KG BROKER
UBEZPIECZENIA

CYBERBEZPIECZEŃSTWO

dla MŚP - 9 kroków do odporności

Czyli co powinna zrobić **firma,** aby się zabezpieczyć przed wszelkimi zagrożeniami

www.gawron-broker.pl

Firmy, również z sektora MŚP, coraz częściej korzystają z cyfrowych narzędzi i rozwiązań.

Tym samym są coraz bardziej narażone na różnego rodzaju cyberzagrożenia.

Z raportu KPMG wynika, że w ciągu roku aż 83% przedsiębiorstw doświadcza co najmniej jednego incydentu związanego z cyberbezpieczeństwem.

Niestety, badanie Agencji Unii Europejskiej ds. **Cyberbezpieczeństwa (ENISA) pokazuje, że większość firm z sektora MŚP nie zdaje sobie sprawy z cyberzagrożeń,** sądząc, że to dotyczy tylko największych podmiotów.

Tymczasem na działanie cyberprzestępców narażone są wszystkie przedsiębiorstwa, nawet najmniejsze. **Na szczęście nawet mała firma może podjąć kroki, które zwiększą jej odporność na cyberataki.**

www.ochronacyber.pl

Spis treści

Czego dowiesz się z tego artykułu?

- **Jak ocenić** najważniejsze obszary wymagające wzmocnienia w Twojej firmie w związku z cyberzagrożeniami?
- **Jakie działania** pozwolą zwiększyć cyberodporność operacyjną przedsiębiorstwa?
- **Jak zbudować procesy,** które realnie ograniczają skutki cyberataków?
- **Jak przygotować zespół** do reagowania na incydenty w praktyce?
- **Jak zaplanować rozwój** cyberbezpieczeństwa na kolejne miesiące?

Krok 1:

Wyznaczenie osoby odpowiedzialność za cyberbezpieczeństwo

Proces zwiększania cyberbezpieczeństwa w małej lub średniej firmie warto rozpocząć od wyznaczenia pracownika odpowiedzialnego za ten obszar.

To powinna być osoba

- **z zarządu**
- **dyrekcji**
- **istotnego działu**

Ważne, żeby potrafiła koordynować działania związane z cyberbezpieczeństwem.

Oczywiście najlepiej, gdyby był to specjalista od cyberbezpieczeństwa, ale trudno oczekiwać, żeby najmniejsze firmy było stać na taką osobę, tym bardziej że już teraz na świecie brakuje niemal 5 mln takich profesjonalistów .

Chodzi o to, żeby osoby zarządzające firmą zdały sobie sprawę, iż **cyberbezpieczeństwo to nie tylko zadanie dla działu IT,** którego w małych podmiotach nawet nie ma.

Strategiczna odpowiedzialność spoczywa na osobach zarządzających firmą, ponieważ **cyberbezpieczeństwo wykracza poza kwestie technologiczne,** a każdy incydent może powodować poważne konsekwencje (paraliż przedsiębiorstwa, kradzież danych, utrata reputacji u klientów itp.).

Osoba odpowiedzialna za **cyberbezpieczeństwo ułatwia wdrażanie rozwiązań** z tego obszaru i pilnuje przestrzegania procedur, a także raportuje do zarządu.

Krok 2:

Ocena ryzyka i inwentaryzacja zasobów

Niezwykle ważna jest identyfikacja najcenniejszych zasobów firmy (dane, systemy) oraz potencjalnych zagrożeń (np. phishing, ransomware).

Bez takiej wiedzy nie sposób dobrać odpowiednich zabezpieczeń ani przygotować planu odzyskiwania danych po ataku.

1. Warto zatem sporządzić listę najważniejszych zasobów i przeprowadzić prostą ocenę ryzyka: **co im grozi i jakie byłyby skutki w przypadku wystąpienia incydentu.**
2. Potem trzeba taką listę **regularnie aktualizować wraz ze zmianami w firmie lub po cyberatakach,** których efekt nie został zminimalizowany.
3. **Dzięki temu będzie można poprawić to, co zawiodło.**

Krok 3:

Przygotowanie polityki i procedury bezpieczeństwa

Kolejny krok zwiększania cyberbezpieczeństwa to **spisanie podstawowych zasad korzystania z firmowych systemów,**
np. używania e-maila, haseł czy urządzeń prywatnych.

Takie zasady muszą zostać sporządzone w formie **polityki bezpieczeństwa,** a wszystkie zapisy powinny być zrozumiałe dla pracowników.

Stopień zrozumienia należy bezwzględnie **sprawdzić.**

Dokument powinien być krótki i napisany prostym językiem,
a także musi uwzględniać wymogi prawne (np. RODO).

Politykę bezpieczeństwa należy włączyć do regulaminu pracy i omawiać podczas wdrażania nowych pracowników,
żeby każdy znał podstawowe reguły cyberbezpieczeństwa w firmie i konsekwencje ich łamania.

Krok 4:

Budowanie świadomości i szkolenie pracowników

Wiele incydentów zaczyna się od ludzkiego błędu,
np. od kliknięcia zainfekowanego linku lub załącznika.

Z tego względu trzeba regularnie szkolić pracowników z cyberbezpieczeństwa.
Tymczasem z raportu firmy ESET wynika, że

52% zatrudnionych!

w polskich firmach nie przeszło takiego szkolenia w ciągu ostatnich 5 lat.

Program minimum powinien obejmować:

- **rozpoznawanie phishingu i innych oszustw,**
- **bezpieczne korzystanie z e-maili i internetu,**
- **ochronę haseł (w tym używanie MFA),**
- **zasady bezpiecznej pracy zdalnej.**

Szkolenia muszą objąć wszystkich i warto je urozmaicać np. testowymi kampaniami phishingowymi.

Krok 5:

Zarządzanie tożsamością i dostępem

W kolejnym kroku warto postawić na **właściwe zarządzanie dostępami.**

01 To bardzo **skuteczne podniesienie poziomu cyberbezpieczeństwa** bez dużych wydatków.

02 Pracodawca powinien wymagać od pracowników **tworzenia unikalnych, silnych haseł do wszystkich kont** (najlepiej z użyciem menedżera haseł) i włączenia wszędzie uwierzytelniania dwuskładnikowego (MFA).

03 **To jedno z najskuteczniejszych zabezpieczeń,** a tymczasem korzysta z niego mniej 25% firm w Polsce.

04 Pracodawca powinien także **ograniczyć uprawnienia użytkowników** do niezbędnego minimum.

05 Musi również pamiętać o **odbieraniu od razu dostępu po odejściu pracownika,** żeby żadne nieużywane konto nie pozostało aktywne.

Krok 6:

Podstawowe zabezpieczenia techniczne

Żadna firma, nawet najmniejsza, nie może zapomnieć o cyberhigienie, która jest wręcz podstawą.

Trzeba pamiętać o systematycznym aktualizowaniu systemów i aplikacji (łatki bezpieczeństwa).

Koniecznym krokiem jest także zainstalowanie **oprogramowania antywirusowego** na wszystkich urządzeniach.

- Wydaje się, że tooczywistość, tymczasem jedynie 59% firm w Polsce korzysta z antywirusów.
- Warto także stosować zaporę sieciową (firewall) między siecią firmową a internetem (zarządza ruchem wychodzącym i przychodzącym, jest ważnym narzędziem ochrony).
- Najlepiej także wyłączyć zbędne usługi i podzielić sieć na segmenty (oddzielić np. sieć dla gości czy IoT od sieci głównej, używanej na co dzień przez firmę).
- Działania te znacząco podnoszą odporność organizacji na ataki.

Krok 7:

Kopie zapasowe i procedury działania

Backupy to ostatnia linia obrony przed cyberkatastrofą.

Z tego powodu firmy powinny regularnie tworzyć **kopie zapasowe najważniejszych danych** i przechowywać je w odseparowanych miejscach zgodnie z zasadą

3-2-1: **trzy kopie na dwóch różnych nośnikach, w tym jedna offline.**

To jednak nie wszystko. Trzeba także testować odtwarzanie systemów z backupów, aby mieć pewność, że w razie ataku dane można będzie przywrócić.

Warto też przygotować **krótką checklistę na wypadek ataku ransomware** – kogo zawiadomić i jakie działania podjąć, aby zminimalizować szkody.

Krok 8:

Przygotowanie planu reagowania na incydenty i ćwiczenia

Ostatni krok zwiększania cyberbezpieczeństwa w firmie to przygotowanie planu reagowania na incydent, czyli co robić podczas ataku.

Celem nie jest całkowite uniknięcie incydentów, lecz szybkie opanowanie sytuacji.

1

W takim planie trzeba określić, **jak rozpoznać incydent,** kto decyduje, jak odciąć zaatakowane systemy oraz kogo powiadomić (np. CERT Polska).

2

Aby się upewnić, że **plan rzeczywiście działa,** należy przeprowadzać regularne ćwiczenia. To może być np. raz do roku symulowanie ataku z udziałem kadry kierowniczej.

3

Bez takich ćwiczeń nikt nie wie, czy procedury zadziałają i czy trzeba coś w nich poprawić.

RAPORT ESET

ujawnia, że jedynie 32% firm w Polsce wykonuje takie testy, a to bardzo **duży błąd.**

Krok 9:

Ubezpieczenie Cyber

Ubezpieczenie cyber pomoże w sytuacji ataku hakerskiego, wycieku danych lub nieuprawnionego dostępu do systemów informatycznych firmy. Zapewnia pokrycie kosztów reakcji na incydent, w tym działań informatyków, specjalistów IT oraz firm zajmujących się odzyskiwaniem danych.

Obejmuje także **wsparcie prawne i pokrycie kosztów obrony** w przypadku roszczeń związanych z naruszeniem ochrony danych osobowych (RODO).

Ubezpieczenie **pokrywa koszty powiadomienia klientów i kontrahentów o naruszeniu bezpieczeństwa danych.**

Dodatkowo **może finansować działania naprawcze i wizerunkowe,** w tym komunikację kryzysową. Chroni również przed stratami finansowymi wynikającymi z przerwy w działalności spowodowanej incydentem cybernetycznym.

Dzięki temu przedsiębiorca może szybciej wrócić do normalnego funkcjonowania po zdarzeniu.

Podsumowanie

Firmy z sektora MŚP muszą zdawać sobie sprawę,
że cyberbezpieczeństwo nie jest jednorazowym działaniem, ale procesem.

Firmy z sektora MŚP muszą zdawać sobie sprawę, że **cyberbezpieczeństwo nie jest jednorazowym działaniem,** ale procesem.

Przestępcy nieustannie rozwijają metody ataków i używają do tego coraz bardziej zaawansowanych narzędzi (np. sztuczną inteligencję). To wymaga od firm ciągłego rozwijania cyberodporności, cyklicznego przeglądu procedur i technologii oraz dostosowywania ich do zmieniających się zagrożeń i ryzyka.

Warto potraktować przedstawione w tym artykule kroki jako plan rozłożony na tygodnie i konsekwentnie wdrażać poszczególne etapy, nie zapominając o regularnych szkoleniach pracowników **z cyberbezpieczeństwa i o przeprowadzaniu ćwiczeń pozorujących cyberatak.**

FAQ

Czy mała firma bez działu IT jest w stanie samodzielnie podnieść swój poziom cyberbezpieczeństwa?

Tak, wiele podstawowych działań (np. szkolenia z phishingu, aktualizacje systemów, proste procedury) można wdrożyć samodzielnie. W bardziej złożonych obszarach (np. konfiguracja chmury, segmentacja sieci) warto zdecydować się na współpracę ze specjalistą od cyberbezpieczeństwa.

Jak często MŚP powinno aktualizować swoje procedury i politykę bezpieczeństwa?

Dobrą praktyką jest ich przegląd przynajmniej raz w roku oraz po każdym poważniejszym incydencie, po wdrożeniu nowej technologii lub wejściu w życie istotnych zmian prawnych. Regularne aktualizacje pozwalają uwzględnić nowe typy zagrożeń, zmiany w modelu pracy (np. większy udział pracy zdalnej) i doświadczenia z realnych sytuacji w firmie.

Czy korzystanie z darmowego oprogramowania jest bezpieczne dla firm?

Darmowe rozwiązania mogą być lepsze niż brak ochrony, ale często mają ograniczoną funkcjonalność, słabsze wsparcie i brak funkcji istotnych z punktu widzenia biznesu (np. raportowanie, SLA). W przypadku systemów krytycznych dla działalności firmy (np. poczta, systemy finansowe) zaleca się korzystanie z rozwiązań komercyjnych lub usług profesjonalnych dostawców.

Ile kosztuje dobra polisa Cyber?

Koszt dobrej polisy Cyber dla średniej firmy w Polsce najczęściej mieści się w przedziale 2 000–8 000 zł rocznie, ale ostateczna składka zależy od kilku kluczowych czynników.

Największy wpływ mają: wielkość firmy i obroty, ilość oraz rodzaj przetwarzanych danych (zwłaszcza danych osobowych), branża, poziom zabezpieczeń IT oraz wybrana suma ubezpieczenia (np. 500 tys. zł, 1 mln zł lub więcej). Dla firmy zatrudniającej ok. 20–50 pracowników, z obrotami kilku–kilkunastu mln zł rocznie i sumą ubezpieczenia 1 mln zł, typowa składka wynosi około 3 000–5 000 zł rocznie.

Wyższe składki pojawiają się w branżach bardziej narażonych (IT, e-commerce, finanse, medycyna) lub przy słabszych zabezpieczeniach.

W zamian polisa zapewnia realne wsparcie finansowe, techniczne i prawne w razie cyberataku, co często kosztowałoby wielokrotnie więcej niż sama składka.

KG BROKER
UBEZPIECZENIA

www.gawron-broker.pl