SIERPIEŃ 2024

RAPORT interaktywnie.com

OCHRONA FIRMY PRZED CYBERZAGROŻENIAMI

SPONSOR PLATYNOWY

Synology®

POD PATRONATEM

WP money.pl GAZETA.PL

SPIS TREŚCI

RAPORTY INTERAKTYWNIE

2024

STYCZEŃ

E-commerce.
Jak sprzedawać w internecie

LUTY

Agencje marketingowe

MARZEC

Jak promować w internecie kancelarię prawną?

Jak przygotować się na KSeF

KWIECIEŃ

Software house

MAJ

Agencje SEO i marketing w wyszukiwarkach - wszystko o SEO i SEM

CZERWIEC

Content marketing i agencje content marketingowe

Projektowanie stron internetowych

LIPIEC

E-mail marketing i marketing automation

SIERPIEŃ

Wideo w internecie

Cyberbezpieczeństwo

WRZESIEŃ

Agencje social media

Agencje brandingowe

PAŹDZIERNIK

Programmatic buying

Podstawy marketingu internetowego

LISTOPAD

Sklepy internetowe

GRUDZIEŃ

Reklama w internecie – trendy w 2025 roku

Rezerwacja powierzchni reklamowej
reklama@interaktywnie.com
+48 693 710 118

interaktywnie.com

ZAPREZENTUJ SIĘ W NASZYCH EBOOKACH

Ebooki z raportami przygotowane przez redakcję Interaktywnie.com
czytają marketerzy, którzy decydują o przeznaczeniu budżetów promocyjnych.
Dotrzesz do nich prezentując w tych publikacjach siebie i swoją ofertę!

interaktywnie.com

Zapytaj o ofertę

ZAMÓW PAKIET REKLAMOWY

w ebookach Interaktywnie.com

JAKUB KARCZMARCZYK

jk@interaktywnie.com

tel.: 721 115 702, kom.: 693 710 118

Inwestuj w cyberbezpieczeństwo firmy. Jeśli o nim zapomnisz, szybciej niż później, stracisz!

Wojna hybrydowa, jaką prowadzi Rosja przeciwko państwom NATO opiera się przede wszystkim na generowaniu cyberzagrożenia. W związku z tym świadome i odpowiedzialne firmy wydają coraz więcej na ochronę danych oraz infrastruktury IT - do 2030 roku kwota ta w skali globalnej przekroczy 650 miliardów dolarów.

Jak więc zabezpieczyć przedsiębiorstwo? W jakie rozwiązania inwestować przede wszystkim? Jak wybrać partnera biznesowego, który w tym nam pomoże? Na te pytania odpowiedzą z pewnością eksperci z Comarch i Synology - firm, które postanowiły zaprezentować w tym ebooku swoją wiedzę oraz ofertę.

Zapraszam do lektury i kontaktu z Partnerami merytorycznymi tego opracowania.

Tomasz Bonek, redaktor naczelny Interaktywnie.com

Synology GmbH

Adres
Grafenberger Allee 295
40237 Düsseldorf, Niemcy

Dane kontaktowe
E-mail: pl_marketing@synology.com
Strona www: synology.com/pl-pl

Opis działalności
Synology dostarcza kompleksowe rozwiązania monitoringu wizyjnego, zapewniając wysoki poziom bezpieczeństwa, spójność danych i ciągłość pracy. Ich produkty charakteryzują się efektywnością kosztową i szerokim zakresem funkcji dostosowanych do różnych potrzeb biznesowych.

Klienci Synology mają dostęp do aplikacji do backupu całej infrastruktury IT, obejmującej komputery, serwery fizyczne i maszyny wirtualne. Firma umożliwia również uruchamianie maszyn wirtualnych, w tym systemów Windows i Linux, oraz konfigurację klastrów wysokiej dostępności dla nieprzerwanego działania kluczowych systemów.

Synology zapewnia narzędzia usprawniające współpracę zespołu, takie jak udostępnianie i synchronizacja danych, klient poczty elektronicznej, komunikator oraz platforma biurowa Synology Office.

Misją firmy jest dostarczanie produktów odpowiadających bieżącym potrzebom, rozwijanie przyszłościowych rozwiązań i świadczenie usług najwyższej jakości, spełniających oczekiwania najbardziej wymagających klientów.

Wybrani klienci

- ATM Grupa
- WUP
- IDEA Bank
- PolandRock
- BVB
- Wykop.pl

NAJPOWAŻNIEJSZE CYBERZAGROŻENIA DLA FIRM W 2024 ROKU

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

1

Ransomware oraz Network breach to według Statisty jedne z najczęściej powtarzających się cyberataków. Najczęściej atakowane są podmioty z sektora produkcyjnego, finansowego oraz ubezpieczeniowego. W związku z rozległymi zagrożeniami firmy wydają coraz więcej na cyberochronę - do 2030 roku kwota ta w skali globalnej przekroczy 650 miliardów dolarów. Jednak mimo tych starań, jak wskazują dane ISACA, to człowiek odpowiada za blisko 90 procent naruszeń danych w środowisku firmowym.

Najpowszechniejsze cyberataki

Według danych Statisty, najczęściej identyfikowanymi cyberatakami jest Ransomeware - stanowi około 70 procent wykrytych incydentów. Ogranicza on w całości lub częściowo dostęp do systemów użytkownika oraz zgromadzonych danych, celem wyłudzenia okupu za ich odblokowanie.

Na drugim miejscu zestawienia uplasował się tzw. „Network breach". Jest to naruszenie bezpieczeństwa danych wynikające z nieautoryzowanego uzyskania dostępu do nich z zamiarem popełnienia przestępstwa. Tego typu atak często nie wiąże się wyłącznie ze stratami finansowymi a także utratą reputacji, w tym relacji z klientami. Nieuprawnione wykorzystanie danych osobowych poszkodowanych może bowiem narazić na dodatkowe straty. Przykładem tego typu incydentu jest wyciek danych pacjentów szpitala lub gości hotelowych.

Wśród wymienionych zagrożeń jest również data extortion, czyli wyłudzenie danych, często objawiające się zjawiskiem phishingu. Udział tego typu ataków w zestawieniu wszystkich według danych Statisty to 7,14 procent. Przestępca wyłudza dane wrażliwe, stosując zabiegi psychologiczne, np. podszywanie się pod znaną markę, podmiot lub instytucję.

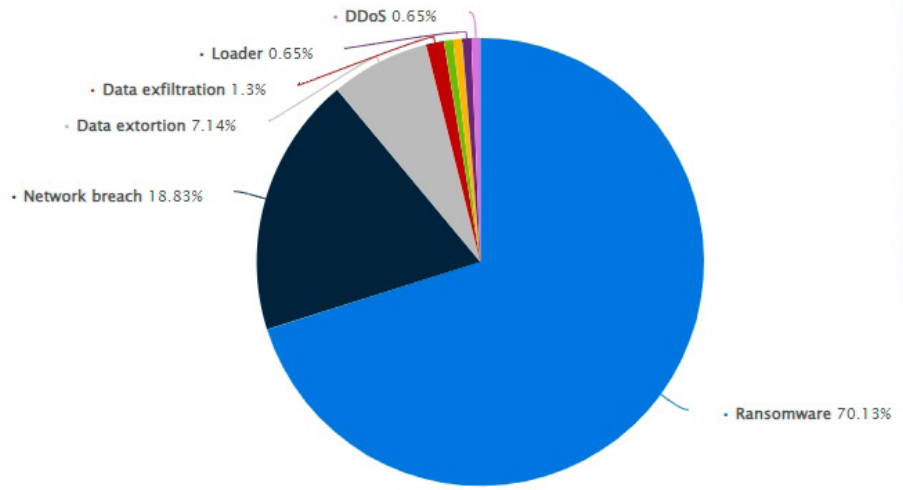
Synology®

Pełny ekosystem IT

Nie poddaj się i dbaj o bezpieczeństwo Twoich danych

Liczba urządzeń podłączonych do sieci stale rośnie, zwiększając skalę ataków hakerskich. Przejdź przez listę kontrolną i zidentyfikuj szybko luki w zabezpieczniach Twojej sieci. Zeskanuj kod QR już teraz!

Globalny udział poszczególnych rodzajów cyberataków wykrytych w 2023 roku



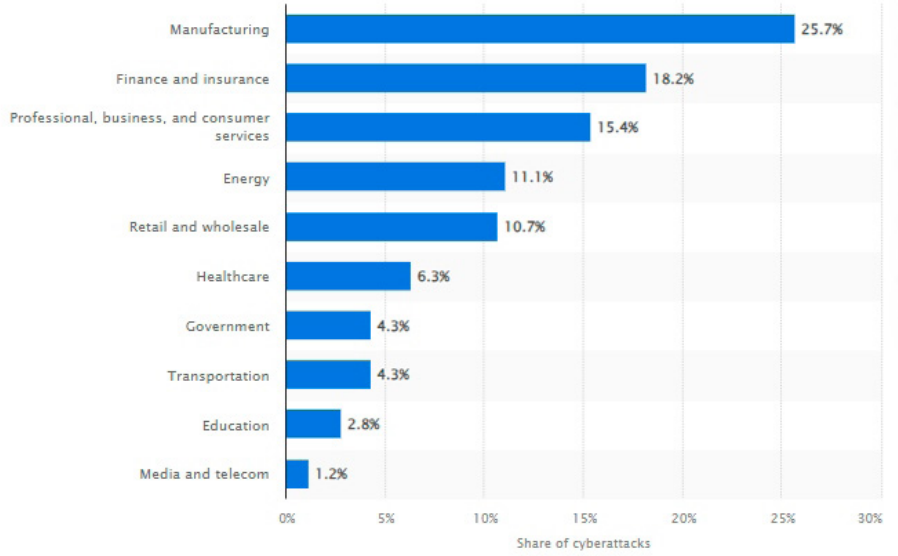
Źródło: Statista

Warto zwrócić również uwagę na zagrożenia typu DDoS, czyli atak pozwalający na zablokowanie komputera ofiary poprzez przeciążenie systemu danymi.

Cyberataki i ich konsekwencje dla biznesu

Dane Statisty wskazują, że najczęściej atakowane są firmy z segmentu produkcyjnego. W 2023 roku aż 25,7 procent tego typu incydentów dotyczyło właśnie tej branży. Na drugim miejscu jest segment finansowy oraz ubezpieczeniowy. Tam odsetek ataków wynosi 18,2 procent. Na trzecim miejscu znalazła się branża obejmujące szeroko pojęte usługi dla biznesu oraz obsługę klienta - 15,4 procent. Ponad 10-procentowy udział ma również branża energetyczna, detaliczna i magazynowa. Odsetek ataków na podmioty z branży ochrony zdrowia, transportu, edukacji, mediów, a także instytucje rządowe, to w przypadku każdej z nich mniej niż 10 procent.

Globalny udział branż narażonych na cyberataki w 2023 roku



Źródło: Statista

Wśród konsekwencji cyberataków wymienić należy w pierwszej kolejności utratę wrażliwych danych. Mogą one zostać

wykorzystanie przeciwko podmiotowi których dotyczą, ale nie tylko przeciwko samej firmie, lecz także jej klientom.

Utrata danych klientów wiąże się z utratą reputacji firmy, co w dłuższej perspektywie może mieć dużo gorsze konsekwencje. Brak klientów uniemożliwia bowiem prowadzenie biznesu, co w konsekwencji prowadzi do braku przychodów i bankructwa.

Wymienić należy również przestoje w działalności. Cyberatak może również uniemożliwić działalność przedsiębiorstwu, poprzez brak dostępu do kluczowych systemów firmowych oraz danych a to natomiast generuje straty finansowe.

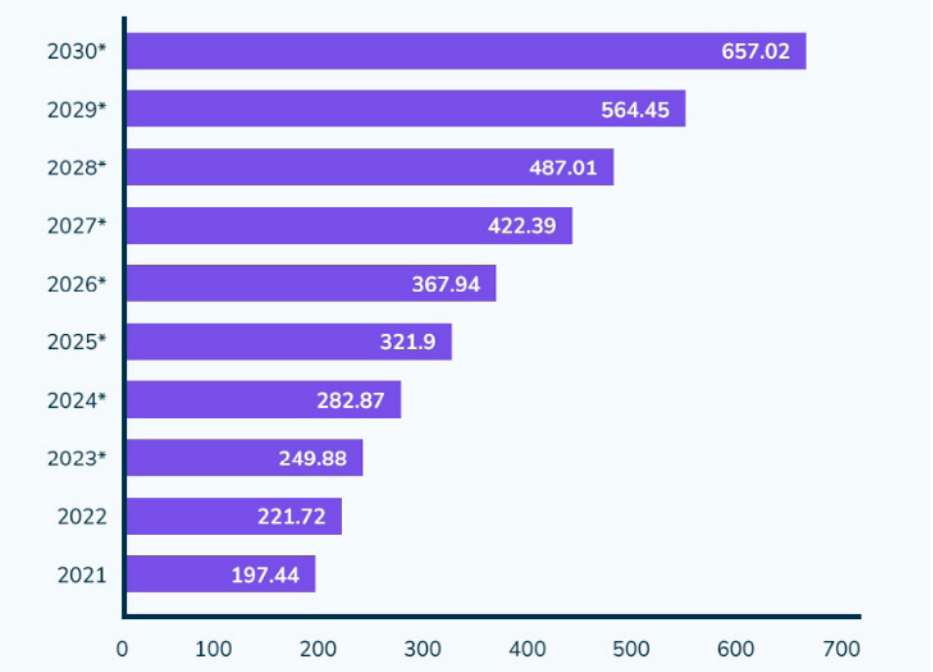
Upadek firmy to daleko idąca konsekwencja cyberataku związana z brakiem możliwości prowadzenia działalności z wymienionych powyżej powodów.

Cyberataki niosą ze sobą również ryzyko nałożenia na firmę kary finansowej przez instytucje nadzorcze. Utrata danych klientów może pociągnąć za sobą kontrolę, a w przypadku wykrycia nieprawidłowości również dotkliwe kary finansowe.

Brak specjalistów z zakresu cyberbezpieczeństwa

Zapotrzebowanie na ekspertów z dziedziny cyberbezpieczeństwa rośnie. Według danych ISC2 - Międzynarodowego Konsorcjum Certyfikacji Bezpieczeństwa Systemów Informatycznych, liczba pracowników zajmujących się cyberbezpieczeństwem przekroczyła w 2023 roku 5,5 miliona, a w latach 2022-2023 ich liczba wzrosła o 8,7 procent. Największy wzrost dotyczył regionu Azji, Afryki, Bliskiego Wschodu, a także Ameryki Północnej.

Wartość globalnego rynku cyberbezpieczeństwa w latach 2021-2030 (w mld dolarów)

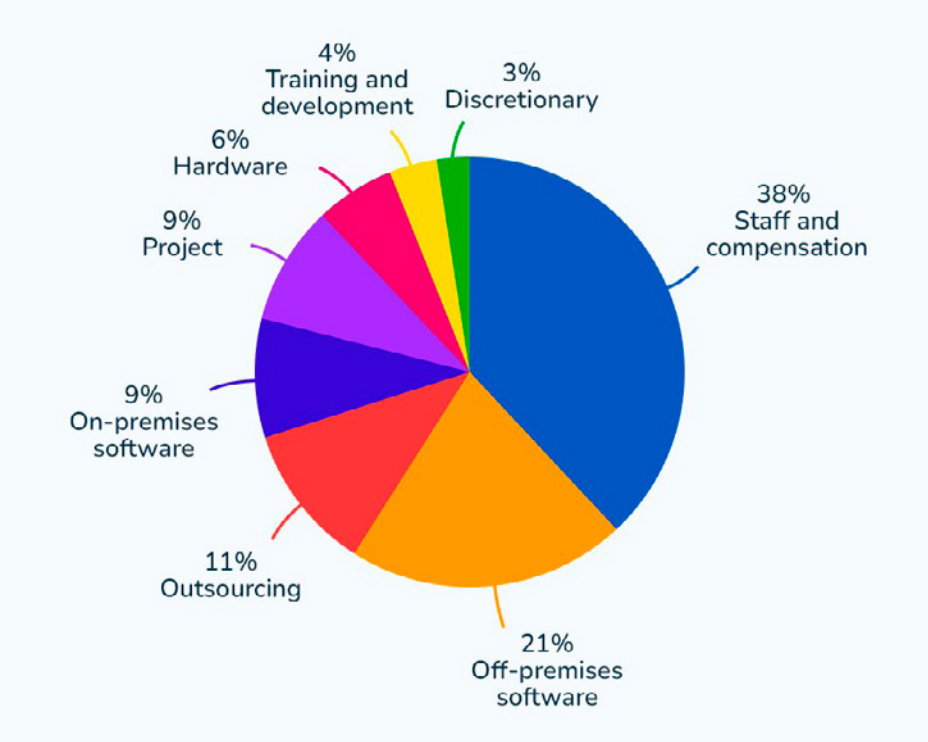


Źródło: SationX

Na podstawie powyższych danych widać, że dużą część rynku zabezpieczeń przed cyberatakami stanowią specjaliści z tej

dziedziny. Według danych serwisu SationX, w 2023 roku wydatki z zakresu cyberbezpieczeństwa sięgnęły prawie 250 mld dolarów. W 2024 roku ma to być 283 mld dolarów, a w kolejnych dwóch latach ponad 300 mld dolarów. Według danych StationX, w 2030 roku rynek związany z zapobieganiem cyberatakom przekroczy 650 mld dolarów.

Procentowy podział środków przeznaczanych na zapewnienie cyberbezpieczeństwa w firmach



Źródło: StationX

Jaka jest zatem część budżetów przeznaczanych na zapewnienie cyberbezpieczeństwa pożytkowana na specjalistów z tego zakresu? Według danych zebranych przez StationX, jest to aż 38 procent, co stanowi największy udział spośród wszystkich przedstawionych kategorii. Istotnym elementem jest również oprogramowanie, które pochłania 21 procent budżetu (oprogramowanie zewnętrzne). Na oprogramowanie lokalne, firmy wydają 9 procent budżetu. 11 procent wydatków dotyczy outsourcing, natomiast elementy o udziale poniżej 10 procent przedstawia poniższa grafika.

Pracownik najsłabszym ogniwem?

ISACA, z ang. Information Systems Audit and Control Association, czyli międzynarodowe stowarzyszenie osób zajmujących się zawodowo zagadnieniami dotyczącymi audytu, kontroli oraz bezpieczeństwa, wskazało osiem najczęściej popełnianych błędów w strategii cyberbezpieczeństwa.

- **Brak strategii** - szczebel zarządczy często nie posiada strategii dotyczącej cyberbezpieczeństwa. Powodem jest niechęć do ponoszenia dodatkowych kosztów związanych z infrastrukturą lub nietraktowanie tego tematu z należną mu powagą.

- **Niezabezpieczona sieć** - brak odpowiednich zabezpieczeń pozwala hakerom na dostęp do innych urządzeń i systemów do nich podłączonej.

- **Niezabezpieczona komunikacja** - poufne dane powinny być przesyłane wewnątrz organizacji z pomocą zabezpieczonych środków komunikacji.

- **Niezabezpieczone błędy w oprogramowaniu** - zwykle tego rodzaju błędów firma nie jest świadoma. Te w warstwie ochronnej oprogramowania mogą prowadzić do zainfekowania całego systemu.

- **Przestarzały system** - brak aktualizacji lub ich bagatelizacja sprawiają, że podmiot jest bardziej narażony na cyberataki.

- **Niedostateczne monitorowanie** - odpowiednio szybkie rozpoznanie ataku często pozwala zminimalizować jego skutki.

- **Wysoki poziom komputeryzacji i mechanizacji** - choć zwiększa produktywność biznesu, to ten czynnik z punktu widzenia cyberbezpieczeństwa uznawany jest za słabość z uwagi na mnogość potencjalnych punktów podatności.

- **Niewyszkoleni i nieodpowiedzialni pracownicy** - według danych ISACA, blisko 90 procent naruszeń danych jest spowodowanych błędem ludzkim. Dotyczy to sytuacji, gdy pracownik loguje się do systemu na fałszywej stronie podłożonej przez hakera lub otwiera podejrzane linki przychodzące na jego skrzynkę e-mail na służbowym komputerze. Częstym błędem jest również wykorzystywanie zbyt prostych haseł dostępnych jak np. "1234". Z tego względu tak ważne jest regularne szkolenia pracowników.

Przygotowując strategię cyberbezpieczeństwa warto zwrócić uwagę na raport ENISA Threat Landscap autorstwa europejskiej agencji do spraw cyberbezpieczeństwa. Publikowany co roku dokument dotyczący bezpieczeństwa cybernetycznego. Eksperci zwracają w nim uwagę na implementację oprogramowania ora mechanizmów pomagających szybko rozpoznać zagrożenie. Dodatkowo regularne audyty bezpieczeństwa mogą pomóc zidentyfikować słabe punkty w systemie. Ważne jest również, aby śledzić trendy związane z cyberbezpieczeństwem, aby reagować na zmieniające się zagrożenia. Raport opisuje wszystkie zagrożenia w podziale na ich rodzaje.

Outsourcing IT

Jest to strategia polegająca na zlecaniu obsługi IT zewnętrznym podmiotom. Serwis grandviewresearch przewiduje, że do 2030 roku rynek ten będzie rósł w tempie 8 procent rocznie, aż osiągnie 1180,42 mld dolarów. Możemy go podzielić na kilka kategorii:

- **Outsourcing onshore (domestic outsourcing)** - usługi zlecane są firmie informatycznej znajdującej się w tym samym kraju co podmiot zlecający. Pozwala to na ściślejszą współpracę pomiędzy firmami bez barier językowych i kulturowych.

- **Outsourcing nearshore** - dotyczy korzystania z usług firm znajdujących się w krajach sąsiadujących. Często pozwala na oszczędność kosztową, przy stosunkowo niewielkich różnicach kulturowych oraz braku różnic w strefach czasowych. Często stosowane przez firmy z Europy Zachodniej w kierunku krajów z Europy Środkowo-Wschodniej.

- **Outsourcing offshore** - usługi zlecane są firmom w dowolnej części świata. Nie ma tutaj znaczenie lokalizacja.

- **Outsourcint pełny** - dotyczy firm, które całkowicie planują zrezygnować z utrzymywania personelu IT.

- **Outsourcing częściowy** - w tym przypadku firma zleca jedynie niektóre czynności.

Wojna hybrydowa i zagrożenie ze strony Rosji

Według danych Microsoft zawartych w Microsoft Digital Defense Report 2023, 84 procent wszystkich cyberataków z Rosji wymierzonych jest w Ukrainę lub członków NATO. Według raportu, Rosja prowadzi wojnę hybrydową. Skoncentrowano się na atakach na nieco mniejsze podmioty niż miało to miejsce wcześniej, ale popularna pod tym względem pozostaje infrastruktura krytyczna oraz sektor edukacji. Badany jest również wpływ manipulowania opinią publiczną m.in. poprzez wspieranie ruchów protestacyjnych popierających Rosję.

Według Microsoft, rosyjski rząd wspiera cyberprzestępców, aby uzyskać dostęp do obiektów i sieci znajdujących zarówno na terenach Ukrainy, jak i w krajach NATO. Tamtejsza doktryna mówi, że każdy rząd, polityk lub organizacja znajdująca się w kraju, który zapewnia Ukrainie wsparcie polityczne, wojskowe lub humanitarne, jest narażony na rosyjskie cyberataki.

W przypadku Chin, kontynuowane są działania szpiegowskie. Tutaj również tego typu działania są wspierane przez państwo. Poszukiwane są wrażliwe dane głównie ze Stanów Zjednoczonych, a także z państw leżących nad Morzem Południowochińskim.

Dodatkowo cyberprzestępczość wykorzystywana jest do szerzenia negatywnych informacji na temat amerykańskich instytucji oraz promowaniu Chin poprzez wielojęzycznych influencerów. Chińskie władze obserwują w ten sposób również kraje regionu, takie jak Wietnam, Malezja, Filipiny oraz Indonezja.

ARTYKUŁ PROMOCYJNY

JAK SKUTECZNIE CHRONIĆ SWOJE DANE?

Przemysław Biel
Country Sales Manager Poland w Synology GmbH

2

Ostanie lata na zawsze zmieniły cyberprzestrzeń, zmuszając firmy do przeniesienia dużej części ich działalności do Internetu. Ogromny przyrost użytkowników zachęcił także hakerów do większej aktywności. Potrzeba szybkiej modernizacji infrastruktury, niestety, niosła ze sobą nie zawsze dobrze przemyślane wdrożenia.

Świadomość zabezpieczania danych z roku na rok rośnie, natomiast umiejętne planowanie oraz przemyślana strategia bezpieczeństwa to niestety ciągle rzadkość. Świadomość personelu w firmach też pozostawia wiele do życzenia.

Planowanie, automatyzacja, weryfikacja, bezpieczeństwo

Aby skutecznie chronić dane, należy przemyśleć cały proces i zaplanować go tak, aby zminimalizować potencjalne problemy. Musimy zadać sobie pytanie, na utratę jakiej ilości danych możemy sobie pozwolić oraz na jak długą przerwę w dostępie do tych danych nas stać. Dla jednej firmy może to być kwestia godzin lub dni natomiast dla innej minuty mogą decydować o milionowych stratach. Strategia bezpieczeństwa bierze pod uwagę specyfikę działalności, ilość danych, czas robienia ich kopii oraz czas ich przywracania, oraz czynnik ludzki. Niezbędna jest automatyzacja oraz weryfikacja procesów i danych oraz jakości kopii zapasowych i skuteczności ich przywracania.

Odpowiednie narzędzia oraz ich optymalne wykorzystanie

Firma Synology jest między innymi dostawcą kompletnych rozwiązań typu All in One, czyli serwerów NAS (Network Attached Storage). Tego typu pamięci

masowe zawierają szereg mechanizmów oraz dodatkowych aplikacji, pozwalając na dostosowanie strategii bezpieczeństwa danych do bardzo różnych środowisk, klientów oraz scenariuszy. Klient wybiera jakie elementy pasują najlepiej do jego potrzeb i na tej podstawie buduje system, który działa optymalnie dla niego. Do dyspozycji ma takie mechanizmy jak zaawansowana kontrola dostępu, deduplikacja i kompresja. Dostępne są także aplikacje do kopii zapasowej oraz synchronizacji, kopie migawkowe, szyfrowanie danych oraz transmisji, mechanizmy niezmienności danych typu WORM oraz wiele innych. To wszystko w ramach jednego rozwiązania dostępne w cenie urządzenia.

Przyjrzyjmy się kilku kluczowym funkcjonalnościom, które powinny być elementem każdego systemu bezpieczeństwa danych.

Istotnym aspektem jest deduplikacja. Jest to proces, który wykrywa powtarzające się bloki danych i zapisuje tylko te unikalne, przez co uzyskujemy więcej przestrzeni na dane. Taką funkcjonalność, czyli globalną deduplikację i kompresję obsługuje bezlicencyjny pakiet Active Backup Suite od Synology. Składa się on z trzech pakietów: Active Backup for Business, Active Backup for Microsoft 365 oraz Active Backup for Google Workspace.

Active Backup oferuje kopie przyrostowe typu Bare Metal, dzięki czemu przesyłamy tylko dane, które się zmieniają oraz mamy możliwość przywrócenia pracy całego urządzenia od podstaw, przy pomocy nośnika odzyskiwania.

W przypadku usług chmurowych, kopia może być wykonywana w sposób ciągły, dzięki czemu każda zmiana użytkownika ląduje także w kopii zapasowej.

Mając dane na serwerze trzeba zadbać także o ich bezpieczeństwo i skopiować je do innej lokalizacji, pozwala na to między innymi

narzędzie Synology Hyper Backup. Miejscem docelowym może być inny serwer lub usługa chmurowa.

Kolejnymi bardzo istotnymi narzędziami są kopie migawkowe oraz tzw. WORM (Write Once Read Many).

To co wyróżnia kopie migawkowe to ich szybkość. W przypadku serwerów Synology, mogą one być wykonywane nawet co 5 minut oraz mogą być także kopiowane na inne serwery Synology. Jest także możliwość tworzenia niemodyfikowalnych kopii migawkowych dzięki mechanizmowi WORM, dzięki czemu nawet przy uzyskaniu uprawnień administratora złośliwe oprogramowanie nie jest w stanie ich skasować. Odpowiednie wykorzystanie tego mechanizmu pozwala zapewnić dodatkową warstwę zabezpieczeń.

Wszędzie tam, gdzie dostępność danych jest kluczowa i akceptowalna przerwa w pracy to kwestia minut, niezbędne są dodatkowo mechanizmy wysokiej dostępności, które Synology także oferuje w dwóch formach. Pierwsza to możliwość połączenia dwóch serwerów Synology w klaster wysokiej dostępności. Drugą formą są urządzenia zbudowane z dwóch tzw. kontrolerów, które dzielą tylko przestrzeń dyskową, a cała reszta jest niezależna (procesor, pamięć, zasilacz itd…).

Trzymaj się zasady tworzenia kopii zapasowych 3-2-1

Złotym standardem w bezpieczeństwie danych jest zasada kopii zapasowej 3-2-1, której przestrzegają firmy na całym świecie. Zgodnie z tą radą, należy przechowywać przynajmniej trzy różne kopie danych na minimum dwóch różnych nośnikach, przy czym co najmniej jedna z nich powinna znajdować się w innej lokalizacji niż oryginał. Zapewnienie ciągłej dostępności danych, aplikacji i usług to konieczność by zapobiec utracie zysków i nadszarpnięcia reputacji firmy.

Wszelkie narzędzia potrzebne do wdrożenia tej zasady są zawarte w rozwiązaniu Synology NAS.

Kopia off-site

Kopię do innej lokalizacji można zrealizować na kilka sposobów, może to być między innymi inny serwer lub usługa chmury publicznej. W przypadku serwera, może być on w innym oddziale firmy lub, tak jak często nasi klienci robią, u usługodawcy w profesjonalnym centrum danych. Synology oferuje zarówno przestrzeń na kopie w chmurze, czyli usługę Synology C2 Storage, ale również kompletne rozwiązanie do kopii zapasowej, bezpośrednio do chmury, czyli Synology C2 Backup.

Active Backup vs ActiveProtect

Jak widać, cały proces budowania strategii bezpieczeństwa nie jest prosty i wymaga pewnej wiedzy oraz nakładów pracy. Synology dostarcza wszystkie elementy do zbudowania takiego systemu wykorzystując sprzęt oraz aplikacje dostarczane wraz z serwerami NAS. Jest to na pewno podejście bardzo efektywne kosztowo, gdyż aplikacje są bezlicencyjne i dostarczane w ramach rozwiązania.

Jest jednak część odbiorców, która wymaga więcej i potrzebuje systemu, który będzie oferował zarządzanie kopiami w strukturach rozproszonych zarówno w chmurze jak i na serwerach lokalnych

czy w innych lokalizacjach. Wszystko to powinno być zarządzane i monitorowane z jednego miejsca w prosty i szybki sposób.

Na postawie uwag i opinii klientów Synology przygotowało klasyczne rozwiązanie typu purpose-built backup appliance, zarządzane przez specjalny system operacyjny ActiveProtect, który został zaprojektowany właśnie w tym celu. To rozwiązanie będzie takim centralnym repozytorium kopii zapasowych i będzie współpracować ze wszystkimi możliwymi źródłami danych – urządzeniami końcowymi, serwerami, wirtualizatorami, innymi systemami pamięci masowej, bazami danych oraz usługami Microsoft 365 i Google Workspace. Każde urządzenie ActiveProtect może działać samodzielnie lub w trybie zarządzania w klastrze, a jego pojemność można rozszerzać za pomocą rozwiązań Synology NAS/SAN, usług C2 Object Storage oraz innych urządzeń ActiveProtect w klastrze.

Dane to najcenniejszy zasób Twojej firmy

Utrata danych bez posiadania kopii zapasowej jest zawsze kosztowna. W przypadku firmy, mogą to być konsekwencje, które doprowadzą do poważnych problemów finansowych lub prawnych, a nawet upadłości. Warto zatem zapobiegać takim przypadkom przez prowadzenie przemyślanej polityki bezpieczeństwa danych oraz kierowania się zasadami omawianymi w tym artykule.

Aby zabezpieczyć swoje dane i poznać wszystkie kluczowe elementy efektywnej strategii ochrony, warto skorzystać z darmowej listy kontrolnej. Lista ta pomoże Ci przeanalizować i wdrożyć niezbędne kroki w celu zapewnienia bezpieczeństwa Twoich danych.

Pobierz darmową listę kontrolną na stronie Synology tutaj:
https://event.synology.com/pl-pl/digital-security-checklist?utm_source=3rdparty2b&utm_medium=cpc&utm_campaign=security_interaktywnie_raport_link-2024-_Artykuł

BEZPIECZEŃSTWO INFRASTRUKTURY IT PRZEDSIĘBIORSTWA

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

3

Nieco ponad miesiąc temu, 19 lipca 2024, globalna awaria spowodowana aktualizacją oprogramowania w systemach Windows sparaliżowała linie lotnicze, media, banki i sprzedawców detalicznych na całym świecie, powodując nie tylko ogromne straty finansowe, ale trudny do opisania chaos. Ten incydent, już dzisiaj opisywany jako „największa awaria IT w historii", przypomniał również o tym, jak ściśle powiązane są światowe usługi i jak dalece zależne są od stabilności infrastruktury IT, oraz o potencjalnych konsekwencjach, gdy coś pójdzie nie tak.

To, co zaczęło się od opóźnień na lotniskach, szybko przerodziło się w masowe odwoływanie lotów, a zakłócenie komunikacyjne wpływało dalej na globalne łańcuchy dostaw; przerwano również transmisje w stacjach telewizyjnych i radiowych, a działalność supermarketów i banków została sparaliżowana. Szybko okazało się, że przyczyną była aktualizacja oprogramowania CrowdStrike's Falcon Sensor w systemach Microsoft Windows. Pracownicy napotykali na „niebieski ekran śmierci" przy każdej próbie logowania, a system wpadał w pętlę.

Przyczyna problemu została znaleziona i naprawiona stosunkowo szybko, ale proces odzyskiwania pełnej sprawności przez poszczególne organizacje zajął więcej czasu, powodując trudne do oszacowania konsekwencje finansowe. Najbardziej zaskakujące jest jednak nie to, że błąd w ogóle wystąpił, ale jak wielka była jego skala. Zastosowanie się do stopniowego wdrażania aktualizacji na zdrowy rozsądek wydaje się kluczową strategią zarządzania systemami IT, więc w przypadku firmy o tej renomie to, co się wydarzyło, wydaje się co najmniej nieprawdopodobne; a jednak - stało się!

I nie był to wyjątek. W maju 2024 roku z systemów edukacyjnych lokalnego rządu Helsinek wykradziono dane osobowe uczniów i opiekunów, a usterka oprogramowania w JPMorgan 2021 roku doprowadziła do naruszenia danych dotyczących niemal pół miliona klientów.

Lista kontrolna bezpieczeństwa cyfrowego

Sprawdź krok po kroku, czy pozwalasz na nieautoryzowany dostęp do krytycznych danych!

Zeskanuj kod QR!
Pobierz darmowo

Przykładów można by jeszcze mnożyć, ale wszystkie mówią jedno: niezawodna infrastruktura IT jest kluczowa dla biznesu, bez względu na to, w jakim sektorze działa.

Jak i jakie rozwiązania infrastrukturalne IT zapewniają bezpieczeństwo IT?

Wśród najważniejszych komponentów, które stanowią fundament każdej nowoczesnej infrastruktury IT, znajdują się sprzęt, czyli serwery, komputery, urządzenia magazynujące i sprzęt sieciowy; oprogramowanie, czyli systemy operacyjne, aplikacje i bazy danych - kluczowe dla działania biznesu; sieci, usługi chmurowe i wiele innych elementów. Ale wdrożenie solidnych środków bezpieczeństwa jest kluczowe dla ochrony wszystkich danych i zasobów IT przed zagrożeniami.

W zakresie zapewnienia bezpieczeństwa infrastruktury IT istotne są następujące komponenty:

- **Firewalle** - chronią sieci poprzez monitorowanie i kontrolowanie ruchu przychodzącego i wychodzącego, działając jako bariera między zaufanymi a niezaufanymi sieciami. Dzięki nim można skutecznie zapobiegać nieautoryzowanemu dostępowi do systemów.

- **Systemy wykrywania i zapobiegania włamaniom (IDPS)** - identyfikują i reagują na potencjalne zagrożenia poprzez monitorowanie ruchu sieciowego pod kątem podejrzanych działań. Są kluczowe dla wczesnego wykrywania i neutralizowania zagrożeń.

- **Oprogramowanie antywirusowe** - jest niezbędne do wykrywania i eliminowania złośliwego oprogramowania oraz wirusów, chroniąc integralność danych i systemów. Regularne aktualizowanie tego oprogramowania jest kluczowe dla utrzymania ochrony przed nowymi zagrożeniami.

- **Systemy szyfrujące danych** - chronią wrażliwe informacje, przekształcając je w bezpieczny format, który jest nieczytelny bez klucza deszyfrującego. Gwarantuje to poufność i integralność danych.

- **Systemy kontroli dostępu** - regulują, kto lub co może uzyskać dostęp do systemów IT, zapewniając, że tylko uprawnieni użytkownicy mają dostęp do kluczowych komponentów infrastruktury.

Tyle teorii. W praktyce komponowanie bezpiecznej infrastruktury IT to natomiast koronkowa robota, która wymaga wiedzy, doświadczenia i dogłębnej analizy nie tylko poszczególnych elementów, ale i przepływów pracy między nimi, co - zwłaszcza przy tzw. legacy systemach, czyli tych, które do najnowocześniejszych nie należą - jest arcytrudnym zadaniem. Bo choć obecnie dostępnych jest wiele nowoczesnych

Docieraj do 93% Polskich użytkowników internetu dzięki WP ads

Sam ustawisz kampanię.

Sam wybierasz rodzaj rozliczenia.

Sprawdź

WP SKONTAKTUJ SIĘ Z NAMI

sales@ads.wp.pl

tel: 22 57 67 890

rozwiązań, niewiele firm może i chce pozwolić sobie na pełną, a więc ryzykowną i kosztowną migrację. Większość firm decyduje się więc na podejście granularne, stopniowo zastępując poszczególne, niespełniające wymogów bezpieczeństwa elementy, nowszymi.

I tutaj jednak sprawa nie jest prosta, bo oferta nawet tych uznanych dostawców infrastruktury IT takich jak IBM, Oracle, Dell czy Cisco, jest bardzo zróżnicowana. Wszyscy oferują zaawansowane funkcje zabezpieczeń, takie jak sprzętowe moduły TPM (Trusted Platform Module), wbudowane mechanizmy kryptograficzne oraz zabezpieczenia przed atakami typu DDoS, przy jednoczesnym minimalnym zużyciu energii i wysokiej niezawodności.

Wiele firm oferuje jednak rozwiązania projektowane specjalnie z myślą o zwiększonym bezpieczeństwie, tak jak serwery IBM Power10, dzięki którym można bezpiecznie przechowywać dane wrażliwe w zasobach prywatnych, jednocześnie korzystając z wysokiej mocy obliczeniowej chmury publicznej, idealnej dla zmiennego ruchu, jak w sklepach internetowych. Ponadto te serwery wyposażono w oprogramowanie zabezpieczające każdy poziom systemu - od procesora i pamięci aż po oprogramowanie, takie jak system operacyjny, wirtualizator (hypervisor) czy krytyczne aplikacje. Alternatywą dla rozwiązań proponowanych przez IBM mogą być Dell PowerEdge Rack Servers, Lenovo ThinkSystem Rack Servers, Cisco UCS Series czy Oracle SPARC Servers.

Jakie są koszty przestoju infrastruktury IT?

Koszty przestoju infrastruktury IT mogą być oszałamiające i wpływać na firmy każdej wielkości w różnych branżach. Wpływ finansowy przestoju różni się w zależności od branży, wielkości firmy i okoliczności awarii. Jednak ogólny trend jest jasny: w miarę jak firmy coraz bardziej polegają na operacjach cyfrowych, koszt przestoju nadal rośnie.

Średnio przestoje mogą dziś kosztować firmy około 9000 USD za minutę, w porównaniu z 5600 USD za minutę, jak podano w badaniu Gartnera z 2014 r. W przypadku mniejszych firm straty finansowe są stosunkowo niższe i wahają się od 137 do 427 USD za minutę. Jednak nawet te pozornie skromne kwoty mogą być druzgocące dla MŚP, potencjalnie zagrażając ich stabilności finansowej i długoterminowej rentowności.

Duże firmy, ze względu na skalę i globalny charakter swoich operacji, ponoszą jeszcze wyższe koszty. Przestoje mogą przekraczać 16 000 USD na minutę, co przekłada się na ponad 1 milion USD na godzinę. Dla tych organizacji jedna godzina przestoju może mieć daleko idące konsekwencje, wpływając na wszystko, od obsługi klienta po zarządzanie łańcuchem dostaw.

ARTYKUŁ PROMOCYJNY

JAK SKUTECZNIE ZABEZPIECZAĆ DANE KLIENTÓW W CHMURZE?

Mateusz Kaleta
Specjalista ds. cyberbezpieczeństwa w sektorze Comarch Enterprise Solutions

4

Klienci coraz częściej poszukują rozwiązań dostosowanych nie tylko do swoich potrzeb, ale też takich, które zapewnią, że ich dane będą bezpieczne. W Chmurze Comarch dla małych i średnich przedsiębiorstw priorytetowo dba się o bezpieczeństwo przed zewnętrznymi i wewnętrznymi zagrożeniami cybernetycznymi oraz lukami w zabezpieczeniach.

Firmy w szybkim tempie dokonują cyfrowej transformacji. Dzisiaj z firmowymi zasobami mogą łączyć się z dowolnego miejsca na świecie i z niemal dowolnego sprzętu. To wszystko dzięki możliwościom chmury obliczeniowej.

– *Bezpieczeństwo w chmurze jest bardzo podobne do bezpieczeństwa lokalnych centrów danych; tylko bez kosztów utrzymania obiektów i sprzętu. W chmurze nie trzeba zarządzać fizycznymi serwerami ani urządzeniami pamięci masowej. Zamiast tego klient używa narzędzi bezpieczeństwa opartych na oprogramowaniu do monitorowania i ochrony przepływu informacji* – mówi **Kamil Migacz, menadżer ds. cybersecurity w sektorze Comarch Enterprise Solutions.**

Chmura Comarch – w trosce o najlepszy poziom bezpieczeństwa

Każdy z modeli usług (IaaS, SaaS, PaaS) oraz modeli wdrożenia (chmura publiczna, prywatna, hybrydowa) różni się aspektami bezpieczeństwa. Zawsze jest jednak ono współdzielone pomiędzy dostawcę usług a klienta.

– *W **Chmurze Comarch dla małych i średnich przedsiębiorstw** wdrażamy najlepsze praktyki w zakresie zasad, architektury i procesów operacyjnych Comarch, stworzone w celu spełnienia wymagań naszych najbardziej wrażliwych na bezpieczeństwo klientów* – mówi Kamil Migacz.

– Infrastruktura Comarch Cloud spełnia wymogi zgodności z rynkowymi standardami bezpieczeństwa i regulacjami, m.in. Benchmarkami CIS, PCI DSS, ISO 27001 i najlepszymi praktykami w zakresie security. Nasze centra przetwarzania danych są regularnie kontrolowane przez inżynierów i niezależnych specjalistów pod kątem bezpieczeństwa, prywatności, zgodności z obowiązującym prawem, w tym RODO – dodaje ekspert.

Comarch Cloud jest monitorowany 24/7, co umożliwia natychmiastową reakcję na wszelkie nieprawidłowości w systemie i incydenty bezpieczeństwa. W razie incydentu zespół ds. bezpieczeństwa może sprawdzić logi zdarzeń, aby uzyskać informacje o potencjalnych atakach, zmianach lub nieprawidłowościach. Może to pomóc w szybkim wykrywaniu i reagowaniu na wszelkie zdarzenia.

Uwierzytelnienie dwuskładnikowe i ochrona antyDDoS

Wszystkie kluczowe komponenty i infrastruktura krytyczna są częścią centralnego **Centrum Operacji Bezpieczeństwa** (ang. SOC – Security Operations Center), w którym analitycy mają możliwość reagowania na incydenty na jak najwcześniejszym etapie. Model bezpieczeństwa „zero trust" umożliwia szczególne podejście do kontrolowania dostępu do zasobów chmurowych i izolację aplikacji oraz zasobów o znaczeniu krytycznym od sieci chmurowej. Pełna ochrona danych poprzez szyfrowanie danych pomaga zapewnić ich integralność. Hardeningi (tj. zabezpieczania systemu poprzez zmniejszanie jego powierzchni podatności na ataki) zapewniają bezpieczną konfigurację kluczowych komponentów dostarczanych produktów poprzez bezpieczną konfigurację zgodnie z najlepszymi praktykami.

*– Do korzystania z zasobów Chmury Comarch wykorzystuje **uwierzytelnianie dwuskładnikowe (2FA)**, które jest podstawowym*

mechanizmem zabezpieczeń zasobów chmurowych i pozwalającym na sprostanie współczesnym wymogom w zakresie bezpieczeństwa – mówi Kamil Migacz.

2FA dodaje dodatkową warstwę ochrony przed nieuprawnionym dostępem, co odbywa się poprzez wprowadzenie loginu i hasła (coś, co znam – pierwszy składnik) oraz potwierdzenia w aplikacji (coś, co mam – drugi składnik uwierzytelniania). Chmura Comarch wdraża politykę haseł zgodną z polityką organizacji, a kontrola dostępu w oparciu o zasadę minimalnych uprawnień pozwala na skuteczne wykrywanie i blokowanie prób nieautoryzowanego dostępu do danych.

Ochrona antyDDoS to kolejna ważna funkcja, która zapewnia nieprzerwaną pracę serwerów i aplikacji w Chmurze Comarch. Oprogramowanie antywirusowe i antymalware są stale aktualizowane, aby zapewnić skuteczną ochronę przed nowymi zagrożeniami. Chmura przechodzi regularne audyty bezpieczeństwa i testy penetracyjne, wykonywane przez wykwalifikowanych inżynierów, w celu wykrycia i powstrzymywanie zagrożeń na jak najwcześniejszych etapach ich wykrycia.

Zasada 3-2-1 jako gwarancja bezpieczeństwa danych

Regularne kopie zapasowe zasobów chmurowych gwarantują, że kluczowe dane przetrwają każde z możliwych zagrożeń.

*– W Chmurze Comarch stosujemy **zasadę 3-2-1**, tj. przechowujemy przynajmniej trzy kopie swoich danych na dwóch różnych nośnikach/technologiach, z czego jedno znajduje się w innej lokalizacji poza głównym centrum przetwarzania danych. Backupy gwarantują wysoką dostępność Chmury Comarch* – mówi menadżer cyberbezpieczeństwa.

O bezpieczeństwo aplikacji Comarch dba już na poziomie wytwarzania oprogramowania, wdrażając w firmie **model SSDLC** (ang. Secure Software Development Lifecycle). Dzięki temu organizacja kontroluje je na każdym etapie wytwarzania oprogramowania, od pierwszych faz planowania, przez cały proces produkcji. Zwiększa tym samym ich efektywność przy niższych kosztach wynikających z wcześniej wykrytych błędów.

– Wszystkie te mechanizmy działają na podstawie naszej polityki bezpieczeństwa. Comarch gwarantuje dostępność usług Chmury Standard i Enterprise na poziomie 99% czasu w skali roku, a Comarch Hosting na poziomie 99% - 99,8% czasu w skali roku, w zależności od wybranego poziomu SLA. Zapewnia on naszym klientom pewność, że ich usługi będą działać bez przestojów, a wykryte podatności zostaną naprawione zgodnie z ustalonymi warunkami – podsumowuje Kamil Migacz.

Chmura Comarch oferuje dla przedsiębiorstw systemy ERP, e-commerce, narzędzia do zarządzania dokumentami, sprawozdania finansowe, zarządzanie pracownikami,

aplikacje usprawniające logistykę czy kompleksowe rozwiązanie do zarządzania kopiami zapasowymi. O produktach w Chmurze Comarch i modelach sprzedaży można dowiedzieć się więcej na https://www.comarch.pl/chmura.

Cyberbezpieczeństwo i ochrona danych firmowych jest obecnie jednym z najważniejszych wyzwań jakie są stawianie przed przedsiębiorstwami. Niezwykle ważna jest ciągła edukacja pracowników na temat zagrożeń w sieci, ponieważ są oni najbardziej narażeni na ataki hakerskie i wyłudzenie poufnych danych przez osoby trzecie. Specjaliści z firmy Comarch na podstawie swoich wieloletnich doświadczeń opracowali bezpłatny Kurs Cyberbezpieczeństwa z certyfikatem, który dedykowany jest wszystkim, którzy chcą poszerzyć swoją wiedzę i nabyć niezbędne umiejętności pozwalające na bezpieczne korzystanie z technologii. Kurs dostępny jest w wersji online na naszej stronie. Zachęcamy do wzięcia udziału w szkoleniu i zdobycia certyfikatu.

CHMURA I BACKUP DANYCH W SŁUŻBIE BEZPIECZEŃSTWA BIZNESU

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

5

Wartość ponad 2 mld dolarów może do 2032 roku osiągnąć rynek cloud computingu. Usługi chmurowe prężnie rozwijają się również nad Wisłą, gdzie w ubiegłym roku na ten cel wydano prawie 4 mld złotych. Jedną z głównych zalet tego rozwiązania jest bezpieczeństwo danych z uwagi na stosowane zabezpieczenia i kopie zapasowe.

Cloud computingu to zestaw usług związany z przechowywaniem danych firmy lub użytkownika na serwerach zewnętrznego podmiotu. Oprócz tego usługodawca wraz z przestrzenią dyskową udostępnia również komplementarne narzędzia oraz wsparcie techniczne. Użytkownik natomiast otrzymuje dostęp do danych za pośrednictwem internetu. Usługi chmurowe to także backup, czyli wykonywanie kopii zapasowych zgromadzonych danych. W ten sposób firma dodatkowo zabezpiecza swoje dane.

Rynek usług chmurowych

Według danych Marketusa, w 2023 roku wartość rynku cloud computingu sięgnęła 633 mld dolarów, natomiast w tym roku może wynieść nawet 722 mld dolarów. Serwis podaje również, że jeszcze w tej dekadzie rynek rozwiązań chmurowych przekroczy poziom miliarda dolarów, a w 2032 będzie to ponad 2,3 mld dolarów.

Z kolei wartość rynku cloud computingu w Polsce sięgnęła w 2023 roku 3,9 mln złotych, co daje wzrost na przestrzeni roku na poziomie 34 procent. Raport PMR wskazuje, że w 2024 roku poziom ten wzrośnie o kolejne 24 procent i osiągnie 4,8 mld złotych. Wcześniej w latach (2021, 2022) było to odpowiednio 2,2 oraz 2,9 mld złotych.

JAK BRAK BEZPIECZNEJ KOPII ZAPASOWEJ MOŻE WPŁYNĄĆ NA NASZĄ FIRMĘ?

Wyobraźmy sobie sytuację, w której w ciągu kilku minut przestajemy mieć dostęp do danych stanowiących fundament pracy naszego przedsiębiorstwa. Istnieje niezliczona ilość przyczyn, które mogą doprowadzić do takiej sytuacji – zainfekowana wiadomość e-mail, luki w zabezpieczeniach, uszkodzenie infrastruktury IT czy pożar budynku. Istnieją również skuteczne sposoby, aby się przed taką sytuacją obronić lub zniwelować jej skutki. Kluczem do sukcesu jest posiadanie kopii zapasowej, z której dane mogą zostać prawidłowo przywrócone. Kolejnym warunkiem jest bezpieczeństwo serwera, na którym nasze dane są przechowywane.

Skuteczna ochrona danych

Przykładem rozwiązania, które możemy wykorzystać do ochrony danych jest serwer NAS. Zaletą takiego wyboru jest szerokie spektrum dostępnych zastosowań. Serwer może jednocześnie udostępniać dane użytkownikom korzystającym z różnych systemów operacyjnych, umożliwiać wspólną pracę na plikach, ale przede wszystkim pozwala zabezpieczyć środowisko IT. Firma Synology w swoim portfolio oferuje skalowalne rozwiązania biznesowe, zarówno dla mniejszych firm, jak i dużych przedsiębiorstw. Znaczenie mają tutaj nie tylko koszty sprzętu, ale również oprogramowania. Z tego powodu wbudowane narzędzia Active Backup Suite do tworzenia kopii zapasowej środowiska IT, które nie wymaga dodatkowych opłat są niewątpliwą zaletą. Dodatkowo, integralność danych chroniona jest przez zaawansowany system plików Btrfs.

Pamiętajmy jednak, że dane te muszą być także chronione przed niepowołanym dostępem. Ochrona rozpoczyna się już na poziomie połączenia z serwerem NAS. Synology przygotowało szereg narzędzi, które zablokują próby przełamania hasła czy ograniczą dostęp tylko dla wybranych urządzeń za pomocą zapory sieciowej. Aby zapewnić, że do serwera logują się tylko uprawnieni użytkownicy, należy włączyć logowanie dwuetapowe. Pierwszym etapem będzie wpisanie hasła, drugim może być jednorazowy kod generowany na naszej komórce, zatwierdzenie logowania w aplikacji Synology Secure SignIn czy klucz sprzętowy. Nie należy również zapominać o regularnych aktualizacjach, które wzmacniają bezpieczeństwo systemu i używanych aplikacji.

Jak o tym wszystkim pamiętać?

Ponieważ ilość ustawień bezpieczeństwa wymagających ciągłej kontroli może przyprawić o zawrót głowy, możemy skorzystać z Doradcy ds. zabezpieczeń – narzędzia dostępnego w systemie Synology DSM. Pozwala ono na cykliczne skanowanie systemu pod kątem ewentualnych infekcji i luk w zabezpieczeniach, przedstawi sugerowane zmiany, a także ostrzeże nas o podejrzanych logowaniach do systemu.

Nieocenioną pomocą będzie także usługa chmurowa Active Insight, pozwalająca na monitorowanie i zarządzanie wieloma serwerami Synology NAS. Może ona m.in. monitorować podejrzane działania na plikach świadczące o infekcji oprogramowaniem ransomware. Wykryte zdarzenie wyzwoli utworzenie niezmiennej migawki bazującej na technologii WORM, dzięki czemu nawet nieuprawniony dostęp na poziomie administratora nie pozwoli na skuteczne skasowanie chronionych danych. Niezmienne migawki możemy wdrożyć oczywiście dużo wcześniej, przed ewentualnym wystąpieniem incydentu.

Czynności kontrolne nie ograniczają się jednak wyłącznie do serwera NAS. Z tego powodu Synology przygotowało listę kontrolną, która pomoże administratorowi sprawdzić najistotniejsze punkty ochrony infrastruktury IT.

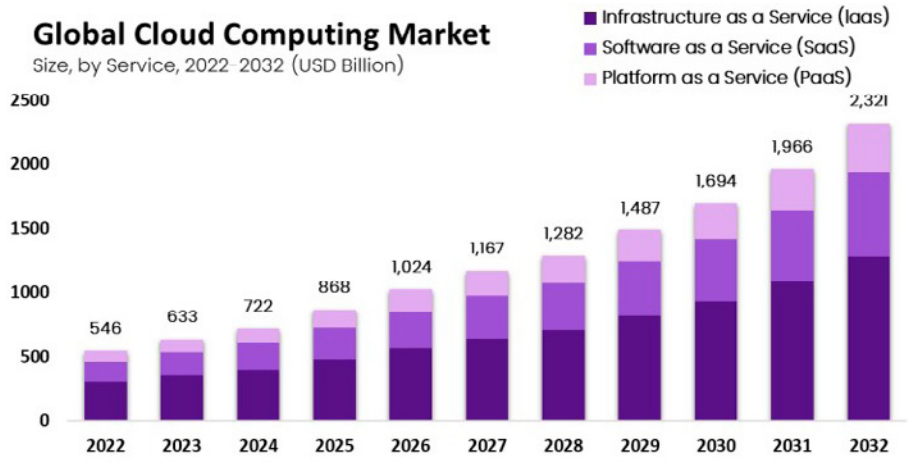
Lista dostępna jest bezpłatnie pod poniższym linkiem:
https://sy.to/lista

Tomasz Iwańczuk
Synology Solution Engineer w Synology GmbH

Synology®

Jak czytamy w raporcie, mimo szybkiego wzrostu, cloud computing jest niewielką częścią całego rynku usług IT w Polsce. Dynamiczny wzrost może wynikać z szybkiej transformacji cyfrowej, jaką przechodzą polskie przedsiębiorstwa. Eksperci w raporcie wskazują, że aż 73 procent dużych przedsiębiorstw planuje lub już zwiększyło wydatki na cloud computing w tym roku.

Wartość globalnego rynku cloud computingu w latach 2022-2032 (w mld dolarów)



Źródło: market.us

Jak tego typu rozwiązania chronią firmy?

Według Data Attack Surface, do 2025 roku na świecie będzie przechowywanych co najmniej 200 zetabajtów danych. Składają się na to prywatne i publiczne systemy informatyczne, rozwiązania chmurowe i urządzenia osobiste. W przypadku cloud computingu eksperci szacują, że będzie to 100 zetabajtów danych, czyli około połowa wszystkich światowych danych.

Według Cloud Security Spotlight Report, wśród technologii stosowanych w ramach cloud computingu, które chronią użytkowników należy wymienić:

- szyfrowanie danych
- szyfrowanie sieci
- kontrola dostępu
- zapory sieciowe
- zarządzanie hasłami oraz logami
- dostępność specjalistów IT z zakresu bezpieczeństwa
- monitorowanie aktywności pracowników
- filtrowanie treści
- antywirusy.

Buduj biznes i skaluj sprzedaż wykorzystując sprawdzony i rozpoznawalny brand

money.pl

22 mln UU 117 mln PV

Źródło: dane wewnętrzne, listopad 2023

Buduj z nami content wideo:

NEWS Cykle redakcyjne

Na łamach serwisu money.pl redakcja stale porusza tematy, które dotykają wielu aspektów codziennego życia. Ofertujemy możliwość obecności przy ważnych i aktualnych tematach gospodarczych.

Short poradniki wideo

Cykl poradników wideo o zagadnieniach często wyszukiwanych przez użytkowników. Seria poradników przygotowywana jest przez redakcję wspólnie z ekspertami ze strony Partnera. Dzięki swojej zwięzłej formule i napisom, które dodajemy do każdego wideo, materiały idealnie sprawdzają się w mediach społecznościowych.

Obecność przy poradnikach B2B i B2C

Money.pl to ponad 1800 poradników dla przedsiębiorców oraz konsumentów, które przede wszystkim są odwiedzane przez użytkowników szukających konkretnych informacji w sieci.

SKONTAKTUJ SIĘ Z NAMI

reklama@grupawp.pl

tel: 22 57 67 890

Wady i zalety rozwiązań chmurowych

Zalety:

- **Wzrost mobilności danych** - rozwój pracy zdalnej sprawił, że dostępność danych firmowych spoza lokalnej sieci jest pożądany. Dotyczy to nie tylko pracowników pracujących z domu, ale także np. przedstawicieli handlowych.
- **Bezpieczeństwo** - dzięki tworzonej automatycznie kopii zapasowej, dane firmy są zabezpieczone na wypadek cyberataku lub awarii.
- **Oszczędności kosztowe** - wdrożenie systemu z ang. Software as a Service, pozwala na obniżenie kosztów wynikających z braku konieczności utrzymywania własnej obsługi oraz infrastruktury IT.
- **Elastyczność rozwiązania** - duży wybór rozwiązań chmurowych sprawia, że firma z łatwością może dobrać odpowiednie rozwiązanie - zarówno pod względem kosztowym jak i w kwestii zakresu usług.
- **Skalowalność** - prowadzone przez zewnętrzną firmę usługi z łatwością mogą zostać zwiększone lub rozbudowane w miarę rozwoju biznesu. Zarząd nie musi się martwić o to, że lokalna sieć firmowa będzie barierą rozwojową.
- **Możliwość zmiany usługodawcy** - w przypadku braku zadowolenia z zakresu jak i jakości świadczonych usług, dostawcę rozwiązań chmurowych można zmienić.

Wady:

- **Konieczność udostępnienia danych zewnętrznej firmie** - mimo że firmy świadczące usługi cloud computingu posiadają odpowiednie zabezpieczenia i niejednokrotnie są one skuteczniejsze od tych zaimplementowanych w firmach, to decyzja o rozpoczęciu korzystania z rozwiązania chmurowego wymaga często przełamania bariery psychologicznej.
- **Kompetencje wdrażających** - źródłem ryzyka związanym z wdrożeniem takiego systemu może być sam konsultant wdrażający. Niezrozumienie charakteru działalności może prowadzić do błędów, które będą uciążliwe w dłuższej perspektywie czasu.
- **Ryzyko wdrożenia** - istnieje ryzyko, że wdrożenie się nie powiedzie.
- **Uzależnienie od internetu** - w przypadku rozwiązań lokalnych, z danych firmowych można korzystać z pominięciem internetu. W przypadku rozwiązań chmurowych, gdzie dane mogą być lokalizowane dziesiątki lub setki kilometrów dalej, niezbędny jest internet. To samo dotyczy pracowników mobilnych (np. przedstawicieli handlowych), którzy za pośrednictwem sieci będą korzystać z danych zdalnie.

Koszty cloud computingu

To, ile dana firma wyda na wdrożenie oraz współpracę z firmą zewnętrzną w ramach cloud computingu zależy od jej wielkości, postawionych wymagań czy renomy i umiejętności samego usługodawcy. Według danych Oracle, dzięki inwestycjom w usługi chmurowe, większość firm działa wydajniej, a ich koszty są niższe w stosunku do tradycyjnych rozwiązań lokalnych.

Zgodnie z raportem Deloitte US Future of Cloud Survey Report, 88 procent badanych pozytywnie oceniło wyniki inwestycji w rozwiązanie chmurowe, w zakresie wydajności. Z kolei 83% wskazało na korzyści w zakresie dotyczące obniżenia i optymalizacji kosztów.

Eksperci Oracel zwracają również uwagę na zalety związane ze zmniejszeniem ryzyka regulacyjnych dotyczących przechowywania danych oraz szybszy rozwój biznesu i jego cyfryzację.

Powszechność i najpopularniejsze rozwiązania chmurowe

Według danych Statisty, już ponad 60 procent danych korporacyjnych jest przechowywana w chmurze. Wynik ten uległ podwojeniu w stosunku do danych z 2015 roku. Według przewidywań, do 2026 roku odsetek ten wzrośnie do 75 procent.

Dgtlinfra wymienia natomiast dziesięć najpopularniejszych rozwiązań chmurowych. Wśród nich zdecydowanym liderem jest Amazon Web Service z dostępnością w 33 krajach. Co ciekawe Amazon pokonał rozwiązanie Microsoft Azure dostępne w aż 64 krajach. Na najniższym stopniu podium znalazła się platforma Google Cloud, Alibaba Cloud oraz IBM Cloud.

Najpopularniejsze na świecie rozwiązania chmurowe wraz z liczbą rynków, na których są dostępne

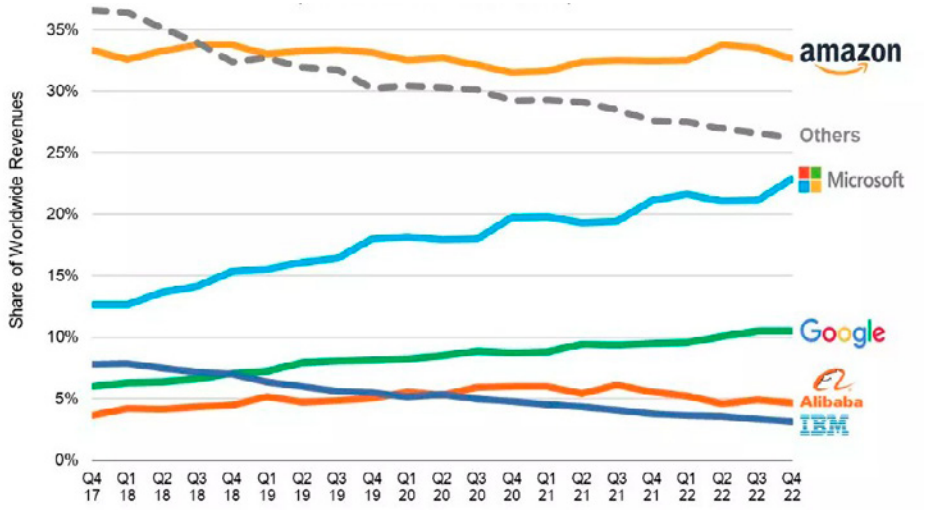
#	Cloud Service Provider	Regions
1	Amazon Web Services (AWS)	33
2	Microsoft Azure	64
3	Google Cloud Platform (GCP)	40
4	Alibaba Cloud	30
5	Oracle Cloud	48
6	IBM Cloud	10
7	Tencent Cloud	21
8	OVHcloud	17
9	DigitalOcean	9
10	Linode (Akamai)	20

Źródło: dgtlinfra

Lider zestawienia oferuje ponad 200 różnych usług w tym nie tylko dotyczące przechowywania danych, ale także m.in. funkcji obliczeniowych.

Przychody Amazon Web Service odpowiadają za ponad 30 procent globalnych wydatków na rozwiązania chmurowe. Wicelider Microsoft Azure obejmuje ponad 20 procent „tortu" usług. Około 10 procent rynku stanowi Google Cloud Platfom, natomiast Alibaba oraz IBM dzielą się przychodami na poziomie 5 procent rynku cloud computingu.

Udział w rynku cloud computingu poszczególnych rozwiązań w latach 2017-2022



Źródło: Synergy Research Group

OCHRONA DANYCH FIRMOWYCH

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

6

Cyfrowe zagrożenia i wyrachowane taktyki oszustów stale ewoluują, ale większość z tych najpowszechniejszych i najbardziej udanych nadal w dużym stopniu opiera się na wykorzystywaniu powszechnych luk, takich jak „niezałatane" oprogramowanie lub nieprawidłowo skonfigurowane systemy. Tymczasem 55% liderów biznesowych uważa, że ich klienci powierzają im więcej danych niż dwa lata temu; jednocześnie coraz mniej ufają, że są one bezpieczne. By pokryć tę lukę, firmy potrzebują czegoś więcej niż tylko reaktywnych środków bezpieczeństwa. Muszą proaktywnie chronić komponenty fizyczne, sieciowe i aplikacyjne, zachowując jednocześnie przejrzystość i solidne zasady bezpieczeństwa.

Audyty jako podstawa bezpieczeństwa

Jednym z podstawowych kroków w zapewnieniu bezpieczeństwa danych jest przeprowadzanie regularnych audytów bezpieczeństwa. Audyty, wykonywane co najmniej raz w roku, pozwalają specjalistom ds. bezpieczeństwa na ocenę obecnych środków, identyfikację luk oraz rekomendowanie ulepszeń.

Dzięki regularności przeprowadzanych analiz, firmy mogą dostosowywać się do ciągle zmieniającego się krajobrazu zagrożeń cyfrowych. Nawet jeśli ich wewnętrzna infrastruktura, polityka czy zasoby nie zmieniają się tak często, audyty biorą pod uwagę także zgodność z zewnętrznymi regulacjami i podatność na zewnętrzne zagrożenia.

Oto, z jakich sekcji powinien składać się typowy audyt bezpieczeństwa:

1. **Zakres i cele audytu oraz zastosowana metodologia**
   Określenie granic audytu, w tym systemów, procesów i działów objętych badaniem, połączone z opisem podejścia, narzędzi i technik stosowanych podczas analizy.

2. **Ocena zgodności z regulacjami**
   Ocena, w jakim stopniu organizacja spełnia odpowiednie standardy branżowe, przepisy oraz wewnętrzne polityki.

3. **Wyniki i estymacja ryzyka**
   Priorytetyzacja zidentyfikowanych zagrożeń na podstawie ich potencjalnego wpływu i prawdopodobieństwa wystąpienia. Taka analiza pomaga organizacji skoncentrować zasoby na najważniejszych kwestiach.

4. **Rekomendacje**
   Praktyczne porady dotyczące sposobu rozwiązania każdego z wykrytych problemów. Zalecenia powinny być precyzyjne, wykonalne i dostosowane do zasobów oraz możliwości organizacji.

5. **Plan działań**
   Proponowany harmonogram i strategia wdrażania zaleceń wynikających z audytu.

Kontrola dostępu, to nie tylko mocne hasła

Najpopularniejsze hasła w 2024 roku niezmiennie pokazują niepokojący trend, w którym użytkownicy polegają na łatwych do odgadnięcia kombinacjach typu „123456", „password", „123456789", „qwerty", co czyni je głównymi celami cyberprzestępców stosujących ataki siłowe lub techniki wypełniania danych uwierzytelniających.

Rozpowszechnienie tych słabych haseł podkreśla kluczowy problem w praktykach bezpieczeństwa, mimo że eksperci ds. cyberbezpieczeństwa podkreślają potrzebę przyjęcia przez użytkowników lepszych praktyk. Ich rekomendacje obejmują używanie haseł, które zawierają kombinację wielkich i małych liter, cyfr i znaków specjalnych. Ponadto korzystanie z menedżerów haseł może pomóc użytkownikom generować i przechowywać silne, unikalne hasła dla każdego z ich kont, zmniejszając obciążenie związane z zapamiętywaniem.

Ale to nie wszystko. W firmach zalecane jest wdrożenie uwierzytelniania wieloskładnikowego (MFA), które dodaje dodatkową warstwę bezpieczeństwa, wymagającą od użytkowników podania dwóch lub więcej czynników weryfikacji w celu uzyskania dostępu do zasobu. Czynniki te mogą obejmować coś, co użytkownik zna (np. hasło), posiada (np. smartfon lub token bezpieczeństwa) i czym się identyfikuje (np. odcisk palca lub rozpoznawanie twarzy).

Kontrola dostępu oparta na rolach (RBAC) jest kolejnym kluczowym elementem silniejszej kontroli danych. RBAC należy stosować w celu ograniczenia dostępu do danych na podstawie przyznanej roli. Zapewnia to, że pracownicy mają dostęp wyłącznie do informacji, których potrzebują do wykonywania swoich obowiązków. Zasada ta pomaga zminimalizować potencjalne szkody, które mogą wystąpić w przypadku naruszenia konta użytkownika.

Regularne przeglądanie i aktualizowanie uprawnień użytkowników jest niezbędne do utrzymania skuteczności kontroli dostępu. Proces ten, często nazywany ponowną certyfikacją dostępu, obejmuje okresowe przeglądanie i weryfikowane praw dostępu użytkowników w celu zapewnienia, że pozostają one odpowiednie. Jest to szczególnie ważne, gdy pracownicy zmieniają role w organizacji lub całkowicie opuszczają firmę. Zautomatyzowane narzędzia mogą pomóc usprawnić ten proces, zwłaszcza w dużych organizacjach z wieloma użytkownikami i złożonymi strukturami dostępu.

Oprócz tych środków organizacje mogą też rozważyć wdrożenie adaptacyjnego uwierzytelniania, które dostosowuje wymagany poziom uwierzytelniania na podstawie czynników kontekstowych, takich jak lokalizacja użytkownika, urządzenie i wzorce zachowania.

Zagrożenia zewnętrzne

Firmy powinny wdrożyć szyfrowanie danych przesyłanych z jednej lokalizacji do drugiej przez sieci, co obejmuje wdrożenie protokołów Secure Sockets Layer (SSL) lub Transport Layer Security (TLS). Tworzą on szyfrowane łącze między serwerem internetowym a przeglądarką, zapewniając, że wszystkie dane przesyłane między nimi pozostają prywatne i integralne. Wirtualne sieci prywatne (VPN) powinny z kolei być używane do zdalnego dostępu, tworzą bowiem szyfrowane tunele, przez które dane można bezpiecznie przesyłać przez sieci publiczne.

Równie ważne jest szyfrowanie danych w spoczynku, co odnosi się do informacji przechowywanych na dowolnym urządzeniu lub w sieci. Powinno to obejmować pełne szyfrowanie dysku dla wszystkich urządzeń, od serwerów i komputerów stacjonarnych po laptopy i urządzenia mobilne. Pełne szyfrowanie dysku chroni wszystkie dane na urządzeniu, niezależnie od typu pliku lub lokalizacji, co czyni je niezbędnym zabezpieczeniem w przypadku kradzieży fizycznej lub nieautoryzowanego dostępu do utraconych urządzeń. Szyfrowanie bazy danych to kolejny kluczowy aspekt, chroniący przechowywane informacje zarówno przed zagrożeniami zewnętrznymi, jak i potencjalnymi zagrożeniami wewnętrznymi.

Kopie zapasowe i archiwa, często pomijane w strategiach szyfrowania, również powinny być nim objęte. Te repozytoria często zawierają ogromne ilości poufnych danych historycznych, a szyfrowanie zapewnia, że pozostaną one chronione, nawet jeśli fizyczne urządzenia pamięci masowej zostaną naruszone lub wpadną w niepowołane ręce. Jest to szczególnie ważne w przypadku kopii zapasowych przechowywanych poza siedzibą firmy lub rozwiązań pamięci masowej w chmurze.

Kluczowe jest również rozważenie szyfrowania typu end-to-end w przypadku wysoce poufnych komunikatów lub transferów danych. Zapewnia to, że dane są zaszyfrowane w systemie nadawcy przed transmisją i odszyfrowywane tylko w systemie

odbiorcy, chroniąc przed potencjalnym przechwyceniem lub manipulacją podczas przesyłania.

Co więcej, firmy muszą zrównoważyć wykorzystanie szyfrowania z potrzebami operacyjnymi i wymogami regulacyjnymi. Niektóre przepisy mogą nakazywać określone standardy szyfrowania lub praktyki zarządzania kluczami. Inne mogą wymagać od firm możliwości odszyfrowania danych na zgodne z prawem żądanie, co wymaga starannego zaplanowania wdrożenia szyfrowania.

Aktualizacje i testy

Starsze systemy, które nie otrzymują już aktualizacji zabezpieczeń, również mogą być łatwym celem dla cyberataków, a często są także niekompatybilne z nowoczesnymi rozwiązaniami, co może prowadzić do powstania luk w ogólnym podejściu organizacji do zabezpieczeń.

Dodatkowo, brak wsparcia dostawców utrudnia szybkie reagowanie na problemy, także te związane z bezpieczeństwem, a - jako że starsze systemy są często bardzo złożone i słabo udokumentowane - pracownicy zwykle mają spore trudności, żeby radzić sobie na bieżąco.

Aby złagodzić te ryzyka, organizacje powinny regularnie oceniać swoje systemy dziedziczone i priorytetyzować ich aktualizację lub wymianę. W miarę możliwości starsze systemy powinny być izolowane od głównej sieci, a dodatkowe środki bezpieczeństwa, takie jak zapory sieciowe i systemy wykrywania włamań, powinny być wdrażane. Warto również opracować długoterminowy plan modernizacji systemów oraz zapewnić specjalistyczne szkolenia dla personelu IT zajmującego się starszymi rozwiązaniami. Rozważenie wirtualizacji starszych aplikacji na nowszej, bardziej bezpiecznej infrastrukturze może również przyczynić się do poprawy ogólnego stanu bezpieczeństwa organizacji.

Człowiek jako najsłabsze ogniwo

Chociaż rozwiązania technologiczne są kluczowe, czynnik ludzki nadal odgrywa istotną rolę w bezpieczeństwie danych. Kompleksowe szkolenia z zakresu cyberbezpieczeństwa dla wszystkich pracowników są niezbędne do stworzenia kultury świadomej eliminacji zagrożeń.

Edukacja ta powinna obejmować szeroki zakres tematów, od rozpoznawania prób phishingu po właściwe obchodzenie się z poufnymi danymi. Regularne odświeżanie tych szkoleń oraz informowanie pracowników o nowych zagrożeniach może przekształcić personel w skuteczną pierwszą linię obrony przed cyberzagrożeniami.

Wdrożenie tych wzajemnie powiązanych strategii pozwala firmom na stworzenie solidnego, wielowarstwowego podejścia do bezpieczeństwa danych.

Jakie nowoczesne narzędzia IT mogą zminimalizować ryzyko naruszeń?

W obliczu rosnących zagrożeń cybernetycznych, ochrona danych wymaga wielowymiarowego podejścia, które łączy zaawansowane narzędzia technologiczne z kompleksowymi strategiami bezpieczeństwa. Na przykład IBM oferuje szereg rozwiązań, które pomagają organizacjom skutecznie zarządzać ryzykiem i przeciwdziałać zagrożeniom, a jednym z kluczowych jest IBM Security Randori Recon. To rozwiązanie koncentruje się na zarządzaniu powierzchnią ataku poprzez ciągłe odkrywanie i priorytetyzację zasobów cyfrowych. To narzędzie nie tylko identyfikuje luki w zabezpieczeniach, ale także ujawnia elementy shadow IT, które mogą stanowić potencjalne zagrożenie. Dzięki temu organizacje zyskują pełny obraz swojej infrastruktury i mogą proaktywnie podejmować działania zapobiegawcze.

Główne korzyści z wdrożenia Randori Recon w firmie to:

1. **Kompleksowe zarządzanie powierzchnią ataku**
   - narzędzie pozwala ocenić, którymi drogami haker może próbować dostać się do infrastruktury IT firmy.

2. **Automatyczne wykrywanie zagrożeń**
   - Randori Recon samodzielnie odnajduje potencjalne luki w zabezpieczeniach, bez konieczności wskazywania konkretnych miejsc do analizy.

3. **Priorytetyzacja zadań**
   - technologia Target Temptation analizuje opłacalność potencjalnych ataków, co pozwala firmie skupić się na najpilniejszych zagrożeniach.

4. **Poprawa bezpieczeństwa danych klientów**
   - poprzez eliminację luk w systemie IT.

5. **Ochrona reputacji firmy**
   - minimalizacja ryzyka wycieków danych i związanych z tym roszczeń klientów.

6. **Oszczędności**
   - zapobieganie atakom jest tańsze niż usuwanie ich skutków.

7. **Efektywny nadzór nad pracą zespołu IT**
   - narzędzie pozwala skutecznie monitorować działania w zakresie cyberbezpieczeństwa.

8. **Poprawa wydajności całego systemu IT**
   - dzięki eliminacji luk w zabezpieczeniach.

9. **Ciągłe monitorowanie i aktualizacja informacji o zagrożeniach**
   - narzędzie działa w sposób ciągły, zapewniając aktualny obraz sytuacji.

Połączenie tych narzędzi z odpowiednimi praktykami zarządzania bezpieczeństwem tworzy holistyczny model ochrony danych, który znacząco wzmacnia odporność organizacji na cyberzagrożenia. Kompleksowe podejście pozwala nie tylko minimalizować ryzyko, ale także skutecznie reagować na zmieniające się warunki i ewoluujące zagrożenia.

O REDAKCJI

Redakcja

Tomasz Bonek
redaktor naczelny
tb@interaktywnie.com

Paweł Musiał
redaktor Interaktywnie.com
pm@interaktywnie.com

Robert Cieszawski
redaktor Interaktywnie.com
rc@interaktywnie.com

Kaja Grzybowska
redaktor Interaktywnie.com
kg@interaktywnie.com

Przemysław Ławrowski
redaktor Interaktywnie.com
pl@interaktywnie.com

Reklama

Jakub Karczmarczyk
sales director
+48 693 710 118
jk@interaktywnie.com

O INTERAKTYWNIE.COM

Adres i siedziba redakcji

interaktywnie.com

Interaktywnie.com Press Group
ul. Ofiar Oświęcimskich 19 lok. 401 - IV piętro,
50-069 Wrocław
tel.: +48 693 710 118
redakcja@interaktywnie.com

Interaktywnie.com to specjalistyczny magazyn dla wszystkich pracujących w branży internetowej oraz tych, którzy się nią pasjonują. Serwis zintegrował także społeczność, klika tysięcy osób, które wymieniają się tu doświadczeniami, doradzają sobie, piszą blogi, rozmawiają o najnowszych rozwiązaniach.

Interaktywnie.com istnieje od 2006 roku, na początku był branżowym blogiem. W ciągu trzech pierwszych lat znacząco poszerzył się zarówno zakres tematyczny jaki i liczba autorów, którzy w nim publikują. Zostało to docenione przez jury WebstarFestival i uhonorowane statuetką Webstara Akademii Internetu. Oprócz tego wortal jest laureatem Grand Webstara 2008 dla strony roku.

Dziś Interaktywnie.com to nowoczesne internetowe medium tematyczne z codziennie nowymi newsami z rynku polskiego i międzynarodowego, artykułami, wywiadami oraz omówieniami najciekawszych stron internetowych.

Jego redakcja przygotowuje też cykliczne, obszerne raporty branżowe, dystrybuowane do najlepszej grupy odbiorców. Wśród nich są specjaliści zarejestrowani w Interaktywnie.com. Są to szczegółowe opracowania dotyczące poszczególnych segmentów rynku internetowego i zmian, które na nim zachodzą.

Raporty promowane są także każdorazowo w największych polskich serwisach: wp.pl, gazeta.pl, money.pl.
Więcej raportów: interaktywnie.com/biznes/artykuly/raporty-interaktywnie-com

Zdjęcia pochodzą z banku zdjęć Pixabay, licencja CC, dozwolony użytek.