MARZEC 2022

EBOOK Z RAPORTEM interaktywnie.com

CYBER-BEZPIECZEŃSTWO

SPONSOR PLATYNOWY

Synology®

POD PATRONATEM

WP money.pl GAZETA.PL

SPIS TREŚCI

Wojna na Ukrainie wymusza inwestycje firm w cyberbezpieczeństwo

Od początku pandemii wiele firm zmagało się z rosnącą falą cyberataków, a po napaści Rosji na Ukrainę jest ich jeszcze więcej. Największy ich odsetek notowany jest wciąż w branży hotelarskiej - aż 56 procent badanych firm z tej branży zgłaszało tego typu problem. Na drugim miejscu zestawienia plasuje się sektor edukacyjny (50 procent), a w następnej kolejności firmy z branży usług finansowych (41 procent) i produkcji (38 procent). Również sektor publiczny zgłasza tego typu problemy - aż 31 procent badanych instytucji rządowych stwierdziło, że już w 2021 roku było w większym stopniu narażone na cyberataki.

Pora więc by zadbać o cyberbezpieczeństwo nawet małej czy średniej firmy.

Dobrze wiedzą to eksperci z przedsiębiorstwa Synology, którzy postanowili zaprezentować swoją wiedzę w tym raporcie.

Polecam zapoznanie się z ich wiedzą i ofertą.

Tomasz Bonek, prezes zarządu i redaktor naczelny Interaktywnie.com

Synology GmbH

Adres
Grafenberger Allee 295,
40237 Düsseldorf, Germany

Dane kontaktowe
E-mail: pl_marketing@synology.com, pl_sales@synology.com
Strona www: synology.com/pl-pl
Telefon: +49 211 9666 9634

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.

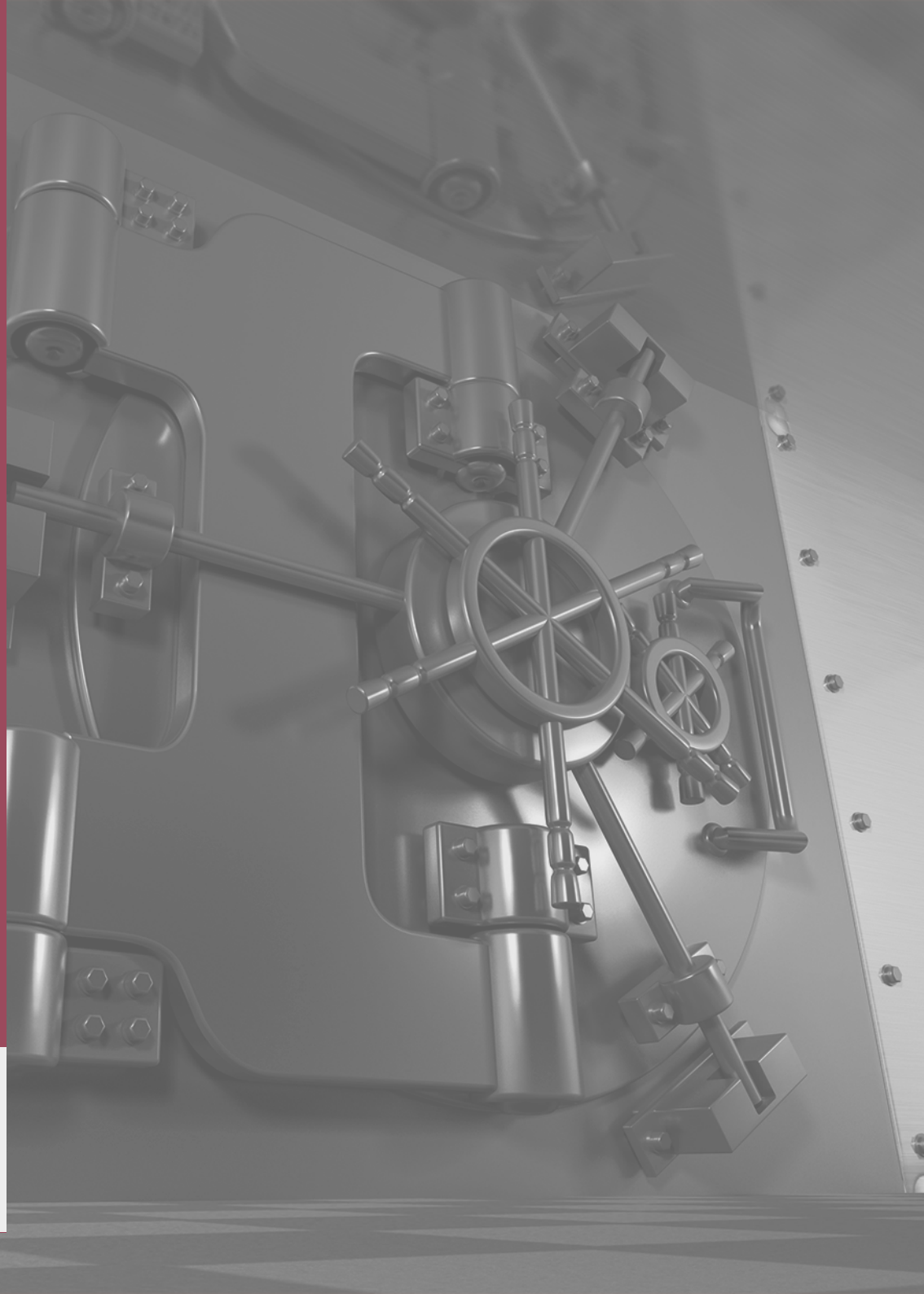
Trzeci raz z rzędu jesteśmy nagradzani przez Quality Control Leader jako najlepsze rozwiązanie NAS dla SMB w Polsce.

Wybrani klienci
PolAndRock, WOŚP, Idea Bank, UNESCO

ATAKI CYBERNETYCZNE NA FIRMY. CO IM GROZI?

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com



1

Kradzież danych, zablokowanie urządzenia czy uszkodzenie infrastruktury - to tylko niektóre z możliwych konsekwencji ataków cybernetycznych. Z badań nad różnego rodzaju zagrożeniami wynika, że średnio co druga firma na świecie była narażona na cyberataki, a straty z tego tytułu w zależności od regionu świata to średnio 4 mld dolarów. Sytuacji nie poprawiła pandemia COVID-19, która w ocenie 55 procent firm badanych przez KPMG, przyczyniła się do wzrostu zagrożenia ze strony hakerów. Chcąc chronić firmę przed zagrożeniem w sieci, należy zwrócić uwagę m.in. na ataki z grupy maleware, ransomware oraz phishing.

Z raportu "Cost of Cybercrime Study" autorstwa Accenture wynika, że 43 procent ataków hakerskich wymierzonych jest w małe firmy. Z kolei Cybersecurity Ventures wylicza, że do 2025 roku, koszty ponoszone przez firmy w związku z obroną oraz neutralizacją skutków cyberataków przekroczą 10,5 bln dolarów - to ponad 3-krotnie więcej niż miało jeszcze w 2015 roku. Warto zauważyć, że koszty, a także utrata ważnych i wrażliwych danych, to tylko niektóre z możliwych skutków ataków cybernetycznych. Mogą się one również wiązać z uszkodzeniem posiadanej infrastruktury.

Nawet 45 procent firm badanych przez Ponemon Institute jest zdania, że stosowane przez nie zabezpieczenia są niewystarczające, natomiast 66 procent doświadczyło cyberataku w ciągu ostatnich 12 miesięcy. Niepokojący jest również fakt, że 69 procent badanych przedsiębiorców ocenia ostatnie ataki za bardziej zaawansowane niż wcześniej, a do tego ukierunkowane na osiągnięcie określonego celu.

Liczba ataków rośnie

Złośliwe oprogramowanie określane jako malware to skrót pochodzący od słów "malicious software". Jego celem jest kradzież danych, uszkodzenie sprzętu lub dezorganizacja pracy użytkownika (osoby prywatnej lub firmy).

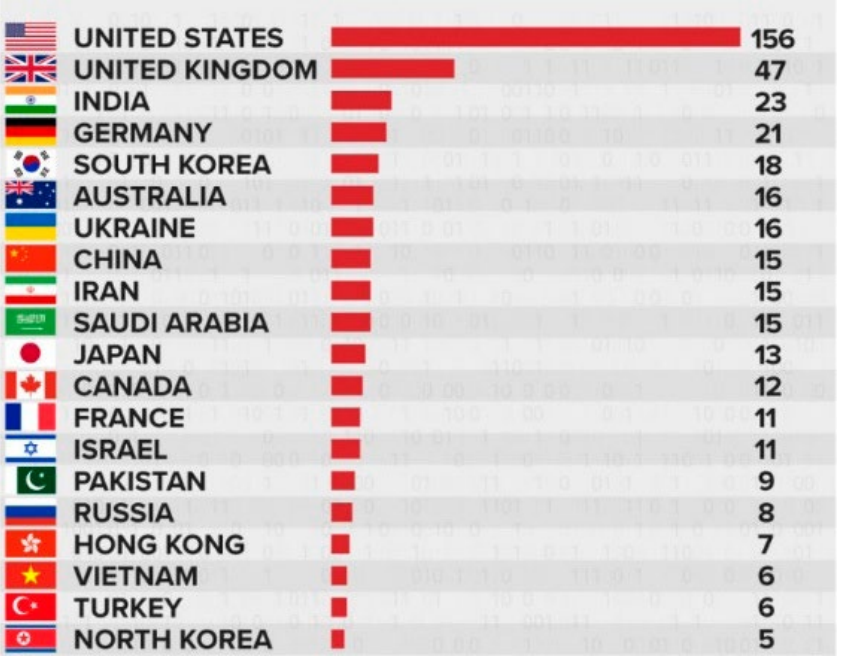
Jak wskazuje raport KPMG, ogólny charakter tego typu cyberataków sprawia, że firmy oceniają ten rodzaj zagrożenia jako jeden z najniebezpieczniejszych.

Atak cybernetyczny może również prowadzić do blokady urządzenia (komputera, smartfona, tabletu), uszkodzenia jego funkcjonalności, a także wprowadzenie takich zmian w całym ekosystemie firmy, aby kolejny atak był łatwiejszy. Jednym z celów malware może być również wyłudzenie okupu od osoby lub firmy poszkodowanej, która w ten sposób może odzyskać dane lub dostęp do urządzenia.

Według danych serwisu Purplesec, w latach 2009-2019 liczba ataków malware wzrosła 65-krotnie. Jeszcze w 2009 roku ich liczbę szacowano na 12,4 mln, natomiast dekadę później zanotowano ich już ponad 800 mln.

Z kolei, jak czytamy w raporcie Specops Software, krajami najbardziej narażonymi na cyberataki są Stany Zjednoczone i Wielka Brytania. Autorzy badania zwracają uwagę tutaj na incydenty istotne z punktu widzenia funkcjonowania państwa, jakie nastąpiły w przeciągu ostatnich 15 lat. Na najniższym miejscu podium uplasowały się Indie. W przypadku lidera tego zestawienia odnotowano 156 ataków, co na tle pozostałych krajów to dużo. Na liście znalazły się również takie kraje jak Niemcy, Ukraina, Chiny, Japonia, Izrael, Pakistan czy Rosja.

Liczba istotnych z punktu widzenia bezpieczeństwa kraju incydentów w latach 2006-2021



Źródło: Specops Software

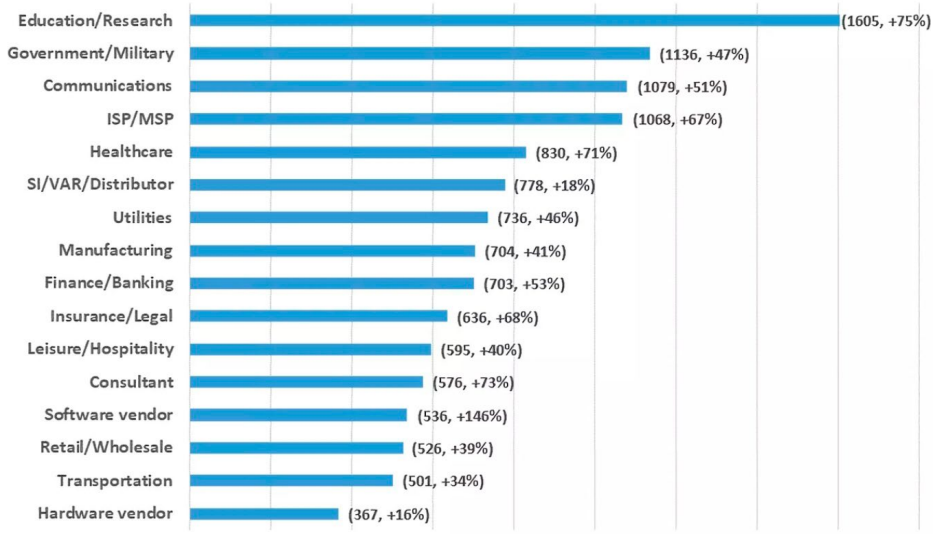
Jako przykład istotnego naruszenia bezpieczeństwa cybernetycznego należy wymienić ujawniony przez Narodową Agencję Bezpieczeństwa (NSA) błąd w popularnym serwisie pocztowym, pozwalający na kradzież danych milionów użytkowników. Z kolei w przypadku Wielkiej Brytanii można wymienić cyberataki na platformy brytyjskiej Partii Pracy podczas kampanii wyborczej w 2019 roku.

Synology®

Ochrona danych bez kosztów licencji dzięki Synology NAS!

Jakie firmy są najczęściej atakowane?

Branże najbardziej narażone na ataki cybernetyczne wraz z danymi o tygodniowej liczbie ataków



Źródło: Check Point Research

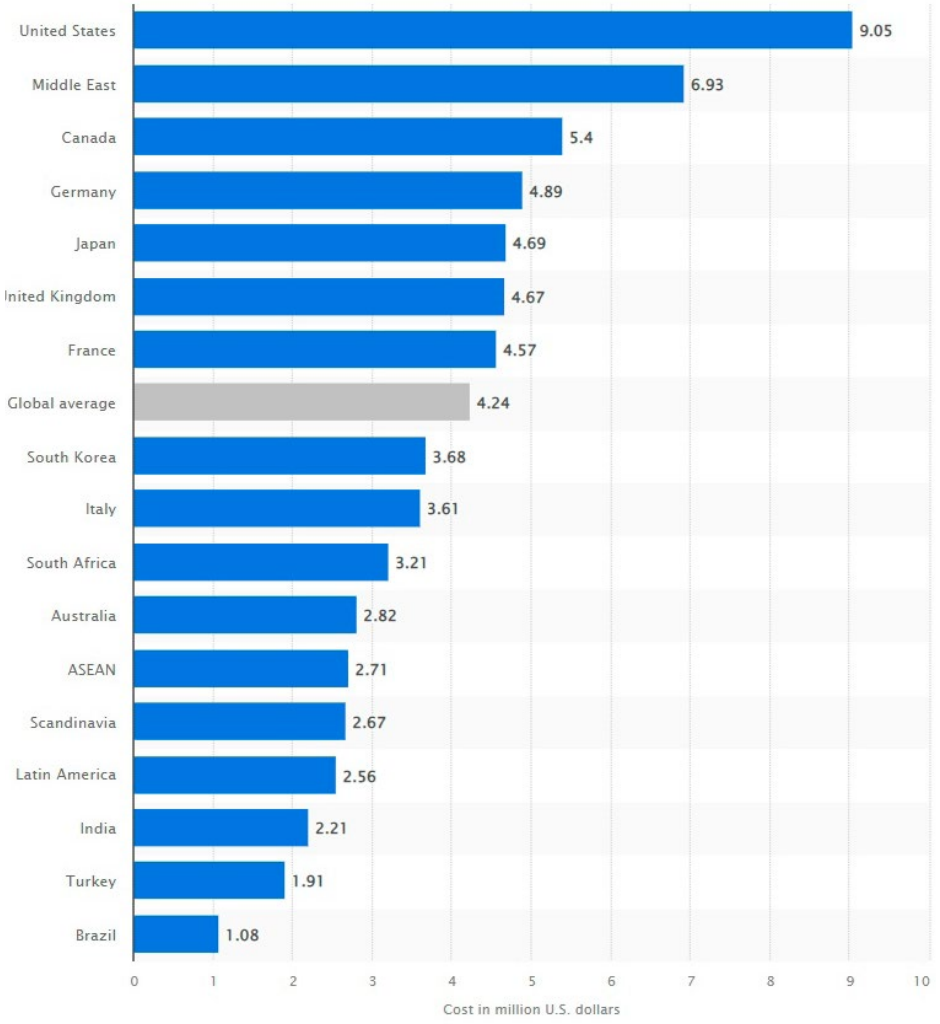
Według badania „2021 Security Outcomes Study" autorstwa Cisco, w ciągu ostatnich dwóch latach wiele firm zmagało się z rosnącą falą cyberataków. Autorzy raportu wskazują, że największy ich odsetek działał w branży hotelarskiej - aż 56 procent badanych firm tej branży zgłaszało tego typu problem. Na drugim miejscu zestawienia jest sektor edukacji (50 procent), a w następnej kolejności mamy firmy z branży usług finansowych (41 procent) i produkcji (38 procent). Również sektor publiczny zgłaszał tego typu problemy - łącznie 31 procent badanych instytucji rządowych stwierdziło, że w 2021 roku było w większym stopniu narażone na cyberataki. Z kolei 26 procent podmiotów świadczących usługi publiczne, również zgłaszało tego typu problem.

Dane dotyczące cyberataków w 2021 roku podsumowała również firma Check Point Research. Według jej raportu za najbardziej narażony na ataki hakerskie sektor uznano branżę edukacyjną i badawczą. W tym przypadku wskazano, że tygodniowo dochodziło aż do 1605 ataków. Na drugim miejscu są podmioty związane z bezpieczeństwem, militariami, a także agendy rządowe (1136 ataków miesięcznie). Ponad tysiąc ataków tygodniowo notowały także podmioty z branży telekomunikacyjnej.

Skala strat wywołanych cyberatakami

Według danych serwisu Statista, globalny koszt cyberataków w zależności od regionu świata w 2021 roku wyniósł średnio 4,24 mld dolarów. Największe straty cyberataki przyniosły amerykańskim firmom. Tam strata z tego tytułu to aż 9,05 mld dolarów. Wiceliderem pod tym względem jest Bliski Wschód z wynikiem 6,93 mld dolarów, a następna w kolejności jest Kanada, gdzie strata wynikająca z cyberataków to 5,4 mld dolarów. Z kolei średnio ponad 4 mld dolarów straty odnotowano w Niemczech, Japonii, Wielkiej Brytanii i Francji.

Koszt cyberataków w podziale na regiony i kraje



Źródło: Statista

Najpoważniejsze zagrożenia

Firma konsultingowa KPMG podzieliła zagrożenia ze strony hakerów, na które może być narażona organizacja na 12 kategorii. Wśród nich są:

- wyciek danych za pośrednictwem złośliwego oprogramowania
- wyłudzenie danych uwierzytelniających (phishing)
- ogólne kampanie ransomware
- wyciek danych w wyniku kradzieży lub zgubienia nośników lub urządzeń mobilnych
- kradzież danych przez pracowników
- podsłuchiwanie ruchu i ataki Man-in-the-Middle
- ataki typu odmowa usługi (DoS/DDos)
- kradzież danych na skutek naruszenia bezpieczeństwa fizycznego
- zaawansowane ukierunkowanie ataki
- ataki na sieci bezprzewodowe
- ataki wykorzystujące błędy w aplikacjach
- włamania do urządzeń mobilnych

Eksperci KPMG zwracają uwagę, że obecnie jednymi z najpoważniejszych zagrożeń są ataki typu malware, ransomware oraz phishing.

Ransomware

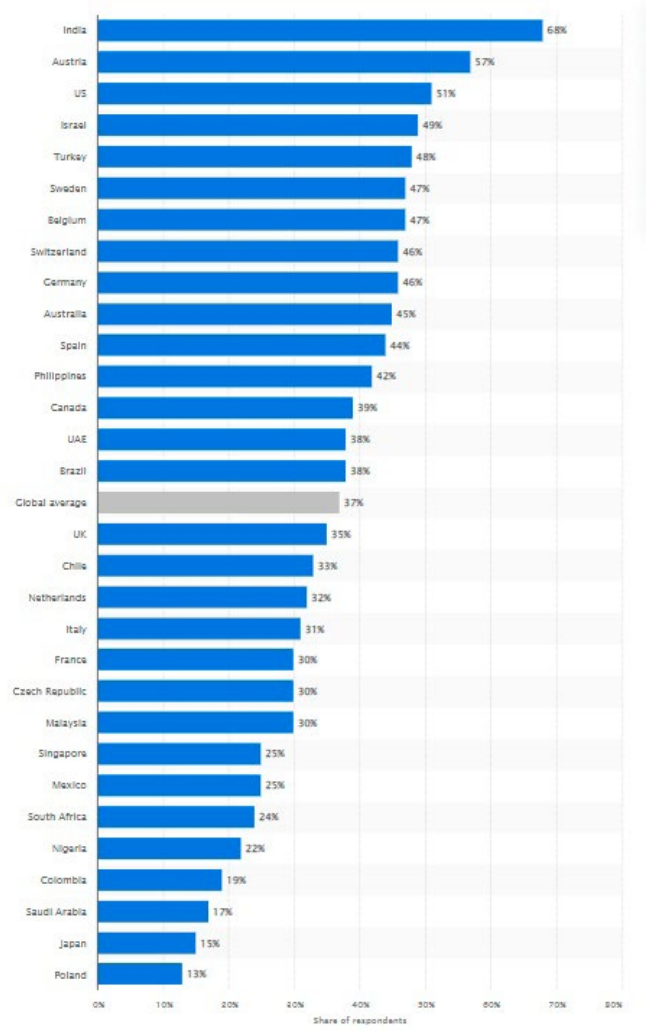
Jest to rodzaj ataku cybernetycznego polegający na zablokowaniu dostępu do plików bądź całego systemu komputerowego użytkownika lub firmy z żądaniem zapłaty okupu w zamian za jego odblokowanie.

Według serwisu Statista, nawet 37 procent organizacji na świecie padło ofiarą tego typu ataku. Najwyższy wskaźnik ataków ransomware zanotowały Indie, gdzie odsetek ten wynosi aż 68 procent. Ponad 50-procentowy wskaźnik notuje również Austria i Stany Zjednoczone. Polska w tym zestawieniu znajduje się na dole zestawienia z wynikiem na poziomie 13 procent.

COVID-19 i wojna na Ukrainie

Według raportu "Barometr Cyberbezpieczeństwa" autorstwa KPMG, dla 55 procent badanych firm wybuch pandemii COVID-19 przyczynił się do wzrostu ryzyka cyberataków. Z kolei 64 procent organizacji zmagało się z co najmniej jednym atakiem cybernetycznym w 2020 roku.

Odsetek firm, które doświadczyły ataku Ransomware w podziale na kraje

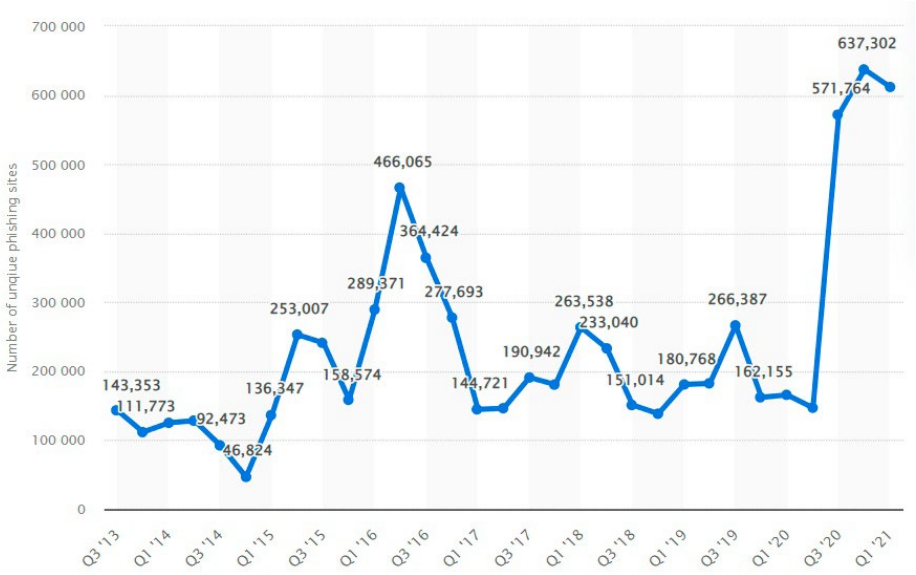


Źródło: Statista

Phishing

W tym przypadku haker podszywa się pod osobę lub instytucję, którą odbiorca darzy zaufaniem, celem wyłudzenia ważnych, wrażliwych danych lub informacji, takich jak login i hasło do konta, karty kredytowej czy skrzynki mailowej. Tego typu cyberatak jest o tyle niebezpieczny, gdyż nie wymaga od twórcy zaawansowanej wiedzy.

Kwartalna liczba ataków phishingowych na świecie w latach 2013-2021



Źródło: Statista

Eksperci firmy ESET przekazują kilka wskazówek, jak uniknąć oszukania i wesprzeć darowizną faktycznie istniejące organizacje.

- Należy sprawdzić historię i dokonania organizacji zanim przekażemy darowiznę.
- Pieniądze najlepiej przekazać za pośrednictwem oficjalnej strony internetowej lub innej formy oficjalnej komunikacji.
- Należy ignorować prośby o wsparcie, gdyż profesjonalne organizacje tego nie praktykują.
- Nie należy klikać linków oraz otwierać załączników zamieszczonych w mailach oraz w wiadomościach przesyłanych za pośrednictwem mediów społecznościowych.
- Z zasady należy podchodzić z nieufnością do przesyłanych wiadomości, nawet tych pochodzących zaufanych źródeł.
- Nie należy poddawać się presji.

Tylko w pierwszym kwartale 2021 roku wykryto prawie 640 tysięcy ataków phishingowych, co przekłada się na prawie 4-krotny wzrost względem analogicznego okresu 2020 roku.

Cyberprzestępcy podszywają się najczęściej pod bank, instytucje publiczne lub firmy kurierskie. Obecnie dodatkowym elementem

wykorzystywanym do tego typu ataków jest wojna na terytorium Ukrainy. Próby wyłudzenia danych lub bezpośrednio pieniędzy dotyczą prośby o bezpośrednią pomoc lub wsparcie organizacji charytatywnej. W rzeczywistości w takim przypadku ani pieniądze, ani inny rodzaj pomocy nie trafia do potrzebujących.

Podobne zasady wystrzegania się zagrożenia cybernetycznego będą skuteczne w przypadku różnych innych metod wyłudzeń phishingowych.

Słabość systemów bezpieczeństwa w firmach

Jak czytamy w raporcie KPMG dotyczącym cyberbezpieczeństwa, polskie firmy cały czas prezentują zbyt małą świadomość zagrożeń. Ryzyko ataku cybernetycznego dodatkowo wzrosło z uwagi na rozpowszechnienie się pracy zdalnej. Aż 83 procent firm, której pracownicy pracują z domu, wdrożyło rozwiązanie VPN. Mimo tego eksperci podkreślają, że najnowocześniejsze rozwiązania z zakresu bezpieczeństwa na nic się zdadzą, w przypadku braku odpowiednio wyszkolonego personelu.

Z kolei raport firmy Capgemini sugeruje, że wśród użytkowników często pomijane są takie elementy jak aktualizacja oprogramowania. Do tego powinno się zwracać uwagę na szkolenie pracowników pod kątem tego co wolno, a czego nie wolno otwierać zarówno poprzez pocztę firmową, służbową, jak i media społecznościowe. Do tego eksperci zwracają uwagę na konieczność stosowania podwójnego uwierzytelniania.

Wydatki na cyberbezpieczeństwo

Jak podaje serwis embroker, tempo wzrostu wydatków na cyberbezpieczeństwo będzie rosło o 12-15 procent rocznie. Okazuje się, że w latach 2017-2021 na ten cel wydano już ponad bilion dolarów.

Według ekspertów, największe fundusze z zakresu cyberbezpieczeństwa firmy przeznaczą na wynagrodzenia ekspertów z tej dziedziny. Pochłonie to blisko połowę kwoty, która w 2020 roku w skali globalnej wyniosła prawie 65 mld dolarów.

Następne w kolejności są wydatki na cloud computing, a zatem działania związane z przechowywaniem kluczowych danych w tzw. Chmurze.

Istotną pozycją są również wydatki sprzętowe mające na celu zabezpieczenie sieci, a także narzędzia związane z identyfikacją tożsamości użytkownika. Na oba elementy w 2020 roku wydano ponad 13 mld dolarów.

Wydatki będą dotyczyły również systemów zarządzania zabezpieczeniami, programów antywirusowych oraz bezpośredniej ochrony danych na dysku użytkownika.

ARTYKUŁ PROMOCYJNY

CHMURA I BACKUP DANYCH. DLACZEGO WARTO?

Przemysław Biel
Senior Key Account Manager Poland, Synology

2

Nie wiem, czy jest jeszcze ktoś, kogo trzeba przekonywać, iż kopie zapasowe to niezbędna rzecz w obecnych czasach, zarówno jeśli chodzi o dane firmowe jak i osobiste. Żyjemy w realiach cyfrowego społeczeństwa, gdzie codziennie przewija się mnóstwo danych. Bezpieczeństwo wiadomości pocztowych, plików multimedialnych, dokumentów, ale także całych procesów biznesowych, zależy od tego jak jesteśmy przygotowani na awarie, katastrofy, włamania czy najzwyklejszy błąd ludzki.

Ciągle jednak zdarzają się sytuacje, gdzie duża instytucja czy korporacja traci ogromne ilości danych lub dostęp do nich. Gdzie zatem tkwi problem?

Kopia zapasowa to jeden z wielu elementów całego systemu zabezpieczeń, które powinny być brane pod uwagę w firmach i instytucjach, jest on jednym z tych najważniejszych.

Potrzeby

Jednym z pierwszych kroków, który powinien być podjęty w budowie planu zabezpieczeń jest określenie potrzeb. Wydawałoby się to proste, jednak ogromna większość firm nie zdaje sobie sprawy, jak dużo danych jest przetwarzanych i przechowywanych przez ich organizację oraz jak bardzo tragiczne skutki może mieć brak dostępu do nich. Należy sobie zadać pytania, co by się stało, gdyby np.: przez parę dni firma nie mogła wystawiać faktur albo nie miała dostępu do poczty firmowej? Jak by to wpłynęło na produktywność i ostatecznie na zyski firmy?

Każda organizacja ma swą specyfikę, dlatego dla jednych, byłby to minimalne straty, dla innych ogromne, a w niektórych przypadkach, mogłyby doprowadzić do poważnych problemów. Aby zdefiniować łatwiej takie parametry, wymyślono dwa wskaźniki, które należy

rozpatrzyć: RPO (docelowy punkt odzyskiwania) oraz RTO (docelowy czas odzyskiwania). RPO (Recovery Point Objective) określa dopuszczalną ilość utraconych danych, natomiast RTO (Recovery Time Objective) definiuje jak szybko infrastruktura powinna zostać przywrócona do stanu sprzed awarii.

Mając określone te współczynniki, możemy się zabrać za dobór narzędzi i opracowanie planu zabezpieczeń.

Zasady podstawowe

Wybierając narzędzia czy platformę dla naszych kopii zapasowych nie powinniśmy popadać w skrajności oraz dobrać rozwiązanie tak, by jak najlepiej pasowało do specyfiki działalności. W większości przypadków podejście hybrydowe sprawdzi się najlepiej, czyli kopie lokalne w połączeniu z kopiami w zdalnych lokalizacjach.

Popularyzacja usług chmurowych, wytworzyła u niektórych błędne przeświadczenie, iż jeśli coś jest w chmurze to jest bezpieczne. Należy tutaj odróżnić pojęcia kopii zapasowej od synchronizacji i geo-redundancji. Pierwsza pozwala na przywrócenie danych z dowolnego punktu w czasie, druga utrzymuje zawsze aktualną wersję danych w chmurze, trzecia pozwala na dostęp do danych, nawet jeśli jedno z centrów danych jest niedostępne.

Nie można tych pojęć stosować zamiennie, można te metody jednak łączyć, tak aby podnieść efektywność naszego rozwiązania.

Na przykładzie rozwiązań Synology, można zbudować plan awaryjny dla firmy w bardzo prosty sposób.

Kopie zapasowe całego środowiska firmowego można wykonywać na serwer Synology NAS, tutaj jest dostępny pełen pakiet narzędzi począwszy od urządzeń końcowych (PC, Windows, Linux, Mac) po serwery i maszyny wirtualne. Dane na serwerze, należy także zabezpieczyć i w tym wypadku narzędzia są pod ręką. Kopie migawkowe i odpowiedni ich harmonogram, pozwalają na szybkie przywrócenie danych w przypadku niezamierzonego usunięcia danych, czy ich zaszyfrowania. Takie kopie także można replikować i należy to robić w razie możliwości na inny serwer.

Aby mieć kopię „na zewnątrz" można skorzystać z serwera Synology NAS w innej lokalizacji lub urządzenia zgodnego z protokołem rsync i tam robić okresowo kopię danych. Innym sposobem jest robienie kopii do chmury publicznej, na przykład Synology C2 (obsługa wielu platform jest zintegrowana w narzędziach serwera).

Bardzo istotne jest staranne zaplanowanie harmonogramów i retencji danych, tak aby zawsze mieć możliwość ich przywrócenia do stanu, na którym nam zależy, z okresu który nas interesuje.

Teoria kontra praktyka

W teorii wszystko wygląda prosto i przejrzyście, natomiast praktyka bywa różna i czasem, czy to w wyniku

ograniczeń budżetowych czy braku wiedzy, cały skrzętnie przygotowany plan kopii jest nieskuteczny.

Zrobienie kopii zapasowej to jest pierwszy etap całego procesu, aby mówić o jej skuteczności, ważne jest by była ona zweryfikowana. Na nic się nie przyda kopia, której nie można przywrócić, niestety wielu administratorów zapomina o tym kroku. Nowoczesne systemy kopii zapasowych pozwalają na automatyzację całego procesu.

Częstym błędem jest robienie kopii wszystkich danych do tej samej lokalizacji, a czasem nawet na to samo urządzenie, co nie ma totalnie sensu. W przypadku awarii takiego urządzenia, kopii brak, to samo tyczy się sytuacji awaryjnych typu pożar, powódź.

Innym błędem, z którym można się spotkać, to źle zaprojektowany harmonogram kopii i retencja danych, nakładające się daty, częstotliwość czy podobne okresy robienia kopii w kilku zadaniach powodują, iż taki plan jest nieskuteczny np.: w przypadku ataku ransomware.

Odpowiednie narzędzia i budżet

Aby zapewnić firmie bezpieczeństwo, należy dobrać narzędzia, które pozwolą na zabezpieczenie danych skutecznie, sprawnie i nie zrujnują budżetu w dłuższym okresie. Pieniądze niestety są najczęstszym powodem oporu wśród przedsiębiorców, przed dobrym planem kopii zapasowych.

Dla niektórych inwestycja większej kwoty na początek, tak aby mieć zapas na parę lat może być odstraszająca, więc mogą zacząć od usług chmurowych oferujących całościowy profesjonalny backup danych firmowych np.: Synology C2 Backup.

Jeśli ilości danych są bardzo duże, idące w dziesiątki terabajtów, obecnie serwer NAS i rozwiązania on-premise są dużo bardziej efektywne kosztowo w dłuższej perspektywie czasu. Tu niestety wielu dostawców oprogramowania do kopii licencjonuje swoje aplikacje na zasadzie subskrypcji lub ogranicza wsparcie do jakiegoś okresu, potem trzeba je wykupić ponownie. W przypadku rozwiązań Synology takich jak Active Backup Suite i innych narzędzi zawartych w rozwiązaniu NAS, nie ma opłat licencyjnych.

Ważnym aspektem, jest także to jak dane są przechowywane i jakie mają mechanizmy pozwalające na zapewnienie integralności tych danych oraz szybkie wykonywanie i odtwarzanie kopii. Tutaj przydaje się mechanizm globalnej deduplikacji, który w przypadku Synology działa na poziomie aplikacji, co umożliwia stosowanie go nawet na tańszych urządzeniach i oszczędzanie pieniędzy, nie tylko dzięki niższym

kosztom zakupu takiego rozwiązania, ale także dzięki temu, iż unikalne bloki danych są zapisywane na serwerze tylko raz.

Na rynku obecnie jest bardzo wielu producentów rozwiązań do kopii zapasowych, co dla odbiorców jest bardzo dobre, gdyż każdy może dobrać odpowiednie narzędzie dla siebie. Ważne jest by projektować plan zabezpieczeń, mając na uwadze dłuższą perspektywę czasu, jej koszty, nakłady na administrację i zarządzanie. Dobre rozwiązanie nie zawsze jest najdroższe i najbardziej skomplikowane. Wybierajmy mądrze z dbałością o bezpieczeństwoi budżet.

OBRONA PRZEDSIĘBIORSTWA PRZED CYBERATAKIEM. CO FIRMA POWINNA WDROŻYĆ: PROCEDURY, SOFTWARE, HARDWARE.

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

3

Cyfrowa transformacja, która obejmuje przedsiębiorstwa z każdego sektora - od usług finansowych przez handel detaliczny aż po sektor opieki zdrowotnej - pociąga za sobą konieczność zwiększenia inwestycji w bezpieczeństwo systemów informatycznych, czego świadome są jednak przede wszystkim większe przedsiębiorstwa. Małe i średnie firmy wciąż mają w tym zakresie wiele do zrobienia.

Ledwie przed chwilą Google za kwotę 5,4 mld dolarów przejął firmę Mandiant, zajmującą się cyberbezpieczeństwem. Dzięki tej akwizycji firma zyska więcej narzędzi do ochrony swoich klientów w chmurze. Przejęciem Mandianta zainteresowany był również Microsoft, ale w ostatniej chwili wycofał się z rozmów.

Mandiant został założony prawie dwie dekady temu przez Kevina Mandię, byłego oficera Sił Powietrznych Stanów Zjednoczonych i szybko zyskał, dzięki błyskawicznym usługom reagowania na incydenty, sporę renomę. I trudno się dziwić. Rok 2021 był rokiem, w którym po raz kolejny liczba naruszeń przebiła sufit. Wywołany pandemią exodus z rzeczywistych interakcji w kierunku ich cyfrowych odpowiedników zwiększył o kilka rzędów wielkości obszar, na którym mogą wystąpić problemy związane z bezpieczeństwem. W rezultacie naruszenia danych zaniepokoiły zarówno sektor publiczny, jak i prywatny, a żądania oprogramowania ransomware osiągnęły nowy poziom, stanowiąc egzystencjalne zagrożenie dla firm. A chodzi oczywiście o pieniądze.

Siedem na każde 10 naruszeń jest motywowanych chęcią zysku. Cybersecurity Ventures przewidział, że do 2021 r. co 11 sekund nastąpi atak ransomware na firmę, a artykuł w Newsweeku powołując się na badanie

Synology®

Zaprojektowane,

aby chronić Twoje dane.

100% własności danych, 0 zł za licencje!

Censuswide wykazał, że „80% firm, które zapłaciły po ataku ransomware, przeżyło drugi atak". Niektóre żądania ransomware ze strony cyber złodziei mają teraz podobno cenę 40 milionów dolarów i będą nadal rosły, ponieważ analizy kosztów i ryzyka wielu firm skłaniają je do płacenia. Według niektórych szacunków koszt oprogramowania ransomware na całym świecie przekroczy 265 miliardów dolarów do 2031 roku.

Na szczęście, wraz z bezczelnością cyberterrorystów, rośnie też świadomość osób decyzyjnych w firmach, które coraz śmielej i pewniej inwestują w zasieki mające ich chronić. Od czego powinni zacząć?

Program antywirusowy to za mało

Typowe oprogramowanie antywirusowe jest skuteczne w walce z większością znanych zagrożeń, ale kluczowe słowo to „większość". Istnieją bowiem nieznane im zagrożenia, przed którymi antywirus uchronić nas zwyczajnie nie może. Inżynierowie zajmujący się zwalczaniem złośliwego oprogramowania najpierw dowiadują się, jak działa dany wirus, a potem „instruują" oprogramowanie, jak go wykrywać i eliminować. To jednak oznacza, że - zanim ochrona antywirusowa zostanie odpowiednio dostosowana przez producentów zabezpieczeń zdąży on narobić sporo szkód.

A cyberprzestępcy stale udoskonalają swoje metody. Badanie przeprowadzone przez Bromium wykazało, że 4 z 5 stron internetowych, które udostępniają narzędzia do „wydobywania kryptowalut", to serwisy społecznościowe. Cyberprzestępcy stosują w tych witrynach takie taktyki, jak złośliwe aplikacje, reklamy, wtyczki i linki, aby nakłonić użytkowników do nieświadomego pobrania oprogramowania do wydobywania kryptowalut na swoje urządzenie.

Tradycyjne rozwiązania antywirusowe nie mogą też chronić danych trzymanych w chmurze, a to z nich coraz częściej korzystają przedsiębiorstwa. Jak zatem mogą one zwiększyć bezpieczeństwo?

W przeszłości można było to robić unikając podejrzanych linków i złośliwych stron internetowych, ale dzisiaj zwykła strona internetowa albo reklama mogą być źródłem złośliwego oprogramowania. Ataki wykorzystujące złośliwe reklamy są bowiem bardzo różnorodne i mogą wykorzystywać legalne, ale zhakowane witryny internetowe, wprowadzające w błąd podpowiedzi skłaniające do wyrażenia zgody lub po prostu działać w tle.

Zagrożenia związane z bezpieczeństwem zwiększyły się jeszcze bardziej w czasach powszechnej pracy hybrydowej, kiedy telefony komórkowe, laptopy i inne urządzenia, czasem również prywatne, są używane do celów zawodowych. Dzisiaj stare powiedzenie, że „ludzie są najsłabszym ogniwem" w każdym programie cyberbezpieczeństwa, jest prawdziwsze niż kiedykolwiek. Szkolenie pracowników powinno więc być główną linią obrony.

Cyberprzestępcy żerują bowiem na pracownikach zdalnych. Ankieta Tessian wykazała, że 88 procent naruszeń danych było spowodowanych właśnie błędami ludzkimi. W hybrydowym środowisku pracy pracownicy w mniejszym stopniu zwracają uwagę na zasady bezpieczeństwa albo po prostu częściej popełniają błędy zmuszeni poruszać się w półprywatnej przestrzeni.

Pracownicy powinni więc być zapoznani z obowiązującą polityką bezpieczeństwa, a także regularnie aktualizować wiedzę np. w ramach cyklicznych szkoleń czy warsztatów. Informacje na temat największych zagrożeń i ich potencjalnych skutków powinny być powtarzane tak, żeby stały się częścią biurowej rzeczywistości, a nie kolejnym abstrakcyjnym wymysłem HR-u. Bez inwestycji w edukację pracowników, inwestycja w systemy IT nie przyniesie spodziewanych korzyści. Nie można jednak zaniedbywać ani jednego, ani drugiego, a wszelkie działania warto poprzedzić konsultacjami.

Dlaczego urządzenia IoT to potencjalne ryzyko ataku?

Dodatkowym potencjalnym źródłem ataku mogą być także coraz powszechniejsze inteligentne urządzenia. Internet Rzeczy (IoT) opiera się na różnorakich czujnikach, które gromadzą, komunikują się, analizują i działają na zdobytych informacjach. Dzięki temu oferują nowe sposoby tworzenia wartości dla firm, ale też stwarzają nowe możliwości narażenia wszystkich tych informacji na szwank. A nie tylko więcej danych jest udostępnianych za pośrednictwem IoT, wśród znacznie większej liczby uczestników, udostępniane są także dane coraz bardziej wrażliwe. W rezultacie ryzyko jest wykładniczo większe.

Szeroka gama podłączanych urządzeń, między innymi telewizory, termostaty, zamki do drzwi, alarmy, koncentratory inteligentnego domu, otwieracze drzwi garażowych, tworzy bowiem niezliczone punkty połączeń, dzięki którym hakerzy mogą uzyskać dostęp do ekosystemów IoT, a tym samym dostęp do informacji o klientach, a nawet możliwość przeniknięcia do systemów zaplecza producentów.

Wiele firm technologicznych, medialnych i telekomunikacyjnych już zmaga się z tymi wyzwaniami związanymi z cyber ryzykiem. Z jednej strony jest to kwestia pewnej niedojrzałości rynku, który jest w fazie, w której cyberbezpieczeństwo nie jest uważane za priorytet, z drugiej to tu właśnie jest problem. Troska o bezpieczeństwo projektu IoT w momencie, gdy projekt został już wdrożony, właściwie uniemożliwia poprawne wykonanie go. A dodatkowo problemem jest również złożoność zarządzania rozproszonym, zdalnym i niezwykle heterogenicznym środowiskiem IoT.

Cyberryzyka związane z IoT należy więc oceniać na każdym poziomie organizacji - od stanu przed zagrożeniem po zdarzenie

- a systemy zabezpieczeń powinny koncentrować się na przewidywaniu i zapobieganiu, a także na możliwie najszybszym przywróceniu normalnego działania. Niezbędne jest również ciągłe monitorowanie każdego urządzenia IoT – albo poprzez audyty bezpieczeństwa, albo poprzez wykorzystanie rozwiązań do oceny bezpieczeństwa w celu znalezienia luk w zabezpieczeniach, zidentyfikowania podejrzanych zachowań i zapewnienia, że ryzyko pozostaje na akceptowalnym poziomie.

Jednym ze sposobów osiągnięcia tego celu jest ustalenie poziomu „normalnej" aktywności danych, a następnie monitorowanie ewentualnych odchyleń od tej normy. Może to pomóc w identyfikacji wszelkich odchyleń lub nietypowych zachowań, które można następnie przejrzeć w celu wyeliminowania zagrożeń związanych z danymi.

ARTYKUŁ PROMOCYJNY

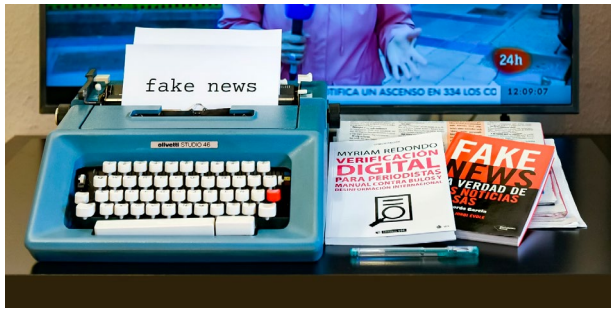
DEZINFORMACJA NA WYCIĄGNIĘCIE RĘKI

Michał Wąsowski
Zastępca redaktora naczelnego Money.pl

4

Od kilku lat, a od kilku tygodni szczególnie, hasło "fake news" jest odmieniane przez wszystkie przypadki. Fake news dotyczące najpierw pandemii i szczepionek, teraz **fake news** dotyczące wojny. Nic dziwnego - internet, szczególnie media społecznościowe, są od lat pełne kłamstw i fałszywych informacji, ale w ostatnich latach zjawisko dezinformacji nabrało na sile. I paradoksalnie, jawnie fałszywe informacje są w nim jednym z mniejszych problemów.

Dezinformacja to dzisiaj zjawisko dużo szersze niż fake news. Problemem nie są bowiem kłamliwe newsy, fałszywe informacje - choć jest ich dużo, największym zagrożeniem dezinformacyjnym są dzisiaj manipulacje i propaganda. Z prostego powodu: zwykle wykorzystują one ziarno prawdy, które sprawia, że ludzie wierzą lub przynajmniej zaczynają pewne rzeczy kwestionować.



https://unsplash.com/photos/34zq7tzqRSw

O ile jednak mechanizmy tworzenia się dezinformacji czy tworzenia propagandy są znane i rozmawia się o nich - szczególnie ostatnio - sporo, to kwestią mniej poruszaną jest to, dlaczego tak trudno jest zwalczać dezinformację. Bo choć dysponujemy ogromną i coraz większą wiedzą, choć dysponujemy licznymi narzędziami, to walka z manipulacjami jest trudniejsza niż kiedykolwiek wcześniej.

Dlaczego? W zasadzie wszelkie przyczyny takiego stanu rzeczy wynikają z rozwoju technologii i idącej za tym skali komunikacji. Same mechanizmy manipulacji ludźmi, informacjami, siania dezinformacji czy propagandy, są nam znane od lat. Fundamentalnie nie ulegają one zmianom

- opierają się o te same schematy. Obecna rosyjska propaganda, dotycząca wojny w Ukrainie, nie różni się zbytnio na poziomie fundamentów i mechanizmów od tej szerzonej np. za czasów ZSRR. Zmieniło się jednak otoczenie i forma realizacji tej propagandy.

aleks-marinkovic-nSb50DF_ML0-unsplash

Zmiana ta wynika właśnie z technologii. Internet i strony internetowe, następnie blogi, aż do obecnie mediów społecznościowych i smartfonów. Na każdym z tych etapów rosła skala komunikacji między ludźmi. W efekcie dzisiaj zarówno informacja, jak i dezinformacja są na wyciągnięcie ręki.

Wystarczy włączyć smartfon i jakikolwiek komunikator, aplikację społecznościową - od ręki znajdziemy tam przykłady kłamliwych narracji, fake news, manipulacji. I często nie są to nawet świadomie ani intencjonalne działania, a jedynie powtarzanie zasłyszanych opinii czy półprawd, które nasz mózg akurat uznał za wygodne do uwierzenia.

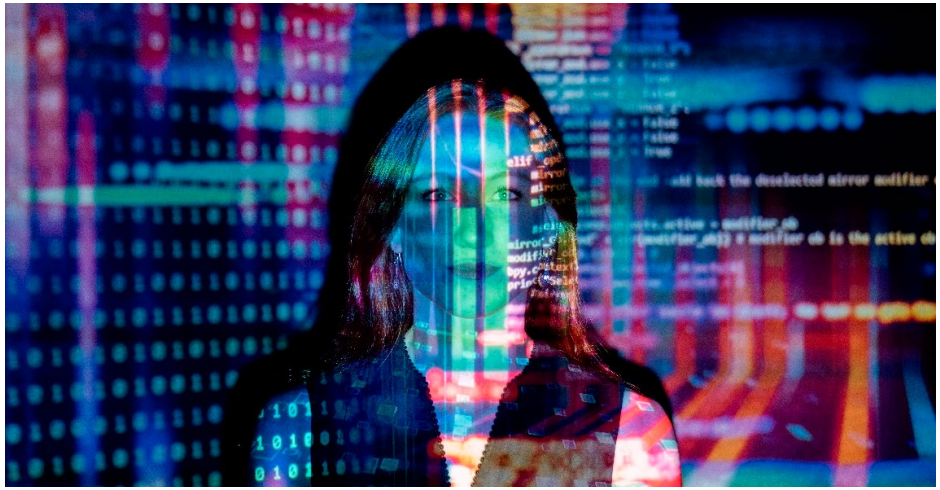
Informacje rozchodzą się po świecie tak szybko, jak nigdy i na niespotykaną wcześniej skalę. I to właśnie powoduje, że walka z dezinformacją jest tak trudna. Skala oraz tempo rozchodzenia się informacji - fałszywych i prawdziwych - jest dziś prawdziwie "wiralowe". Według danych Instytutu Badań Internetu i Mediów Społecznościowych, 3 marca odnotowano wzrost incydentów dezinformacyjnych o... 20 tys. proc. Tylko w ciągu 24h pojawiło się wówczas 120 tys. wpisów dezinformujących w temacie wojny w Ukrainie. Gros tych incydentów dotyczyło mediów społecznościowych - 69 proc. z nich znalazło się na Facebooku, a 24 proc. na Twitterze. Tylko 8 proc. tych działań odbyło się na tradycyjnych portalach internetowych.

Co jednak istotne, według IBiMS większość profili, które szerzyły wówczas prorosyjską propagandę dotyczącą wojny, wcześniej była aktywna w temacie pandemii i szczepionek - oczywiście, prezentując narrację antyszczepionkową. Tym samym, po wybuchu wojny w Ukrainie, zdecydowanie przycichła w sieci propaganda antyszczepionkowa, a zastąpiła ją narracja prorosyjska i antyukraińska.

IBiMS niemal co dnia dostarcza kolejnych danych dotyczących skali dezinformacji odnośnie wojny w Ukrainie. Instytut podał 15 marca, iż w ciągu doby zawieszono lub zlikwidowano cztery „gniazda" dezinformacyjne, skupiające ok. 3 tys. kont. Z danych dziennych, pokazywanych przez Instytut, wynika, że każdej doby dochodzi nawet do kilkunastu tysięcy incydentów dezinformacyjnych. W pierwszych dniach wojny najniższy poziom odnotowano 5 marca: 10 tysięcy. To pokazuje skalę problemu, z którym muszą zmierzyć się demokratyczne społeczeństwa.

Trzeba jedna odnotować, że dezinformacja za pomocą trolli i botów nie pojawiła się w czasie pandemii, a niektóre kraje - Rosja, Chiny czy Iran - wykorzystują te techniki od lat. Już w 2018 r. Twitter udostępnił badaczom ponad 10 milionów tweetów, wygenerowanych przez 4600 kont powiązanych z irańską i rosyjską propagandą. Problem ten dotyczy zarówno wielkich państw, jak i tych najmniejszych – jak np. Mjanmy, gdzie Facebook był wykorzystywany do szerzenia propagandy dotyczącej ludu Rohingja.

Skala ta sprawia, że dzisiaj kłamstwo powtórzone kilka razy nawet przez anonimowe boty, za pomocą sieci powiązań, może szybko przesiąknąć do mainstreamu. A kłamstwo powtórzone przez wpływowe osoby szybko staje się kłamstwem powtarzanym w tysiącach domów. Obalenie fałszywych narracji niewiele daje, bo… zwykle prawdziwa informacja czy sprostowanie zwyczajnie nie cieszą się już takim samym zainteresowaniem.



pexels-thisisengineering-3861969

Jeszcze trudniej jest walczyć z manipulacjami, które zawierają np. ziarno prawdy - a właśnie w ten sposób działała chociażby propaganda antyszczepionkowa. Dlatego w gruncie rzeczy mniej ważna jest sama walka z dezinformacją niż edukacja w zakresie tego, jak dezinformacja i manipulację działają. Walka z dezinformacją zawsze będzie bowiem poniekąd walką z wiatrakami i walką z hydrą - możemy w niej tylko ograniczać szkody dokonywane przez manipulantów, trudno jest liczyć obecnie na pełną wygraną. Edukując jednak zarówno najmłodszych, jak i osoby starsze, możemy sprawić, że przynajmniej część z nas - a może kiedyś i większość społeczeństwa - stanie się odporna na manipulacje. I do tego, w pierwszej kolejności, powinniśmy dążyć, ale jednocześnie nie ustając w walce z dezinformacją.

JAK ZABEZPIECZYĆ DANE FIRMOWE?

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

5

Niespełna 370 mld dolarów była warta globalna branża usług cloud computingu w 2021 roku. W Polsce poziom zastosowania tego typu usług nadal jest stosunkowo niewielki, jednakże plany ich wdrożenia deklaruje 35 procent firm. Za zastosowaniem cloud computingu, a także tworzeniem kopii zapasowych (tzw. backup) przemawia nie tylko bezpieczeństwo, ale także efektywność, elastyczność, mobilność tego typu rozwiązań, a także często generowane przez nie oszczędności kosztowe.

Rozwiązania chmurowe, czyli tzw. cloud computing to rodzaj usługi, w której dane użytkownika przechowywane są na serwerach zewnętrznej firmy. Usługodawca jednak nie tylko udziela dostępu do przestrzeni dyskowej, ale także do odpowiednich narzędzi związanych ze świadczeniem danej usługi. W zależności od potrzeb mogą tam być przechowywane dane, a także multimedia takie jak zdjęcia czy filmy. Dostęp do danych odbywa się za pomocą łączy internetowych.

Jak podaje serwis grandviewsearch, wartość globalnego rynku cloud computingu w 2021 roku wyniosła 368,97 mld dolarów. Według szacunków, wydatki te będą rosnąć do 2030 roku w średniorocznym tempie 15,7 procent. Eksperci prognozują również, że rozwój technologii w zakresie sztucznej inteligencji oraz uczenia maszynowego będzie dodatkowym impulsem w rozwoju tej branży. Z kolei w ostatnich latach do rozwoju tego rynku przyczyniła się pośrednio pandemia koronawiursa, która wymusiła przeniesienie wielu codziennych czynności do internetu.

Największym rynkiem rozwiązań chmurowych są Stany Zjednoczone. W 2021 roku wydatki firm z nimi związane wyniosły 135 mld dolarów, co stanowi jedną trzecią globalnych wydatków na ten cel. Prognoza granviewsearch

NASZE DANE SĄ CENNE. CZY SĄ BEZPIECZNE?

Backup jest jednym z kluczowych elementów zabezpieczeń środowiska IT. Zdarza się, że umieszczany jest niżej na liście priorytetów. W rezultacie firmy często płacą za to wysoką cenę. Istnieją jednak gotowe rozwiązania pozwalające na jego proste i szybkie wdrożenie.

Jedną z ważnych decyzji dotyczących kopii zapasowej jest jej lokalizacja. Kierując się zasadą 3-2-1, nie powinniśmy polegać tylko na jednej kopii, ani opierać backupu na jednej lokalizacji. Coraz więcej usług jest przez nas lokowanych w chmurze. Ma to wiele zalet, np. odciążenie lokalnej infrastruktury, redukcja kosztów, a także skalowalność. Z drugiej strony mamy szeroki wybór urządzeń instalowanych lokalnie. Ich obsługa nie musi być wymagająca. Serwer NAS może stać się kluczowym, lokalnym elementem naszego backupu, oferując przy tym niezliczoną ilość dodatkowych usług.

Podział obowiązków

Czy chcąc osiągnąć powyższą równowagę, musimy decydować się na wielu dostawców i naukę różnych technologii? Wprost przeciwnie, kompletne rozwiązanie może dostarczyć nam jeden producent. Serwer Synology NAS umożliwia stworzenie prywatnej chmury za pomocą Synology Drive – aplikacji, w której użytkownicy mogą synchronizować i udostępniać dane, a także tworzyć ich kopię. Obsługa wielu wersji pozwala na cofnięcie czasu i odzyskanie utraconych informacji. Dane można synchronizować do wielu lokalizacji, pomiędzy komputerami oraz serwerami NAS.

Co w przypadku potrzeby zabezpieczenia większego środowiska IT? Dla większości modeli Synology NAS dostępne jest w pełni bezpłatne narzędzie Active Backup Suite. Centralnie zarządzane, pozwalające na backup komputerów, serwerów fizycznych, serwerów plików oraz maszyn wirtualnych Hyper-V i VMware. Pełny obraz dysku pozwala na przywrócenie wybranych plików i folderów, a także całego systemu w trybie bare-metal. W sytuacjach krytycznych pozwala także na uruchomienie backupu w formie maszyny wirtualnej. Wkrótce pojawi się opcja backupu całego systemu Synology DSM.

Ile przestrzeni potrzebujemy? Funkcja deduplikacji pozwala na zredukowanie potrzeb do minimum. Kopia przyrostowa skróci czas wykonywania backupu, a szyfrowanie kluczem AES-256 zwiększy bezpieczeństwo. Backup może być wyzwolony harmonogramem oraz zdarzeniami, np. po wylogowaniu.

Powyższe rozwiązanie chroni też usługi chmurowe Microsoft 365 i Google Workspace. Czy jest to potrzebne? Szeroko opisywane przypadki niedostępności popularnych usług nie powinny pozostawiać żadnych złudzeń.

Mam backup lokalny. Co dalej?

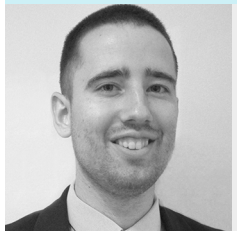
Zamiast kalkulować ryzyko, powinniśmy zadbać o redundancję naszych danych. Nieważne, czy dane mają trafić na inny serwer, czy do chmury publicznej, zajmie się tym aplikacja Hyper Backup. Okresowo sprawdzi również, czy backup wykonał się poprawnie.

Synology udostępnia także szeroki zakres usług chmurowych. Bezpieczną przestrzeń dla backupu zapewni usługa C2 Storage. Jednym z jej atutów jest opcja chmury hybrydowej. Serwer Synology zamienimy w lokalny bufor przestrzeni w chmurze. Backup komputerów możemy wysyłać do chmury także bezpośrednio, dzięki Synology C2 Backup.

Niezależnie od lokalizacji danych i wykorzystywanych usług, Synology spełnia wyśrubowane normy bezpieczeństwa, tak ważne w dzisiejszych czasach. Dodatkowo otrzymujemy kompletne rozwiązanie od jednego producenta: serwer NAS, usługi w chmurze, oprogramowanie, a opcjonalnie także dyski.

Tak stworzony ekosystem infrastruktury IT przynosi szereg korzyści, na czele z ułatwionym wsparciem i łatwością wdrożenia, a przede wszystkim ciągłością pracy firmy.

Synology oferuje dla firm możliwość bezpłatnego wypożyczenia serwerów w celu testowania rozwiązania we własnym środowisku. W przypadku chęci przetestowania, zapraszamy do kontaktu: pl_sales@synology.com

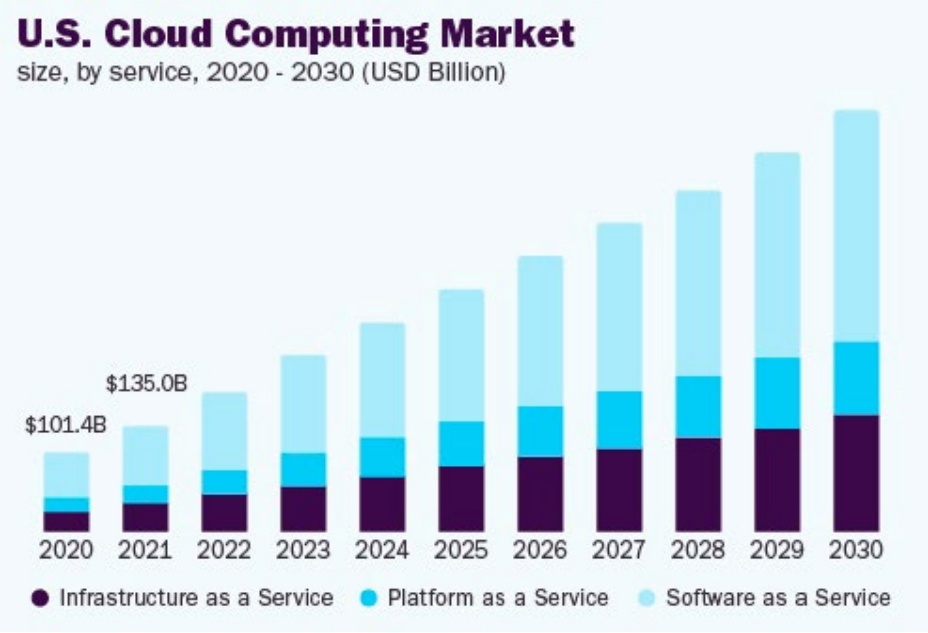


Tomasz Iwańczuk
Synology Solution Engineer

Synology®

pokazuje te dane w podziale na oprogramowanie "Infrastructure as a Sevice", "Platform as a Service", oraz "Software as a Service" przy prognozowanym średniorocznym wzroście na poziomie 14,8 procent aż do 2030 roku.

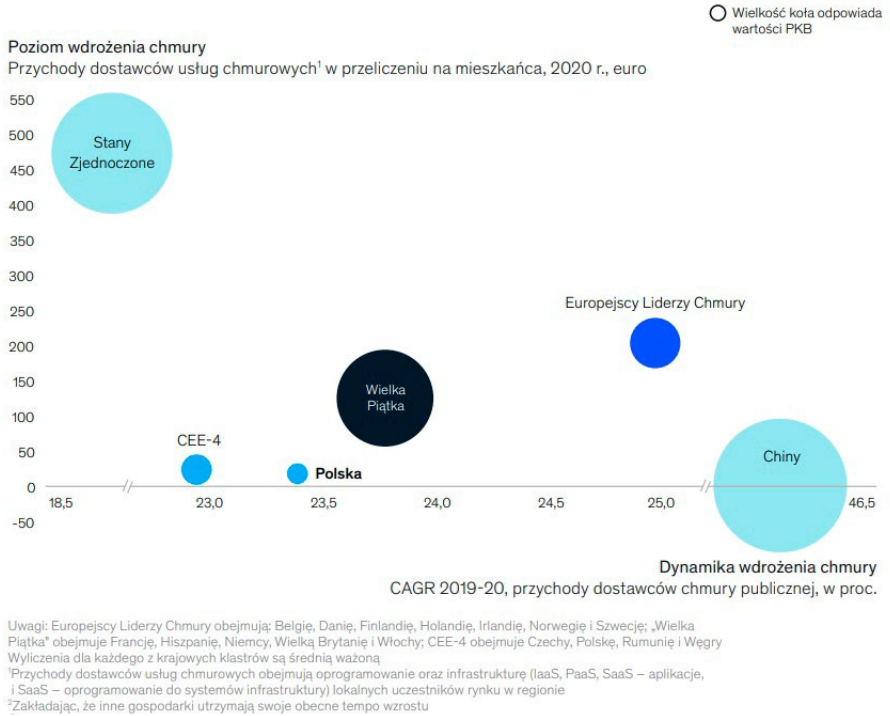
Amerykański rynek cloud computingu w latach 2020-2030



Źródło: grandviewresearch

W Polsce jak szacuje serwis Equinix, plany przejścia posiadanego systemu do tzw. "chmury" ma 35 procent firm. Rosnącą popularność rozwiązań chmurowych potwierdza fakt, iż 70 procent osób odpowiedzialnych za infrastrukturę IT w firmach jest zdania, że rozwiązania chmurowe niedługo staną się kluczową inwestycją. Oprócz tego 85 procent osób na tym stanowisku podkreśla znaczenie bezpieczeństwa w kwestii cloud computingu.

Rozwój rynku rozwiązań chmurowych w podziale na kraje i regiony świata

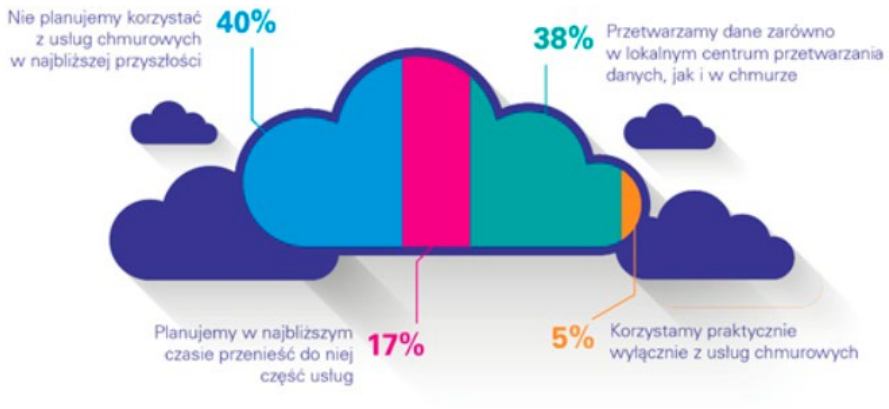


Uwagi: Europejscy Liderzy Chmury obejmują: Belgię, Danię, Finlandię, Holandię, Irlandię, Norwegię i Szwecję; „Wielka Piątka" obejmuje Francję, Hiszpanię, Niemcy, Wielką Brytanię i Włochy; CEE-4 obejmuje Czechy, Polskę, Rumunię i Węgry
Wyliczenia dla każdego z krajowych klastrów są średnią ważoną
[1]Przychody dostawców usług chmurowych obejmują oprogramowanie oraz infrastrukturę (IaaS, PaaS, SaaS – aplikacje, i SaaS – oprogramowanie do systemów infrastruktury) lokalnych uczestników rynku w regionie
[2]Zakładając, że inne gospodarki utrzymają swoje obecne tempo wzrostu

Źródło: McKinsey, OECD,Komisja Europejska, IDC

Nadal jednak wśród polskich firm rozwiązania z zakresu cloud computingu występują stosunkowo rzadko. Poziom ich wdrożenia zbadała firma McKinsey, według której, aby Polska mogła pod tym względem dorównać europejskim liderom, musiałaby się w tym zakresie do roku 2030 rozwijać w tempie około 50-60 procent rocznie.

Korzystanie z rozwiązań chmurowych w Polsce



Źródło: KPMG "Barometr bezpieczeństwa"

Wśród polskich przedsiębiorców aż 40 procent deklaruje, że w najbliższej przyszłości nie będzie korzystało z usług chmurowych. Jak czytamy w raporcie KPMG, niewiele mniej korzysta jednocześnie z rozwiązania lokalnego i chmurowego, a 17 procent zamierza w najbliższym czasie przenieść do chmury część swoich usług.

Strategie chmurowe

Badając temat rozwiązań chmurowych warto zwrócić uwagę na strategie chmurowe, takie jak cloud backup, multi-cloud oraz cloud-native.

Cloud Backup - jest to narzędzie do wykonywania kopii bezpieczeństwa na serwerach zewnętrznych, należących np. do dostawcy hostingowego. Tworzenie kopii zapasowej następuje automatycznie i jest wykonywane co pewien czas, dzięki czemu rozwiązanie to poprawia bezpieczeństwo danego podmiotu. Sposób tworzenia oraz częstotliwość wymaga często początkowej konfiguracji.

Multi-Cloud - rozwiązanie nie bazujące wyłącznie na jednej chmurze obliczeniowej, a na kilku. Firma działająca w ramach tej strategii ma podpisaną umowę z co najmniej dwoma dostawcami tego typu usług, a każdy z nich ma przypisaną swoją odrębną funkcję. Przykładowo jeden może się zajmować analizowaniem, drugi przetwarzaniem, a trzeci wykonywaniem kopii zapasowych.

Cloud-Native - jest to trzecia również innowacyjna forma zastosowania chmury. Rozwiązanie opiera się na tworzeniu firmowego systemu w ramach chmury, ale zbudowanego z kilku mniejszych i niezależnych od siebie elementów. Dzięki temu, można je przenosić pomiędzy systemami chmurowymi, co stanowi dla firmy dodatkowy element bezpieczeństwa.

Zastosowanie systemów chmurowych w Polsce

Rozwiązania chmurowe możemy podzielić na kilka podstawowych kategorii.

IaaS, czyli z ang. Infrastructure as a Service, w ramach którego klient otrzymuje cały potrzebny sprzęt.

PaaS, czyli z ang. Platform as a Service, gdzie klient w ramach usługi chmurowej nabywa dostęp do środowiska pracy w postaci dedykowanej platformy.

SaaS, czyli z ang. Software as a Service, w ramach której klient otrzymuje nie tylko platformę, ale również zestaw aplikacji dostępnych za pośrednictwem internetu przy pomocy specjalnego panelu. Nie musi on również instalować otrzymanych programów, ani nabywanać licencji. Jedynce co robi, to ponosi opłatę za użytkowanie systemu.

Z badania firmy McKinsey oraz danych Eurosatu wynika, że systemów SaaS firmy najczęściej używają do prowadzenia poczty firmowej, gromadzenia danych na potrzeby prowadzenia biura, a także korzystania z oprogramowania ERP oraz CRM. W przypadku IaaS zwrócono uwagę na kwestię przechowywania plików oraz udostępniania mocy obliczeniowej. Z kolei przy PaaS, dominującym elementem jest hosting baz danych.

Zalety i wady rozwiązań chmurowych

Bezpieczeństwo to jedna z najważniejszych zalet rozwiązań chmurowych. Według danych KPMG, dwie trzecie firm, które stosują tego typu rozwiązanie uważa, że pozytywnie wpłynęło ono na poziom ich zabezpieczenia przed cyberatakami.

Oszczędności kosztowe dotyczy zarówno potrzebnej infrastruktury, jak i zatrudniania do jej obsługi odpowiednio wyszkolonych specjalistów.

Duża liczba rozwiązań chmurowych oraz konkurencja na tym rynku sprawia, że dostępność tego typu usług jest wysoka.

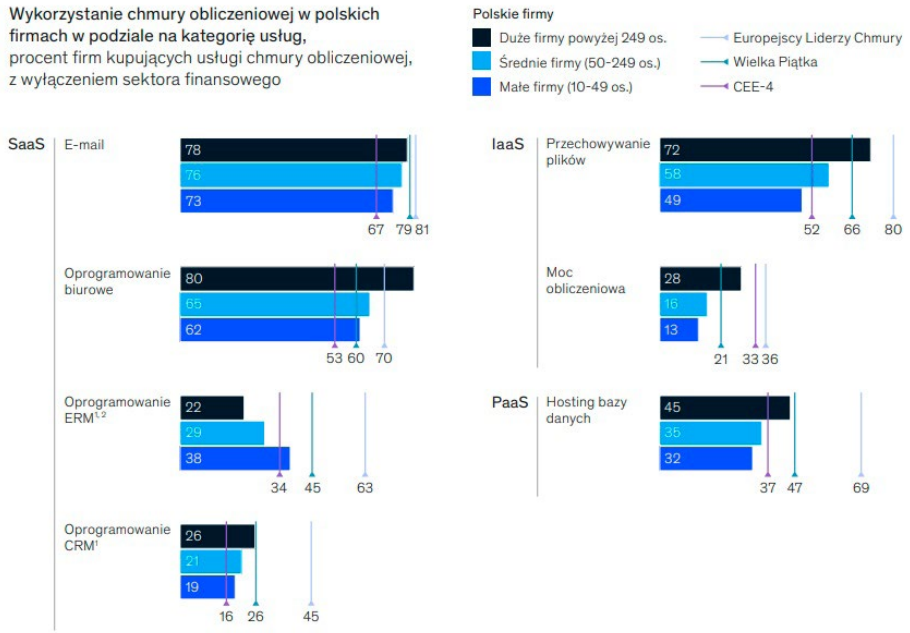
Powierzenie przechowywania danych specjalistycznemu usługodawcy, którym jest firma chmurowa przekłada się natomiast na jakość proponowanych rozwiązań. Firmy chmurowe dzięki efektowi skali mogą bowiem zaproponować wysoką jakość świadczonych usług za stosunkowo niewygórowaną cenę.

Skalowalność systemu oraz możliwość jego przeniesienia przy wykorzystaniu rozwiązań cloud domputingowych pozwalają z kolei na łatwą rozbudowę systemu, a w razie konieczności możliwość jego przeniesienia do innego usługodawcy.

Mobilność i prostota dostępu systemy chmurowych w łatwiejszy sposób dają dostęp do danych firmowych. Ma to znaczenie w przypadku pracowników pracujących poza biurem.

Powierzenie danych obcemu podmiotowi może tworzyć dyskomfort związany z oddawaniem, często poufnych danych w obce ręce.

Sposoby wykorzystania rozwiązań chmurowych w Polsce oraz wśród firm działających w innych krajach europejskich



Źródło: McKinsey, Eurostat

Backup ważniejszy niż kiedykolwiek

Magazynowanie cennych danych poza firmą może być zaletą. W dobie zwiększonej aktywności hakerów dane powierzane są specjalistom również z zakresu cyberbezpieczeństwa. Dodatkowo wykupując usługę chmurową za bezpieczeństwo danych odpowiada firma zewnętrzna. Dodatkowo częstotliwość tworzenia kopii zapasowej jest dowolna, a w przypadku problemów, wrócić można do ostatniej stabilnej wersji systemu. Warto dodać także, że dzięki takiemu rozwiązaniu, to firma przechowująca dane będzie bardziej przyciągała potencjalne cyberataki, odwracając uwagę od firmy zlecającej wykonanie usług.

Rola AI w cyberbezpieczeństwie

W ramach usług chmurowych coraz bardziej widoczny jest trend tworzenia tzw. AIaaS, czyli z ang. Artificial Intelligence as a Service. W ten sposób przedsiębiorca może skorzystać z możliwości sztucznej inteligencji bez konieczności tworzenia kosztownych i często długich projektów wdrożeniowych.

Sztuczna inteligencja może być wykorzystana w analizie danych, funkcjonowaniu aplikacji, wyszukiwaniu informacji, a także w narzędziach stosowanych do prowadzenia biura. Tego typu rozwiązanie często znajduje zastosowanie w chatbotach, które pomagają klientom rozwiązać standardowe problemy dotyczące produktów lub usługą firmy. Dzięki AIaaS, dostępność tego typu narzędzi jest znacznie większa.

Według danych Adobe, ze sztucznej inteligencji korzysta około 15 procent firm. Z kolei BrightEdge zwraca uwagę, że w ramach działań marketingowych, przedsiębiorstwa planują wdrożenie większej personalizacji klienta przy składaniu zamówień, zastosowanie sztucznej inteligencji, a także wprowadzenie wyszukiwania głosowego. Dodatkowo eksperci PwC są zdania, że sztuczna inteligencja będzie miała duże znaczenie przy tworzeniu przewagi biznesowej.

BEZPIECZEŃSTWO DANYCH. NA CO ZWRACAĆ SZCZEGÓLNĄ UWAGĘ? CZY TECHNOLOGIA BLOCKCHAIN MOŻE BYĆ RECEPTĄ NA KŁOPOTY?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

6

Cyberatak może potencjalnie doprowadzić do upadku nawet firmy o ugruntowanej pozycji rynkowej. Naruszenia danych powodują bowiem nie tylko znaczne straty finansowe, ale są również główną przyczyną utraty zaufania klientów, którzy na kwestie prywatności są coraz bardziej wyczuleni. I tu wkracza blockchain. Ta technologia, mimo że wciąż kojarzona z bitcoinem, wyrasta właśnie na jeden z najbardziej obiecujących kierunków w segmencie cyberbezpieczeństwa.

Blockchain to rozproszony i zdecentralizowany rejestr operacji, w którym informacje o kolejnych działaniach zapisuje się w postaci bloków danych. Potem łączone są one w tzw. łańcuchy. Dostęp do tego rejestru mają wszyscy użytkownicy danej sieci peer-to-peer (P2P), którzy mogą śledzić historię transakcji od samego początku, ale nie mogą wprowadzać nieautoryzowanych zmian. Każda bowiem przed zatwierdzeniem jest „rozgłaszana" w całym rejestrze, zbudowanym z wielu elementów, z których wszystkie pełnią funkcję centralnego, ale żaden nim nie jest.

Wprowadzone zmiany nie od razu zostają też autoryzowane. Dopiero, kiedy zostaną zaszyfrowane, a poszczególne węzły sieci uzyskają tak zwany konsensus - zgodę odnośnie do tego, co ma zawierać następny blok - zostaje on dołączony do łańcucha. Transakcje dokonują się jedynie pomiędzy nadawcą a odbiorcą (z pominięciem elementu centralnego), z których każdy na bieżąco może śledzić postępy w dokonywanym procesie. W połączeniu z pozostałymi zaletami sprawia to, że blockchain jest tańszym, szybszym i bezpieczniejszym sposobem przekazywania np. własności.

W zdecentralizowanym blockchainie zaczęto więc dostrzegać remedium na długotrwałą walidację stron trzecich, wrażliwość systemów ewidencjonowania

Jak dbać o siebie w cyberprzestrzeni?

Uniknięcie typowych problemów = świadomość najważniejszych zagrożeń i rozsądek

	Klasyczny phishing	SMS-y	Spoofing	Trojany
Co to?	• podszywanie się pod znane podmioty, dużych dostawców jak poczta, banki, kurierzy • niestety bywają często bardzo dobrze dopracowane do treści autentycznych przesyłek	• udające wiadomości od firmy kurierskiej, poczty głosowej czy Blika - załączony link, który prowadzi do fałszywej strony lub aplikacji • fałszywe linki do spreparowanych stron celem wyłudzenia pieniędzy z konta bankowego	• podszywanie się np. pod pracowników banków w rozmowach telefonicznych • manipulacja z rzekomym zagrożeniem środków na koncie w tle, która zmierza do zmuszenia ofiary do instalacji oprogramowania zdalnego dostępu w telefonie lub komputerze	• zainfekowane aplikacje i tworzenie z pozoru bezpiecznych programów, które dopiero z czasem pobierają szkodliwy kod z zewnętrznych serwerów • korzystanie z zainfekowanej aplikacji może prowadzić do utraty danych, pieniędzy konta, jeśli program przechwytuje SMS-y, ekran czy klawiaturę, a ofiara korzysta z aplikacji bankowych
Jak się bronić?	• WERYFIKUJ adres nadawcy	• PRZEKAŻ wszystkie fałszywe wiadomości do analizy bezpieczeństwa ekspertom z CERT Polska **https://incydent.cert.pl**	• NIE klikaj w żadne linki w SMS	• KORZYSTAJ tylko z oficjalnych sklepów, pobierając nową aplikację na telefon. Podczas instalacji nie wyrażaj machinalnie zgody na wszystkie żądane uprawnienia (np. dostępu do kamery czy mikrofonu). Zastanów się, czego potrzebujesz do działania programu

1login od WP

- bezpieczne i darmowe logowanie się do serwisów WP za pomocą jednego loginu i hasła
- dowolny adres e-mailowy do założenia 1login od WP
- szybkie logowanie się widgetem 1login od WP
- dwuskładnikowe uwierzytelnianie
- powiadomienia o autoryzacji każdego nowego logowania na koncie
- **już 10,5 mln aktywnych kont**

Przeczytaj więcej

poczta **nr 1 w Polsce** (7,8 mln realnych użytkowników)

Źródło: Mediapanel, styczeń 2022

https://1login.wp.pl/informacje

na oszustwa i cyberataki, ponowną weryfikację danych i potrzebę szybszego obsługiwania transakcji.

Zalety blockchaina:

Blockchain daje pewność, że dane, które otrzymujemy są dokładne i aktualne, a poufne rekordy łańcucha bloków są udostępniane tylko tym członkom sieci, którym przyznano dostęp.

By autoryzować zmianę od wszystkich członków sieci wymagany jest tzw. konsensus, a wszystkie zweryfikowane transakcje są niezmienne. Nikt, nawet administrator systemu, nie może usunąć transakcji.

Dzięki rozproszeniu i decentralizacji uzgadnianie rekordów jest bardzo przyspieszone. Aby przyspieszyć transakcję, zestaw reguł - zwany inteligentną umową - może być przechowywany w łańcuchu bloków i wykonywany automatycznie.

Dlaczego blockchain jest bezpieczny?

Blockchain opiera się na zasadach kryptografii, decentralizacji i konsensusu, które zapewniają zaufanie do transakcji. W większości łańcuchów bloków lub technologii rozproszonej księgi (DLT) dane są podzielone na bloki, a każdy blok zawiera transakcję lub pakiet transakcji. Każdy nowy blok łączy się ze wszystkimi wcześniejszymi blokami w łańcuchu kryptograficznym w taki sposób, że manipulowanie przy nim jest prawie niemożliwe. Wszystkie transakcje w ramach bloków są weryfikowane i uzgadniane przez mechanizm konsensusu, zapewniając, że każda transakcja jest prawdziwa i poprawna.

Dzięki decentralizacji, nie ma też pojedynczego punktu awarii, a pojedynczy użytkownik nie może zmienić zapisu transakcji. Jednak technologie blockchain różnią się kilkoma krytycznymi aspektami bezpieczeństwa.

Phishing - wyłudzanie danych uwierzytelniających użytkownika. W przypadku sieci blockchain oszuści wysyłają właścicielom kluczy do portfela wiadomości e-mail zaprojektowane tak, aby wyglądały, jakby pochodziły z legalnego źródła. E-maile proszą użytkowników o podanie danych uwierzytelniających za pomocą fałszywych hiperłączy. Posiadanie dostępu do danych uwierzytelniających użytkownika i innych poufnych informacji może spowodować straty dla użytkownika i sieci blockchain.

Routing - blockchainy polegają na dużych transferach danych w czasie rzeczywistym. Hakerzy mogą przechwytywać dane przesyłane do dostawców usług internetowych. W ataku routingowym uczestnicy blockchain zwykle nie widzą zagrożenia, więc wszystko wygląda normalnie. Jednak za kulisami oszuści wydobyli poufne dane lub waluty.

Nie oznacza to jednak, że blockchain jest całkowicie kuloodporny. Precyzyjniej byłoby stwierdzić, że nawet jeśli technologia blockchain tworzy „księgę" odporną na manipulacje, to sieci

(infrastruktura) blockchain bynajmniej nie są odporne na cyberataki i oszustwa. Cyber złodzieje zagrażają sieciom blockchainowym chociażby poprzez phishing i routing.

Blockchain pozwala śledzić zamówienia, płatności i transakcje w bardziej przejrzysty i tańszy - dzięki eliminacji pośredników - sposób. Dlatego też zainteresowanie implementacją technologii opartej na rozproszonych rejestrach wykazują już niemal wszystkie branże - od finansów, przez nieruchomości, aż po branżę rozrywkową.

Zwolennicy blockchaina podkreślają, że góruje on nad tradycyjnymi systemami, bo o ile łatwo włamać się do jednego, centralnego rejestru danych, to ten rozproszony siłą rzeczy wymaga więcej zachodu. Przeciwnicy zauważają jednak, że włamania na platformy kryptowalutowe zdarzają się bardzo często, więc to czy sama technologia jest bezpieczniejsza nie ma większego znaczenia.

I rzeczywiście blockchaina trudno dzisiaj uznać za remedium na wszystkie problemy związane cyberbezpieczeństwem. Decentralizacja zasobów faktycznie eliminuje ryzyko pojedynczych ataków, ale implementacja platform opartych o blockchain wciąż jeszcze nie jest kuloodporna. Z duży prawdopodobieństwem można jednak stwierdzić, że blockchain doczeka się swoich protokołów SSL i stanie się standardem. Pytanie tylko - kiedy.

RAPORTY INTERAKTYWNIE 2022

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 2023 roku

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

interaktywnie.com

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.