SIERPIEŃ 2023

EBOOK Z RAPORTEM interaktywnie.com

CYBERBEZPIECZEŃSTWO FIRM.

JAK CHRONIĆ PRZEDSIĘBIORSTWO I JEGO DANE?

SPONSOR PLATYNOWY

Synology®

POD PATRONATEM

WP money.pl GAZETA.PL

SPIS TREŚCI

RAPORTY INTERAKTYWNIE 2023

STYCZEŃ

E-commerce.
Jak sprzedawać w internecie

LUTY

Agencje marketingowe

MARZEC

Sieci afiliacyjne
i programy partnerskie

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 2024 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.: 71 302 75 35, kom.: 693 710 118

Cyberbezpieczeństwo to podstawa reputacji firmy

Aż 133,8 mld dolarów wydają firmy na całym świecie na ochronę przed cyfrowymi zagrożeniami. W Europie przodują w tym Francja, Hiszpania, Niemcy, Wielka Brytania oraz Holandia. Za najbezpieczniejsze cybernetycznie uznaje się natomiast takie państwa, jak: Holandia, Francja, Wielka Brytania, Finlandia, Kanada, Japonia, Islandia i Niemcy.

A Polska? U nas naprawdę jest jeszcze dużo do zrobienia...
Dobrze wiedzą to eksperci głównego partnera tego ebooka - firmy Synology, która specjalizuje się we wdrażaniu w przedsiębiorstwach rozwiązań wspomagających cyberbezpieczeństwo. Zachęcam do zapoznanie się z wiedzą jej specjalistów oraz ofertą.

Tomasz Bonek, prezes zarządu i redaktor naczelny Interaktywnie.com

Synology GmbH

Adres
Grafenberger Allee 295

Dane kontaktowe
E-mail: pl_sales@synology.com, pl_marketing@synology.com
Strona www: synology.com/pl-pl
Telefon: +49 211 9666 96 34

Opis działalności
W centrum transformacji każdej branży znajdują się dane, a firma Synology odgrywa w tej materii niezwykle ważną rolę. Nasza misja polega przede wszystkim na zarządzaniu światowymi danymi i ich ochronie. Firma Synology umożliwia przedsiębiorstwom zarządzanie danymi oraz ich zabezpieczanie i ochronę, bez względu na to, czy dostęp do nich jest uzyskiwany przez napęd flash, dysk lub architektury wielochmurowe.

Firmie Synology zaufały największe umysły branży IT, przeprowadzając ponad 6 milionów instalacji. Jesteśmy oddani transformacji zarządzania danymi firmowymi, czyniąc je eleganckim, prostym, bezpiecznym i niezawodnym. Jesteśmy dumni z szerokiego wachlarza rozwiązań opartych na wiodących innowacjach i niezawodności sprawdzonej w praktyce. Trzeci raz z rzędu jesteśmy nagradzani przez Quality Control Leader jako najlepsze rozwiązanie NAS dla SMB w Polsce.

Wybrani klienci
Bank Pekao, Wojewódzki Urząd Pracy w Toruniu, Wykop.pl, PolAndRock, WOŚP, Sunrise Festival

WIZYTÓWKI FIRM

nask s.a.

NASK S.A.

Adres
ul. 11 Listopada 23
03-446 Warszawa

Dane kontaktowe
E-mail: kontakt@nasksa.pl
Strona www: nasksa.pl
Kontakt handlowy: +48 22 380 80 80

Opis działalności
Jesteśmy Spółką powołaną przez Państwowy Instytut Badawczy NASK. Integrujemy zaawansowane usługi bezpieczeństwa teleinformatycznego. Zapewniamy bezpieczeństwo danych w cyfrowym świecie biznesu i administracji wykorzystując najnowsze rozwiązania oparte na wiarygodnych i rzetelnych technologiach. Posiadamy 30-letnie know-how w obszarze bezpieczeństwa teleinformatycznego i dwa własne centra przetwarzania danych. Oferujemy indywidualne i kompleksowe podejście do projektów z zakresu cyberbezpieczeństwa.

Wybrani klienci
Ministerstwo Cyfryzacji, Ministerstwo Sprawiedliwości, PAN, CIRF, ITCARD, Warbud

SKALA CYBERZAGROŻEŃ I ICH KONSEKWENCJE DLA BIZNESU

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

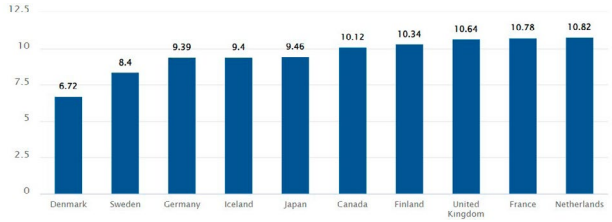
1

Phishing, Maleware, Ransomware to jedne z najczęściej spotykanych cyberataków. Konsekwencje, jakie niosą ze sobą zwykle dają się zmierzyć wielkością strat finansowych jakie generują. Według Statisty, najbardziej dotkliwe są te występujące w branży medycznej i finansowej.

Według Acumen Research and Consulting, globalny rynek oprogramowania chroniącego przed cyberatakami do 2030 roku osiągnie wartość 133,8 mld dolarów.

Dane Hiscox pokazują natomiast, że w Europie największe wydatki na cyberbezpieczeństwo ponosi Francja, Hiszpania, Niemcy, Wielka Brytania i Holandia. Za wydatkami zwykle idzie bezpieczeństwo, bo według danych Comparitech, najbezpieczniejszymi krajami pod względem odporności na atak cybernetyczny są Holandia, Francja, Wielka Brytania, Finlandia, Kanada, Japonia, Islandia i Niemcy.

Najbardziej odporne na cyberataki kraje



Źródło: Finanse Online

Najpoważniejsze zagrożenia

› Phishing

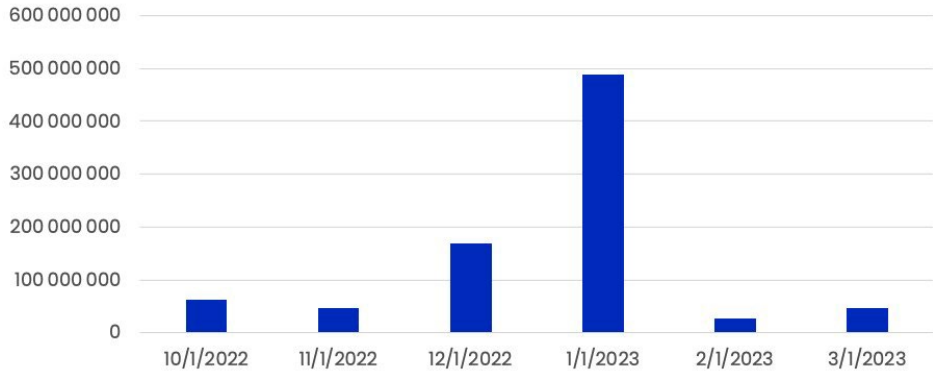
Sposób wyłudzenia wrażliwych danych, stosując zabiegi psychologiczne np. podszywanie się pod znaną markę, podmiot lub instytucję.

Synology®

Zabezpiecz dane zanim będzie za późno!

To jeden z najpopularniejszych typów ataków na świecie. Według Vade, ich szczyt przypadł na pierwszy kwartał 2023 roku, kiedy to wykryto 564 mln e-maili zawierających złośliwe oprogramowanie. To ponad dwukrotnie więcej w stosunku do wcześniejszego kwartału.

Liczba ataków phishingowych w podziale na miesiące w okresie od października do stycznia 2023 roku



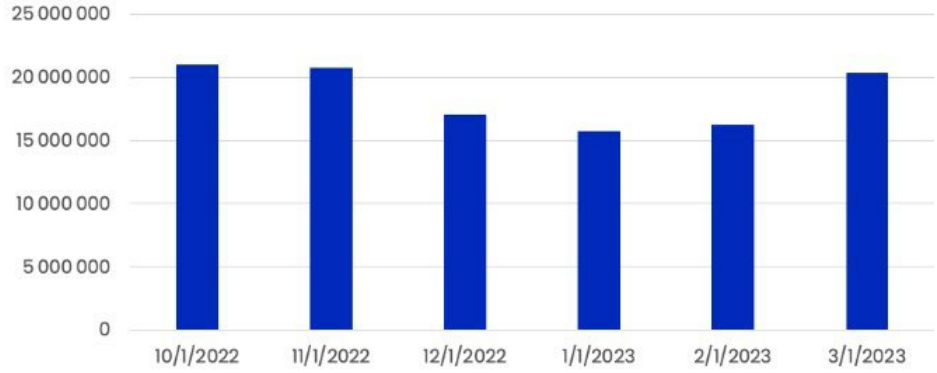
Źródło: Vadesecure

› **Maleware**

Rodzaj złośliwego oprogramowania, które całkowicie lub częściowo ogranicza użytkownikom dostęp do systemu. Ten rodzaj ataku nazywany jest również robakami lub trojanami.

› **Sniffing** - dotyczy nielegalnych działań w sieciach lokalnych (LAN). Haker, posiadający uprawnienia administratora może przechwycić poufne dane zawarte w wiadomościach mailowych.

Liczba ataków Maleware w podziale na miesiące w okresie od października do stycznia 2023 roku



Źródło: Vadesecure

› **Skimming** - kradzież informacji z kart kredytowych.

› **Mail bombing** - polega na "bombardowaniu" skrzynki mailowej niechcianymi mailami, aż do jej całkowitego zapełnienia. Przeciążenie serwera odpowiedzialnego za pocztę atakowanej osoby lub podmiotu powoduje, że odbiera się jej możliwość korzystania z niej.

› **Golden Ticket** - rodzaj ataku wykorzystujący luki w systemach Microsoftu. W jego wyniku użytkownik traci uprawnienia administratora nad własnym systemem operacyjnym.

- **DoS, DDoS, DRDoS** - atak pozwalający na zablokowanie komputera ofiary poprzez przeciążenie systemu danymi.

- **„Man in the middle" (MITM)** - ten rodzaj ataku polega na przechwyceniu rozmowy prowadzonej pomiędzy użytkownikami. Haker przechwytuje wiadomości wysyłane przez obie ze stron, a następnie je przekierowuje i modyfikuje według własnych potrzeb tak, aby strony niczego nie podejrzewały. W ten sposób haker może wejść w posiadanie poufnych danych.

- **Cross – site scripting (XSS)** - przedmiotem ataku jest strona internetowa. Dzięki skryptowi użytkownik zdaje się być kierowany po witrynie. Haker w ten sposób może uzyskać dostęp do plików cookie, historii wyświetlania oraz innych poufnych danych przechowywanych przez przeglądarkę.

- **SQL Injection** - haker umieszcza błędny pod SQL na stronie internetowej wykorzystując luki w systemie. W ten sposób może uzyskać dostęp do wrażliwych danych firmy.

- **Atak brute force** - specjalne oprogramowanie używane w cyberataku, sprawdza różne kombinacje kodu, celem uzyskania dostępu do systemu.

- **Adware** - złośliwe oprogramowanie wyświetlające na urządzenia użytkownika niechciane reklamy

- **Ransomware** - ogranicza w całości lub częściowo dostęp do systemu użytkownika celem wyłudzenia okupu za jego odblokowanie.

Źródło: na podstawie informacji sebITu

Konsekwencje cyberataków

Wśród konsekwencji cyberataków wymienić możemy:

- utrata wrażliwych danych - jest to szczególnie istotne, gdy dane te mogą zostać użyte przeciwko osobie lub podmiotowi, którego dotyczą. Dodatkowo hakerzy mogą odciąć do nich dostęp, co ciągnie za sobą inne konsekwencje związane z brakiem możliwości np. prowadzenia biznesu,

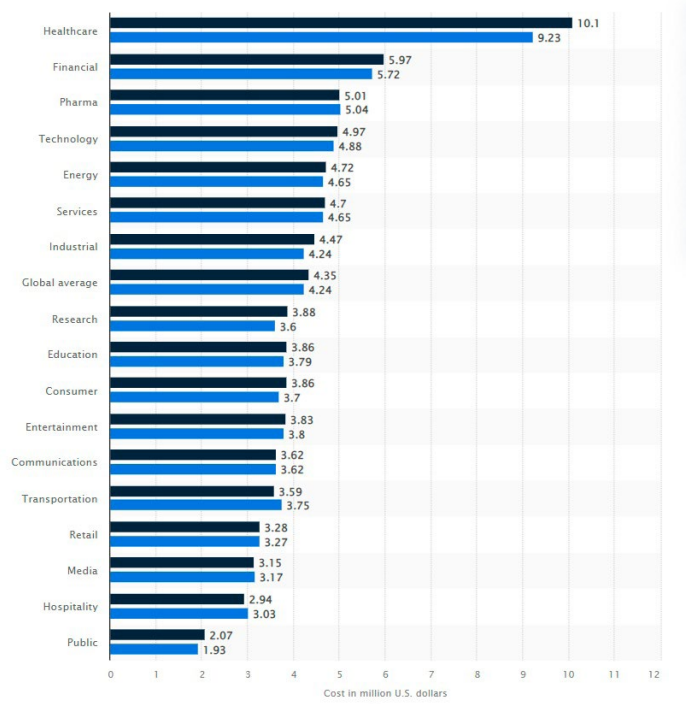
- utrata reputacji - konieczność poinformowania klientów o wycieku ich danych naraża firmę na utratę reputacji, co może mieć dużo dalej idące konsekwencje. Utrata zaufania klientów w wyniku udanego cyberataku narazi firmę na większe straty wynikające ze zmniejszenia liczby klientów w przyszłości,

- przestoje w działalności - cyberatak może również uniemożliwić działalność przedsiębiorstwu, co może doprowadzić do dotkliwych strat finansowych,

- upadek firmy - daleko idące konsekwencje cyberataku, takie jak utrata reputacji, zmniejszenie przychodów może doprowadzić do bankructwa przedsiębiorstwa,

- kary nałożone przez instytucje nadzorcze - utrata danych klientów może pociągnąć za sobą kontrolę, a w przypadku wykrycia nieprawidłowości dotkliwe kary finansowe.

Średni koszt cyberataku w podziale na branże w latach 2020-2022



Źródło: Statista

Straty finansowe wywołane cyberatakami

Niezależnie czy są to przestoje, utrata wiarygodności, czy kary finansowe, każda z konsekwencji cyberataków niesie ze sobą również straty finansowe.

Według danych Statisty, najbardziej dotkliwe finansowo są cyberatatki przeprowadzone na branżę opieki zdrowotnej oraz finansową. W pierwszym przypadku, w latach 2020-2021, średni koszt pojedynczego cyberataku wyniósł nieco ponad 9 mld dolarów. W latach 2021-2022 było to już 10 mld dolarów. Analizując branżę finansową, średni koszt cyberatatku wyniósł prawie 6 mld dolarów.

Na kolejnych miejscach w zestawieniu branż, których finansowo najbardziej dotykają cyberataki uplasowały się kolejno: farmaceutyczna, technologiczna czy energetyczna.

Przykłady udanych cyberataków

Statista podaje, że w ubiegłym roku wśród najpoważniejszych cyberataków należy wymienić styczniowy dotyczący systemów Windows, MacOS i Linux. Doszło również do cyberataku na infrastrukturę krytyczną w USA, a także do włamania do systemów białoruskiej kolei. Odnotowano także duży atak na firmę energetyczną w Kolumbii - Empresas. W przypadku służby zdrowia warto zwrócić uwagę na atak ransomware we Francji.

Czy pracownik w firmie to najsłabsze ogniwo?

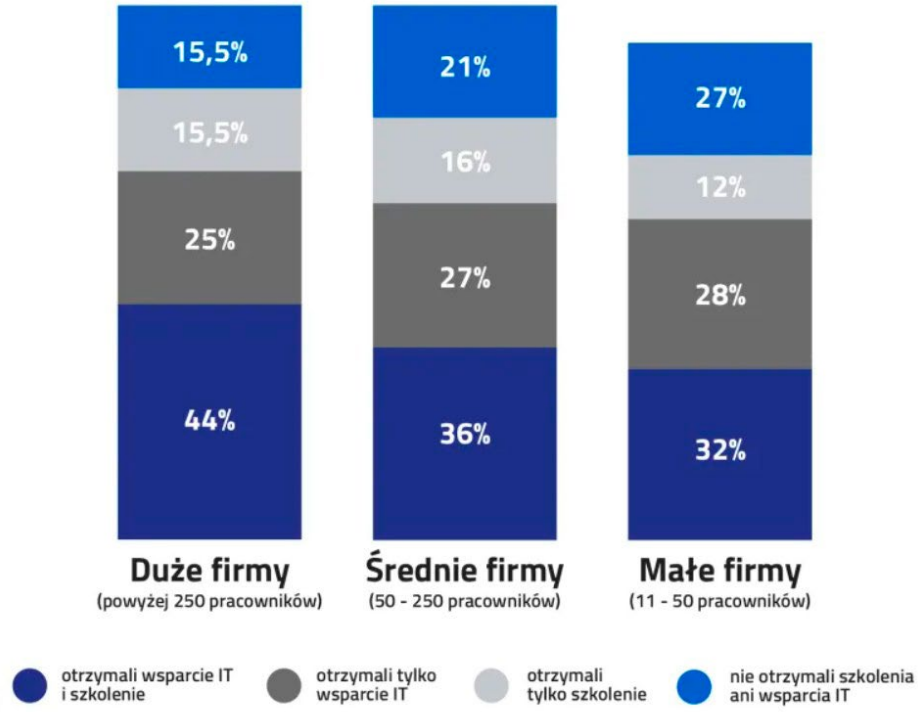
Według Barometru cyberbezpieczeństwa autorstwa KPMG, dla 55 procent badanych firm wybuch pandemii COVID-19 przyczynił się do wzrostu ryzyka cyberataków, głównie ze względu na przeniesienie wielu aspektów życia do internetu.

Działania firm w stosunku do pracowników z zakresu cyberbezpieczeństwa w podziale na trzy kraje: Polskę, Czechy oraz Węgry

Źródło: Sophos

Z raportu dowiadujemy się również, że polskie firmy prezentują stosunkowo nie najlepszą świadomość zagrożeń. Ryzyko ataku cybernetycznego w dużej mierze rośnie wraz ze spadkiem poziomu edukacji pracowników. Jak zatem wygląda to w polskich firmach? Według badania Spohos, 22 procent pracowników w naszym kraju nie mogło liczyć na wsparcie IT lub szkolenie z zakresu cyberbezpieczeństwa. Pozostali zazwyczaj mieli szkolenie albo wsparcie IT związane z tą tematyką. W najlepszym przypadku zostali oni zarówno przeszkoleni, jak i otrzymali wsparcie IT - 37 procent.

Działania firm w stosunku do pracowników z zakresu cyberbezpieczeństwa w podziale na wielkość zatrudnienia



Źródło: Sophos

W badaniu pod uwagę wzięto również rynek czeski i węgierski. Okazuje się, że Polska ma najniższy odsetek pracowników, którzy nie otrzymali żadnego wsparcia z zakresu cyberbezpieczeństwa.

Badanie Sophos bierze również pod uwagę wielkość firm. Nie jest zaskoczeniem, że im większa firma, tym to wsparcie dla pracowników jest większe. Przodują duże firmy, zatrudniające co najmniej 250 pracowników, gdzie 44 procent pracowników zostało zarówno przeszkolonych z zakresu cyberbezpieczeństwa, jak i może liczyć na wsparcie IT.

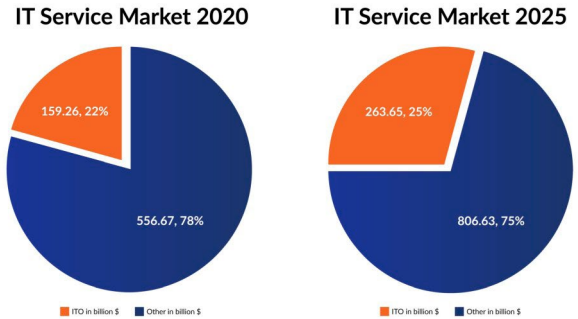
Specjaliści IT z zakresu cyberbezpieczeństwa poszukiwani

Według raportu firmy McKinsey, 87 procent firm doświadcza braków w zespołach IT z zakresu cyberbezpieczeństwa.

Z punktu widzenia bezpieczeństwa IT, według Spaceworks, do kluczowym obowiązków specjalisty do spraw cyberbezpieczeństwa należy:

- zabezpieczenie infrastruktury informatycznej
- skanowanie urządzeń sieciowych
- stworzenie polityki bezpieczeństwa danych w firmie
- stworzenie procedur i procesów związanych z cyberbezpieczeństwem w firmie
- przeprowadzanie szkoleń dla pracowników
- diagnozostanie incycydentow związanych z naruszenie cyberbepzieczeństwa

Rynek usług IT w latach 2022 i 2025 z uwzględnieniem outsourcingu IT



Źródło: Kruche & Company

Outsouricing IT

Według firmy GrandViewResearch, rynek usług IT w 2022 roku był wart około 1250 mld dolarów. Z kolei jak podaje Statista, największą popularnością cieszy się rynek outsourcingu IT (ITO). Według przewidywań serwisu, w 2023 r. osiągnie on wartość 430,53 mld dolarów, a w 2027 roku rynek ten będzie wart 587,3 mld dolarów.

Wojna w Ukrainie i jej konsekwencje cybernetyczne

Jak podaje Google, hakerzy wspierani przez rosyjski rząd podjęli agresywne, wielokierunkowe działania mające na celu uzyskanie decydującej przewagi w czasie wojny w cyberprzestrzeni. Celem jest przede wszystkim Ukraina, w tym ukraiński rząd, infrastruktura wojskowa i cywilna. Wzrosła również częstotliwość ataków phishingowych na kraje NATO. Ich częstotliwość wzrosła o 250 procent w przypadku Ukrainy i 300 procent w przypadku krajów NATO.

Dodatkowo, jak zauważa Google, inwazja wywołała zmianę we wschodnioeuropejskim ekosystemie bezpieczeństwa, co może mieć konsekwencje dla rozwoju i koordynacji grup przestępczych, jak i dla skali cyberprzestępczości na całym świecie w przyszłości.

ARTYKUŁ PROMOCYJNY

JAK TWORZYĆ KOPIE ZAPASOWE DANYCH FIRMOWYCH, BY NIE ZWARIOWAĆ?

Magdalena O`Dwyer
Team Manager Marketing - Eastern Europe w Synology GmbH

2

W dzisiejszym artykule przyjrzymy się w szczególności temu, jak radzić sobie z kopiami zapasowymi od startupów po korporacje. Dlaczego nie należy bać się automatyzacji i że dzięki niej kopie zapasowe są bardziej zaawansowane, niż się obecnie wydaje. I dlaczego posiadanie odpowiednich procesów tworzenia kopii zapasowych ostatecznie uratuje Twój portfel.

Sytuacja związana z koronawirusem na zawsze zmieniła cyberprzestrzeń. Firmy, które w przeciwnym razie przez lata obsługiwałyby wszystko analogowo, zostały zmuszone do przeniesienia się w przestrzeń zdalną. Takie siedlisko stało się rajem dla cyberataków, wysyłając tym niedoświadczonym firmom jeden wymuszony e-mail za drugim.

Wiele z nich nie doceniło cyfrowego świata i odłożyło kopie zapasowe na dalszy plan, podczas gdy inni błędnie wierzyli, że muszą po prostu przeszkolić pracowników, aby sami chronili swoje dane. Jednak w biznesie jeden taki błąd może być dosłownie druzgocący, zarówno pod względem finansowym, jak i reputacyjnym.

Start-upy często nie mają pojęcia od czego zacząć. Nie wiedzą, jak zunifikować wszystkie urządzenia swoich pracowników w ramach jednej platformy; jakie dane należy zarchiwizować; gdzie je zarchiwizować; jak często je zarchiwizować; i jak udostępnić te dane tak szybko, jak to możliwe w przypadku awarii.

Istnieją tysiące różnych odpowiedzi dla tysięcy firm, więc zaprojektowaliśmy system operacyjny, który każda firma i osoba może dowolnie dostosować do swoich obecnych i przyszłych preferencji.

Tam, gdzie startupy widziały paraliżującą liczbę problemów, my znaleźliśmy

możliwości. Nasze urządzenia Synology NAS są wyposażone w system operacyjny Diskstation Manager, który można dodawać na bieżąco z poziomu zintegrowanego centrum aplikacji. Wewnątrz znajdziesz dziesiątki praktycznych dodatków, z których możesz złożyć swoją infrastrukturę. Dla każdej z aplikacji znajdziesz przydatne materiały szkoleniowe w naszym Centrum Wiedzy.

Automatyzacja rządzi światem

Być może każdy zwykły użytkownik dostaje gęsiej skórki na myśl o przedzieraniu się przez swoje dane i walce ze zhakowaną przeglądarką podczas próby skopiowania plików z jednego punktu do drugiego. Chociaż prawdopodobnie w ten sposób tworzyłbyś kopię zapasową swoich zdjęć rodzinnych w domu, tworzenie kopii zapasowych danych firmowych jest nieco bardziej skomplikowaną dyscypliną.

Przede wszystkim należy wziąć pod uwagę wydajność pod względem fizycznym, czasowym i pojemnościowym. Zarządzanie urządzeniami i maszynami wirtualnymi dla całej firmy może być obsługiwane zdalnie za pośrednictwem naszej centralnej aplikacji Active Backup, oszczędzając wiele czasu na chodzenie do lub wokół poszczególnych oddziałów. Późniejsza konserwacja infrastruktury firmy za pośrednictwem naszego oprogramowania jest w pełni zautomatyzowana, aby wykonywać kopie zapasowe określonych typów danych na wybranych maszynach, regularnie o tej samej porze - zazwyczaj w nocy, dzięki czemu obciążenie nie jest nawet zauważalne.

Oczywiście Active Backup oferuje możliwość monitorowania kopii zapasowych w toku i sprawdzania poprzednich. Może powiadamiać o wszelkich błędach na urządzeniach i wysyłać te raporty na skrzynkę pocztową.

Active Backup pozwala maksymalnie wykorzystać pamięć masową

Forma kopii zapasowej Active Backup wykorzystuje również tak zwaną metodę przyrostowej kopii zapasowej i deduplikacji danych. Na przykład, nie ma sensu przechowywać setek kopii pojedynczego arkusza kalkulacyjnego Excel przez cały rok, jeśli dokonujesz tylko jednej edycji w miesiącu.

W przypadku przyrostowej kopii zapasowej, tylko konkretna zmiana w pliku jest rejestrowana w ten sposób, aby zapobiec niepotrzebnemu bałaganowi w pamięci masowej.

Tak zwana deduplikacja to proces, który obserwuje powtarzające się bloki danych i drastycznie zmniejsza obciążenie danymi. To właśnie dzięki deduplikacji można wykonywać częstsze kopie zapasowe bez znaczącego wpływu na ich rozmiar. Jednak w porównaniu do zwykłej synchronizacji danych (gdzie dane są dublowane w wielu repozytoriach, więcej poniżej), trwa to

znacznie dłużej i naturalnie zajmuje więcej miejsca. Ponadto, ponieważ jest to tylko kopia zapasowa zmian, format ten nie jest czytelny w porównaniu do synchronizacji. Łącząc przyrostową kopię zapasową i deduplikację, można przechowywać wiele wersji danych w skompresowanym rozmiarze na pojedynczej konfiguracji pamięci masowej, oszczędzając nawet kilkadziesiąt procent pojemności dysku.

Active Backup Suite składa się z:

- Active Backup for Business (do tworzenia kopii zapasowych systemów Windows, Linux lub maszyn wirtualnych zbudowanych na platformach VMWare i Hyper-V)
- Active Backup for Microsoft 365 (do tworzenia kopii zapasowych danych w Exchange Online, OneDrive, Sharepoint i Teams)
- Active Backup for Google Workspace (do tworzenia kopii zapasowych danych w Google, Dysku, Gmailu, Kontaktach i Kalendarzu).

Trzymaj się zasad tworzenia kopii zapasowych 3-2-1

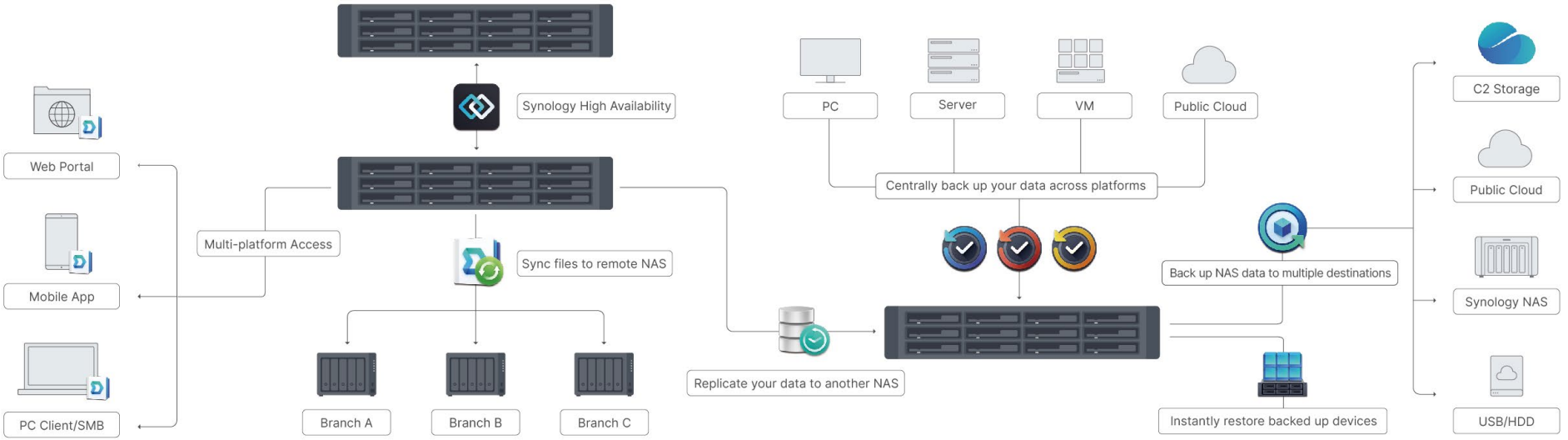
Złotym standardem w bezpieczeństwie danych jest tak zwana kopia zapasowa 3-2-1, której przestrzegają firmy na całym świecie. Zgodnie z tą radą, należy starać się przechowywać trzy różne kopie zapasowe na dwóch różnych nośnikach, przy czym jedna z nich powinna znajdować się w innej lokalizacji niż oryginał. Zapewnienie ciągłej dostępności danych, aplikacji i usług zapobiegnie utracie zysków i nadszarpnięciu reputacji firmy.

Chesz się dowiedzieć więcej? Sprawdź naszą stronę pod linkiem tutaj: https://www.synology.com/pl-pl/dsm/solution/data_backup

Skorzystaj z pomocy chmury

Korzystanie z usług w chmurze w celu uzyskania trzech kopii zapasowych na dwóch różnych nośnikach stało się ostatnio powszechne, najlepiej w połączeniu z drugą sieciową pamięcią masową zlokalizowaną w innym oddziale lub hostowaną w centrum danych innej firmy. Poziom bezpieczeństwa zależy oczywiście od wielkości i możliwości firmy. Możemy zapewnić infrastrukturę chmury w ramach naszego rozwiązania C2 Storage.

Nasza aplikacja Hyper Backup, która tworzy kompletne kopie zapasowe, zapisuje konfiguracje aplikacji i statusy plików ze znacznikami czasu, ułatwi proces tworzenia kopii zapasowych danych z jednej sieciowej pamięci masowej do innych miejsc docelowych. Jednym z najważniejszych punktów prawidłowego planu tworzenia kopii zapasowych jest możliwość powrotu do punktu sprzed awarii. Hyper Backup zapewnia możliwość wycofania całego systemu i ochrony przed nieregularnymi



aktualizacjami, które w przeciwnym razie spowodowałyby zamknięcie firmy na czas nieokreślony.

Tworzenie kopii zapasowych chroni nie tylko istniejący czas, ale także przyszły portfel

Tworząc kopie zapasowe całych zwirtualizowanych komputerów na serwerze Synology NAS, można również wyeliminować skutki cyberataku po ataku ransomware. Dane mogą być szyfrowane na serwerze Synology NAS w celu ochrony przed naruszeniami bezpieczeństwa i cyberatakami. Po całkowitym wyczyszczeniu można szybko przywrócić komputer do stanu, w którym nie został zaatakowany, z kopii zapasowej przechowywanej na serwerze NAS.

Utrata danych bez kopii zapasowej jest zawsze loterią, ponieważ w przeciwieństwie do zwykłych „domowych" danych ze zdjęciami i filmami, nawet jeden brakujący fragment może oddzielić rekonstrukcję całorocznej analizy korporacyjnej od sukcesu. Nie wspominając już o czasochłonności i kosztowności takiego procesu, a nawet potencjalnych konsekwencjach czy karach, takich jak brak udokumentowania wszystkich faktur do urzędu skarbowego z powodu ich utraty.

Uzyskaj bezpłatne porady od naszych ekspertów i przetestuj rozwiązania pamięci masowej i oprogramowania Synology dla przedsiębiorstw we własnym środowisku pod linkiem tutaj.

BEZPIECZEŃSTWO IT CZYLI JAK TECHNOLOGIA MOŻE CHRONIĆ PRZEDSIĘBIORSTWO? JAK WYBIERAĆ SERWERY, MACIERZE ITP.?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

3

W 2017 roku agencja oceny kredytowej Equifax padła ofiarą cyberprzestępców, którzy wykorzystując luki w systemie ujawnili dane osobowe około 147 milionów klientów, narażając ich na ryzyko kradzieży tożsamości. Firma zapłaciła rekordową grzywnę, bo - jak się okazało w czasie śledztwa - doskonale wiedziała o tym, że hakerzy mogą wykorzystać luki w jej systemie.

Wyciek danych objął takie informacje, jak: imiona, numery ubezpieczenia społecznego, daty urodzenia oraz adresy zamieszkania. Firma, która stanęła w obliczu surowej krytyki ze strony rządu i organów regulacyjnych, została zobowiązana do zapłaty ogromnej kary wynoszącej 700 milionów dolarów, a klienci ruszyli z cywilnymi roszczeniami.

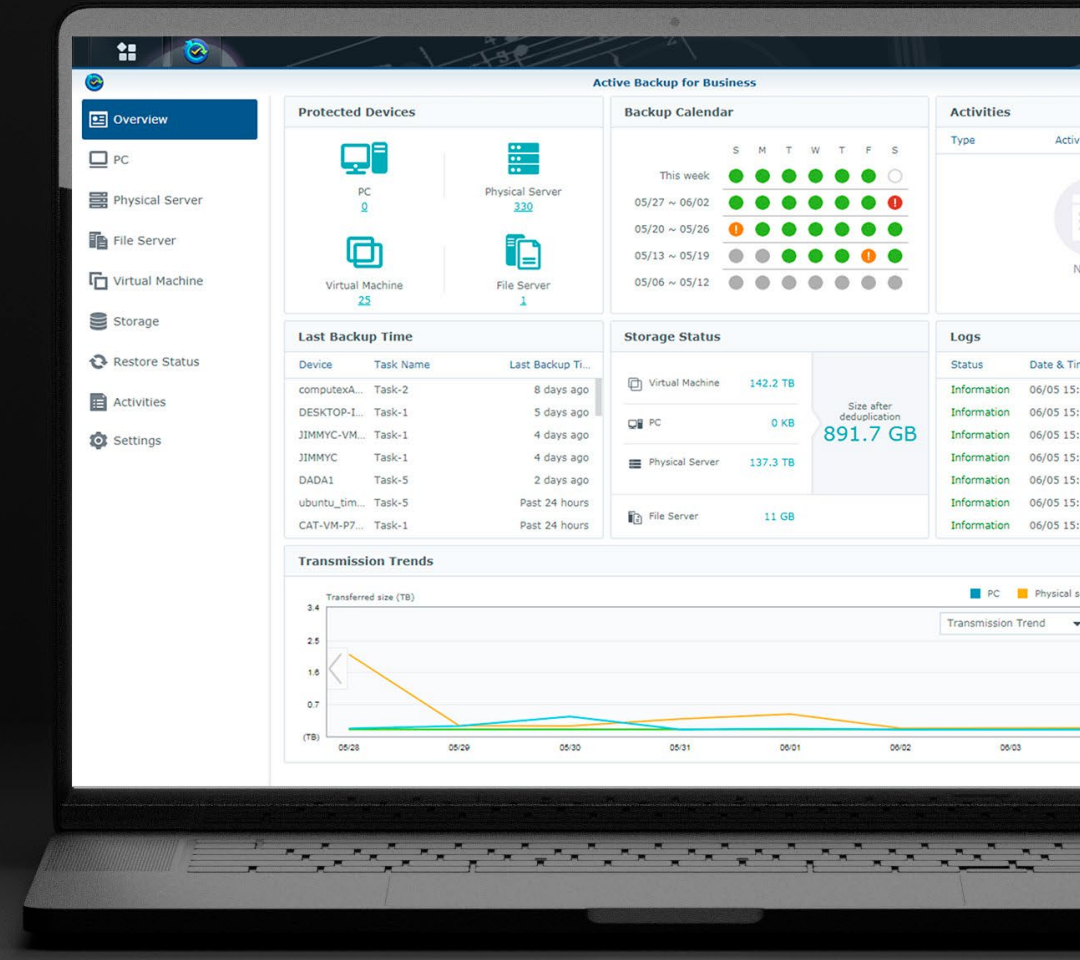
- Chybione działania, zaniedbania i luźne standardy bezpieczeństwa tej firmy zagroziły tożsamości połowie populacji Stanów Zjednoczonych - stwierdziła wtedy prokurator generalny stanu Nowy Jork, Letitia James. - Czas, aby firma uczyniła to, co słuszne i nie tylko zrekompensowała straty milionom ofiar naruszenia danych, ale także zapewniła każdemu Amerykaninowi, którego bardzo wrażliwe informacje były dostępne, narzędzia potrzebne do walki z kradzieżą tożsamości w przyszłości.

Dane osobowe nie od dzisiaj są przedmiotem szczególnej ochrony, której brak może słono kosztować i coraz mniejsza jest toleracja - zarówno konsumentów, jak i regulatorów - wszelkich nonszalancji w tym zakresie. Brak wiedzy i doświadczenia nie jest już żadnym usprawiedliwieniem zaniedbań, tym bardziej, że na rynku istnieje już spora liczba narzędzi gotowych do wdrożenia, a także firm skoncentrowanych na konsultingu w tym obszarze.

Synology®

Backup danych i ciągłość biznesowa

Firma Synology pomaga zmniejszyć stres związany z rosnącymi wymaganiami w zakresie pamięci masowej i ochrony danych dzięki opcjom sprzętowym i niezawodnym funkcjom oprogramowania, które spełniają różne potrzeby klientów.



Uzyskaj kompleksową kopię zapasową dla:

- Komputerów
- Serwerów
- Maszyn wirtualnych
- Microsoft 365 i G Suite

40% firm nigdy nie otwiera się ponownie po katastrofalnej utracie danych

50% firm pozostaje nieprzygotowanych na katastrofę

Ważne dane dotyczące konsekwencji biznesowych

- Średni koszt naruszenia danych w USA wynosi 8,64 miliona dolarów.
- Globalny koszt cyberprzestępczości oszacowany jest na 6 bilionów dolarów i ma wzrosnąć do 10 bilionów dolarów do 2025 roku.
- W 2020 roku 300 milionów ludzi zostało dotkniętych naruszeniami danych.

Jak zabezpieczyć infrastrukturę IT przed atakiem?

Niestety odpowiedź na tak sformułowane pytanie musi brzmieć „to zależy". Poziom bezpieczeństwa infrastruktury IT zależy bowiem od potrzeb infrastrukturalnych firmy oraz środowiska regulacyjnego - małe i średnie biznesy będą miały inne wymagania dotyczące bezpieczeństwa i prywatności niż firma z branży zdrowotnej przechowująca informacje medyczne lub operator finansowy. Są jednak uniwersalne zasady, od których warto zacząć myślenie o bezpieczeństwie IT.

- **Chmura**
  Przez lata zaufanie do chmury było relatywnie niskie, ale dzisiaj kiedy rynek zdominowany jest przez Wielką Trójkę (Google, Microsoft i Amazona) - z, odpowiednio, GCP, Azure i AWSem - platformy chmurowe wydają się dużo bezpiecznym wyborem niż serwery współlokowane lub zarządzane, hostowane w tradycyjnym centrum danych.

  Opcja samodzielnie zarządzana poza chmurą może być odpowiednia dla firm posiadających wiedzę i zasoby w zakresie bezpieczeństwa infrastruktury. Jednak dla przeciętnej firmy wielkie platformy chmurowe oferują lepszy balans pomiędzy kosztami i bezpieczeństwem.

  Niestety, bynajmniej, nie oznacza to jednak, że platformy chmurowe są 100-proc. bezpieczne. Nie są, ale zapewniają solidne podstawy, na których firmy mogą budować bezpieczną infrastrukturę, dokładając do niej kolejne usługi. Należy jednak pamiętać, że budowa infrastruktury w chmurze nie zwalnia firm z obowiązków związanych z bezpieczeństwem, a te, które nie stosują się do najlepszych praktyk lub w ogóle nie mają własnej polityki bezpieczeństwa danych, narażają swoje dane na ryzyko.

- **Polityka bezpieczeństwa**
  Polityka bezpieczeństwa IT to dokument strategiczny, który definiuje zasady, wytyczne i procedury związane z bezpieczeństwem informacji i infrastruktury w organizacji. W jej ramach wyznaczane są role i odpowiedzialności różnych osób w organizacji, związane z bezpieczeństwem IT oraz poziom ich uprawnień dostępowych.

Zdefiniowanie tych ról, które obejmuje ustalenie, kto ma prawo dostępu do określonych zasobów, jakie procedury uwierzytelniania i autoryzacji są wymagane, oraz w jaki sposób zarządzane są uprawnienia wymaga klasyfikacji danych, czyli określenia różnych poziomów poufności informacji oraz metod ich oznaczania.

Dokument oprócz kwestii organizacyjnych wyjaśnia, jakie środki techniczne i narzędzia są stosowane w celu ochrony systemów i danych.

- **Specjalista od bezpieczeństwa**
  Dobrą, choć dość nową praktyką, jest zatrudnianie w firmie własnego specjalisty od bezpieczeństwa, który będzie odpowiedzialny za odpowiednie skonfigurowanie wybranej platformy. AWS, Microsoft Azure, czy GCP zapewniają - jak wskazaliśmy - bezpieczne podstawy, ale błędy wdrożeniowe mogą powodować luki. Zatrudnienie eksperta, który zadba o odpowiednie właściwie ustawione zapory ogniowe, szyfrowanie czy konfiguracje certyfikatów SSL to odpowiedź na to wyzwanie.

- **Kopie zapasowe**
  Najważniejszą ochroną przed atakami ransomware jest posiadanie działających kopii zapasowych. A kopie zapasowe nie tylko chronią przed ransomware i innym złośliwym oprogramowaniem, ale także przed utratą danych i problemami spowodowanymi przypadkowym lub złośliwym usunięciem danych, awarią sprzętu lub innymi katastrofami, takimi jak pożary i powodzie, pisze w swoich materiałach promocyjnych firma specjalizująca się w cyberbezpieczeństwie Synology. A dobra kopia zapasowa jest niezawodna, elastyczna, wymaga niewielkiej konserwacji i zapewnia bezpieczeństwo w dłuższej perspektywie.

Jak i jakie rozwiązania infrastrukturalne IT zapewniają bezpieczeństwo IT?

Mimo że najsłabszym ogniwem większości zabezpieczeń wdrażanych w firmach jest wciąż człowiek, równie istotnym wyzwaniem jest zbudowanie solidnej infrastruktury, która domyślnie będzie redukowała wiele ryzyk. I mimo że nowoczesnych rozwiązań dostępnych jest w tej chwili bez liku, w wielu firmach wciąż ten właśnie aspekt kuleje.

Infrastruktura w wielu firmach oparta jest bowiem na przestarzałych systemach (tzw. legacy system), które nie nadążają za narzędziami i aplikacjami wymagającymi coraz większych zasobów obliczeniowych. Takie systemy zwykle nie są już wspierane przez dostawców, co oznacza, że nie otrzymują nowych aktualizacji ani łatek bezpieczeństwa. A trzeba pamiętać, że w miarę rozwoju technologii ewoluują również zagrożenia. Systemy niewspierane stają się łatwym celem dla nowych typów ataków, którym nie są w stanie skutecznie im przeciwdziałać.

Nie wspominając już o tym, że mogą nie spełniać przepisów regulacyjnych dotyczących ochrony danych, a to z kolei naraża organizację na kary finansowe i straty wizerunkowe.

Korzystanie z przestarzałych rozwiązań wymaga więc poniesienia dodatkowych kosztów związanych z wprowadzeniem dodatkowych środków bezpieczeństwa, ale zwykle modernizacja lub migracja do nowszych i lepiej zabezpieczonych rozwiązań, okazuje się prędzej czy później niezbędna.

A kiedy już decyzja zapadnie, nie warto iść na kompromisy w kwestii jakości. Budując nowoczesną infrastrukturę IT, dobrze wybierać spośród dostawców o uznanej renomie takich jak IBM, Oracle, Dell, czy CISCO oferujące zaawansowane funkcje zabezpieczeń, takie jak sprzętowe moduły TPM (Trusted Platform Module), wbudowane mechanizmy kryptograficzne czy zabezpieczenia przed atakami typu DDoS, przy jednoczesnym, możliwie jak najmniejszym zużyciu energii i niezawodności.

Przestoje, które skutkują zakłóceniem dostępności biznesowych aplikacji, to bowiem wymierna i bezpośrednia strata dla biznesu. Według ITIC ponad 30% przedsiębiorstw stwierdziło, że jedna godzina przestoju kosztuje je od miliona do pięciu milionów dolarów. Z kolei 80% organizacji oszacowało straty na poziomie 300 000 dolarów, a do tego dochodzi jeszcze utrata reputacji. Klienci, którzy podczas korzystania z danej aplikacji trafią na zakłócenia, mogą już nie powrócić, bo cierpliwość nie jest ich najmocniejszą stroną - aż 47% z nich opuszcza stronę internetową, gdy ta nie ładuje się w ciągu dwóch sekund. W firmach np. produkcyjnych awaria serwera może natomiast skutkować karami umownymi.

ARTYKUŁ PROMOCYJNY

DLACZEGO WARTO INWESTOWAĆ W CYBERBEZPIECZEŃSTWO ORGANIZACJI?

Melania Walaszczyk
Dyrektor Pionu Strategii i Komunikacji w NASK S.A.

4

Liczba zagrożeń bezpieczeństwa w sieci z roku na rok nieustannie wzrasta. Jak wynika z najnowszych danych udostępnionych przez Check Point Research, w drugim kwartale 2023 r. nastąpił 8% wzrost średniej liczby cyberataków na świecie[1]. Wzmożoną aktywność cyberprzestępców na przestrzeni lat obserwujemy również w Polsce, o czym świadczy znaczny wzrost liczby zgłoszeń incydentów do CERT Polska. Według opublikowanego przez tę instytucję w maju br. raportu „Krajobraz bezpieczeństwa polskiego Internetu w 2022 roku" odnotowano ponad 322 tys. zgłoszeń o incydentach bezpieczeństwa, co oznacza 34% wzrost w porównaniu do roku poprzedniego[2].

Celem cyberataku może stać się każda organizacja niezależnie od jej wielkości czy profilu działalności. W związku z tym właściciele firm oraz dyrektorzy operacyjni stoją przed szeregiem wyzwań, związanych z odpowiednim zabezpieczeniem biznesu, m.in. przed wyciekami i kradzieżą danych, złośliwymi oprogramowaniami, które są konsekwencją cyberataków i na wiele tygodni mogą sparaliżować funkcjonowanie organizacji.

Obecnie wiele mówi się na temat cyberbezpieczeństwa. Eksperci podkreślają, iż powinno stanowić priorytet dla organizacji, a działania prewencyjne powinny być uwzględniane w strategii dla jej działalności. Niestety, pomimo tego w dalszym ciągu wiele firm nie daje się przekonać do nowych inwestycji w tym zakresie, dopóki nie zdarzy się niekontrolowany cyberatak powodujący, np. kradzież lub wyciek danych. Dopiero po fakcie okazuje się, że zbagatelizowanie nawet drobnych problemów, które wydawałyby się nieistotne może pociągnąć za sobą gigantyczne straty finansowe i wizerunkowe dla organizacji.

Dlaczego każda organizacja jest narażona na kradzież lub wyciek danych?

W każdej organizacji występują pewne słabe punkty, które w sprytny sposób są wykorzystywane przez cyberprzestępców.

[1] *Weekly Intelligence Report, Check Point Research, https://research.checkpoint.com/wp-content/uploads/2023/07/Threat_Intelligence_News_2023-07-17.pdf*
[2] *Raport roczny z działalności CERT POLSKA 2022. Krajobraz bezpieczeństwa polskiego internetu, NASK-PIB/CERT Polska, s. 36.*

Jednym z newralgicznych punktów może być przestarzała infrastruktura informatyczna, posiadająca słabości systemowe, wynikające np. z braku przeprowadzenia niezbędnych aktualizacji systemowych, błędów wewnętrznych oprogramowania lub niepoprawnej konfiguracji. W konsekwencji może narazić to organizację na niekontrolowany wyciek danych lub ich kradzież. Z kolei korzystanie z aplikacji firmowych, mających luki w zabezpieczeniach stanowią dla cyberprzestępców łatwe wejście do systemów niczego nieświadomych użytkowników w celu przeprowadzenia cyberataków. Źle zabezpieczony sprzęt firmowy i miejsce pracy, tj. brak procedur firmowych i narzędzi, które organizują codzienną pracę niezależnie od miejsca jej wykonywania to kolejny punkt, wykorzystywany przez przestępców do podjęcia skutecznego cyberataku. Brak odpowiedniej wiedzy pracowników organizacji z zakresu cyberbezpieczeństwa i ich podatność na działania socjotechniczne. W tym przypadku cyberprzestępcy nie atakują infrastruktury informatycznej, a wykorzystują zachowania pracowników, ich obawy, lekkomyślność, a także brak wiedzy, wywierając na nich wpływ i manipulując nimi w celu wyłudzenia i kradzieży danych firmowych czy też złamania najróżniejszych zabezpieczeń.

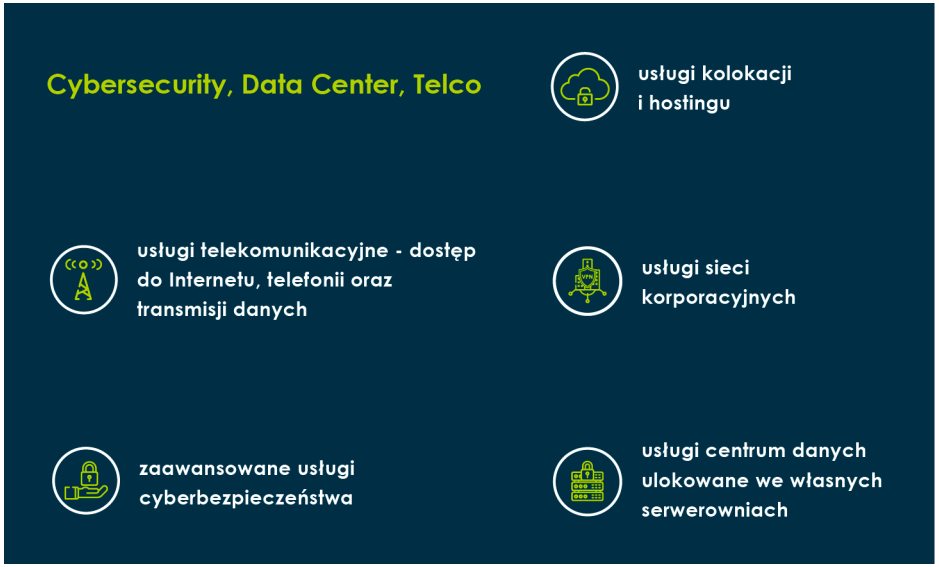
Co zyskuje organizacja inwestując w cyberbezpieczeństwo?

Przede wszystkim większe zaufanie klientów - cyberataki często osłabiają wizerunek biznesowy organizacji. Incydenty powodują nie tylko utratę klientów, ale i trudności w pozyskiwaniu nowych partnerów do współpracy. Relacje biznesowe z organizacjami, które doświadczyły skutków takich ataków mogą być traktowane jako bardzo ryzykowne. Dzięki inwestycjom w cyberbezpieczeństwo można skutecznie zredukować ryzyko i zidentyfikować potencjalne zagrożenia, na jakie narażona jest organizacja oraz zaplanować wdrożenie nowych procedur i wytycznych w tym zakresie. Sama świadomość wprowadzenia przez firmę restrykcyjnych procedur poprawiających cyberbezpieczeństwo może zniechęcić hakerów do podejmowania cyberataków na daną organizację. Pozwalają

również wyciągnąć wnioski na temat efektywności i wydajności pracy działów IT oraz niwelować luki w bezpieczeństwie systemów informatycznych. Z kolei regularne szkolenia pracowników z obszaru cyberzagrożeń przyczyniają się do wzrostu ochrony zasobów organizacji. Takie osoby są bardziej świadome zagrożeń oraz nie dają łatwo nabrać się na cyberatak np. z wykorzystaniem socjotechnicznych manipulacji. Oczywiście należy jeszcze wspomnieć o kwestiach finansowych - oszczędnościach, które są efektem inwestycji w cyberbezpieczeństwo. Wdrożenie kilku usług z tego zakresu lub przeszkolenie pracowników będzie tańszym rozwiązaniem niż kilkudniowy, a nawet kilkutygodniowy przestój w funkcjonowaniu organizacji lub niwelowanie skutków wycieku lub kradzieży danych.

Indywidualne i kompleksowe rozwiązania z zakresu cyberbezpieczeństwa

W NASK S.A. stawiamy na cyberbezpieczeństwo naszych klientów, ponieważ wiemy, że w obecnych czasach stanowi kluczowy element skutecznego biznesu oraz jest warunkiem niezbędnym do sprawnego funkcjonowania organizacji.



Jak działamy w NASK S.A.?

Przede wszystkim wspomagamy rozwój i dbamy o bezpieczeństwo naszych klientów. Oferujemy indywidualne i kompleksowe podejście do projektów z zakresu cyberbezpieczeństwa, ponieważ wiemy, że każda organizacja jest unikalna, a jej

potrzeby determinują czynniki zewnętrze, jak i wewnętrzne. Rozwiązania wdrażamy projektowo, wykorzystując przy tym wiedzę i doświadczenie naszej wykwalifikowanej kadry inżynierów oraz analityków. Dzięki ścisłej współpracy z Państwowym Instytutem Badawczym NASK korzystamy z 30-letniego know-how w obszarze bezpieczeństwa teleinformatycznego oraz możemy liczyć na wsparcie kadry naukowców z NASK PIB. Dążymy, aby każdy projekt rozpocząć od audytu na podstawie, którego przygotowujemy rzetelne rekomendacje wdrożeniowe, poprawiające bezpieczeństwo i funkcjonowanie organizacji. W NASK S.A. zajmujemy się również techniczną realizacją zaleceń poaudytowych oraz operacyjnym utrzymaniem usług i dbaniem o ich bieżącą aktualizację. Naszym klientom zapewniamy wsparcie techniczne specjalistów i gwarantujemy dobór najbardziej optymalnego rozwiązania, spełniającego wszelkie wymagania funkcjonalne oraz dedykowane pod konkretną potrzebę organizacji. Prowadzimy również szkolenia Security Awareness, zwiększające odporność pracowników na cyberzagrożenia. Szkolenie zawiera szereg informacji o dobrych praktykach i zachowaniach w Internecie. Jego zadaniem jest podniesienie świadomości na temat zagrożeń i niebezpieczeństw, na jakie narażeni są użytkownicy komputerów, a które mają bezpośredni wpływ na bezpieczeństwo całej sieci teleinformatycznej. To właśnie dzięki kompleksowemu działaniu i indywidualnemu podejściu gwarantujemy najwyższy możliwy poziom cyberbezpieczeństwa organizacji niezależnie od jej wielkości i branży.

Należy pamiętać, że działania podnoszące poziom cyberbezpieczeństwa organizacji to nie koszty a inwestycje, które w przyszłości mogą uchronić przed nieprzyjemnymi konsekwencjami udanego cyberataku. Dodatkowo są pomocne w kontaktach z kontrahentami. Jeśli Twoi klienci wiedzą, że aktywnie działasz na rzecz cyberbezpieczeństwa, ich zaufanie do Twoich produktów i usług wzrośnie. W cyberbezpieczeństwo warto, a nawet trzeba inwestować. Nie zawsze muszą być to najdroższe rozwiązania. O wiele istotniejsze jest dostosowanie podjętych działań do specyfiki firmy, tj. branży, struktury organizacji czy sposobu jej działania. Dodatkowo warto pamiętać o szkoleniach pracowników z zakresu cyberbezpieczeństwa, ponieważ najsłabszym ogniwem w organizacji jest człowiek.

CHMURA I BACKUP DANYCH JAKO MUST HAVE BEZPIECZNEGO BIZNESU

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

5

Amazon, Microsoft i Google to główni gracze na rynku rozwiązań chmurowych. Według danych serwisu Statista, w 2023 roku rynek ten może osiągnąć wartość niespełna 600 mld dolarów. Nie zawsze jednak wybór tego typu rozwiązania jest oczywisty. Warto bowiem zwrócić uwagę na kwestie jakości, bezpieczeństwa, a także kosztów.

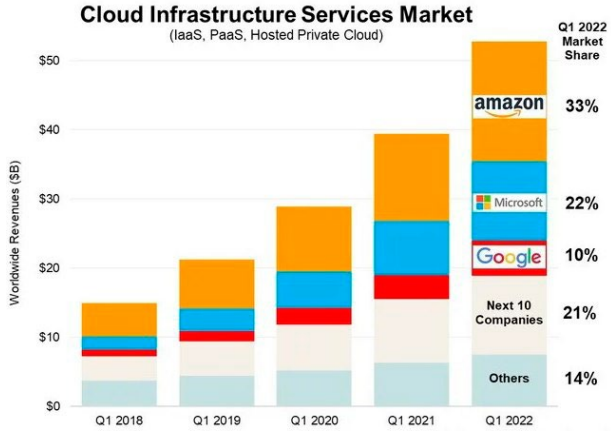
Mianem rozwiązań chmurowych, czyli tzw. cloud computingu określamy usługi, w których dane użytkownika przechowywane są na serwerach zewnętrznej firmy. Usługodawca oprócz przestrzeni dyskowej udostępnia często także narzędzia związane ze świadczoną usługą, a także w określonym obszarze wsparcie techniczne. Dostęp do danych odbywa się za pomocą łączy internetowych.

Wielka trójka cloud computingu

Amazon, Google i Microsoft zajęły łącznie 65 procent globalnego rynku colud computingu w pierwszym kwartale 2022 roku. Kolejne 21 procent należało do dziesięciu kolejnych firm, natomiast pozostałe 14 procent jest rozdrobniona.

Według Synergy Research Group, przychody z tego rynku wyniosły w tym okresie 52,7 mld dolarów.

Udziały w rynku cloud computingu w latach 2018 do 2022 roku (dane kwartalne)



Źródło: Synergy Research Group

Jakie są główne ryzyka i koszty związane z utratą danych w firmach oraz jakie możliwości skutecznej ochrony przed tymi zagrożeniami są dostępne?

W erze cyfrowej, bezpieczeństwo danych staje się priorytetem dla firm. Obejmuje to analizę ryzyka i kosztów utraty danych oraz możliwych metod ochrony. Dostępne raporty dostarczają nam cennych informacji w tym zakresie. Istnieją skuteczne rozwiązania, takie jak platforma Synology, pozwalające na bezpieczne przechowywanie danych, wykonywanie zaawansowanych kopii zapasowych i szyfrowanie pamięci masowej. Kluczowe jest również wykorzystanie innowacji, takich jak chmura pozwalająca na wykrywanie zdarzeń i naruszeń oraz nowoczesne kamery służące ochronie fizycznej z wykorzystaniem metod sztucznej inteligencji.

Jakie są główne koszty i ryzyka związane z utratą danych dla firm?

Badania przeprowadzone przez organizacje branżowe ujawniają, że ponad 60% firm było celem ataków na ich infrastrukturę IT w 2020 roku. Konsekwencje takich incydentów mogą obejmować odcięcie dostępu do pojedynczych stanowisk pracy, a w skrajnych przypadkach doprowadzić do paraliżu całej firmy, co niesie za sobą poważne problemy prawne i finansowe.

Jakie zagrożenia związane z utratą danych są obecne oraz jakie skuteczne metody ochrony można zastosować, aby im przeciwdziałać?

Badania wskazują, że ponad 80% firm, których pracownicy pracują zdalnie, wdrożyło rozwiązania VPN. Pandemia skłoniła Synology do zwolnienia na stałe z opłat za licencje VPN w swoich routerach, wspierając tym samym klientów w trudnym czasie. Niemniej jednak, w systemach bezpieczeństwa to człowiek nadal pozostaje najsłabszym ogniem. Wielu użytkownikom brakuje wystarczającej wiedzy o zagrożeniach, dlatego oprócz budowania właściwej struktury zabezpieczania danych, kluczowe stają się szkolenia pracowników.

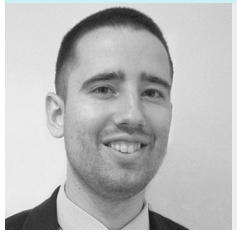
Jakie elementy są niezbędne do osiągnięcia efektywnej ochrony danych?

Efektywna ochrona danych wymaga holistycznego podejścia. Obejmuje to kontrolę dostępu, zastosowanie biometrii czy kluczy sprzętowych, a także wdrożenia systemów kopii zapasowych z mechanizmami szyfrowania i weryfikacji oraz wysoką dostępnością. W połączeniu z odpowiednio przeszkolonym personelem, takie rozwiązania minimalizują ryzyko, a w przypadku incydentu umożliwiają szybkie przywrócenie funkcjonowania firmy.

Aktualne trendy wskazują na eliminację z procesów uwierzytelniania haseł jako jedynego etapu weryfikacji, są one bowiem słabym punktem systemów IT. Przykładem zmian jest usługa Synology Secure SignIn, umożliwiająca logowanie do serwera z wykorzystaniem biometrii i autoryzację z użyciem kluczy sprzętowych. Wprowadza się również centralne systemy uwierzytelniania i zarządzania tożsamością, aby uprościć proces logowania do różnych usług online. Wbudowane, bezlicencyjne rozwiązania do kopii zapasowych, takie jak Active Backup Suite od Synology, sprawiają, że zaawansowana kopia zapasowa staje się przystępna cenowo, a mechanizmy wysokiej dostępności są dostępne nawet dla małych firm.

Podsumowując, bezpieczeństwo danych jest priorytetem dla każdej firmy. Zrozumienie ryzyka, kosztów i skutecznych strategii ochrony jest kluczowe dla minimalizacji zagrożeń. Koszty wdrożenia odpowiednich zabezpieczeń staja się relatywnie niskie w stosunku do ewentualnych nakładów związanych z odzyskiwaniem danych. Technologie, przeszkolenie personelu i nowoczesne rozwiązania, takie jak te oferowane przez Synology, stanowią klucz do skutecznej ochrony przed utratą danych i utrzymania stabilności działalności firmy.

Jesteś zainteresowany naszymi rozwiązaniami? Uzyskaj bezpłatne porady i przetestuj rozwiązania pamięci masowej i oprogramowania Synology dla przedsiębiorstw we własnym środowisku. Umów się na konsultację już teraz.

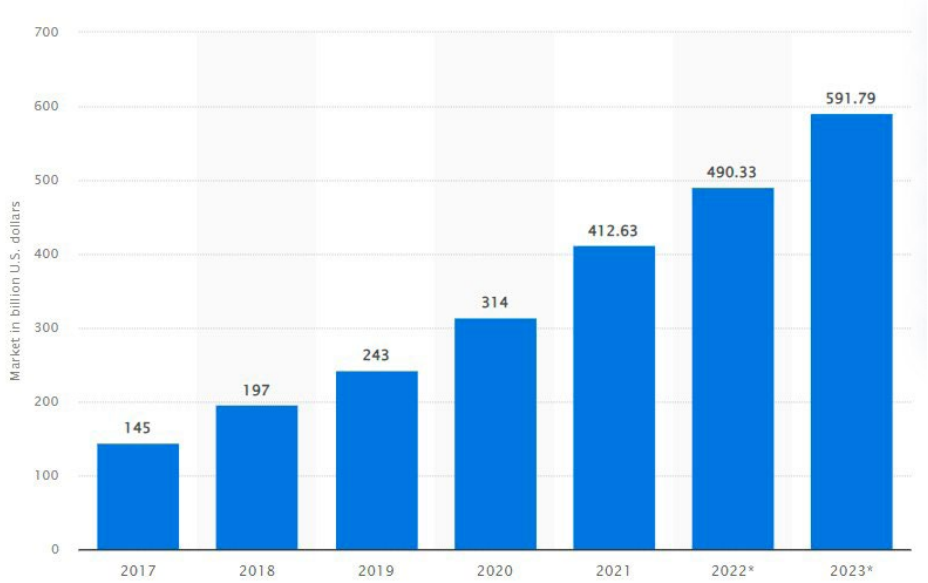


Tomasz Iwańczuk
Synology Solution Engineer

Synology®

Wyjątkiem na rynku usług chmurowych są Chiny, gdzie wymienieni giganci mogą funkcjonować sprawnie nie mogą. Z tego powodu prym na tym rynku wiodą takie platformy jak Tencent Cloud oraz Alibaba Cloud.

Wartość rynku cloud computingu w latach 2017-2023 (w mld dolarów)



Źródło: Statista

Z kolei jak podaje Statista, w 2023 roku rynek cloud computingu osiągnie poziom niespełna 600 mld dolarów. Dla porównania, w 2022 roku było to 490 mld dolarów, a w 2021 roku 413 mld dolarów. Usługi te obejmują m.in. dostęp do przestrzeni pozwalającej przechowywać dane, ale także infrastrukturę, oprogramowanie, zarządzanie procesami bezpieczeństwa, usługi reklamowe czy dodatkowe usługi związane z administracją publiczną.

Najpopularniejszym modelem w ramach cloud computingu jest tzw. mechanizm "pay-as-you-go". Właściciel systemu zarządza i utrzymuje system, natomiast klient płaci jedynie za jego użytkowanie.

Cloud Computing w Polsce

Według danych Statisty, w 2023 roku rynek Cloud Computingu w Polsce będzie miał wartość 1,369 mld dolarów. Szacuje się również, że do 2027 roku rynek ten osiągnie poziom 2,417 mld dolarów przy średniorocznym tempie wzrostu przekraczającym 15 procent.

Przeniesienie do chmury. Czy to się opłaca?

Według danych Cloudwards, najczęściej stosowanym produktem chmurowym na świecie jest Google Dysk. Korzysta z niego aż 94,4 procent firm, które przechowują tam swoje dane. Na drugim miejscu jest Dropbox z wynikiem 66,2 procent, na trzecim OneDrive (39,35 procent), a czwartym - iCloud (38,89 procent). Ale to oczywiście narzędzia niewystarczające do prowadzenia profesjonalnego biznesu.

Buduj biznes i skaluj sprzedaż wykorzystując sprawdzony i rozpoznawalny brand

money.pl

16 mln UU **95 mln PV**

Źródło: dane wewnętrzne, lipiec 2023

Zostań partnerem contentu redakcyjnego

Partnerstwo cyklu cyberbezpieczeństwo

Cyberbezpieczeństwo to stała tematyka poruszana przez redakcję na łamach serwisu dobreprogramy.pl oraz money.pl. Nieustanie sprawdzamy, dbamy i doradzamy w sprawach bezpieczeństwa w sieci. Mamy własne newsy, śledzimy trendy i wyłapujemy nowe zagrożenia, które czyhają na każdego Polaka.

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.

NEWS

Program money.pl

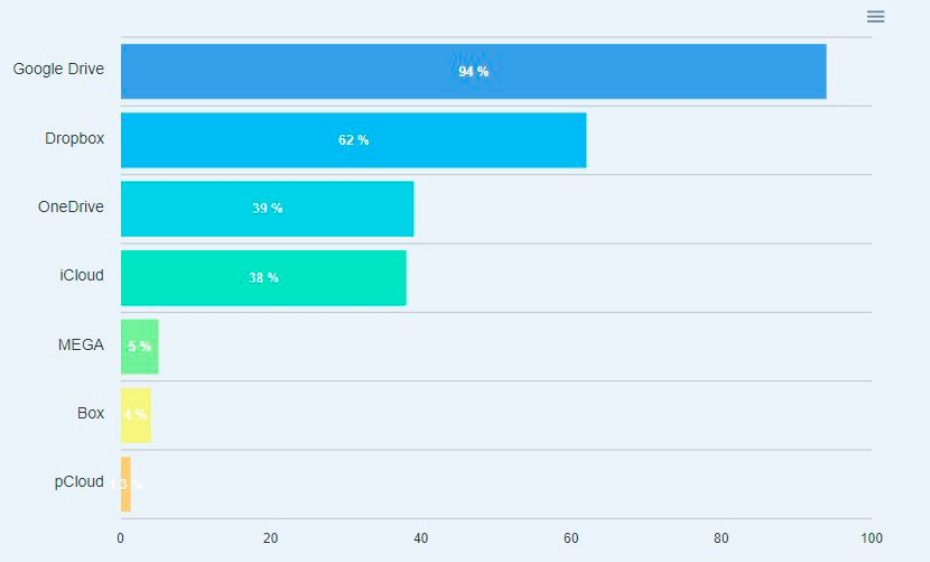
Redakcyjny program wideo, emitowany na stronie głównej WP oraz w social mediach. Do studia zapraszamy ekspertów z każdej istotnej gałęzi polskiej gospodarki i wspólnie diagnozujemy, omawiamy oraz tłumaczymy bieżącą sytuację gospodarczą w Polsce i na świecie.

SKONTAKTUJ SIĘ Z NAMI

reklama@grupawp.pl

tel: 22 57 67 890

Odsetek użytkowników cloud computingu korzystających z poszczególnych rozwiązań chmurowych oferowanych na rynku



Źródło: cloudwards

Odpowiedź na pytanie czy warto korzystać z tego typu rozwiązań częściowo dają dane dotyczące popularności rozwiązań chmurowych. Informacje zebrane przez Cloudwards pokazują, że już w 2018 roku liczba użytkowników Google Dysk przekroczyła miliard, a cała platforma Google Workspace w 2020 roku osiągnęła poziom 2 mld użytkowników. Z kolei Dropbox może się pochwalić liczbą użytkowników przekraczającą 700 mln.

W popularności cloud computingu przodują użytkownicy z Ameryki Północnej, którzy stanowią 61 procent tego rynku, 21 procent to Europa Zachodnia, a 18 procent pozostałe regiony świata.

Rozwiązania chmurowe i backup. Czy to jest bezpieczne?

Kategorie rozwiązań chmurowych

- **IaaS, czyli z ang. Infrastructure as a Service** - w ramach tego rozwiązania klient dostaje w użytkowanie cały potrzebny sprzęt, płacąc przy tym odpowiednią miesięczną opłatę.
- **PaaS, czyli z ang. Platform as a Service** - klient w ramach usługi chmurowej nabywa dostęp do środowiska pracy w postaci dostosowanej do jego potrzeb platformy.
- **SaaS, czyli z ang. Software as a Service** - w tym przypadku klient otrzymuje nie tylko platformę, ale również zestaw aplikacji dostępnych za pośrednictwem internetu, do których loguje się przy pomocy specjalnego panelu. Nie musi on również instalować otrzymanych programów, ani nabywać licencji. Ponosi jedynie opłatę za użytkowanie.

Bezpieczeństwo rozwiązań chmurowych jest ważnym tematem w procesie decyzyjnym dotyczącym tego typu inwestycji.

Zalety rozwiązań chmurowych

- Choć zarządzanie kosztami to jedno z największych wyzwań cloud computingu, to użytkownicy często jako jedną z zalet wymieniają oszczędności kosztowe.
- Przeniesienie danych do chmury, a także posiadanie możliwości backup'u danych sprawia, że według KPMG, dwie trzecie firm, które wdrożyły takie rozwiązania, odnotowało wzrost poczucia bezpieczeństwa.
- Zaletą jest także duża liczba dostępnych rozwiązań chmurowych.
- Jakość świadczonych usług po stronie dostawcy jest wysoka w przypadku wyboru jednej renomowanego dostawcy.
- Rozwiązania chmurowe są skalowalne, co pozwala na łatwą rozbudowę systemu.
- Możliwość stosunkowo łatwej zmiany usługodawcy.
- Mobilności jaką dają rozwiązania chmurowe również jest zaletą. Dzięki temu osoby pracujące w terenie mają łatwy dostęp do danych firmowych.
- Możliwość łatwego tworzenia kopii zapasowej w sposób automatyczny (backup).

Wady rozwiązań chmurowych

- Wśród wad należy wymienić niepewność związaną z bezpieczeństwem danych.
- Konieczność przekazania obcemu podmiotowi wrażliwych danych.
- Brak odpowiednich kompetencji osób wdrażających rozwiązanie po stronie zamawiającego.
- Mniejsza kontrola nad powierzonymi danymi.
- Działanie rozwiązań chmurowych jest uzależnione od internetu. W przypadku jego braku, firma może zostać pozbawiona dostępu do nich.

Według Resmo, 79 procent firm uważa za jedno z największych wyzwań zapewnienie bezpieczeństwa rozwiązań związanych z cloud computingiem. W analizie badania dodano również, że główną przeszkodą w odpowiednim zabezpieczeniu rozwiązań chmurowych jest brak specjalistycznej wiedzy osób ją wdrażających - zwraca uwagę serwis Statista.

Oprócz wyzwania związanego z bezpieczeństwem Resmo wskazuje również na problem zarządzania kosztami w rozwiązaniach chmurowych (82 procent), brak specjalistycznej wiedzy w tym zakresie (78 procent), rozłożenie odpowiedzialności

związanej z bezpieczeństwem pomiędzy dostawcą rozwiązania, a jego użytkownikiem.

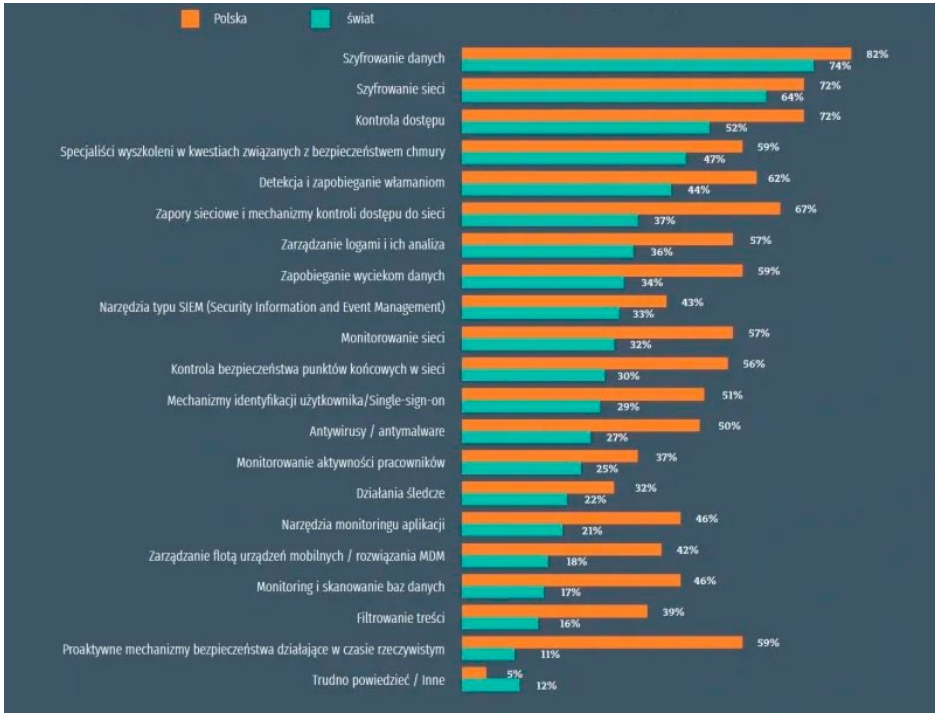
Wśród technologii, które w ramach rozwiązań chmurowych zapewniają użytkownikom największą ochronę są wymieniane: szyfrowanie danych, kontrola dostępu, detekcja i zapobieganie włamaniom, czy zapory sieciowe. Szczegóły w tej kwestii widać na załączonym wykresie.

Koszty cloud computingu i backupów

Warto zwrócić uwagę, że oprócz wspomnianych korzyści, jakie niesie ze sobą cloud computing, należy wziąć pod uwagę niekiedy wysokie koszty związane z tym rozwiązaniem.

Jak podaje Itpedia, koszty chmury mogą być nawet 5 razy większe w stosunku do środowiska lokalnego. „Pierwszym elementem jest samo oprogramowanie oraz jego koszt. Do tego dochodzi czas migracji danych do chmury, co może wiązać się z zatrudnieniem dodatkowych konsultantów lub specjalistów z tego zakresu. W umowie warto zapewnić sobie również odpowiedni transfer i przepustowość chmury, bo jest to element, na którym dostawcy infrastruktury potrafią zarabiają najwięcej".

Technologie, które w największym stopniu zapewniają ochronę danych zgromadzonych w cloud computingu (dane Polskie i globalne)



Źródło: Cloud Security Spotlight Report

MONITORING IT PODSTAWĄ BEZPIECZEŃSTWA PRZEDSIĘBIORSTWA

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

6

Solidna strategia bezpieczeństwa danych nie tylko chroni informacyjne zasoby organizacji przed działaniami cyberprzestępczymi, ale także przed błędami ludzkimi, które wciąż pozostają jednymi z głównych przyczyn naruszeń danych. Jakie narzędzia i rozwiązania obejmują jej poprawne wdrożenie?

Praktyki związane z bezpieczeństwem danych muszą adresować wszystkie wyzwania związane z zabezpieczaniem danych przechowywanych najczęściej w rozproszonych środowiskach. Obejmuje to zrozumienie, gdzie znajdują się dane, śledzenie, kto ma do nich dostęp oraz zablokowanie działań, które wiążą się z ryzykiem naruszeń.

Rozwiązania, które to umożliwiają obejmują natomiast implementację narzędzi do odkrywania i klasyfikacji danych, które pozwalają oddzielić informacje szczególnie wrażliwe i umieścić je w specjalnych repozytoriach od tych, które pozwalają monitorować wszelkie operacje wykonywane na danych. Narzędzia związane z monitoringiem wykrywają wzorce użytkowania danych, umożliwiając zespołom ds. bezpieczeństwa nadzorowanie, kto ma dostęp do danych, wykrycie anomalii i zidentyfikowanie ryzyka.

Monitoring IT sprawdza ponadto, czy sprzęt informatyczny działa zgodnie z oczekiwaniami oraz jak rozwiązywane są wszelkie zidentyfikowane problemy. Niektóre technologie mogą przeprowadzać też podstawową ocenę sprzętu w całym środowisku informatycznym, podczas gdy inne mogą automatyzować identyfikację i naprawę problemów związanych ze sprzętem.

Technologie monitorowania wykorzystywane są też do oceny sieci, systemów i punktów końcowych pod kątem ataków cybernetycznych oraz naruszeń danych. Dostępne są różne technologie, w tym zarządzanie informacją i zdarzeniami związane z bezpieczeństwem (SIEM), zarządzanie wykrywaniem i reagowaniem (MDR) oraz oferty monitorowania sieci.

Kluczowe jest jednak powiązanie infrastruktury ze zmianą na poziomie organizacyjnym, czyli tzw. kulturą organizacji, bo wciąż jednym z największych ryzyk, z którym zmagają się firmy, są pracownicy.

Jakie wyzwania związane są z bezpieczeństwem danych?

W wielu przypadkach naruszenia danych są wynikiem zachowania pracowników, takiego jak np. przypadkowe przesłanie wrażliwych informacji do niewłaściwego odbiorcy lub pozostawienie dokumentów na widocznym miejscu. Pracownicy mogą też działać również celowo, próbując wykraść lub skopiować wrażliwe dane w celu późniejszego ich wykorzystania lub ujawnienia. To może obejmować zarówno wrażliwe informacje o klientach, jak i wewnętrzne dokumenty firmy.

By zminimalizować wewnętrzne zagrożenia związane z bezpieczeństwem danych, organizacje powinny inwestować w edukację pracowników na temat przepisów bezpieczeństwa, prowadzić regularne szkolenia, monitorować aktywność pracowników w sieci oraz implementować systemy kontroli dostępu i audytu.

Więcej niż jedna trzecia firm na całym świecie (34 procent) mierzy się z naruszeniami bezpieczeństwa co roku. Większość z nich wynika z niedbalstwa, wiele jest jednak wynikiem celowych działań.

Jak zapewnić bezpieczeństwo danych?

Istnieje szeroki zakres metod i technik, które firmy mogą zastosować, aby osiągnąć silną ochronę danych. Jedne z najważniejszych to:

- **Szyfrowanie danych**
  Szyfrowanie zapewnia, że nawet jeśli same dane zostaną naruszone, będą one nieczytelne dla osób nie posiadających odpowiedniego upoważnienia lub dostępu do specjalnych kluczy.

- **Kontrola dostępu i uwierzytelnianie**
  Dzięki kontroli dostępów jedynie upoważniony użytkownik może przeglądać i edytować wrażliwe dane.

- **Bezpieczeństwo poczty elektronicznej**
  Poczta to wciąż jeden z ulubionych kanałów, przez który cyberprzestępcy uzyskują dostęp do sieci. Silna ochrona przed problemami takimi jak phishing jest niezbędna.

- **Firewall**
  To pierwsza linia obrony w zakresie bezpieczeństwa sieciowego.

- **Kopie zapasowe i odporność danych**
  Jeśli dane zostaną usunięte lub zaszyfrowane przez grupy ransomware, możliwość skorzystania z regularnie aktualizowanych kopii zapasowych sprawia, że wszelkie zakłócenia są minimalizowane.

- **Usuwanie danych**
  Chociaż zazwyczaj bardziej dotyczy to kwestii prywatności danych, przechowywanie danych poza ich okresem użytkowania daje hakerom więcej opcji do celowania, dlatego potrzebny jest klarowny plan usuwania danych, gdy już spełniły one swoje zadanie.

- **Przeciwdziałanie wydostawaniu się danych (ADX)**
  Narzędzia ADX zapewniają, że nawet jeśli przestępcy naruszą obręb danej sieci, nie będą w stanie wydostać danych na zewnątrz.

Kultura bezpieczeństwa organizacji. Jak ją zbudować?

Kultura bezpieczeństwa, czyli wszystkie procedury regulujące zachowania pracowników, to wciąż jednak najważniejszy element strategii bezpieczeństwa organizacji. Większość firm zaczyna to rozumieć i wychodzi poza taktyczne, epizodyczne podejścia do bezpieczeństwa, budując strategię na poziomie całej firmy, skupiając się na edukacji i komunikacji, zamiast na nakazach ze strony IT i ciągłym strumieniu nowych polityk.

Bez zrozumienia idei, które za nimi stoją, wśród pracowników i tak będzie panowało zamieszanie co do tego, co powinni, a czego nie powinni robić, aby chronić informacje firmowe. Nawet coś tak pozornie prostego, jak używanie skutecznych haseł, było w wielu firmach przyczyną problemów. Przez ostatnie 30 lat eksperci ds. bezpieczeństwa szkolili pracowników, aby robić wszystko, od zmieniania haseł co 30 dni, przez niezmienianie ich, chyba że zostali dotknięci naruszeniem, do ograniczenia liczby znaków do samych cyfr lub liter, aż po wymaganie różnych rodzajów cyfr, symboli, liter i wielkości liter. Nic dziwnego, że pracownicy nie tylko są zagubieni, ale także wyczerpani zmieniającymi się i trudnymi do zrozumienia wytycznymi.

Słabe ogniwa w organizacji a ryzyko ataków i problemów biznesowych

Incydenty związane z bezpieczeństwem danych, pochłaniają zasoby firmy, prowadząc do wzrostu kosztów prowadzenia działalności. W 2022 roku globalny średni koszt naruszenia danych wyniósł 4,35 miliona dolarów, podczas gdy w Stanach Zjednoczonych ta liczba jest ponad dwukrotnie wyższa i wynosi średnio 9,44 miliona dolarów.

Jedną z najlepszych broni przeciwko ransomware jest regularne tworzenie kopii zapasowych i stosowanie redundantnych procesów. Dobrym pomysłem jest bezpieczne przechowywanie ważnych plików na zewnętrznym nośniku (wystarczy skopiować i wkleić je na zewnętrznym nośniku poprzez eksplorator plików, ale dużo wygodniejszym i zautomatyzowanym działaniem, będzie utworzenie pełnej kopii zapasowej systemu operacyjnego i danych komputera przy użyciu dedykowanych serwerów - pisze w swoich materiałach promocyjnych firma Synology.

Te wydatki mogą obejmować wszystko, począwszy od płatności okupu i utraconych przychodów, aż po przestoje w działalności, usuwanie skutków, opłaty prawne i opłaty za audyt. Na przykład opłaty za audyt dla firm po wystąpieniu naruszeń danych mogą być o około 13,5% wyższe niż dla firm bez naruszeń.

Miliony dolarów strat mogą doprowadzić do bankructwa małej firmy, ale sprawiają też problemy wielkim firmom. Na przykład ataki ransomware miały znacznie większy wpływ finansowy na sektor opieki zdrowotnej, w którym tylko w 2021 roku z powodu przestoju firmy straciły ponad 7,8 miliarda dolarów.

O REDAKCJI

Redakcja

Tomasz Bonek
prezes zarządu i redaktor naczelny
tb@interaktywnie.com

Paweł Musiał
redaktor Interaktywnie.com
pm@interaktywnie.com

Robert Cieszawski
redaktor Interaktywnie.com
rc@interaktywnie.com

Barbara Chabior
redaktor Interaktywnie.com
bch@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, +48 71 302 75 35
jk@interaktywnie.com

O INTERAKTYWNIE.COM

Adres i siedziba redakcji

interaktywnie.com

Interaktywnie.com sp. z o.o.
ul. Oławska 17 lok. 6 - III piętro
50-123 Wrocław
tel.: 71-302-75-35
redakcja@interaktywnie.com

NIP: 898-215-19-79
REGON: 020896541

Spółka zarejestrowana we Wrocławiu, kod pocztowy 50-302, przy ul. Jedności Narodowej 152/177, przez Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000322917

Kapitał zakładowy 6 000,00 zł

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

Wykorzystane do raportu zdjęcia pochodzą z banku zdjęć Pixabay.