Kompleksowa Cyberochrona – porównanie zakresów

	Cyber **M**	Cyber **XL***
Zdarzenie ubezpieczeniowe		
Atak komputerowy	✓	✓
Naruszenie bezpieczeństwa danych	–	✓
Błąd ludzki	–	✓
SEKCJA I / Ubezpieczenie danych elektronicznych		
przywrócenie danych	✓	✓
odtworzenie danych	✓	✓
zakup nowego oprogramowania	–	✓
odblokowanie dostępu do danych	✓	✓
zakres terytorialny cały świat	✓	✓
dane w chmurze obliczeniowej	–	✓
e-kradzież	–	✓
SEKCJA II / Koszty dodatkowe		
porada prawna	✓	✓
public relations	–	✓
notyfikacja klientów (RODO)	✓	✓
poszukiwanie sprawcy szkody	–	✓
kary administracyjne (RODO)	✓	✓
okup / wymuszenie	–	✓
zakup nowego sprzętu elektronicznego	–	✓
PCI DSS	✓	✓
SEKCJA III / Odpowiedzialnosć cywilna		
odpowiedzialność za naruszenie prywatności i zachowanie poufności (RODO)	✓	✓
odpowiedzialność za bezpieczeństwo sieci	–	✓
informatyka śledcza	–	✓
działalność multimedialna	✓	✓
postępowania i kary administracyjne osób trzecich	–	✓
SEKCJA IV / Utrata zysku		
utrata zysku	–	✓
zwiększone koszty działalności	–	✓

* w celu zawarcia ubezpieczenia Cyber XL prosimy o kontakt z Underwriterami Przedstawicielstw Korporacyjnych

Niniejszy materiał ma charakter wyłącznie marketingowy oraz nie stanowi oferty w rozumieniu art. 66 Kodeksu Cywilnego. Służy wyłącznie celom informacyjnym.

www.cyberochrona.ergohestia.pl

MATERIAŁ WEWNĘTRZNY

Cyber M

Cyberochrona
dla małych i średnich przedsiębiorstw

www.cyberochrona.ergohestia.pl

Wniosek o przystąpienie do ubezpieczenia

Ocena ryzyka

Czy w Państwa firmie:

1.	obrót za ostatni zamknięty rok kalendarzowy był mniejszy niż 15.000.000 PLN?	☑ TAK	☐ NIE
2.	na wszystkich komputerach i serwerach są zainstalowane i regularnie aktualizowane licencjonowane zabezpieczenia antywirusowe?	☑ TAK	☐ NIE
3.	kopia zapasowa danych wykonywana jest przynajmniej raz w tygodniu?	☑ TAK	☐ NIE
4.	korzysta się jedynie ze wspieranych przez producenta systemów komputerowych, które są regularnie aktualizowane, nie później niż miesiąc od daty dostępności aktualizacji?	☑ TAK	☐ NIE
5.	używa się zapór sieciowych (firewall)?	☑ TAK	☐ NIE
6.	potwierdza się, że w ostatnich 3 latach nie było incydentów cybernetycznych?	☑ TAK	☐ NIE
7.	hasła używane do logowania w systemach komputerowych mają minimum 8 znaków, w tym przynajmniej jeden znak specjalny oraz jedną wielką literę?	☑ TAK	☐ NIE

Zawarcie polisy możliwe wyłącznie w przypadku odpowiedzi „TAK" na wszystkie z powyższych pytań. W przypadku odpowiedzi „NIE" na którekolwiek z pytań, oferta może być przedstawiona wyłącznie po konsultacji z Underwriterem z przedstawicielstwa.

Wybór wariantu

Matryca składki CYBER M* (PLN)		Limit odpowiedzialności na jedno i wszystkie zdarzenia (PLN)			
		100.000	**200.000**	**500.000**	**1.000.000**
Obrót roczny (PLN)	do 2 mln	400	600	1.000	1.500
	do 5 mln	–	900	1.300	1.900
	do 8 mln	–	–	1.600	2.100
	do 15 mln	–	–	1.800	2.900

Wybieram wariant ze składką .....

.....

data i podpis Ubezpieczającego

* Matryca składki nie dotyczy szkół, gdzie wielkość klienta badana jest po liczbie uczniów.

Instrukcja do wniosku o przystąpienie do ubezpieczenia

Mamy świadomość, że charakter oceny ryzyka w produktach cyber jest szczególny. Dla pełnego zrozumienia zadanych pytań udostępniamy Państwu materiały, który stanowią instrukcję do wniosku niezbędnego do zawarcia ubezpieczenia Cyber M.

1.	Czy w Państwa firmie na wszystkich komputerach i serwerach są zainstalowane i regularnie aktualizowane zabezpieczenia antywirusowe?	Oprogramowanie antywirusowe jest programem komputerowym, który wykrywa i usuwa znane zagrożenia w postaci wirusa komputerowego. **Posiadanie licencjonowanego oprogramowania antywirusowego dla firm jest standardowym zabezpieczeniem i stanowi minimum bezpieczeństwa.**
2.	Czy w Państwa firmie używa się zapór sieciowych (firewall)?	Zapora sieciowa, inaczej firewall, to sprzęt / oprogramowanie, które broni przed niepowołanym dostępem do sieci lub komputera. **Posiadanie zapory sieciowej dla firm jest standardowym zabezpieczeniem i stanowi minimum bezpieczeństwa.**
3.	Czy w Państwa firmie kopia zapasowa danych wykonywana jest przynajmniej raz w tygodniu?	Tworzenie kopii zapasowej jest niezbędne do szybkiego przywrócenia danych i odzyskania kontroli nad firmą, a tym samym normalnego funkcjonowania przedsiębiorstwa. **Regularne wykonywanie kopii zapasowej nie gwarantuje bezpieczeństwa przechowywanych danych, jednakże minimalizuje ryzyko ich utraty.**
4.	Czy w Państwa firmie korzysta się jedynie ze wspieranych przez producenta systemów komputerowych, które są regularnie aktualizowane, nie później niż miesiąc od daty dostępności aktualizacji?	Wspierane systemy operacyjne to takie, które są regularnie aktualizowane przez dział techniczny producenta. **Niektóre systemy operacyjne np. Windows XP / 7 zostały pozbawione wsparcia producenta. Oznacza to, że systemy te nie są regularnie aktualizowane, a co się z tym wiąże, są podatne na wszelkie nowe zagrożenia, takie jak wirusy komputerowe.** *Dla systemu Windows 7 zaleca się jedno z poniższych rozwiązań:* *1. Zaktualizowanie Windows 7 do Windows 10.* *2. Wykupienie 3-letniego wsparcia producenta dla Windows 7.* *3. Odseparowanie stacji roboczych z systemem Windowsa 7 od sieci internetowej (offline).* *Jeśli klient wykonał krok 2 lub 3 z powyższego zalecenia, można traktować system Windows 7 jako wspierany na potrzeby oceny ryzyka.*
5.	Czy w Państwa firmie w ostatnich 3 latach nie wystąpiły incydenty cybernetyczne?	Za incydent cybernetyczny uznajemy atak hakerski lub działanie złośliwego oprogramowania, które skutkowało poniesioną stratą finansową np. zapłatą specjalistycznej firmie, wymianą sprzętu. Jeżeli klient miał zdarzenie cybernetyczne, ale nie poniósł z tego tytułu żadnych kosztów, nie uznajemy tego za zdarzenie cybernetyczne. **W przypadku wystąpienia incydentów cybernetycznych prosimy o uzyskanie dodatkowych informacji, takich jak: poniesione straty, okoliczności zdarzenia i przedsięwziętych działań na przyszłość. Pozwoli to nam na podjęcie decyzji o możliwym ubezpieczeniu.**
6.	Czy w Państwa firmie hasła używane do logowania w systemach komputerowych mają minimum 8 znaków, w tym przynajmniej jeden znak specjalny oraz jedną wielką literę?	Posiadanie hasła o odpowiedniej sile chroni przed niepowołanym dostępem osób postronnych, w tym nieuczciwych pracowników. **Hasło jest pierwszym i podstawowym zabezpieczeniem dostępu do infrastruktury sieciowej i stanowi minimum bezpieczeństwa.**