FIZYCZNE ZAMIENIA SIĘ W CYFROWE

NAJLEPSZE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA CYBERNETYCZNEGO

IRON MOUNTAIN®

NAJLEPSZE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA CYBERNETYCZNEGO

Naruszenia danych stanowią poważny problem dla organizacji, co widać na przykładzie ostatnich badań.

- **Niemal połowa** respondentów badania przeprowadzonego wśród 4200 europejskich i amerykańskich firm zgłosiła naruszenie w ciągu ostatniego roku[1].
- **Średni koszt** naruszenia danych szacuje się na 3,86 mln USD[2].

Ryzyko dla przedsiębiorstw nie polega jedynie na wysokości kar. Pozwy zbiorowe, spadek cen akcji, utrata zaufania klientów i szkody dla reputacji będą miały znaczący wpływ na markę.

Istnieje wiele narzędzi, które firmy mogą wdrożyć, próbując odeprzeć ataki. W tym artykule przedstawiamy szerszą perspektywę. Jak można **wprowadzić najlepsze praktyki w zakresie bezpieczeństwa cybernetycznego** w całej organizacji, aby chronić poufność, integralność i dostępność systemów informatycznych oraz odzyskać sprawność działania w przypadku naruszenia danych?

1. Hiscox/bezpieczeństwo oparte na ryzyku: Raport dotyczący naruszeń danych w 2017 r
2. Instytut IBM/Ponemonon: Koszty naruszenia danych w 2018

CZY WIELKOŚĆ FIRMY MA ZNACZNIE W PODATNOŚCI NA CYBERATAKI?

Atakujący nie zwracają uwagi na wielkość przedsiębiorstwa. O ile liczba danych o klientach przechowywanych przez duże organizacje może być dla nich kusząca, o tyle dostęp do systemów dostaw i płatności w mniejszych firmach jest prostszy.

Pod pewnymi względami problem ten jest jeszcze większy w przypadku mniejszych firm. Mają one ograniczone budżety na środki bezpieczeństwa, ale nie mogą sobie pozwolić na bycie poza siecią przez dłuższy czas.

ZROZUMIEĆ KRAJOBRAZ ZAGROŻEŃ

Czy wiesz, jakie rodzaje ataków są możliwe i w jaki sposób mogą wpłynąć na Twoją działalność? Istnieje wiele rodzajów zagrożeń, na które może natknąć się Twoja firma.

- Statystyki pokazują, że największe zagrożenie nadal stanowi oprogramowanie typu **malware**, czyli złośliwe, z którym mamy do czynienia codziennie. Wirusy komputerowe, konie trojańskie i oprogramowania szpiegujące to tylko kilka z przykładów. Wystarczy kliknąć niewinnie wyglądający link, aby zainfekować system komputerowy.

- Z kolei oprogramowanie typu **Ransomware** cieszy się coraz większą popularnością. Z organizacją kontaktuje się cyberprzestępca, który twierdzi, że zainfekował jej dane i usunie wirusa tylko po zapłaceniu okupu. Organizacja nie wie, czy zagrożenie jest realne i zapłacenie okupu rzeczywiście ochroni dane, ale z pewnością odczuje negatywne skutki, jeżeli doszło do infekcji.

- **Programy phishingowe** skupiają się na użytkownikach, kusząc ich wiarygodnie wyglądającymi wiadomościami e-mail i namawiając, aby podali swoje dane osobowe i finansowe.

Istnieje wiele innych rodzajów ataków prowadzonych przez różnych graczy, od państw, przez przestępczość zorganizowaną, po hackerów. Na rynku pełnym wszelkiego rodzaju danych, skala i wyrafinowanie cyberataków będzie ewoluować w szybkim tempie.

Eksperci są zgodni. Nie chodzi o to, aby zastanawiać się, czy dojdzie do naruszenia danych, ale o to, aby być gotowym, kiedy to nastąpi. Opracowanie strategii zapobiegania atakom jest niezbędne dla firmy każdej wielkości.

ZROZUMIEĆ POSIADANE DANE

Czy wiesz, jakie dane posiadasz i dlaczego je posiadasz? Czy narażasz na ryzyko informacje, których nie powinieneś posiadać?

Zrozumienie zgromadzonych danych jest ważnym pierwszym krokiem. **Zarządzanie i ochrona** zasobów w sposób efektywny i zgodny z prawem jest niezwykle istotna. Oznacza to stosowanie właściwego ładu informacyjnego, zrozumienie, w jaki sposób dane przepływają przez organizację i ich zabezpieczenie na każdym etapie cyklu życia.

OPRACOWANIE STRATEGII OPARTEJ NA RYZYKU

Podstawowe rodzaje ryzyka, jakimi należy zarządzić to: **ryzyko działalności operacyjnej, utraty reputacji, braku zgodności** (compliance) i **ryzyko prawne**. Chociaż nie ma jednego uniwersalnego podejścia do zarządzania ryzykiem cybernetycznym, ważne jest dostosowanie się do uznanych ram bezpieczeństwa, takich jak norma ISO 27001 czy wytyczne amerykańskiego Krajowego Instytutu Norm (NIST).

Warto porozmawiać ze swoim ubezpieczycielem, które zasady ramowe najlepiej pasują do konkretnej sytuacji.

UWZGLĘDNIJ CAŁĄ PERSPEKTYWĘ BIZNESOWĄ

Cyberbezpieczeństwo to nie tylko technologia. Łączy ono wiedzę z zakresu IT, prawa i bezpieczeństwa w celu opracowania ram działania i przeciwstawienia się zagrożeniom. Chodzi o to, aby wszyscy w organizacji byli świadomi tego, jak łatwo można dać się oszukać.

WSPIERANIE KULTURY PRACY UWZGLĘDNIAJĄCEJ KWESTIE BEZPIECZEŃSTWA

Element ludzki ma kluczowe znaczenie w tworzeniu strategii bezpieczeństwa.

Słabe punkty to nie zawsze złośliwe zachowanie ludzi, ale także niewinne kliknięcia niewłaściwego przycisku, które mogą umożliwić przestępcy wejście do systemu.

Pracownicy muszą zdawać sobie sprawę z ryzyka i swoich obowiązków, a świadomość i edukacja w zakresie bezpieczeństwa są tu kluczowe. Należy prowadzić szkolenia odpowiednie dla danych odbiorców, wyjaśniające znaczenie konkretnego zachowania i przestrzegania zasad.

Jednocześnie konieczne jest zajęcie się kwestią niezadowolonych lub byłych pracowników poprzez:

- **monitorowanie ich zachowania** i zwracanie uwagi na widoczne niezadowolenie,
- **wdrożenie procesów** oceny i zwolnień pracowników stanowiących zagrożenie,
- wdrożenie systemu **uprawnień dostępu** opartego na rolach i ograniczenie dostępu do najbardziej krytycznych systemów i danych.

CZYTAJ WIĘCEJ ▷

ROZWIJAJ SILNE ZARZĄDZANIE

Aby strategia odniosła sukces, organizacja potrzebuje silnego **zarządzania i przywództwa**. Dzięki temu cała firma będzie mogła **dostosować się do strategii bezpieczeństwa cybernetycznego**, ograniczyć skutki naruszeń oraz wdrożyć lepszy podział zasobów bezpieczeństwa i zarządzanie nimi.

Silne zarządzanie obejmuje:

- zaangażowanie kierownictwa wyższego szczebla,
- wyznaczenie jednej osoby odpowiedzialnej za bezpieczeństwo cybernetyczne,
- jasną politykę i procedury,
- silną kulturę bezpieczeństwa cybernetycznego,
- przygotowany plan działania w przypadku kryzysu.

ZBUDUJ WIELOPOZIOMOWĄ OBRONĘ

Mechanizmy ochronne mogą zostać naruszone, dlatego ważne jest stosowanie wielopoziomowej ochrony posiadanych zasobów, począwszy od otoczenia danych aż po punkt końcowy. Jeżeli przestępca przebije się przez jedną linię obrony, mamy do dyspozycji kolejne.

Na przykład: bezpieczeństwo fizyczne powinno uniemożliwić dostęp osobom nieupoważnionym.

Jednocześnie, obok zaawansowanych narzędzi ochrony przed zagrożeniami, należy stosować tradycyjne środki, takie jak kontrola sieci i systemów, zabezpieczenia typu firewall, środki zapobiegania włamaniom i kontroli dostępu.

DISASTER RECOVERY: OPRACUJ PLAN NA NAJGORSZE, CO MOŻE SIĘ ZDARZYĆ

Wiele firm posiada **plany disaster recovery i zachowania ciągłości działania**, ale historycznie dotyczą one przygotowania na niespodziewane zdarzenia fizyczne, takie jak powódź czy pożar. Jednak cyberataki prowadzące do zaprzestania działalności firmy, są równie katastrofalne w skutkach.

Należy uwzględnić zakres wpływu, jaki atak może mieć na firmę i zaplanować zarządzanie taką sytuacją.

Pytania, które należy zadać w firmie:

- Jak długo firma może przetrwać awarię i jakie są krytyczne aplikacje, których działanie należy przywrócić jak najszybciej? Mniejsze firmy są bardziej narażone na atak, jeżeli ma on wpływ na przepływy pieniężne.
- Ile jesteś gotów wydać, aby przetrwać atak? Na przykład przechowywanie danych w wielu miejscach może być droższe, ale również bardziej efektywne.
- Czy uwzględniasz każdy aspekt redundancji w swojej konfiguracji, aż po światłowody, które zapewniają łączność do i z centrum danych?
- Czy szkolisz personel na wypadek cyberataku, regularnie testujesz programy odzyskiwania danych po awarii. Czy w tych działaniach uwzględniasz swoich dostawców i partnerów?

Formalny plan reagowania ułatwia działanie w sytuacji ataku i sprawne przywrócenie działalności biznesowej po jego wystąpieniu.

W praktyce oznacza to stworzenie zespołu reagowania na incydenty i ciągłe jego szkolenie. Planuj i ćwicz, jak zminimalizować błędy ludzkie. Dobrym pomysłem może być **zaangażowanie profesjonalnej** firmy zajmującej się reagowaniem na incydenty i podpisanie z nią umowy zanim dojdzie do jakiegokolwiek naruszenia.

- Opracuj plan zarządzania kryzysowego, który obejmie zarówno wewnętrznych, jak i zewnętrznych interesariuszy, co umożliwi jego realizację i utrzymanie zaufania.
- Na wszelki wypadek załóż w planach, że normalna łączność może nie działać podczas zdarzenia.
- Na koniec upewnij się, że masz dobre kopie zapasowe danych.

OBEJRZYJ NASZ FILM O TWORZENIU PLANU DISASTER RECOVERY

OPRACUJ PLAN DISASTER RECOVERY I ZACHOWANIA CIĄGŁOŚCI DZIAŁANIA?

CZYTAJ WIĘCEJ ▷

JEŻELI DOJDZIE DO NARUSZENIA - DZIAŁAJ SZYBKO

Średni czas wykrycia naruszenia danych wynosi 197 dni, a średni czas do powstrzymania zidentyfikowanego naruszenia to 69 dni[3]. Im szybciej zadziałasz, tym mniejsze skutki i koszty ataku odczujesz. Firmy, które opanowały naruszenie danych w czasie krótszym niż 30 dni zaoszczędziły podobno ponad milion dolarów.

UJAWNIJ NARUSZENIE JAK NAJWCZEŚNIEJ

Jeżeli pomimo całego planowania dojdzie do naruszenia ochrony danych, należy ujawnić je jak najszybciej, nawet jeżeli później trzeba będzie aktualizować zgłoszenie. Dzięki temu można znacznie zaoszczędzić na poziomie kary, która zostanie ostatecznie zapłacona.

DBAJ, ABY PLANY BYŁY AKTUALIZOWANE

Regularnie pojawiają się nowe technologie zarządzania i analizowania danych, a przedsiębiorstwa muszą być na bieżąco z ich rozwojem i uwzględniać je w planowaniu bezpieczeństwa cybernetycznego.

Możesz stosować nowe technologie, takie **jak sztuczna inteligencja (AI) i uczenie maszynowe (ML)**, aby doskonalić zabezpieczenia, ale pamiętaj, że przestępcy robią to samo.

Bezpieczeństwo cybernetyczne nadal będzie „grą w kotka i myszkę", dlatego ważne jest, aby zachować czujność.

3. Instytut IBM/Ponemonon: Koszty naruszenia danych w 2018

MĄDRZE WYBIERZ CENTRUM DANYCH

Jeżeli wolisz przenieść **swoje systemy** do zewnętrznego centrum danych, pamiętaj, że jesteś klientem i masz prawo zadawać pytania o wszystko - od środowiska fizycznego po politykę i procedury. Czy czujesz się komfortowo z tym, kto ma dostęp do Twojego środowiska? Czy masz podpisaną umowę, która gwarantuje, że zostaniesz powiadomiony o wszelkich naruszeniach? Czy masz prawo do prowadzenia audytu? Czy jesteś pewny, że dostawca stosuje się do norm takich jak ISO 27001?

UWZGLĘDNIJ SWOICH DOSTAWCÓW I PARTNERÓW

Niezależnie od tego, jak dobrze radzisz sobie z bezpieczeństwem cybernetycznym, Twoja firma nie jest samotną wyspą.

Przyjrzyj się swoim kontaktom z firmami zewnętrznymi i postaraj się objąć je takim samym nadzorem i kontrolą, jak w przypadku własnej organizacji - choć nie zawsze będzie to łatwe.

ZNAJDŹ POMOC Z ZEWNĄTRZ, JEŻELI NIE MOŻESZ ZROBIĆ WSZYSTKIEGO SAM

Konsultant zewnętrzny może przyjrzeć się zasobom tam, gdzie się znajdują oraz określić, czy należy poddać je klasyfikacji. Opracuje także różne modele zagrożeń.

Małe i średnie przedsiębiorstwa prawdopodobnie nie będą w stanie utrzymać pełnoetatowych pracowników ochrony. **Zamiast tego znajdź partnera**, który może przychodzić kilka razy w roku, aby przeprowadzić przegląd i udzielić porady. Miej jego dane pod ręką, aby móc się z nim szybko skontaktować w przypadku ataku. Być może ubezpieczyciel od zagrożeń cybernetycznych wskaże kogoś zaufanego.

Im więcej zainwestujesz w program zabezpieczeń, tym lepiej będzie on funkcjonował. Istnieje wiele firm, które nie tylko przeprowadzą szkolenie, ale będą w stanie sprawdzić wiedzę użytkowników.

Jeżeli naprawdę nie możesz zatrudnić firmy zewnętrznej, istnieją **organizacje online**, takie jak SKA i IACPA. Można również znaleźć szablony oceny zagrożenia, które wypełnisz samodzielnie.

CHCESZ UZYSKAĆ WIĘCEJ INFORMACJI NA TEMAT KONTROLOWANIA, OCHRONY I OPTYMALIZACJI INFORMACJI O ZNACZENIU KRYTYCZNYM DLA BIZNESU W DZISIEJSZYM HYBRYDOWYM ŚRODOWISKU INFORMACYJNYM?

POBIERZ NASZ E-BOOK ▷

O IRON MOUNTAIN

Firma Iron Mountain Incorporated® (NYSE: IRM) powstała w 1951 roku i jest światowym liderem w dziedzinie usług magazynowania i zarządzania informacjami. Ciesząca się zaufaniem ponad 225 000. organizacji na całym świecie, posiadająca sieć nieruchomości obejmującą ponad 8,6 milionów metrów kwadratowych w około 1450 obiektach w 56 krajach, Iron Mountain przechowuje i chroni cenne zasoby, w tym krytyczne informacje biznesowe, wrażliwe dane oraz artefakty kulturowe i historyczne. Zapewniając rozwiązania obejmujące bezpieczne przechowywanie dokumentacji, zarządzanie informacjami, transformację cyfrową, bezpieczne niszczenie, a także centra danych, usługi w chmurze oraz przechowywanie dzieł sztuki i logistykę, Iron Mountain pomaga klientom obniżyć koszty i ryzyko, zapewnić zgodność z przepisami prawa, przywrócić działalność w przypadku wystąpienia katastrofy i umożliwić bardziej cyfrowy sposób pracy. Aby uzyskać więcej informacji, odwiedź stronę www.ironmountain.com.

801800802 | IRONMOUNTAIN.PL

IRON MOUNTAIN®

CHRONIMY TO, CO DLA CIEBIE NAJBARDZIEJ CENNE