Cyberbezpieczeństwo w małej i średniej firmie

Cyberbezpieczeństwo jest wpisane w rzeczywistość małych i średnich firm. Rodzaj branży i wielkość firmy mają coraz mniejsze znaczenie – zagrożenie atakami cybernetycznymi dotyczy niemalże wszystkich przedsiębiorców. Sprawdź, jak zwiększyć bezpieczeństwo firmy w cyberprzestrzeni.

Które firmy są zagrożone atakami

70% firm w Polsce spotkało się z sytuacją, która zagrażała bezpieczeństwu danych i systemów IT przedsiębiorstwa. Jednocześnie sami przedsiębiorcy **oceniają swoją cyberodporność nisko.**

Dla firm cyberataki mogą być bardzo kosztowne. Eksperci oceniają, że przeciętny koszt ataku to ponad 1 milion zł. Jednak całkowity koszt, jako ponosi firma, może być trudny do oszacowania, zwłaszcza jeśli dochodzi do utraty danych czy zaufania partnerów biznesowych i osłabienia pozycji na rynku.

Przeczytaj więcej: Raport ESET „Threat Report".

Rosnące ryzyko cyberataków

Pandemia wywołana wirusem COVID-19 spowodowała, że większość firm w wdrożyła **pracę zdalną lub hybrydową**. Odejście od pracy w biurach i przeniesienie dużej części procesów firmowych do sieci oznacza **wzrost podatności na cyberataki,** zwłaszcza że dotychczasową fizyczną kontrolę dostępu do systemów IT zastąpiły nowe, często niesprawdzone kanały lub narzędzia.

Jednym z głównych zagrożeń związanych z pracą zdalną okazało się to, że pracownicy używali **niezabezpieczonych komputerów**, otwierając tym samym drogę do ataków na sieci firmowe. Powtarzającym się błędem było niesystematyczne sporządzanie kopii zapasowych zasobów i umieszczanie ich wyłącznie w miejscu utworzenia.

Ponadto przesyłane dane firmowe nie były w ogóle lub były w niewystarczającym stopniu szyfrowane. W wielu przypadkach w bardzo krótkim czasie zmieniły się relacje z partnerami – usługodawcami – ze względu na ograniczoną możliwość lub brak możliwości dostarczania niektórych usług on-line.

Równie istotny dla cyberbezpieczeństwa był **wybuch wojny w Ukrainie.** Rozpoczęta razem z tradycyjną wojna hybrydowa obniżyła bezpieczeństwo funkcjonowania firm w przestrzeni cyfrowej. Z jednej strony zwiększył się poziom dezinformacji w mediach społecznościowych, z drugiej – powszechnym zagrożeniem stały się ataki hakerskie. Celem hakerów pozostaje przede wszystkim wykradanie kluczowych danych firm czy instalowanie złośliwego oprogramowania.

W związku z powszechnym przekonaniem, że cyberprzestępcy są sponsorowani przez obce państwa, 2/3 firm (według danych zebranych globalnie, obejmujących przedsiębiorców w Polsce) zmieniło **strategię bezpieczeństwa w cyberprzestrzeni** .

Co to jest cyberbezpieczeństwo

Najczęściej cyberbezpieczeństwo jest kojarzone z **przeciwdziałaniem atakom z zewnątrz na sieci teleinformatyczne**. Jest to jednak szersza kwestia i dotyczy zarówno instytucji publicznych, jak i prywatnych.

Cybebezpieczeństwo obejmuje:

- zapewnienie ochrony i przeciwdziałanie zagrożeniom, które dotykają cyberprzestrzeni
- funkcjonowanie w cyberprzestrzeni.

Cyberprzestrzeń to ogólnoświatowe środowisko informacyjne, czyli zarówno infrastruktura IT, jak i dane, internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory i kontrolery.

W małej i średniej firmie cyberbezpieczeństwo oznacza proces i działania, które **mają chronić dane i systemy wewnętrzne firm** – na przykład oprogramowanie do planowania zasobów przedsiębiorstwa (ERP) czy narzędzia do zarządzania relacjami z klientami (CRM) – przed zagrożeniami, jakie niesie za sobą cyberatak.

Cyberzagrożenia mogą dotykać każdego procesu w firmie, w tym: sprzedaży, marketingu, obsługi klienta, kadr, finansów. Szczególną uwagę trzeba jednak zwrócić na:

- systemy i aplikacje (na przykład systemy do zarządzania finansami i księgowością, aplikacje zapewniająca przejazdy osobowe pracowników)
- urządzenia do przetwarzania informacji (na przykład laptopy, tablety)
- elementy sterowania komunikacją, takie jak serwer i sieć, która jest pomostem między klientami a serwerami
- działania pracowników określane jako błąd użytkownika (na przykład ujawnienie przez pracownika hasła do komputera innym osobom, kliknięcie przez pracownika na link przesłany w zainfekowanym mailu).

Jakie ataki grożą firmom

Jednym z największych zagrożeń, z jakimi stykają się firmy w Polsce, są ataki typu ransomware, czyli **szkodliwe oprogramowanie** wykorzystywane do szyfrowania danych. Celem takiego ataku jest wymuszenie okupu za odzyskanie danych. Metody działania i narzędzia używane przez cyberprzestępców nie wymagają żadnych specyficznych uprawnień

ani działań po stronie atakowanego. Większość ataków typu ransomware zaczyna się od złośliwej wiadomości e-mail. Atak powoduje blokadę podstawowych funkcji na komputerze albo komórce, zmuszając pracownika firmy do zapłacenia okupu za przywrócenie kontroli nad urządzeniami.

Kolejnym zagrożeniem są **ataki phishingowe.** Jest to metoda oszustwa, która polega na nakłonieniu adresata do podjęcia określonego działania, na przykład kliknięcia w zainfekowany link lub pobrania dokumentu. Atak ma na celu instalację złośliwego oprogramowania, które umożliwia kolejne naruszenia, na przykład:

- wyłudzenie poufnych informacji, takich jak dane logowania, dane kart kredytowych
- zainfekowanie komputera szkodliwym oprogramowaniem
- nakłonienie firmy lub pracowników do określonych działań.

Kolejna kategoria ataku to **DoS** (**Denial of Service**), który polega na wysyłaniu dużej liczby danych, zapytań i informacji z wielu (nawet setek tysięcy) komputerów z całego świata, co powoduje przeciążenie liczbą operacji i – w efekcie – niedostępność serwerów.

Ważne! Uciążliwe i groźne naruszenia bezpieczeństwa niekoniecznie muszą pochodzić z zewnątrz. Przykładem **ataku z wewnątrz** (**The Inside Attack**) jest sytuacja, gdy pracownik odchodzi z pracy, ale wciąż ma kontakt z firmą (aktywne konta do logowania, dostęp do aplikacji firmowych, usług firmowych). Dlatego zadbaj o usunięcie kont byłego pracownika i zmianę haseł do wszystkich usług, do których miał dostęp.

Jakie są konsekwencje cyberataków

Pierwszym widocznym efektem cyberataków jest utrudnienie lub paraliż normalnych funkcji przedsiębiorstwa – zwłaszcza kiedy właściciele firmy bądź pracownicy nie mają dostępu do danych, na przykład nie mogą zalogować się zdalnie na skrzynkę pocztową lub uzyskać dostęp do dysku w chmurze.

Czasami nie wszystkie efekty ataku są widoczne od razu. To, co powinno niepokoić i wzbudzić podejrzenia, to **spowolnione działanie urządzeń i aplikacji, nagłe znikanie plików i folderów z urządzenia lub pojawianie się nowych czy rozsyłanie spamu przez urządzenia** (komputer, telefon).

Dotkliwą i kolejną najczęstszą konsekwencją cyberataków są **straty finansowe firm:**

- przerwy w działalności spowodowane cyberatakiem oznaczają utratę przychodów: dane publikowane przez NASK wskazują, że **2/3 firm**, które padły ofiarą cyberataku, odnotowały związany z nim znaczny spadek przychodów
- kosztowna może być również utrata lub uszkodzenie danych. W wielu przypadkach kolejnym i istotnym kosztem są naprawy sprzętu lub infrastruktury i praca związana z tymi naprawami.

W długiej perspektywie cyberatak negatywnie wpływa na **wizerunek firmy** na rynku.

Jak się zabezpieczać przed cyberatakami

Traktuj cyberbezpieczeństwo jako warunek niezakłóconego funkcjonowania twojej firmy na rynku i inwestuj w nie właściwie do zagrożeń.

Chodzi tu zarówno o **inwestycje materialne** – w szczególności w narzędzia lub technologie zabezpieczające przed cyberatakami – jak i o czas poświęcony na **przygotowanie procedur bezpieczeństwa** i zadbanie o to, żeby wszyscy pracownicy je znali i stosowali.

Najdroższe są wydatki na technologię. Średniej wielkości firma w Polsce wydaje na bezpieczeństwo około 24 tys. złotych. Jednak f irmy mają szeroki wachlarz możliwości w tym zakresie, a podstawowe narzędzia bezpieczeństwa można wdrożyć w każdym małym i średnim przedsiębiorstwie, często bez dodatkowych nakładów. D użo mniejsze wydatki wiążą się z opracowaniem polityki bezpieczeństwa firmy i szkolenia pracowników.

Budżet związany z cyberbezpieczeństwem oczywiście będzie zależeć od możliwości firmy, ale zdaniem ekspertów nie powinien spadać poniżej **3% całkowitych nakładów inwestycyjnych firmy**.

Pieniądze powinny zostać przeznaczone na konkretne **rozwiązania technologiczne** polegające na zabezpieczeniu komputerów i urządzeń mobilnych oraz ich aktualizacje, ponieważ to właśnie na nich najczęściej są przechowane najcenniejsze dane.

W 2021 roku 95% przedsiębiorstw w Polsce zastosowało bieżącą aktualizację oprogramowania, wykonywanie zapasowych kopii danych i przekazywanie ich do innych lokalizacji, uwierzytelnianie silnym hasłem, identyfikację i uwierzytelnianie metodami biometrycznymi.

Pamiętaj, że cyberbezpieczeństwo w firmie **nie może ograniczyć się do środków technologicznych.** Równie ważne są inwestycje w wiedzę pracowników, w tym w szczególności – cyberszkolenia.

Strategia cyberbezpieczeństwa musi zaczynać się od ludzi. Świadomość cyberzagrożeń powinni mieć przede wszystkim menedżerzy i kadra zarządzająca. Ich zadaniem jest upowszechniać ją wśród pracowników, ponieważ to właśnie pracownicy są często najsłabszym ogniwem firmy w cyberprzestrzeni:

- jedna trzecia pracowników używa tego samego hasła na wielu platformach
- jedna czwarta wciąż zapomina zablokować komputer, gdy wstaje od biurka
- jedna piąta przechowuje hasło dostępowe na kartce znajdującej się na biurku, na widoku.

Pamiętaj, żeby twoi pracownicy mieli dostęp do aktualnych informacji o procedurach postępowania w sytuacji cyberzagrożenia i cyberataku istniejących w firmie. Jeśli takich procedur nie masz, warto je stworzyć.

Za stworzenie polityki cyberbezpieczeństwa najczęściej odpowiada **administrator bezpieczeństwa danych** bądź **specjalista IT** (to może być pracownik przedsiębiorstwa lub ekspert zewnętrzny).

Ważne są też **szkolenia specjalistyczne**, które pokażą, w jaki sposób reagować na cyberataki, ale też prostsze szkolenia instrukcyjne o metodach zapobiegania cyberatakom dostępnych dla każdej firmie, jak chociażby uwierzytelnianie silnym hasłem i jego regularna zmiana.

Regularnie monitoruj funkcjonujące w firmie zabezpieczenia przed cyberprzestępczością, na przykład:

- systematycznie audytuj używany sprzęt i oprogramowanie
- sprawdzaj aktualność programów do walki z cyberzagrożeniami
- weryfikuj zmiany haseł dostępowych.

W przypadku szkoleń zewnętrznych zwróć uwagę na to, czy szkolenie jest **dostosowane do specyfiki mniejszych firm**, w tym – czy jego dostawca może wykazać się rekomendacjami od klientów.

Standardowy pakiet szkoleniowy powinien objąć kwestię rozpoznawania sytuacji ataku cybernetycznego (pierwsze niepokojące sygnały), zapoznanie ze sposobami działania hakera, podstawy stosowania socjotechnik, przegląd podstawowych typów ataków występujących wśród MŚP (dotyczące używania sprzętu, skrzynki pocztowej, stron internetowych), procedur działania po ataku w firmie.

Warto rozważyć sięgnięcie po bardziej zaawansowane zabezpieczenia, w tym przede wszystkim regularne audyty i certyfikaty. Takie działania to także dowód dla klientów, organów regulacyjnych i twoich partnerów biznesowych, że firma przestrzega zasad prywatności. **Audyt IT** ma na celu sprawdzenie, czy system informatyczny firmy we właściwy sposób chroni jej majątek, utrzymuje integralność danych i dostarcza właściwych informacji. Audyt pozwala również na **sprawdzenie reakcji pracowników w sytuacjach zagrażających cyberbezpieczeństwu** (testy penetracyjne), które służą wykryciu luk w zabezpieczeniach. Pamiętaj, że zakres audytu powinien zostać dopasowany indywidulanie do potrzeb i sytuacji twojej firmy, „uszyty na miarę".

Ostatnią istotną kwestią pozostaje wdrożenie odpowiedniej **polityki bezpieczeństwa**, czyli zbioru reguł dotyczących postępowania z danymi i dostępami do systemów, w tym odpowiednia polityka haseł i danych dostępu. Zadbanie o silne hasła, wyłączanie kont po wielokrotnych próbach logowania i korzystanie z zasady uwierzytelnienia dwuskładnikowego (two-factor authentication, 2FA) to przykłady dobrych praktyk, które mogą być promowane w ramach polityki bezpieczeństwa firmy.

Pracownicy w firmie muszą mieć świadomość tego, jak są pozyskiwane dane, kto ma uprawienia do ich przetwarzania, czy i gdzie dane są przechowywane i wreszcie na jakich warunkach odbywa się ich niszczenie. Polityka obejmuje również sprzęt (laptopy, tablety) – zasady ich aktualizacji, przechowywanie urządzeń, zasady zgłaszania utraty danych i kradzieży.

Certyfikacja bezpieczeństwa cyfrowego

Na czym polega certyfikacja

Certyfikacja cyberbezpieczeństwa to potwierdzenie zgodności rozwiązań z zakresu cyberbezpieczeństwa wdrożonych w przedsiębiorstwie z określonymi standardami. Certyfikację przeprowadza **niezależny podmiot** na podstawie przeglądu, oceny lub audytu.

Firma może się starać o krajowe, europejskie lub międzynarodowe certyfikaty cyberbezpieczeństwa.

Certyfikacja obejmuje produkty, procesy lub usługi ICT (dotyczące technologii informacyjno-komunikacyjnych) i służy wykazaniu przez firmę zgodności ze środkami zarządzania ryzykiem w cyberbezpieczeństwie.

Większość certyfikatów cyberbezpieczeństwa jest dobrowolna, a ich pozyskanie – **odpłatne**. Ceryfikaty mają różny okres ważności. Niektóre wygasają, a inne wymagają odnowienia lub przedłużenia.

Certyfikat warto mieć z wielu powodów. Przede wszystkim certyfikat cyberbezpieczeństwa to:

- element przewagi konkurencyjnej firmy
- dowód, że procesy, produkty i usługi są przetestowane i spełniają odpowiednie normy bezpieczeństwa
- potwierdzenie większej zdolności firmy do skutecznego zapobiegania i reagowania na incydenty.

Certyfikat może być warunkiem dopuszczającym do udziału w przetargu publicznym.

Jak uzyskać certyfikat

W przypadku każdego certyfikatu obowiązuje inna procedura. Jednak standardowo zaczyna się **od złożenia** w jednostce certyfikującej **deklaracji** wraz z odpowiednimi załącznikami przez firmę zainteresowaną certyfikacją.

Jednostka certyfikująca **wycenia usługę certyfikacji** i przedstawia umowę szczegółowo opisującą warunki jej przeprowadzenia.

Po podpisaniu umowy następuje **ewaluacja** prowadzona przez laboratorium pod nadzorem jednostki certyfikującej. Ewaluacja może obejmować badania, testy czy analizę dokumentacji.

W następnym kroku następuje analiza zebranego materiału. W przypadku pozytywnej oceny jednostka certyfikująca wydaje firmie certyfikat.

Certyfikat w programie Firma Bezpieczna Cyfrowo

Od 2023 roku firmy działające na rynku polskim mogą pozyskać certyfikat oferowany w programie **Firma Bezpieczna Cyfrowo.**

Program realizuje Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (Ministerstwo Rozwoju i Technologii oraz Ministerstwo Cyfryzacji).

Program Firma Bezpieczna Cyfrowo ma na celu:

- ochronę informacji firmowych przed zagrożeniami z internetu
- podniesienie świadomości cyfrowej i cyberbezpieczeństwa wśród **małych i średnich firm**
- upowszechnienie w **małych i średnich** firmach wdrożenia standardu cyberbezpieczeństwa.

Zakres oceny obejmuje **infrastrukturę informatyczną**, z której przedsiębiorca korzysta. Są to wszystkie urządzenia, które mają **dostęp do danych**, takich jak wiadomości e-mail, dane klientów, strona internetowa, usługi online oraz informacje w chmurze.

Certyfikat, który można uzyskać w programie Firma Bezpieczna Cyfrowo, potwierdza, że przedsiębiorca:

- bezpiecznie korzysta z narzędzi cyfrowych
- przywiązuje wagę do cyberbezpieczeństwa
- potrafi prawidłowo korzystać z usług cyfrowych.

Ważne! Firma Bezpieczna Cyfrowo to nie tylko certyfikacja, lecz także **bezpłatne narzędzie**, które weryfikuje stan cyberbezpieczeństwa i umiejętności cyfrowych firmy poprzez ankietę i przygotowuje firmę do certyfikacji.

Przeczytaj więcej o diagnozie przygotowującej do certyfikacji w programie Firma Bezpieczna Cyfrowo.

Przedsiębiorca, który weźmie udział w programie:

- zabezpieczy firmę przed cyberzagrożeniami i atakami z internetu
- uruchomi adres e-mail zabezpieczony przed spamem i próbami wyłudzenia według rekomendacji
- będzie efektywniej zarządzał kanałami komunikacji elektronicznej B2B, w tym e-płatnościami
- będzie prawidłowo korzystał ze środków identyfikacji elektronicznej (profil zaufany, mObywatel, warstwa elektroniczna w dowodzie lub podpis kwalifikowany)
- wykorzysta e-usługi administracji publicznej (aplikację mObywatel, e-usługi GOV, eDoręczenia, usługi e-Urzędu Skarbowego, serwisu Biznes.gov.pl i Konta Przedsiębiorcy w CEIDG, PUE ZUS)
- stworzy chronioną wizytówkę w popularnych portalach i mediach społecznościowych.

Przeczytaj więcej informacji na temat programu Firma Bezpieczna Cyfrowo.

https://www.biznes.gov.pl/pl/portal/004175