przedsiębiorstw i instytucji.

Pokazują to dane [cert.gov.pl](http://cert.gov.pl), gdzie ilość incydentów, do których dochodzi poprzez sieć internetową nieustannie wzrasta.

### Ryzyka cybernetyczne



#### Legenda

Rok	Zgłoszone podejrzenia incydentów	Faktyczne incydenty
	<span style="color: red;">■</span>	<span style="color: grey;">■</span>
2014	12.017	7.498
2013	8.817	5.670
2012	1.168	457
2011	854	249
2010	621	155



## Zagrożenia

Każde przedsiębiorstwo, które gromadzi dane elektroniczne, ponosi ryzyko związane z ich utratą lub kradzieżą. Żadna firma nie jest zabezpieczona w taki sposób, aby być pewną braku zagrożenia. Powstające nowe grupy hakerów oraz tworzone nowe złośliwe oprogramowanie sprawia, że trudno jest zwalczać wszelkie możliwe zagrożenia, zarówno wewnętrzne (nieuczciwi pracownicy) jak i zewnętrzne (ataki hakerskie).

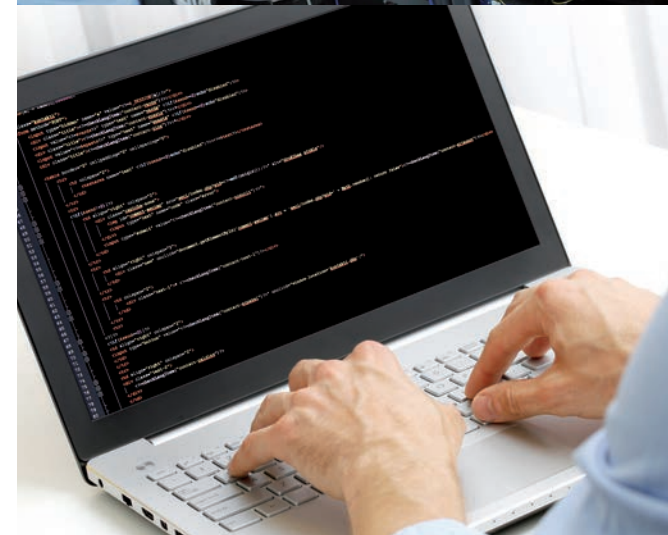
## Dla kogo?

Każde przedsiębiorstwo, bez względu na jego wielkość, liczbę zatrudnionych pracowników czy rodzaj branży, narażone jest na ataki cyberprzestępców. Duże firmy przeznaczają znaczne nakłady finansowe na utrzymanie i ulepszanie własnej infrastruktury informatycznej. To powoduje, że średnie i małe podmioty, ze względu na mniejsze możliwości finansowe, mogą być łatwiejszym celem ataków.

## Oferta

Skierowana jest do polskich przedsiębiorstw, które przetwarzają dane elektroniczne m.in.:

-  firmy produkcyjne
-  firmy handlowe
-  e-commerce sklepy internetowe
-  hotele
-  firmy i hurtownie budowlane
-  pośrednictwo finansowe
-  edukacja
-  ochrona zdrowia / szpitale



## Zakres ubezpieczenia

**ERGO Hestia oferuje ubezpieczenie od ryzyk cybernetycznych.** Nie trzeba się obawiać kosztów związanych z utratą lub uszkodzeniem danych elektronicznych oraz kosztów odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim w wyniku ataku komputerowego. Jeżeli doszło do ataku hakerskiego i/lub system został zainfekowany wirusem komputerowym pokryjemy koszty związane z utratą danych.

### Sekcja I ubezpieczenia

dane elektroniczne

- a. koszty przywrócenia danych elektronicznych
- b. koszty zakupu nowego oprogramowania
- c. koszty odtworzenia danych elektronicznych
- d. koszty usunięcia złośliwego oprogramowania
- e. koszty przywrócenia dostępu do danych elektronicznych

### Sekcja II ubezpieczenia

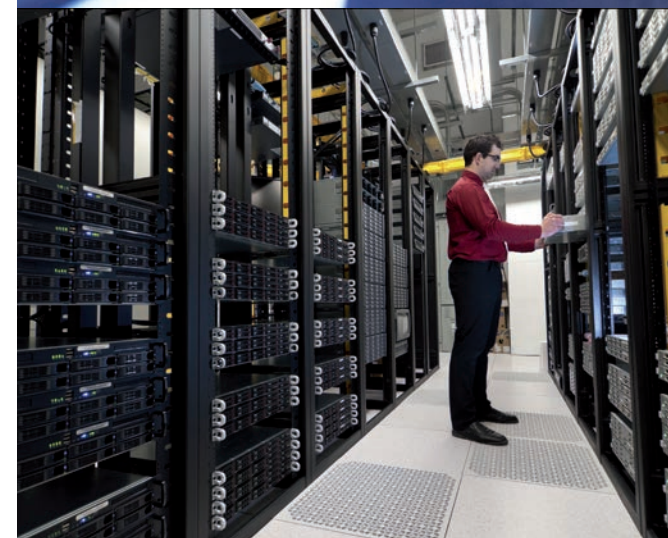
koszty dodatkowe

- m.in.
- a. koszty public relations w celu przywrócenia reputacji lub wizerunku publicznego
- b. koszty przeniesienia nieutraconych danych na inne serwery
- c. koszty porady prawnej
- d. koszty ograniczenia skutków utraty danych

### Sekcja III ubezpieczenia

odpowiedzialność cywilna

- a. koszty odtworzenia danych elektronicznych u poszkodowanych (osób trzecich)
- b. koszty przywrócenia danych elektronicznych u poszkodowanych (osób trzecich)
- c. koszty przywrócenia systemu u poszkodowanych (osób trzecich)
- d. koszty działania specjalistów z zakresu informatyki śledczej poniesione na poszukiwanie sprawcy ataku komputerowego
- e. koszty postępowań administracyjnych związanych z ochroną danych osobowych (GIODO) oraz ochroną prawa własności intelektualnej (Urząd Patentowy)
- f. utracone korzyści poniesione przez osoby trzecie powstałe wskutek uszkodzenia, utraty danych elektronicznych lub powstałych w wyniku wycieku danych personalnych osób trzecich



**W ramach ubezpieczenia oferujemy pomoc od wyspecjalizowanej w informatyce śledczej firmy, która w ciągu 24 h skontaktuje się z Państwem w celu rozpoczęcia procesu zwalczania zagrożenia.**

ERGO Hestia współpracuje z najlepszymi w Polsce firmami zajmującymi się wykrywaniem i analizowaniem incydentów informatycznych tj. włamania do sieci czy nieetycznymi lub niezgodnymi z prawem działaniami hakerskimi. Wystarczy jeden kontakt telefoniczny z naszą infolinią, aby rozpocząć proces usunięcia zagrożenia.

Tylko ubezpieczenie od ryzyk cybernetycznych zapewnia ochronę od szkód spowodowanych przez nieuczciwych hakerów lub pracowników oraz wirusy komputerowe. Ubezpieczenie sprzętu elektronicznego obejmuje bowiem zakresem fizyczne uszkodzenie danych, które zapisane są na urządzeniach mobilnych czy stacjonarnych.

Zakres Ubezpieczenia	Ubezpieczenie Sprzętu Elektronicznego	Ubezpieczenie Danych Elektronicznych od Ryzyk Cybernetycznych
Utrata danych wskutek fizycznego uszkodzenia sprzętu	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Utrata danych i programów wskutek cyberataku	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Utrata danych i programów wskutek złośliwego oprogramowania	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Odpowiedzialność cywilna związana z utratą danych po cyberataku	<input type="checkbox"/>	<input checked="" type="checkbox"/>



## Przykładowe scenariusze szkodowe

### **Kradzież danych przez pracownika (sekcja I i II)**

Pracownik, który nie miał dostępu do poufnych danych, złamał system zabezpieczenia i uzyskał nieautoryzowany dostęp. W wyniku tego doszło do kradzieży i utraty danych elektronicznych.

### **Zablokowanie dostępu do danych i/lub komputerów (sekcja I i II)**

Nieznani sprawcy przeprowadzili atak komputerowy na serwery oraz stacje robocze. Na skutek ataku zablokowany został dostęp do wszystkich danych, co skutkowało wstrzymaniem pracy przez zakład.

### **Uszkodzenie oprogramowania (sekcja I i II)**

Pewna grupa przestępcza przesłała drogą mailową do pracowników firmy zainfekowane załączniki. Ochrona antywirusowa firmy nie była wystarczająco szczelna i doszło do uszkodzenia systemów i programów, które nie działały.

### **Utrata danych klientów (sekcja III)**

Atak hakerski spowodował utratę wrażliwych danych klientów, co skutkowało wszczęciem przez niektórych z nich postępowania przed GIODO. GIODO w trakcie wyjaśnień nakazuje zabezpieczenie danych i przeniesienie ich do innej lokalizacji.

### **Utrata korzyści (sekcja III)**

Wydawca dziennika regionalnego pada ofiarą ataku komputerowego, za który odpowiedzialność ponosi ubezpieczony. Atak skutkuje awarią systemów i utratą danych. W wyniku awarii i utraty danych wydawca gazety nie zdążył na czas wystać do drukarni kolejnego numeru gazety i dzienny nakład nie został sprzedany.



W celu uzyskania szczegółowych informacji, zachęcamy do kontaktu z underwriterami w naszych przedstawicielstwach korporacyjnych.