CYBERBEZPIECZEŃSTWO: SKUTECZNE METODY WALKI Z NARUSZANIEM DANYCH

Przypadki naruszenia danych to rosnący problem dla przedsiębiorstw. Mogą one powodować straty finansowe i uszczerbek na reputacji, w wyniku których, trudno będzie niektórym firmom odzyskać równowagę. Jakie metody ochrony danych są dostępne dla organizacji?

Żyjemy w epoce cyfrowej. W dzisiejszych czasach, dane są towarem, a przechowują duże ilości informacji o swoich klientach, dostawcach i pracownikach. Pomimo, iż ich obowiązkiem jest dbanie o ochronę tych informacji, badanie przeprowadzone w 2018 r. wśród kadry kierowniczej IT wykazało, że większość organizacji jest tylko "umiarkowanie przygotowana" na przeciwdziałanie zagrożeniom bezpieczeństwa cybernetycznego. Szacuje się, że w okresie dwunastu miesięcy 77% firm będzie miało do czynienia z naruszeniem danych, co pociąga za sobą koszty w wysokości ponad 1 biliona USD.

Złośliwe ataki cybernetyczne to tylko jeden ze sposobów na uzyskanie niezgodnego z prawem lub nieupoważnionego dostępu do przechowywanych przez firmę danych. Dla niewłaściwie zabezpieczonych systemów zagrożeniem może być zachowanie pracownika, niezabezpieczone urządzenie mobilne, aplikacje do przechowywania danych w chmurze oraz zewnętrzni usługodawcy. Naruszenia mogą przybierać różne formy, w tym oprogramowania wymuszającego okup (ang. ransomeware), złośliwego oprogramowania, phishingu i odmowy świadczenia usług - a ich wprowadzenie do systemu firmy może być równie proste, jak nieprzemyślane kliknięcie na link w spamie.

KTO JEST ZAGROŻONY?

Najprościej mówiąc - wszyscy. Zgodnie z szacunkami, każdego dnia ryzyko naruszenia integralności danych grozi około siedmiu milionom rekordów. Średnio jedno naruszenie danych wpłynie na 25 tys. rekordów, a przeciętny koszt takiego naruszenia wyniesie 3,26 mln USD. Badanie przeprowadzone przez IBM wykazało, że Stany Zjednoczone są najdroższym krajem, w którym dochodzi do naruszenia danych, a najdroższą branżą jest służba zdrowia. Generalnie, Stany Zjednoczone są w czołówce zarówno pod względem liczby naruszeń danych, jak i kradzieży tożsamości, na drugim miejscu znajduje się Korea Południowa pod względem naruszeń danych, i Francja pod względem kradzieży tożsamości. Liczby te należy jednak rozpatrywać w kontekście kryterium wielkości populacji, zgodnie z którym Holandia i Szwecja posiadają nieproporcjonalnie wysokie wskaźniki naruszania danych. Oczywiście zdarzają się wspólne i ukierunkowane ataki na poszczególne przedsiębiorstwa, ale z analizy danych statystycznych jasno wynika, że słabe zabezpieczenia cybernetyczne i wynikające z nich naruszenia danych dotyczą różnych typów przedsiębiorstw, wszystkich rozmiarów i we wszystkich krajach.

Ofiary i systemy będące celem ataku mogą, na pierwszy rzut oka, wydawać się przypadkowe. Badania przeprowadzone po ujawnieniu poważnego naruszenia danych w USA wykazały, że hakerzy mogliby z łatwością kontrolować co najmniej 55 000 podłączonych do Internetu systemów ogrzewania, wentylacji i klimatyzacji (HVAC). Słabe bezpieczeństwo cybernetyczne towarzyszące systemom HVAC może być wykorzystane do uzyskania dostępu do innych sieci, przeskakując bezpośrednio do głównego systemu korporacyjnego. Ta droga została prawdopodobnie użyta do kradzieży danych dotyczących 40 milionów kart kredytowych i debetowych w USA. Wcześniej hakerzy uzyskali dostęp do systemu HVAC sprzedawcy detalicznego kradnąc niezbędne dane logowania od jego zewnętrznego usługodawcy. To, co dla wielu osób może wydawać się zupełnie niepowiązane - system HVAC z danymi finansowymi - dla hakera może stanowić idealną ścieżkę do kradzieży danych.

Nie ulega wątpliwości, że żadna branża nie jest odporna na te kosztowne naruszenia poufności danych. Branża produkcyjna, edukacyjna, detaliczna, sektor publiczny, hotelarski i finansowy regularnie zgłaszają przypadki naruszenia danych, ale to służba zdrowia jest najbardziej zagrożona. Szacuje się, że u jednego na ośmiu obywateli USA nastąpi ujawnienie informacji medycznych w jakimś momencie życia, przy czym główną motywacją będzie zysk finansowy. W większości (56%), zagrożenia te mają charakter wewnętrzny, a główną przyczyną wycieku jest błąd ludzki.

ZAPOBIEGANIE – ISO/IEC 27001

Rodzina ISO/IEC 27001, zawierająca kilkanaście norm, zapewnia ramy dla organizacji pragnących zarządzać bezpieczeństwem swoich aktywów, w tym informacji finansowych, własności intelektualnej, danych dotyczących pracowników oraz wszelkich innych informacji powierzonych przedsiębiorstwu przez osoby trzecie.

Norma składa się z dwóch części:
ISO/IEC 27001:2013 (Part 2) – formalna specyfikacja wymagań systemu zarządzania bezpieczeństwem informacji (ISMS), względem której organizacja starająca się o certyfikację będzie oceniana. Zawiera ona obowiązkowe wymagania, które organizacja musi spełnić, aby uzyskać certyfikat. Decyzja o tym, które zabezpieczenia są istotne dla organizacji, jest podejmowana po przeprowadzeniu kompleksowej oceny ryzyka.
ISO/IEC 27002:2013 – dobre praktyki zabezpieczania informacji i powiązanych aktywów.

Normy te są zgodne ze strukturą modelu Annex SL, co pomaga podkreślić, że dla wszystkich przedsiębiorstw zarządzanie bezpieczeństwem informacji jest procesem ciągłym, a to z kolei zrównuje je z innymi normami ISO.

Sześcioetapowy proces certyfikacji ISO/IEC 27001 obejmuje indywidualnie dopasowaną ofertę, audyt wstępny, formalny audyt certyfikujący (1 i 2 etap), wizyty kontrolne (audyty nadzoru) w celu sprawdzenia systemu, ponowną certyfikację (recertyfikacja). Certyfikacja potwierdza, że organizacja spełnia wymagania dotyczące ochrony i odzyskiwania danych, bezpiecznego przechowywania danych testowych, zapisów dotyczących postępowania w przypadku incydentów bezpieczeństwa, ochrony narzędzi do przeprowadzania audytu systemów, statusu/szkolenia/niezależności audytorów wewnętrznych i dostępu do informacji z audytów dla najwyższego kierownictwa, dokumentacji procedur bezpieczeństwa informacji.

ZAPOBIEGANIE – ISO/IEC 27001

Norma promuje wdrożenie skoordynowanego i zintegrowanego systemu zarządzania usługami informatycznymi (SMS). Usprawnia i organizuje systemy poprzez podkreślanie możliwości i promowanie ciągłego doskonalenia i większej wydajności w ramach systemu SMS. Jest to możliwe dzięki lepszej harmonizacji personelu i procedur.

Tak jak w przypadku ISO/IEC 27001, ta norma również występuje w dwóch częściach:
ISO 20000-1 – definiuje wymagania, według których organizacja będzie oceniana pod kątem dostarczania zarządzanych usług o akceptowalnej jakości dla stron zainteresowanych.
ISO 20000-2 – jest kodeksem postępowania i opisuje najlepsze praktyki dla zarządzania procesami w zakresie ISO 20000-1.

Przyjęcie zarówno ISO/IEC 27001, jak i ISO/IEC 20000 nie tylko wzmocni systemy bezpieczeństwa IT firmy, ale także jasno pokaże pracownikom, klientom i innym stronom zainteresowanym, że organizacja poważnie traktuje zarządzanie usługami informatycznymi. Inne korzyści płynące z certyfikacji ISO/IEC 20000 to m.in. skuteczny sposób dostarczania zarządzanych usług, pomiaru poziomu usług i oceny ich wydajności, przy jednoczesnym silnym powiązaniu z ITIL. W ten sposób zapewnią Państwo swoich klientów, że ich wymagania odnośnie świadczonych usług, w tym bezpieczeństwo informacji, są spełnione. W cyfrowym świecie, firma może zyskać i stracić reputację na podstawie tego, jak poważnie podchodzi do kwestii zapewnienia bezpieczeństwa posiadanych informacji.

ROZWIĄZANIE SGS

SGS przoduje w zakresie wspierania organizacji w procesie poprawy ich cyberbezpieczeństwa. Dzięki ukierunkowanym danym audytowym z 604 firm, zebranym w okresie sześciu lat, rozumiemy, gdzie najczęściej występują duże i małe niezgodności.

Dowiedz się więcej na temat usług SGS w zakresie ISO 27001

Dowiedz się więcej na temat usług SGS w zakresie ISO 20000

Oprócz usług certyfikacyjnych i audytorskich oferujemy również szereg szkoleń, które pomagają organizacjom zrozumieć i wdrożyć normy ISO/IEC 27001 i ISO/IEC 20000.

Sprawdź listę szkoleń Akademii SGS w zakresie ISO 27001

KONTAKT

pl.certyfikacja@sgs.com

+48 22 329 22 93

www.sgs.pl