LISTOPAD 2023

EBOOK Z RAPORTEM interaktywnie.com

JAK CHRONIĆ DANE W FIRMIE?

KOMPENDIUM WIEDZY DLA MANAGERÓW ZARZĄDZAJĄCYCH FIRMAMI

SPONSOR SREBRNY

OKTAWAVE

POD PATRONATEM

WP money.pl GAZETA.PL

SPIS TREŚCI

RAPORTY INTERAKTYWNIE 2024

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

Nie ma firmy nienarażonej na cyberataki!

W 2022 roku 58 procent firm w Polsce doświadczyło przynajmniej jednego incydentu naruszającego bezpieczeństwo danych. Z kolei 33 procent odnotowało wzrost intensywności ataków związanych z cyberbezpieczeństwem. Odsetek firm, które doświadczyły co najmniej 30 ataków w ciągu roku wyniósł aż 12 procent. Tak źle jeszcze nie było!

Dobrze wiedzą to firmy, które postanowiły zaprezentować w tym ebooku wiedzę swoich ekspertów oraz swoją ofertę: Oktawave, NASK S.A.

Zachęcam do lektury i kontaktu z Partnerami tego opracowania.

Tomasz Bonek, redaktor naczelny Interaktywnie.com

Oktawave S.A.

Adres
ul. Puławska 464
02-884 Warszawa

Dane kontaktowe
E-mail: customer@oktawave.com, sales@oktawave.com
Strona www: oktawave.com
Telefon: +48 22 10 10 555

Opis działalności
Oktawave to polska platforma publicznej chmury obliczeniowej oraz zespół certyfikowanych ekspertów chmurowych. Specjalizujemy się w migracji, monitoringu i zarządzaniu środowiskami IT w oparciu o chmury: Oktawave, GCP, AWS i Azure. Budujemy rozwiązania oparte o zaawansowane technologie, w zgodzie z regułami zarządzania bezpieczeństwem danych i informacji.

Wybrani klienci
TUI, Vision Express, Fabrity, EPAM, Burda Media, PKO Bank Polski

TBMS Sp. z o.o.

Adres
ul. Oławska 17/6
50-123 Wrocław

Dane kontaktowe
E-mail: kontakt@tbms.pl
Strona www: tbms.pl
Telefon: 71 302 75 35

Opis działalności

- Projektujemy i wdrażamy strony internetowe - m.in. sklepy, landing page, firmowe.
- Świadczymy usługi związane z pozycjonowaniem (SEO) i prowadzeniem kampanii w Google Ads.
- Prowadzimy profile w mediach społecznościowych.
- Specjalizujemy się w lead generation oraz w content marketingu i SEO/SEM.
- Pracujemy dla uznanych marek z branży IT, FMCG, medycznej.

Agencja marketingu Internetowego TBMS była odpowiedzialna za wdrożenie polskiej wersji serwisu Business Insider (od strategii monetyzacji, poprzez budowanie zespołu, do wdrożenia). Od 2017 roku jesteśmy certyfikowaną agencją obsługującą IBM w Polsce, a także partnerów biznesowych tej globalnej marki (m.in Comarch, Asseco, Sygnity).

Wybrani klienci
IBM, Comarch, Asseco, Sygnity, Marwit, Hasco Lek, Salesforce, Ringier Axel Springer Polska, Onet, Business Insider Polska, Wydawca Men'sHealth i Women'sHealth

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

RYZYKO CYBERATAKÓW I KONSEKWENCJE UTRATY DANYCH W PRZEDSIĘBIORSTWIE

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

1

Według badania „Barometr cyberbezpieczeństwa" autorstwa firmy KPMG, w 2022 roku 58 procent firm w Polsce doświadczyło przynajmniej jednego incydentu naruszającego bezpieczeństwo danych. Z kolei Statista zwraca uwagę, że ransomware jest najpowszechniejszym cyberatakiem mającym wpływ na bezpieczeństwo przechowywania informacji. Wyniki tych badań świadczą o tym, z jaką powagą należy podchodzić do tematu bezpieczeństwa danych w przedsiębiorstwie.

Ransomware, czyli złośliwe oprogramowanie ograniczające w całości lub częściowo dostęp do systemu lub danych użytkownika, celem wyłudzenia okupu za jego odblokowanie, to według Statisty najczęściej pojawiające się cyberzagrożenie dotyczące danych na świecie. W 2022 roku ransomware stanowiły aż 68,42 procent wszystkich wykrytych cyberzagrożeń, będąc jednocześnie niedoścignionym, niechlubnym liderem zestawienia.

Na drugim miejscu zidentyfikowano zagrożenie pod nazwą „Network breach", czyli naruszenia bezpieczeństwa sieci. Ten rodzaj cyberataku odpowiadał za 18,42 procent wykrytych przypadków naruszeń. Stanowi on nieautoryzowany dostęp do danych, mający na celu wykorzystanie ich do popełnienia przestępstwa. Skutkiem tego typu ataku nie są najczęściej bezpośrednio straty finansowe, a uszczerbek na reputacji. Wykradzione dane mogą bowiem zostać wykorzystane nielegalnie w imieniu ofiary.

Kolejne rodzaje cyberataków odpowiadają za mniej niż 5 procent wykrytych przypadków. To m.in. „Data Exfiltration" czyli nieuprawniony transfer danych z zainfekowanego komputera, który odpowiada za 3,95 procent przypadków cyberataków.

CZAS PRZENIEŚĆ BIZNES DO CHMURY

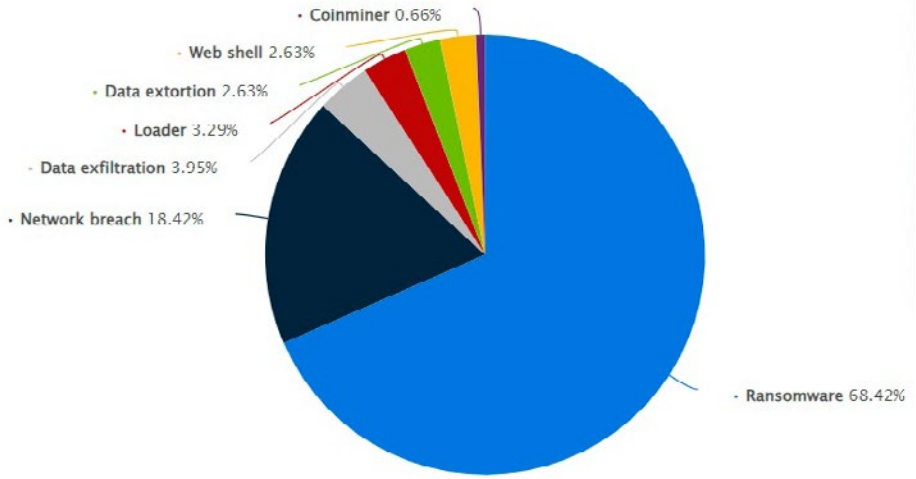
SKORZYSTAJ Z **BEZPŁATNEJ MIGRACJI**
DO CHMURY I OTRZYMAJ ZAPASOWE ŚRODOWISKO
PRZETWARZANIA DANYCH W CENIE

ZMIGRUJ ZA DARMO

OKTAWAVE aws Google Cloud

W zestawieniu znajdziemy również rodzaje cyberataków nazywane jako: „Loader", „Data extortion", „Web shell", czy „Coinminer".

Najczęściej wykrywane cyberataki na świecie w 2022 roku zagrażające bezpieczeństwu danych



Źródło: Statista

Według danych serwisu Aag-it, najwięcej cyberataków odnotowano w Wielkiej Brytanii. W 2022 roku aż 4783 osoby padły tam ofiarą cyberprzestępców na każde 100 tysięcy internautów. Na drugim miejscu znalazły się Stany Zjednoczone z wynikiem 1494 ofiar przypadających na tę samą liczbę użytkowników internetu.

Serwis zwraca również uwagę, że krajami, w których w 2022 roku najmocniej wzrosła liczba incydentów związanych z naruszeniem danych były Chiny, Japonia oraz Korea Południowa.

Serwis Getastra zebrał najważniejsze dane dotyczące liczby cyberataków w 2023 roku:

- atak hakerski na świecie następuje co około 39 sekund
- najczęstszym celem hakerów mającym na celu uzyskanie nieuprawnionego dostępu do danych są podmioty z sektora opieki zdrowotnej
- 92 procent złośliwego oprogramowania zyskuje dostęp do zainfekowanego komputera za pośrednictwem poczty elektronicznej
- około 4,1 miliona witryn internetowych na świecie zawiera złośliwe oprogramowanie
- średni czas interwencji związanej z wykrytym atakiem ransomware to 49 dni
- 74 procent ekspertów IT uważa, że działania wykonywane podczas pracy zdalnej za niebezpieczne z punktu widzenia cyberbezpieczeństwa

Najpoważniejsze skutki cyberataków

› **Utrata wrażliwych danych** - jednym z najpoważniejszych skutków cyberataków jest nieuprawniony dostęp do danych, przez co mogą one zostać użyte w niedozwolony sposób. Dotyczy to przede wszystkim danych osobowych, ale także danych finansowych, biznesowych, których ujawnienie np. pozbawi firmę przewagi konkurencyjnej. Ryzykiem cyberataku jest również ich całkowita utrata, co może wiązać się z brakiem możliwości prowadzenia biznesu.

› **Utrata reputacji** - równie istotnym skutkiem cyberataku może być utrata reputacji przez podmiot będący jego ofiarą. Wyciek danych klientów może wiązać się z ich nieodwracalną utratą, a co za tym idzie brakiem możliwości uzyskania przychodów. Również upublicznienie wrażliwych danych może wywołać niechęć do firmy, która zostanie pozbawiona dużej części klienteli.

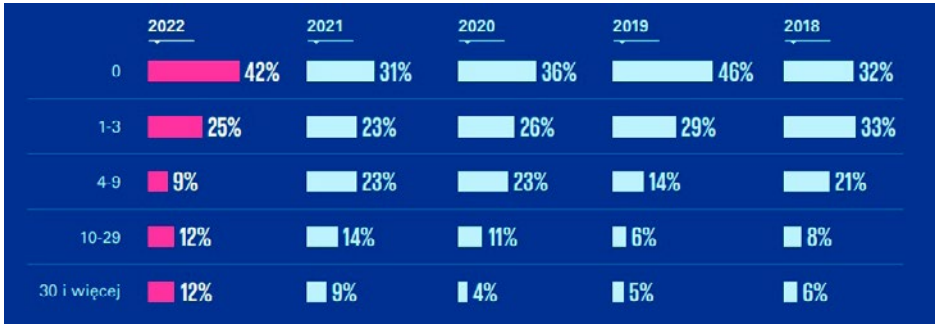
› **Przestoje działalności** - atak hakerski związany z utratą danych może się wiązać także z przestojami w działalności firmy. Zatrzymanie produkcji lub zerwanie łańcuchów dostaw może być dotkliwe i narazić przedsiębiorstwo na duże straty.

› **Kary finansowe** - utrata danych osobowych może się wiązać także z reperkusjami prawnymi oraz kontrolną przedsiębiorstwa pod kątem ich prawidłowego przechowywania. Ujawnione nieprawidłowości mogą wiązać się z karami finansowymi, a także koniecznością naprawy błędnych procedur bezpieczeństwa czy zapłaty odszkodowania.

Otoczenie firm nadal niebezpieczne

Według „Barometru Cyberbezpieczeństwa" autorstwa KPMG, w 2022 roku 58 procent firm w Polsce doświadczyło przynajmniej jednego incydentu naruszającego bezpieczeństwo danych. Z kolei 33 procent odnotowało wzrost intensywności ataków związanych z cyberbezpieczeństwem. Negatywną tendencją jest również fakt, że odsetek firm, które doświadczyły co najmniej 30 ataków w ciągu roku wyniósł aż 12 procent. Jak podaje KPMG, jest to najwyższy poziom w historii badania.

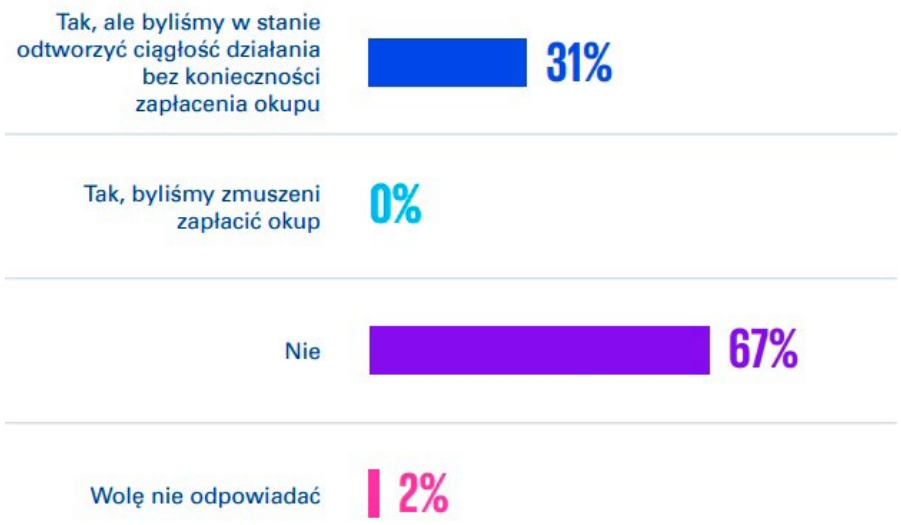
Liczba zarejestrowanych przez firmy incydentów zagrażających ich cyberbezpieczeństwu w latach 2018-2022



Źródło: KPMG „Barometr cyberbezpieczeństwa"

Jak podaje KPMG, firmy najbardziej obawiają się zagrożeń mających na celu wyłudzenia danych dostępowych lub uwierzytelniających (phishing) oraz wycieków danych (maleware). W ostatnim czasie przedsiębiorstwa częściej niż wcześniej ulegają atakom ransomware.

Czy organizacja padła ofiarą znaczącego ataku ransomware?



Źródło: KPMG „Barometr cyberbezpieczeństwa"

Oprócz charakteru ataku, firmy różnicują ataki ze względu na rodzaj atakującego. Oczywiście szczególnie dotkliwy według nich może być atak przeprowadzony przez zorganizowane grupy cyberprzestępcze. Taką odpowiedź w badaniu KPMG wskazało 70 procent przedsiębiorstw. 59 procent obawia się ataków pojedynczych hakerów, a 42 procent cyberterrorystów.

W „Barometrze cyberbezpieczeństwa" pojawiła się również odpowiedź wskazująca na grupy wspierane przez obce państwa. Ma to związek z faktem, iż 20 procent firm w Polsce w 2022 roku zanotowało większą intensywność ataków hakerskich związanych z trwającą agresją Rosji na Ukrainę.

ARTYKUŁ PROMOCYJNY

BACKUP TO NIE WSZYSTKO. DLACZEGO POTRZEBUJESZ DISASTER RECOVERY CENTER?

Maciej Kuźniar
CTO Oktawave

2

Świadomość firm w zakresie backupu i regularnego wykonywania kopii zapasowych danych jest dość wysoka. Zgodnie z raportem PRM „Rynek cyberbezpieczeństwa w Polsce" korzysta z niego ponad 80% organizacji. Jednak w przypadku awarii sama kopia danych to za mało, aby przywrócić działanie systemu. Zestawiając backup z Disaster Recovery Center – backup to proszek gaśniczy (same dane) vs. gaśnica (zapasowa infrastruktura, która te dane odtworzy).

Podobnie jak koło zapasowe w samochodzie, backup danych stanowi zabezpieczenie w przypadku nieprzewidzianych sytuacji losowych i innych incydentów wirtualnych. Jest to kluczowy element zapewniający podstawowe bezpieczeństwo zasobów i możliwość kontynuacji pracy w przypadku utraty nawet znacznej części danych. Korzystając z analogii motoryzacyjnej, backup stanowi świetne koło zapasowe, jednak często potrzebny jest kompleksowy system naprawczy - tu do akcji ratunkowej wkracza Disaster Recovery Center (DRC) wraz ze strategią awaryjnego przywracania danych. Koło zapasowe w postaci backupu ratuje z pojedynczej awarii, podczas gdy DRC zapewnia pełne zabezpieczenie w przypadku poważniejszych katastrof.

Statystyki z raportu Deloitte CE CFO Survey 2023 wskazują na obszar zarządzania ryzykami prawnymi i biznesowymi, jako jedną z najważniejszych korzyści płynących z wdrożenia rozwiązań chmurowych w organizacjach. **Chmura ze względu na wysokie bezpieczeństwo przechowywania danych i niskie ryzyko awarii staje się więc kluczową częścią wielu nowoczesnych strategii biznesowych.** Rozproszona architektura spełnia ważną rolę w przypadku awarii jednego z komponentów. Tak zaprojektowane środowisko pozwala na to, aby w przypadku błędu natychmiastowo przekierować żądanie i kontynuować pracę bez przeszkód. Choć awarie chmurowe statystycznie zdarzają się naprawdę rzadko, warto być przygotowanym na każdy, nawet najczarniejszy scenariusz.

Zabezpiecz się na każdym polu

Disaster Recovery Center (DRC) to ważna część planu postępowania kryzysowego i zapewnienia ciągłości biznesowej w czasie wystąpienia poważnych awarii, takich jak: **kataklizmy naturalne, ataki hakerskie czy błędy systemowe.** Niestety nie ma stu procentowej ochrony przed tego typu incydentami, jednak istnieją sprawdzone sposoby na minimalizację ich skutków. DRC obejmuje całą infrastrukturę, aplikacje oraz dane, zapewniając płynne przywrócenie normalnego funkcjonowania organizacji oraz możliwie szybkie odtworzenie utraconych danych.

Poważny i utrzymujący się przestój, który powoduje blokadę normalnego funkcjonowania firmy, może doprowadzić do istotnych konsekwencji, m.in. utraty dochodów, nadwyrężenia reputacji i wizerunku, a w skrajnych przypadkach nawet do problemów prawnych czy upadku przedsiębiorstwa. **Co ważne, katastrofalne w skutkach awarie mogą zdarzyć się w każdej organizacji, niezależnie od wielkości firmy czy profilu prowadzonej działalności.** Dlatego z punktu widzenia operacji biznesowych plan odzyskiwania danych po awarii to jeden z kluczowych procesów w organizacji. Niezbędne jest więc nie tylko regularne tworzenie kopii zapasowych, ale także opracowanie kompleksowego planu kryzysowego. W tym kontekście warto poznać różnice między backupem danych a strategią Disaster Recovery w chmurze, które mimo podobieństw, pełnią zasadniczo różne role.

Fundament bezpieczeństwa vs kompleksowa ochrona

Backup danych stanowi kluczowy element strategii zabezpieczania informacji. Pozwala na odtworzenie danych w przypadku awarii sprzętu, błędu ludzkiego czy ataku cybernetycznego, stając się jednym z fundamentów planu kryzysowego. Jednak backup sam w sobie nie gwarantuje utrzymania ciągłości działania firmy w przypadku poważniejszych zakłóceń.

Disaster Recovery w chmurze idzie krok dalej, oferując spójną strategią odtwarzania danych po awarii. Jest to zestaw planów oraz reguł, które pozwalają na przywrócenie pełnej funkcjonalności. Proces odzyskiwania może być stosunkowo prosty, jak przywracanie danych z wcześniej utworzonej kopii zapasowej, ale i bardziej skomplikowany, zależnie od dwóch kluczowych czynników: **docelowego czasu, w jakim system ma być przywrócony** (Recovery Time Objective - RTO) oraz **celu punktu odzyskiwania** (Recovery Point Objective - RPO).

RTO określa maksymalny czas, jaki system może pozostać niedostępny zanim zostanie w pełni przywrócony. To może być zarówno kilka dni, jak i godzin, a w przypadku krytycznych systemów jest to kwestia sekund (np. w sektorze bankowym). Kiedy RTO i RPO są krótkie, oznacza to, że firmy powinny bardzo uważnie rozważyć wdrożenie rozwiązań Disaster Recovery.

Czym dokładnie różni się backup od planu Disaster Recovery?

- **Zakres działania:** backup danych koncentruje się głównie na tworzeniu kopii zapasowych w celu ich odtworzenia w przypadku utraty. To często pojedyncza operacja archiwizacji. Disaster Recovery (DR) obejmuje szerszy zakres procedur, polityk i planów mających na celu przywrócenie pełnej funkcjonalności systemu w przypadku katastrofy lub awarii całego systemu. DR uwzględnia infrastrukturę IT, aplikacje oraz procedury przywracania.

- **Czas przywracania:** w przypadku backupu proces odtwarzania danych może być czasochłonny, szczególnie jeśli mamy do czynienia z dużym zbiorem danych. DR zapewnia szybsze przywrócenie systemu do stanu operacyjnego poprzez całościowy plan działania.

- **Zakres ochrony:** backup chroni jedynie kopię informacji, ale niekoniecznie zapewnia kompletną ochronę infrastruktury czy aplikacji. Odtwarza jedynie ostatnią kopię danych, co może prowadzić do utraty informacji z okresu między kopiami zapasowymi. DR pozwala na odtworzenie danych z różnych okresów, w zależności od określonych punktów odzyskiwania (RPO - Recovery Point Objective).

Strategie działania w ramach Disaster Recovery

Popularną praktyką jest wykorzystanie chmury jako zapasowego centrum danych. Dostawcy usług chmurowych, w tym Oktawave rozmieszczają swoje Data Center w oddalonych lokalizacjach, zapewniając w ten sposób maksymalną niezależność. Taka strategia umożliwia szybkie przywrócenie sprawności systemów nawet w przypadku blackoutów czy klęsk żywiołowych.

Inną możliwością jest utworzenie zapasowego centrum danych w chmurze jako środowisko hybrydowe dla lokalnie przechowywanych danych. Rozwiązania multicloud zapewniają

dodatkową ochronę z uwagi na niskie prawdopodobieństwo wystąpienia awarii u kilku dostawców jednocześnie.

W sytuacji dotkliwej katastrofy, zapasowe centrum awaryjne (Disaster Recovery Center), zazwyczaj umiejscowione w innym regionie geograficznym, przejmuje rolę głównego centrum danych. Wtedy zarówno wewnętrzny, jak i zewnętrzny zespół IT może natychmiast rozpocząć proces przywracania systemów. Po odzyskaniu lub wymianie serwerów fizycznych, dane są ponownie migrowane, przywracając normalne funkcjonowanie infrastruktury.

Czy DRC jest opłacalne?

Decyzja o utrzymywaniu Disaster Recovery Center (DRC) jest kluczowym dylematem dla wielu firm, które zastanawiają się nad opłacalnością takiego rozwiązania. **Ważne pytanie brzmi: jak kluczowe dla biznesu są przechowywane dane i jak długo firma może sobie pozwolić na przerwę w działalności?** Koszt DRC zależy od wielu czynników, w tym od ilości danych, częstotliwości tworzenia kopii zapasowych i szybkości przywracania systemu przez dostawcę usług. Im krótsze RTO i RPO, czyli czas i ilość danych, które można zaakceptować jako utracone, tym wyższe mogą być koszty uruchomienia procesu po awarii. Inwestycja w DRC może być opłacalna z długoterminowej perspektywy, ponieważ koszt poszukiwania pomocy po wystąpieniu katastrofy może być znacznie wyższy.

Wykorzystanie usługi Disaster Recovery as a Service (DRaaS) staje się coraz bardziej popularne, eliminując potrzebę posiadania własnych zasobów i zespołu specjalistów do zarządzania infrastrukturą awaryjną. Ponadto, wielu dostawców DRaaS pobiera opłaty tylko w przypadku faktycznego korzystania z ich usług, co dodatkowo może wpłynąć na obniżenie kosztów dla firm.

Dane pod ochroną Oktawave

Oktawave doskonale sprawdza się jako dostawca usług Disaster Recovery (DR), m.in. dzięki rozproszeniu geograficznemu centrów danych, co stanowi doskonałą ochronę np. w zakresie katastrof klimatycznych w jednym regionie dostępności.

Oktawave cechuje także wysoka elastyczność, bowiem zespół inżynierów o multicloudowych kompetencjach może stworzyć Disaster Recovery Plan niezależnie od wykorzystywanej chmury (Oktawave, AWS, Google Cloud czy Microsoft Azure). Dzięki solidnemu know-how oferujemy elastyczne rozwiązania dopasowane do różnych budżetów, także tych niewielkich organizacji.

Oszczędzanie na bezpieczeństwie to jedynie pozorna ekonomia. Proaktywne przygotowanie się na najgorszy scenariusz, staje się tańszą alternatywą niż kosztowne usuwanie skutków awarii. DRC jest więc niezbędne dla współczesnego biznesu – zarówno w aspekcie finansowym, ale także operacyjny i wizerunkowym. Oktawave oferuje kompleksowe rozwiązania, które nie tylko zabezpieczają dane, ale także przygotowują organizację na potencjalne zagrożenia, co może okazać się kluczowe w zapewnieniu ciągłości działania firmy w obliczu krytycznych sytuacji.

BEZPIECZNA FIRMOWA INFRASTRUKTURA IT, CZYLI JAKA? PORADNIK DLA MANAGERÓW NIEZWIĄZANYCH Z IT

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

3

Wyciek wrażliwych danych firmowych może mieć katastrofalne konsekwencje zarówno prawne, jak i finansowe, a zagrożenie rośnie z roku na rok. W 2020 r. odnotowano już 304 miliony ataków ransomware, czyli dwukrotnie więcej niż w roku poprzednim, a średni koszt naruszenia bezpieczeństwa danych w USA wynosi już 8,64 miliona dolarów. Jak uniknąć takich wydatków? Jak zadbać o bezpieczeństwo danych firmowych? Co powinien na ten temat wiedzieć każdy członek zarządu lub manager?

Odpowiedź jest prosta: trzeba zadbać o bezpieczeństwo infrastruktury IT, inwestując w nowoczesne rozwiązania i stale monitorując ich stan. Niestety, w praktyce takie działania są nie tylko kosztowne, ale skomplikowane, bo i sama infrastruktura IT to grupa komponentów, które muszą ze sobą płynnie współpracować, by wspierać, testować i kontrolować wewnętrzne i zewnętrzne operacje firmy. Taka infrastruktura musi być nowoczesna i regularnie modernizowana, aktualizowana, by spełniała swoją rolę.

Zwykle infrastruktura IT składa się z rozwiązań programowych, sprzętu i połączeń sieciowych. Sprzęt obejmuje fizyczne komponenty infrastruktury IT, takie jak komputery osobiste, centra danych, przełączniki, serwery i routery. Oprogramowanie natomiast odnosi się do wszystkich komponentów i aplikacji używanych przez firmę do wykonywania codziennych zadań. Sieć natomiast umożliwia przesyłanie danych pomiędzy poszczególnymi urządzeniami w infrastrukturze IT, obejmując tradycyjne połączenie internetowe, ale także rozwiązania do przechowywania danych.

Kiedy warto inwestować we własną serwerownię, a kiedy skorzystać z usług doświadczonych partnerów, np. data center?

Jednym z kluczowych pytań, na które należy odpowiedzieć przed wdrożeniem nowego systemu centrum danych, jest określenie,

Drożej nie znaczy lepiej (i bezpieczniej)

Wybór odpowiedniego rozwiązania zależny jest od potrzeb i strategii rozwoju firmy. Analiza TCO powinna uwzględniać nie tylko koszty początkowe, ale także koszty operacyjne, utrzymania zespołów inżynieryjnych oraz strategię Disaster Recovery.

Inwestycja we własną serwerownię może być uzasadniona w sytuacji, gdy firma posiada stałe zapotrzebowanie na moc obliczeniową. Warto mieć jednak na uwadze, że zakup własnej infrastruktury często uzależnia od pierwotnie wybranej technologii, która niezwykle szybko się starzeje z czasem utrudniając optymalizację aplikacji i środowiska IT, a w skutek tego - rozwój firmy.

W przypadku biznesów, które doświadczają dynamicznego wzrostu lub sezonowości w konsumpcji mocy obliczeniowej (np. branża e-commerce), zdecydowanie korzystniejszy jest model rozliczenia za rzeczywiste zużycie zasobów. Taką możliwość oferują dostawcy chmury publicznej oraz data center, umożliwiając firmom dostęp do zaawansowanej infrastruktury i najnowszych technologii bez konieczności ponoszenia kosztów związanych z ich budową i utrzymaniem.

Zwolennicy rozwiązań on-premowych (własnych serwerowni) często podnoszą aspekt bezpieczeństwa. Tymczasem związane jest ono nie tylko z koniecznością dodatkowej inwestycji w redundantne systemy na wypadek awarii (najlepiej w odrębnym obszarze geograficznym), ale również zatrudnieniem inżynierów odpowiedzialnych za monitoring i utrzymanie infrastruktury IT. To koszty i odpowiedzialność, z których mogą odciążyć przedsiębiorców zewnętrzni dostawcy. Certyfikowane data center oraz platformy chmury publicznej zobligowane są do przestrzegania restrykcyjnych standardów zarządzania bezpieczeństwem danych i informacji. Platforma Oktawave spełnia dodatkowo rygorystyczne wymogi KNF, co pozwala nam obsługiwać m.in. klientów z sektora finansowego. Posiadamy również kompetencje, tj. zespół doświadczonych architektów i inżynierów chmurowych, który wspiera naszych klientów w transformacji do chmury, a następnie może przejąć opiekę nad ich infrastrukturą w trybie 24/7/365.

Maciej Kuźniar
CTO Oktawave

czy zlecić zarządzanie centrum danych na zewnątrz, czy też zbudować je lokalnie.

Jakie więc są różnice między tymi podejściami?

Własne centra danych są zwykle zlokalizowane na terenie firmy („lokalnie"), zewnętrzne są zlokalizowane poza siedzibą firmy, a dzięki chmurze dane można trzymać dosłownie w dowolnym miejscu.

Choć wielu wyspecjalizowanych dostawców centrów danych oferuje całodobowe zabezpieczenia, które chronią Twoje dane przed uszkodzeniami fizycznymi, w przypadku lokalnych rozwiązań ostateczna odpowiedzialność za bezpieczeństwo spoczywa nafirmie. Wtedy jednak przedsiębiorstwo zyskuje również całkowitą kontrolę nad wszystkim, co się w centrum znajduje, podczas gdy decydując się na „zewnętrzną infrastrukturę" to jego dostawca ostatecznie kontroluje wszystkie komponenty.

Wewnętrzne centra danych są zwykle znacznie trudniejsze do skalowania powyżej pewnego punktu, ponieważ zwyczajnie może zabraknąć miejsca na dołożenie nowego sprzętu. Dlatego też wiele firm rezerwuje lokalne centra danych wyłącznie dla systemów o krytycznym dla biznesu znaczeniu.

Zalety wewnętrznych centrów danych:

- **Własność infrastruktury:** organizacja posiada cały sprzęt i infrastrukturę.
- **Kontrola:** pełna kontrola nad operacjami, bezpieczeństwem i organizacją infrastruktury.
- **Dostosowanie:** możliwość dostosowania centrum danych do specyficznych potrzeb przetwarzania firmy.
- **Inwestycja początkowa:** wymaga większych inwestycji początkowych w sprzęt i infrastrukturę.
- **Zarządzanie:** pełna odpowiedzialność za zarządzanie, utrzymanie i aktualizacje.

Zalety zewnętrznych centrów danych:

- **Własność infrastruktury:** infrastruktura jest własnością dostawcy lub modelu współdzielenia (kolokacja/DCaaS).
- **Kontrola:** ograniczona kontrola nad niektórymi aspektami operacyjnymi i bezpieczeństwa.
- **Dostęp do nowoczesnych technologii:** dostęp do najnowszej technologii i zasobów, często aktualizowanych przez dostawcę.
- **Model płatności:** system płatności typu pay-as-you-go w modelu DCaaS, co może obniżać koszty dla niektórych firm.
- **Redundancja i odzyskiwanie danych:** zapewnienie redundancji i odzyskiwania danych po awarii, co zwiększa bezpieczeństwo danych.
- **Bariery wejścia:** niższe bariery wejścia, szczególnie korzystne dla małych firm i start-upów, które nie mogą sobie pozwolić na kosztowne wewnętrzne centrum danych.
- **Zarządzanie:** dostawca zajmuje się większością aspektów zarządzania, utrzymania i aktualizacji.

Jak i jakie rozwiązania infrastrukturalne IT zapewniają bezpieczeństwo IT?

Najsłabszym ogniwem wszelkich systemów zabezpieczeń wciąż pozostaje człowiek, ale to w gestii organizacji należy zastosowanie takich zabezpieczeń, by jego ewentualny wpływ był jak najmniej brzemienny w skutkach.

W tym celu firmy powinny myśleć wielopoziomowo, wdrażając:

- zabezpieczenia na poziomie fizycznym, co obejmuje takie elementy jak kontrole dostępu, systemy monitoringu,

Docieraj do 93% Polskich użytkowników internetu dzięki WP ads

Sam ustawisz kampanię.

Sam wybierasz rodzaj rozliczenia.

Sprawdź

ochronę zewnętrzną oraz zabezpieczenia antywłamaniowe. Może również zawierać plany awaryjne z lokalizacją zapasowego sprzętu w innym miejscu na świecie.

- zabezpieczenia na poziomie technologicznym, czyli rozwiązania takie jak firewalle, testy penetracyjne, monitorowanie sieci, wirtualne sieci prywatne (VPN), technologie szyfrowania oraz programy szkoleniowe uczące pracowników, jak identyfikować i reagować na próby kradzieży danych, takie jak phishing.

- środki prewencji na poziomie organizacyjnym, czyli szkolenie pracowników z zakresu bezpieczeństwa haseł, znajomości regulaminów i polityk bezpieczeństwa, które 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.

Jak przestoje w IT związane z niewydolną infrastrukturą mogą działać na niekorzyść biznesu?

Bezpieczeństwo infrastruktury IT, które obejmuje nie tylko ryzyko wycieku wrażliwych danych, ale także przestoje wynikające z niewydolnej infrastruktury bezpośrednio wpływają na zdolność operacyjną firmy, a więc jej wyniki finansowe i reputację.

- Według raportu IDC, same awarie aplikacji kosztują rocznie od 1 do 2,5 miliarda dolarów, nie wliczając w to kosztów pośrednich wynikających np. z utraty zaufania wśród klientów i ich obniżonej satysfakcji spowodowanej np. zbyt długim wczytywaniem stron sprzedażowych.

- Bezpośrednie ataki hakerskie tylko zwiększają te straty, narażając firmy na wydatki rzędu około 117 tysięcy dolarów potrzebnych na podniesienie się po doznanych obrażeniach.

Czy można temu zapobiec?

Kluczowe w tym wypadku wydaje się regularne testowanie kopii zapasowych serwerów, aby zapewnić szybką reakcję w przypadku awarii, regularne kontrole fizyczne służące identyfikacji potencjalne zagrożeń, monitorowanie stanu infrastruktury IT i regularne aktualizacje.

Bezpieczeństwo IT nie jest więc obszarem, który da się „zaspokoić" implementacją takiego czy innego oprogramowania. To cały szereg regularnych działań, obejmujących zarówno fizyczne, jak i cyfrowe operacje, dlatego też wiele firm decyduje się

powierzyć je specjalistom, takim jak np. Oktawave. Firma ta oferuje pełny wachlarz rozwiązań, które koncentrują się na zwiększeniu bezpieczeństwa i wydajności infrastruktury IT firm, łącznie z platformą cloud computingową umożliwiającą szybkie wdrażanie wirtualnych serwerów, skalowalność i dostępność.

Kluczowym elementem oferty Oktawave i innych przedsiębiorstw wspierających bezpieczeństwo IT są narzędzia do odzyskiwania po awarii w chmurze. DRC od Oktawave pozwala także zarządzać bezpiecznym ruchem, dzięki któremu firmy mogą zapewnić ciągłość działania w przypadku poważnych awarii. Dodatkowo Oktawave oferuje rozwiązania oparte o konteneryzację i automatyzację, które przyspieszają i zabezpieczają procesy biznesowe.

ARTYKUŁ PROMOCYJNY

SZKOLENIE SECURITY AWARENESS JAKO KLUCZOWY ELEMENT PROCESU OCHRONY DANYCH W ORGANIZACJI

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

4

W dzisiejszych czasach, gdy technologia informatyczna stanowi integralną część działalności większości organizacji, bezpieczeństwo cybernetyczne stało się priorytetem. Cyberataki stają się coraz bardziej zaawansowane i wyrafinowane, a przed tymi zagrożeniami żadna firma nie jest całkowicie odporna. Warto zadać sobie pytanie: kto stanowi najsłabsze ogniwo w organizacji w kontekście bezpieczeństwa informacji? Odpowiedź może być zaskakująca - to pracownicy. Według raportu The Global Risks Report 2022, aż 95% problemów związanych z cyberbezpieczeństwem wynikają właśnie z błędów ludzkich[1].

W miarę, jak cyberprzestępcy doskonalą swoje metody, ludzie stają się bardziej podatni na ataki. Nawet najbardziej zaawansowane systemy zabezpieczeń nie będą skuteczne, jeśli pracownicy nie zostaną odpowiednio przeszkoleni w zakresie cyberbezpieczeństwa. Przekazywanie podstawowych umiejętności związanych m.in. z tworzeniem silnych haseł, rozpoznawaniem oszustw phishingowych, znajomością procedur firmowych, może znacznie poprawić poziom cyberbezpieczeństwa. Dlatego też, szkolenie Security Awareness, ukazujące dobre praktyki korzystania z Internetu czy umiejętnego zabezpieczenia środowiska pracy, staje się coraz bardziej niezbędne w dzisiejszym środowisku biznesowym.

Jak uchronić organizację przed cyberatakami i wyciekami danych?

Szkolenie Security Awareness to kluczowy element strategii ochrony organizacji przed cyberatakami. Ponieważ to właśnie pracownicy, którzy instynktownie klikają w podejrzane linki, otwierają zainfekowane załączniki lub udostępniają poufne informacje często są punktem wejścia dla cyberprzestępców. To ludzie, nieświadomie, mogą uruchomić lawinę problemów związanych z bezpieczeństwem danych.

Szkolenie Security Awareness pozwala pracownikom na:

[1] *The Global Risks Report 2022, 17th Edition, Digital Dependencies and Cyber Vulnerabilities, s.52.*

1. **Rozpoznawanie zagrożeń:** nauczenie pracowników rozpoznawania potencjalnych zagrożeń, takich jak phishing, malware czy ataki socjotechniczne, to pierwszy krok w zapewnieniu bezpieczeństwa.

2. **Bezpieczne zachowania w sieci:** pomaga zrozumieć, jakie zachowania w sieci są bezpieczne, a jakie potencjalnie ryzykowne.

3. **Prawidłową reakcję na incydenty:** w przypadku wykrycia podejrzanego zachowania, pracownicy powinni wiedzieć, jak zgłosić incydent i jakie kroki podjąć, aby zminimalizować straty.

4. **Ochronę danych:** poznanie zasad związanych z ochroną danych osobowych i firmowych jest kluczowe w zapobieganiu wyciekom informacji.

Cyberedukacja pracowników

Szkolenie Security Awareness to nie luźne informacje przekazywane pracownikom. To strukturalny proces edukacji, który ma uświadomić każdemu pracownikowi, jak ważna jest jego rola w zapewnieniu bezpieczeństwa organizacji. Wiedza i umiejętności zdobywane podczas szkolenia mają na celu zmniejszenie ryzyka naruszenia danych oraz zwiększenie ich świadomości.

Warto zaznaczyć, że cyberedukacja pracowników nie jest jednorazową inwestycją. W miarę, jak cyberprzestępcy zmieniają swoje techniki, konieczne jest stałe doskonalenie wiedzy pracowników. Szkolenie Security Awareness powinno być regularnie aktualizowane i dostosowywane do bieżących zagrożeń.

Bezpieczny pracownik

Organizacje, które inwestują w szkolenie Security Awareness, tworzą kulturę cyberbezpieczeństwa, w której każdy pracownik rozumie swoją rolę w ochronie danych i systemów. Bezpieczny pracownik to aktywny element w walce z cyberprzestępczością.

Jeśli twoja organizacja dąży do zapewnienia bezpieczeństwa informacji i uniknięcia kosztownych naruszeń danych, nie ma lepszego sposobu niż zainwestowanie w cyberedukację. W NASK S.A. oferujemy szkolenie w zakresie cyberbezpieczeństwa, które jest dostosowane do różnych potrzeb i poziomów zaawansowania. Nie pozostawiaj bezpieczeństwa organizacji przypadkowi. Chroń swoją firmę przed cyberprzestępczością!

Rola szkolenia Security Awareness

Szkolenie Security Awareness zwiększa odporność pracowników na cyberzagrożenia. Wyszkolony w tym zakresie pracownik jest gwarantem uniknięcia nieprzyjemnych sytuacji związanych z zagrożeniami w sieci i stanowi niejako tarczę ochronną przed działaniami cyberprzestępców. W NASK S.A. oferujemy szkolenie w zakresie cyberbezpieczeństwa w dwóch wariantach: podstawowej i rozszerzonej. Każda z nich jest dopasowana do potrzeb klienta. 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.

Wariant ze szkoleniem podstawowym zawiera jeden moduł opisujący najpopularniejsze oszustwa w Internecie. Trwa 90 minut, podczas których uczestnicy dowiedzą się praktycznych wskazówek, pomocnych przy ochronie danych osobowych i finansowych przed atakami cyberprzestępców. Ta forma szkolenia przeprowadzana jest w formule wykładu online.

Drugi wariant w rozszerzonej wersji uwzględnia pięć modułów, poruszających kwestie oszustw phishingowych, bezpiecznej komunikacji, bezpieczeństwa aplikacji, bezpieczeństwa płatności oraz profesjonalizacji rynku oszustów. Szkolenie trwa 5 godzin i jest prowadzone w formie warsztatów stacjonarnych. Każdy uczestnik uzyskuje dostęp do dodatkowych materiałów wideo. Dodatkowo po zakończeniu każdego modułu przewidziana jest sesja Q&A.

Po ukończeniu każdego ze szkoleń, uczestnik otrzymuje certyfikat.

Niezależnie od poziomu Twojej wiedzy i doświadczenia, mamy dla Ciebie odpowiednie szkolenie. Zainwestuj w bezpieczeństwo organizacji i zdobądź cenne umiejętności, które pomogą chronić zarówno siebie, jak i organizację przed cyberatakami. Należy zatem pamiętać, że działania podnoszące świadomość cyberbezpieczeństwa organizacji to nie koszty a inwestycje, które w przyszłości mogą uchronić przed konsekwencjami udanego cyberataku.

Skontaktuj się z nami, aby uzyskać więcej informacji:
www.nasksa.pl/kontakt

BACKUP DANYCH FIRMOWYCH, CZYLI JAK SIĘ ZABEZPIECZYĆ PRZED ICH UTRATĄ?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

5

Zabezpieczenie danych w firmie jest kluczowe dla utrzymania aktualności i spójności rejestrów, ochrony informacji o klientach, a nawet dla zapewnienia ciągłości operacyjnej. Ich utrata w skrajnych przypadkach może grozić nawet upadłością firmy, utratą zysków, kłopotami prawnymi i uszczerbkiem na reputacji.

Przykładów, kiedy system ochronny największych nawet firm, nie zdołał ochronić danych wrażliwych można wyliczać bez liku, ale - by podkreślić wagę problemu - warto wspomnieć choćby o kilku.

Zacząć wypada od Facebooka, który w 2021 roku ujawnił naruszenie danych, w wyniku którego osobiste informacje ponad 533 milionów użytkowników, w tym prawdziwe imiona, daty urodzenia, lokalizacje i posty opublikowane na ścianach Facebooka dostały się w ręce hakerów. Co jest jednak nie mniej istotne, lukę odkryła firma White Hat Security w 2021 roku, ale istniała ona już w 2019 roku.

Niemniej kompromitujący jest przypadek firmy Sina Weibo. W 2020 ten chiński serwis mikroblogowy poinformował, że przestępcy mieli dostęp do części jego bazy danych i naruszyli dane 538 milionów użytkowników w tym - podobnie jak w przypadku Facebooka - osobiste informacje, takie jak imiona, nazwiska, lokalizacje i numery telefonów. W tym przypadku napastnicy sprzedali bazę danych w „Darknecie".

I *last but not least*, Avast. Ta firma specjalizująca się w systemach antywirusowych padła ofiarą hakerów, którzy chcieli ją skompromitować – pozyskali dane uwierzytelniające VPN pracowników, próbując wstrzyknąć

Buduj biznes i skaluj sprzedaż wykorzystując sprawdzony i rozpoznawalny brand

money.pl

20.9 mln UU **118 mln PV**

Źródło: dane wewnętrzne, październik 2023

Postaw na komunikację w oparciu o cykle redakcyjne:

BizTech

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

Partnerstwo cyklu cyberbezpieczeństwo

Cyberbezpieczeństwo to stała tematyka 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.

Obecność przy poradnikach B2B

Money.pl to ponad 900 poradników dla przedsiębiorców i jednoosobowych działalności gospodarczych, które przede wszystkim są odwiedzane przez użytkowników szukających konkretnych informacji w sieci.

SKONTAKTUJ SIĘ Z NAMI

reklama@grupawp.pl

tel: 22 57 67 890

złośliwe oprogramowanie do produktów Avast. Tutaj atak został odkryty zanim doprowadził do pełnoskalowego naruszenia danych, a jednak wciąż - było blisko.

Każdy z tych ataków był inny i wykorzystywał inne metody naruszeń, ale zawsze polegał na szukaniu słabych punktów w firmowych zabezpieczeniach. Mogą to być powtarzane hasła, luki bezpieczeństwa w oprogramowaniu, insiderzy, złośliwe oprogramowanie wdrażane w systemie docelowym zwykle za pomocą inżynierii społecznej i wiele, wiele innych.

Jak więc uchronić się przed tym ryzykiem?

Aby skutecznie zabezpieczyć swoje dane i infrastrukturę firmy powinny podejść do problemu bezpieczeństwa wielotorowo, zaczynając od zabezpieczeń na poziomie fizycznym. To obejmuje elementy takie jak kontrole dostępu, systemy monitoringu, ochronę zewnętrzną oraz zabezpieczenia antywłamaniowe. Ważne jest również, aby firmy miały opracowane plany awaryjne, które zawierają lokalizację zapasowego sprzętu w różnych miejscach na świecie, by zwiększyć odporność na potencjalne awarie lub ataki.

Na drugim poziomie znajdują się zabezpieczenia technologiczne, które obejmują rozwiązania takie jak firewalle, testy penetracyjne, monitorowanie sieci, wirtualne sieci prywatne (VPN) oraz technologie szyfrowania.

Równie ważne są programy szkoleniowe dla pracowników, które uczą ich, jak identyfikować i reagować na próby kradzieży danych, takie jak phishing. Dodatkowo, na poziomie organizacyjnym, środki prewencji obejmują szkolenie pracowników z zakresu bezpieczeństwa haseł i znajomości regulaminów oraz polityk bezpieczeństwa.

Te polityki definiują zasady, wytyczne i procedury związane z bezpieczeństwem informacji i infrastruktury w organizacji, wyznaczając jednocześnie role i odpowiedzialności różnych osób w organizacji związane z bezpieczeństwem IT oraz poziom ich uprawnień dostępowych.

Backup danych jako podstawa bezpieczeństwa danych

Organizacje powinny także regularnie tworzyć kopie zapasowe swoich danych i ustalać plan odzyskiwania danych po naruszeniu bezpieczeństwa, by zapewnić reakcję na tyle szybką, by można było mówić o jakiejkolwiek szansie na zminimalizowaniu szkód.

Rodzaje kopii zapasowych danych z urządzeń osobistych

Opcje tworzenia kopii zapasowych danych ciągle ewoluują, bo też zmieniają się zagrożenia, którym - potencjalnie - mogą ulegać dane. Dla maksymalnej ochrony idealne jest użycie kombinacji różnych zabezpieczeń, takich jak:

- **Nośniki** - to najprostszy i najbardziej praktyczny sposób przechowywania danych, który obejmuje małe, przenośne urządzenia, takie jak pamięci USB, płyty CD, DVD. Niestety, urządzenia nie dają zbyt wiele miejsca na dane, co okazać się może niepraktyczne.

- **Zewnętrzne dyski twarde** - to popularna opcja, bo można w ciągu kilku chwil przenieść dane z urządzenia na zewnętrzny dysk twardy np. bezprzewodowo, ale zewnętrzne dyski twarde mogą z czasem się zepsuć. Co więcej, podobnie jak w przypadku nośników wymiennych, mogą zostać zgubione lub skradzione.

- **Backup w chmurze** - w tej opcji dane będą przechowywane zewnętrznie, a nie na urządzeniu, które jest w firmie. Backup w chmurze zapewnia dostęp do Twoich danych przez Internet w dowolnym miejscu i czasie. Kluczową kwestią jest tutaj jednak upewnienie się, że korzystamy z usług sprawdzonego dostawcy i stosujemy się do jego wytycznych w zakresie bezpieczeństwa.

- **Backup na komputerze/urządzeniu** - niektóre urządzenia pozwalają na stworzenie kopii zapasowych danych, które są przechowywane na Twoim urządzeniu, co oferuje dużą wygodę. Ważne jest jednak, aby korzystać z tej opcji w połączeniu z co najmniej jednym z innych opisanych powyżej typów backupu.

Magazyny danych

Ważne jest zrozumienie, jakie dane są dla firmy kluczowe - na przykład te używane codziennie czy generujące przychody - i zapewnienie im odpowiedniego poziomu ochrony, czyli na przykład zdecydowanie o tym, jak często robić kopie zapasowe.

Co więcej, raz ustalona strategia nie powinna być wyryta w kamieniu, trzeba ją regularnie testować i monitorować, aby upewnić się, że wszystko działa, bez względu na to, z jakim scenariuszem naruszeń będziemy mieli do czynienia.

Najlepsze strategie łączą różne metody, takie jak pełne kopie, kopie przyrostowe, różnicowe, migawkowe czy w chmurze, w zależności od potrzeb firmy i rodzaju danych. Ważne jest też stosowanie zasady 3-2-1 w tworzeniu kopii zapasowych: trzymać trzy kopie danych, na dwóch różnych nośnikach, z jedną kopią przechowywaną poza firmą.

A na koniec… Automatyzacja procesów tworzenia kopii zapasowych może znacznie ułatwić pracę i zwiększyć

niezawodność, co jest szczególnie ważne dla firm z dużą ilością danych.

Jakie więc rozwiązania do backupu warto wdrożyć?

- Strategia Backupu 3-2-1: Tworzenie trzech kopii danych na co najmniej dwóch różnych nośnikach, z czego jedna powinna być przechowywana zdalnie.
- Storage as a Service: Wielu dostawców oferuje rozwiązania oparte na płatnościach za zużycie dla zasobów przechowywania danych w chmurze.
- Automatyzacja z wykorzystaniem AI: wykorzystanie AI do odkrywania luk w ochronie danych i wspomaganie odzyskiwania danych po atakach ransomware.
- Przygotowanie na awarię SaaS: umożliwienia korzystania z backupów nawet w przypadku awarii dostawcy usług chmurowych.
- Ochrona pracy zdalnej: przyjęcie opartych na chmurze wirtualnych pulpitów do centralizacji przechowywania danych.

ROZWIĄZANIA CHMUROWE A BEZPIECZEŃSTWO DANYCH

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

6

O kilkanaście procent rocznie ma rosnąć wartość rynku rozwiązań chmurowych w najbliższych latach. Dotyczy to zarówno rynku polskiego jak i globalnego. Według danych Statisty, czołowymi graczami na tym polu są Amazon oraz Microsoft. Do zalet takich rozwiązań należą większe bezpieczeństwo danych, możliwość optymalizacji kosztów oraz lepsza dostępność danych. Użytkownicy wskazują jednak na pewne wyzwania związane z użytkowaniem cloud computingu.

Jak podaje Grand View Research, globalny rynek rozwiązań chmurowych w 2022 roku wyceniono na 483,98 mld dolarów. Co więcej, według przytoczonych danych, tempo jego wzrostu w latach 2023-2030 ma wynieść średnio 14,1 procent rocznie. To szybciej niż pokazują prognozy tylko dla amerykańskiego rynku cloud computingu. Tam spodziewany jest wzrost na poziomie 13,1 procent r/r w analogicznym okresie.

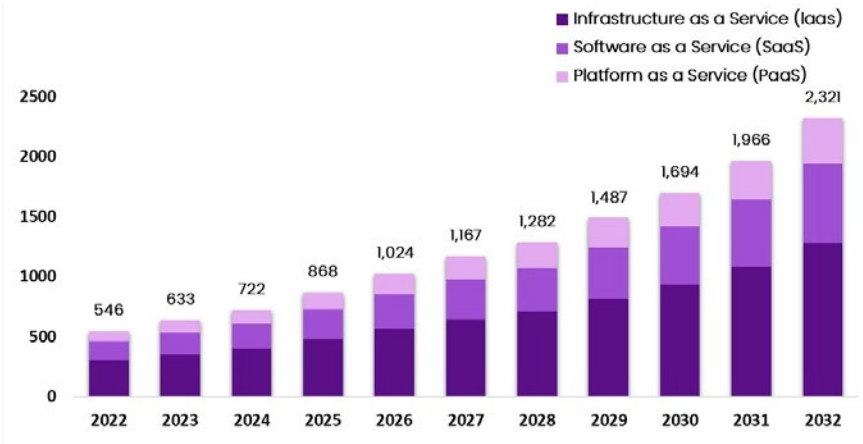
W przypadku rynku polskiego, według Statisty, wartość rynku rozwiązań chmurowych na koniec 2022 roku wyniosła 1,3 mld dolarów. Z kolei dalsze prognozy (do 2027 roku) wskazują, że wartość ta wzrośnie do 3,5 mld dolarów.

Inne szacunki przytacza GlobeNewsWire, według którego globalny rynek rozwiązań chmurowych do 2032 osiągnie średni roczny poziom wzrostu wynoszący 16 procent. W 2023 roku jego wartość wyniesie 633 mld dolarów, w 2024 - 722 mld dolarów, a w 2032 roku - 2,321 bilionów dolarów.

Aby poszerzyć obraz, dane GlobeNewsWire dzielą rynek chmurowy na IaaS (Infrastructure as a Service), SaaS (Software as a Service) oraz PaaS (Platform as a Service).

W przypadku IaaS klient otrzymuje cały potrzebny sprzęt, który nie musi być zainstalowany w siedzibie klienta. Po stronie zamawiającego jest jedynie oprogramowanie.

Globalna wartość rynku rozwiązań chmurowych w latach 2022-2023 (w mld dolarów)



Źródło: GlobeNewsWire

W przypadku SaaS klient otrzymuje nie tylko platformę, ale także zestaw aplikacji dostępnych za pośrednictwem internetu przy pomocy specjalnego panelu. Nie musi on również instalować otrzymanych programów ani nabywać licencji. Do jego jedynych obowiązków należy regulowanie opłaty za użytkowanie systemu.

W przypadku PaaS klient w ramach usługi chmurowej otrzymuje dostęp do środowiska pracy w postaci dedykowanej platformy. Ta natomiast nie jest instalowana na jego komputerze.

Migracja do chmury, czyli jakie przewagi konkurencyjne niesie ze sobą to rozwiązanie?

- elastyczność i mobilność biznesu dzięki swobodnemu dostępowi do danych, co umożliwia cloud computing. Jest to szczególnie ważne w firmach działających na rynku e-commerce lub działających w trybie omnichanel.
- bezpieczeństwo danych z uwagi na tworzone automatycznie kopie zapasowe. Dane KPMG wskazują, że dwie trzecie firm po przejściu na rozwiązanie chmurowe zmniejszyło swoją podatność na cyberzagrożenia.
- lepsza współpraca pomiędzy pracownikami z uwagi na ciągły dostęp do plików zawartych w chmurze.
- zwykle rozwiązania cloud computingowe wiążą się z niższymi kosztami funkcjonowania. Ich zastosowanie często nie wymaga zatrudnienia specjalistów z dziedziny IT lub ograniczanie ich składu. Do tego, w zależności od wybranego rozwiązania, często nie trzeba również inwestować we własnych sprzęt. Oprócz tego firmy chmurowe dzięki efektowi skali mogą zaproponować wysoką jakość świadczonych usług przy rozsądnej cenie.
- rozwiązania chmurowe zapewniają również większą ilość dostępnego miejsca na dane.

- wyższe bezpieczeństwo niż w przypadku autorskich systemów. W przypadku rozwiązania chmurowego, za rozwiązania wpływające na bezpieczeństwo odpowiada dostawca, u którego w sytuacjach krytycznych można domagać się odszkodowania.

- dzięki konkurencji na rynku cloud computingu dostępność tego typu usług jest duża, co daje możliwość lepszej negocjacji oferty.

- skalowalność systemów cloud computingowych pozwala łatwiej rozwijać biznes.

Wady migracji do chmury

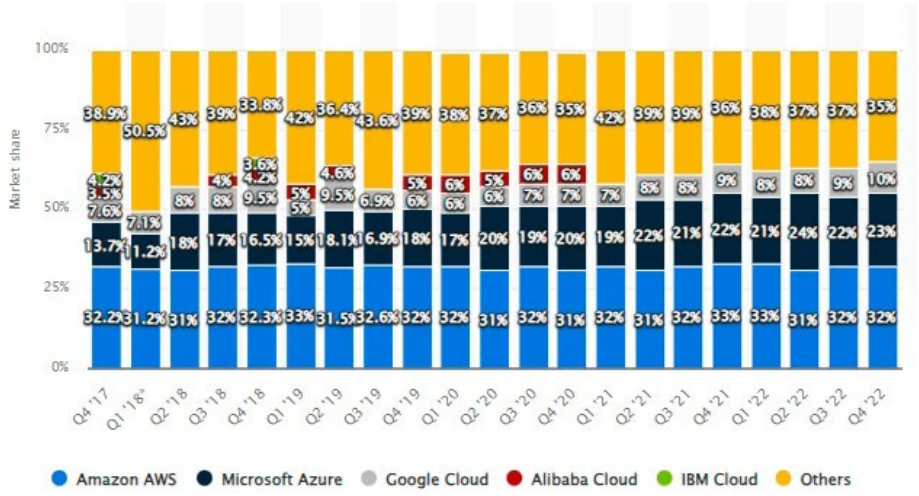
- konieczność posiadania sprawnego łącza internetowego, aby mieć dostęp do danych. To powoduje, że w przypadku awarii internetu firma może zostać pozbawiona tego dostępu.

- mniejsza kontrola nad danymi, bowiem przenosząc je do chmury, znajdują się one w rękach firmy odpowiedzialnej za dostarczenie usługi cloud computingu. Może to wywoływać dyskomfort w szczególności, gdy mamy do czynienia z danymi poufnymi i wrażliwymi.

Najpopularniejsze rozwiązanie chmurowe

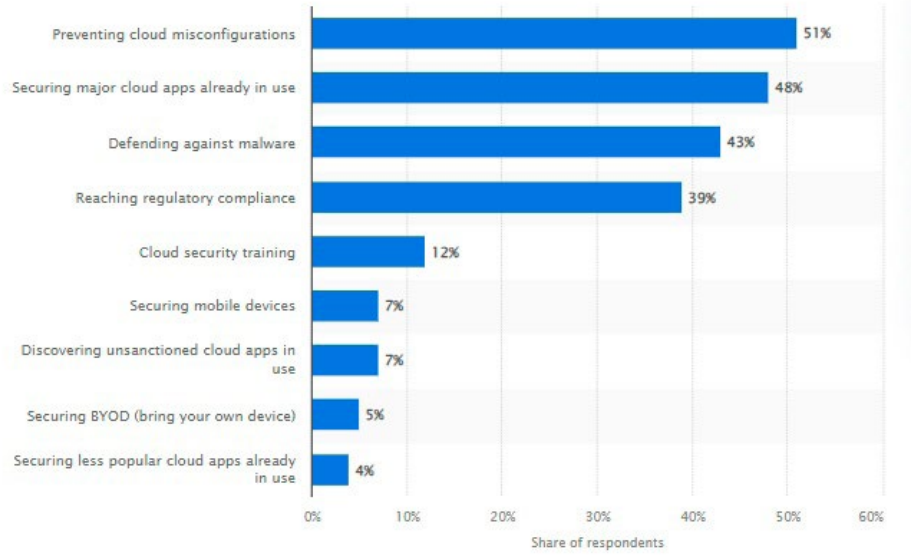
Na rynku jest dostępnych wiele rozwiązań cloud computingowych. Jak podaje Statista, od lat fotel lidera zajmuje Amazon Web Service z udziałem w globalnym rynku przekraczającym 30 procent. Ponad 20 procentowy udział ma Microsoft Azure, a na trzecim miejscu jest Google Cloud - jego udział pod koniec 2022 roku sięgnął 10 procent. Pozostałe rozwiązania mniejszych firm stanowiły 35 procent udziału.

Udział poszczególnych firm w rynku rozwiązań chmurowych na świecie w latach 2017-2022 (dane kwartalne)



Źródło: Statista

Priorytety firm związane bezpieczeństwem cloud computingu



Źródło: Statista

Rodzaje danych przechowywanych w chmurze

Korzystając z rozwiązania chmurowego „na zewnątrz" można przechowywać każdego rodzaje dane. Mowa tu o plikach wideo, dokumentach, zdjęciach, grafikach, danych osobowych, czy oprogramowaniu.

Dostawcy rozwiązań chmurowych dzielą je na trzy kategorie: obiekt, plik oraz blok. Według danych Google, magazyn obiektowy służy do przechowywania dużych zbiorów danych o słabo ustrukturyzowanej strukturze. Pliki natomiast są organizowane w sposób hierarchiczny w folderach. Z kolei w przypadku bloków, każdy z nich jest opatrzony unikalnym identyfikatorem, które następnie przechowywane są jako osobne elementy na serwerze. W ten sposób system przechowuje dane w najbardziej wydajny sposób.

Wyzwania związane z użytkowaniem rozwiązań chmurowych, czyli na co zwrócić uwagę

Expertinsights wylicza na podstawie „Flexera 2022 State of the Cloud Report", z jakimi wyzwaniami użytkownicy rozwiązań chmurowi się borykają. Są to:

- bezpieczeństwo - wskazuje na nie 85 procent użytkowników. Dotyczy to przede wszystkim właściwego korzystania z danych, aby nie narażać ich na cyberataki.
- brak dostatecznej wiedzy - 83 procent użytkowników ma problemów z korzystaniem z tego rozwiązania. Dotyczy to także procedur bezpieczeństwa.
- zarządzanie wydatkami związane z chmurą - 81 procent.
- zarządzanie - 77 procent. Problem stanowi fakt, że wiele firm nie posiada osoby, odpowiedzialnej za prawidłową współpracę z dostawcą rozwiązania chmurowego.

- zgodność - 76 procent - dotyczy to zarówno dopasowania do procedur firmowych, jak i zgodności z obowiązującymi przepisami w danym kraju.

- migracja - 73 procent użytkowników wskazuje problemy związane z procesem przeniesienia danych.

Z kolei Statista wskazuje na najważniejsze priorytety firm związane z bezpieczeństwem cloud computingu. Najwięcej, bo 51 procent użytkowników zwraca uwagę na prawidłową konfigurację rozwiązania. Wśród wskazywanych odpowiedzi znajduje się również obrona przez maleware, szkolenia z zakresu bezpieczeństwa czy zabezpieczenie zdalnego dostępu do danych.

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

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 Press Group
ul. Oławska 17 lok. 6 - III piętro
50-123 Wrocław
tel.: 71-302-75-35
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

Wykorzystane do raportu zdjęcia pochodzą z banku zdjęć Pixabay. pixabay