fundacja instytut
CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo w mikro, małych i średnich przedsiębiorstwach

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Prawo okazuje się skuteczne tylko wtedy, gdy możliwe jest jego efektywne wdrażanie – za pośrednictwem obywateli świadomych jego oddziaływania. W dzisiejszym dynamicznym środowisku biznesowym, w którym technologie cyfrowe stanowią rdzeń funkcjonowania przedsiębiorstw, cyberbezpieczeństwo staje się nieodłącznym elementem codzienności każdej firmy, niezależnie od jej wielkości. Dla mikro-, małych i średnich przedsiębiorstw (MŚP), które często posiadają ograniczone zasoby finansowe i kadrowe, ochrona przed cyberatakami staje się wyzwaniem o szczególnym znaczeniu. W różnych aspektach dbania o bezpieczeństwo danych i systemów informatycznych każdy pojedynczy pracownik odgrywa kluczową rolę.

Źródło: Flickr (CC 2.0)

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Wdrożenie polityki i procedur bezpieczeństwa

Pierwszym krokiem każdej firmy powinno być ustanowienie klarownej polityki i jasnych procedur bezpieczeństwa – w tym informacji. To obejmuje m.in. określenie zasad korzystania z systemów informatycznych, zarządzania hasłami, dostępu do danych oraz postępowania w przypadku incydentów bezpieczeństwa. Pracowników należy dobrze poinstruować na temat tych procedur, a ich przestrzeganie powinno być regularnie monitorowane i egzekwowane. Procedury, niezależnie od wielkości przedsiębiorstwa, muszą być klarowne, aby każdy pracownik był w stanie reagować maksymalnie szybko i skutecznie.

Zgodnie z VI edycją raportu Cyberbezpieczeństwo w polskich firmach1 aż 94,4% ankietowanych deklaruje, że korzysta ze sprzętu firmowego do celów prywatnych. Ponadto wyłącznie 26,4% badanych firm ma przygotowany scenariusz postępowania w przypadku ataku cybernetycznego.

W wielu przedsiębiorstwach słaba komunikacja i brak jasno określonych ram organizacyjnych należą do głównych problemów wpływających na niską efektywność działania względem pierwotnie zakładanego stanu. Identyfikacja wskazanych wyżej problemów może martwić, zwłaszcza gdy wymagane są precyzyjne komunikaty określające zasady reagowania, które muszą być bezzwłocznie wdrażane.

Świadomość i edukacja pracowników

Najistotniejsza w zapewnieniu efektywnego cyberbezpieczeństwa w MŚP jest świadomość pracowników. W przypadku relatywnie małych przedsiębiorstw ludzie są często pierwszą lub nawet jedyną linią obrony przed atakami cybernetycznymi, dlatego konieczne jest, aby pracownicy byli odpowiednio przeszkoleni w zakresie bezpiecznego korzystania z systemów informatycznych, rozpoznawania zagrożeń

1 *Raport. Cyberbezpieczeństwo w polskich firmach*, Vecto, https://vecto.pl/raport-2023.

oraz raportowania podejrzanych sytuacji. Regularne szkolenia są kluczowe dla utrzymania wysokiego poziomu świadomości w zakresie cyberbezpieczeństwa w całej firmie. Bogata oferta darmowych i płatnych szkoleń dostosowanych do wielu rodzajów podmiotów i przedmiotów ich działalności jest dostępna w internecie od ręki – jednak wymagane są chęci i regularne monitorowanie dostępnych możliwości dokształcania. Niezależnie od zajmowanego stanowiska pracownicy muszą być odpowiednio poinformowani o właściwych zachowaniach online i offline, gdyż zagrożenia cybernetyczne nie zawsze wynikają wyłącznie z zachowań pracowników w sieci. Dotyczy to również ich aktywności poza miejscem pracy.

Przykładowe szkolenia dla pracowników

1. Rozpoznawanie phishingu: takie szkolenia mogą pomóc pracownikom w identyfikowaniu podejrzanych e-maili, wiadomości tekstowych i połączeń telefonicznych. Przykładowo należy wyczulić pracowników na nietypowe adresy e-mail nadawców, podejrzane załączniki i prośby o poufne informacje.

2. Zarządzanie hasłami: pracownicy mogą być szkoleni w zakresie tworzenia silnych haseł, ich regularnej zmiany oraz unikania używania do różnych kont tych samych haseł. Można także omówić zasady ich bezpiecznego przechowywania, np. korzystanie z bezpiecznych menedżerów haseł.

3. Bezpieczne korzystanie z technologii mobilnych: w dobie pracy zdalnej i korzystania z urządzeń mobilnych szkolenia dotyczące bezpiecznego korzystania z smartfonów, tabletów i laptopów są niezwykle istotne. Pracownicy mogą być uczeni o konieczności aktualizowania oprogramowania, korzystania z VPNów w przypadku łączenia się z publicznymi sieciami Wi-Fi oraz o ryzyku związanym z instalacją aplikacji z niezaufanych źródeł.

4. Dzielenie się informacjami o charakterze poufnym i/lub tajnym: w trakcie szkoleń pracownicy mogą nauczyć się właściwego obchodzenia się z informacjami poufnymi i/lub tajnymi, tj. o szczególnym znaczeniu, których ujawnienie może nieść za sobą poważne konsekwencje prawne i finansowe.

5. Komunikacja w przedsiębiorstwie: wszyscy pracownicy powinni wiedzieć, w jaki sposób komunikować się między sobą w ramach tematyki zawodowej, a także umiejętnie przekazywać określone informacje poza miejscem pracy, m.in. za pośrednictwem social mediów.

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Zabezpieczenia techniczne

Ważna jest nie tylko ludzka reakcja, lecz także zastosowanie odpowiednich zabezpieczeń technicznych, dotyczy to m.in. stosowania aktualnych wersji oprogramowania, wdrażania rozwiązań antywirusowych i antymalware, konfiguracji zapór oraz regularnego tworzenia kopii zapasowych danych.

W przypadku MŚP, które często nie dysponują własnymi zasobami IT, warto rozważyć outsourcing usług związanych z cyberbezpieczeństwem do profesjonalnych firm świadczących takie usługi. Działania zwiększające jakość bezpieczeństwa cybernetycznego nie muszą być bardzo kosztowne lub trudne do wdrożenia, np. przywołana wyżej dbałość o aktualne wersje oprogramowania. Tym bardziej warto o nich pamiętać, gdyż kary lub straty wynikające z nieuprawnionego działania podmiotów zewnętrznych mogą być bardzo dotkliwe dla przedsiębiorstwa niedysponującego dużymi środkami.

Świadomość zagrożeń i podejmowanie działań prewencyjnych

Istnieją także kosztowne i zaawansowane rozwiązania, których dopasowanie i zastosowanie powinny zostać poprzedzone dokładną analizą potrzeb, uwzględniającą m.in. typ posiadanych danych oraz ich wagę dla nas i naszego klienta. Mikro-, małe i średnie przedsiębiorstwa dysponujące danymi osobowymi lub wyjątkowo cennymi informacjami na temat klientów powinny regularnie aktualizować swoje strategie bezpieczeństwa, opierając się na nowych technologiach i metodach ataków stosowanych przez cyberprzestępców. Ponadto podejmowanie działań prewencyjnych, takich jak audyty bezpieczeństwa i testy penetracyjne, mogą pomóc zidentyfikować słabe punkty w infrastrukturze IT przed wystąpieniem poważniejszych incydentów.

Uniwersalne środki prewencyjne

1. Sprzęt służbowy: niezwykle istotna jest praca wyłącznie za pośrednictwem sprzętu służbowego, zwłaszcza zawierającego stosowne, regularnie aktualizowane zabezpieczenia. Kwestia ta jest niezwykle istotna w przypadku, gdy pracownik jest w posiadaniu danych wrażliwych, których ujawnienie może nieść za sobą poważne konsekwencje.

2. Regularne aktualizacje oprogramowania: w przedsiębiorstwach należy szczególnie o nie zadbać. Dotyczy to systemów operacyjnych, aplikacji biurowych oraz zabezpieczeń antywirusowych i antymalware. Aktualizacje często zawierają poprawki bezpieczeństwa, które pomagają wypełnić luki i zabezpieczyć system przed podatnościami na włamania. Najczęściej aktualizacje odbywają się automatycznie, jednak poza aktualizacją bazy zagrożeń warto pamiętać o skanowaniu komputera w poszukiwaniu ewentualnych problemów niewykrywalnych gołym okiem.

3. Tworzenie kopii zapasowych danych: jest to niezwykle ważne w przypadku ataku ransomware lub innego incydentu, który może spowodować utratę danych. Przedsiębiorstwa powinny korzystać z regularnych harmonogramów tworzenia kopii zapasowych i przechowywać je w bezpiecznych, zewnętrznych lokalizacjach – np. w rozwiązaniach chmurowych. Robienie kopii zapasowych nie tylko zabezpieczy dane, lecz także znacząco usprawni pracę.

4. Monitorowanie działalności sieciowej: używanie narzędzi monitorujących działalność sieciową może pomóc we wczesnym zidentyfikowaniu niepokojących sygnałów i potencjalnych ataków. Można stosować narzędzia do wykrywania intruzów, monitorowania ruchu sieciowego oraz analizy logów zdarzeń.

5. Regularne testy penetracyjne: przeprowadzanie ich przez zewnętrznych ekspertów może pomóc zidentyfikować słabe punkty w infrastrukturze IT przed wystąpieniem prawdziwego ataku. Wyniki testów mogą być wykorzystane do wprowadzenia konkretnych działań naprawczych i ulepszeń w systemach bezpieczeństwa.

W Polsce MŚP, które padły ofiarą cyberataków, mogą skorzystać z pomocy różnych instytucji i organizacji oferujących wsparcie w zakresie reagowania na incydenty cybernetyczne oraz odzyskiwania sprawności działania. Oto kilka miejsc, gdzie takie

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

przedsiębiorstwa mogą zgłosić się po pomoc, zależnie od zidentyfikowanej kategorii zagrożenia:

- Centrum Bezpieczeństwa Cyberprzestrzeni (CERT Polska): jest to narodowy zespół reagowania na incydenty cybernetyczne w Polsce. Przedsiębiorstwa mogą do niego zgłaszać incydenty cybernetyczne, aby uzyskać wsparcie w analizie problemów związanych z atakiem i reagowaniu na nie.
- Stowarzyszenia i fundacje: organizacje pozarządowe, które działają na rzecz promocji bezpieczeństwa cybernetycznego w Polsce, chętnie udzielają wsparcia zaatakowanym przedsiębiorstwom w podjęciu dalszych kroków w celu uniknięcia powtórnych ataków.
- Firmy doradcze: istnieje wiele firm doradczych specjalizujących się w bezpieczeństwie cybernetycznym. Oferują one profesjonalną pomoc w zakresie reagowania na cyberataki, audytów bezpieczeństwa oraz implementacji środków ochronnych. W przypadku korzystania z usług doradczych przedsiębiorca musi liczyć się z relatywnie dużymi kosztami.
- Policja i organy ścigania: w przypadku poważnych incydentów cybernetycznych przedsiębiorstwa mogą zgłosić się do Policji lub organów ścigania, które prowadzą dochodzenia w sprawie przestępstw cybernetycznych. Policja może udzielić pomocy w dochodzeniu oraz ścigać sprawców cyberataków. Warto ją zawiadomić, zwłaszcza, gdy w grę wchodzi zagrożenie bezpieczeństwa danych osobowych.

Jeżeli dane osobowe pracowników były głównym celem, a diagnoza po ataku wykazała, że wykradzione dane były na tyle kompletne, że za ich pomocą możliwe byłoby zaciągnięcie np. zobowiązania kredytowego – wszyscy pracownicy powinni zastrzec swoje dokumenty oraz wyrobić nowe. Takie działanie zablokuje wiele możliwości bezprawnego działania cyberprzestępców.

Zgłoszenie się do powyższych podmiotów może pomóc MŚP w szybkim i skutecznym reagowaniu na cyberatak oraz minimalizacji jego skutków. Ważne jest, aby przedsiębiorstwa zgłaszały incydenty cybernetyczne jak najszybciej po ich zidentyfikowaniu, aby umożliwić szybką reakcję i ograniczyć szkody, które przez wyraźne zaniedbanie mogą być liczone w milionach złotych.

Podsumowanie

W trosce o cyberbezpieczeństwo w MŚP czynnik ludzki odgrywa fundamentalną rolę. Świadomość pracowników, odpowiednie szkolenia, polityka i procedury bezpieczeństwa, a także świadomość zagrożeń i zastosowanie odpowiednich zabezpieczeń technicznych są kluczowe dla efektywnej ochrony przed cyberatakami. Warto zainwestować czas i zasoby w budowanie kultury bezpieczeństwa w firmie, ponieważ skuteczne działania na tym polu mogą znacząco wpłynąć na stabilność i reputację przedsiębiorstwa. Świadomych pracowników warto zaznajamiać z technologiami i zapewniać im odpowiednie narzędzia pracy – od odpowiednio zabezpieczonego sprzętu służbowego do bezpiecznych kanałów komunikacji.

fundacja instytut CYBERBEZPIECZEŃSTWA
Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

fundacja instytut
CYBERBEZPIECZEŃSTWA

www.instytutcyber.pl

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości