RAPORT interaktywnie.com

CYBERBEZPIECZEŃSTWO, CLOUD COMPUTING, BLOCKCHAIN, BACKUP 2021

SIERPIEŃ 2021

SPONSOR PLATYNOWY: Synology®

POD PATRONATEM: WP money.pl GAZETA.PL

SPIS TREŚCI

Cyberbezpieczeństwo firmy to jej stabilność biznesowa i wiarygodność

W przypadku 55 procent firm wybuch pandemii przyczynił się do wzrostu ryzyka wystąpienia cyberataku.

Jeszcze większy odsetek podmiotów odczuł na własnej skórze jego skutki - 64 procent spośród badanych firm w 2020 roku zostało zaatakowanych w sieci. Wynik ten jest o 10 pkt. procentowych wyższy w stosunku do danych z 2019 roku.

Do tego praca zdalna wymusiła większe nakłady na zapewnienie cyberbezpieczeństwa, bo przecież to ono stanowi w głównej mierze o ciągłości biznesowej firmy oraz o jej wiarygodności.

Dobrze to wiedzą przedsiębiorstwa, które postanowiły zaprezentować się w tym ebooku: KIR, Sii, Synology.

Warto zapoznać się z ich ofertą.

Tomasz Bonek, prezes zarządu i redaktor naczelny Interaktywnie.com

Synology®

Synology

Adres
Grafenberger Allee 295
Düsseldorf

Dane kontaktowe
E-mail: pl_sales@synology.com
Strona www: www.synology.com

Opis działalności
Firma Synology produkuje rozwiązania z zakresu pamięci masowej dostępnej sieciowo, nadzoru IP i urządzenia sieciowe, które zmieniają sposób, w jaki użytkownicy zarządzają danymi i siecią oraz realizują zadania związane z nadzorem w erze usług chmurowych. W pełni wykorzystując zalety najnowszych technologii, firma Synology zapewnia użytkownikom niezawodne i przystępne cenowo rozwiązania służące do:

- centralizacji pamięci masowej
- tworzenia kopii zapasowych
- wirtualizacji
- udostępniania i synchronizowania danych
- do uzyskania do danych zawsze i wszędzie
- monitoringu wizyjnego tworzenia kopii zapasowych

Wybrani klienci
UNESCO, PolAndRock/WoŚP, Idea Bank, DPD, Audi

Krajowa Izba Rozliczeniowa S.A. (KIR)

Adres
ul. rtm. W. Pileckiego 65
02-781 Warszawa

Dane kontaktowe
kontakt@kir.pl
Strona www: www.kir.pl
Recepcja: tel. +48 22 545 55 00
Infolinia: 801 500 207

Opis działalności
KIR to hub technologiczny i kluczowy podmiot infrastruktury polskiego systemu płatniczego. Jest dostawcą cyfrowych rozwiązań dla gospodarki i administracji. Zapewnia usługi podnoszące poziom digitalizacji procesów. W ofercie firmy się narzędzia do zdalnej weryfikacji tożsamości - mojeID oraz elektroniczny podpis kwalifikowany – Szafir i mSzafir. KIR jest także pionierem technologii blockchain w Polsce.

Sii Polska

Adres
Aleja Niepodległości 69
02-626 Warszawa

Dane kontaktowe
E-mail: contact@sii.pl
Strona www: www.sii.pl
Telefon: +48 22 486 37 37

Opis działalności
Zatrudniając 6000 specjalistów, Sii jest wiodącym dostawcą usług doradztwa technologicznego, transformacji cyfrowej, BPO i inżynieryjnych. Od 15 lat wspiera klientów w zakresie m.in. analiz i testów, rozwoju oprogramowania, zarządzania infrastrukturą, cyberbezpieczeństwa, integracji i utrzymania systemów. Obecnie posiada 14 biur w całym kraju.

Wybrani klienci
Puma, Assa Abloy, Tikkurila, Ingenico Group, QIAGEN, Leica, Reckitt Benckiser, ING Bank, LPP, Mercedes-Benz, Fresenius Netcare

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.
- Kompleksowo realizujemy projekty internetowe - od strategii, poprzez wdrożenie witryny, do pozyskiwania użytkowników i monetyzacji.
- 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

CYBERZAGROŻENIA DLA FIRM. NA CO KAŻDE PRZEDSIĘBIORSTWO POWINNO ZWRACAĆ SZCZEGÓLNĄ UWAGĘ?

Przemysław Ławrowski
redaktor Interaktywnie.com

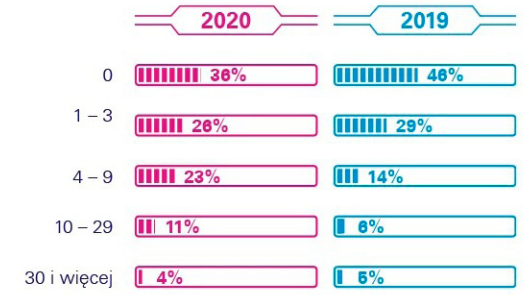
pl@interaktywnie.com

1

Tylko w 2020 roku 64 procent firm borykało się z co najmniej jednym cyberatakiem. Pandemia COVID-19 z jednej strony sprawiła, że proces cyfryzacji gospodarki przyspieszył, równocześnie jednak zwiększyła się aktywność hakerów. Do najczęściej występujących cyberataków możemy zaliczyć: ransomware, maleware i phishing.

Mniejsze firmy częściej sygnalizowały ryzyko cyberataku oraz częściej wskazywały na wyzwania związane z pandemią, co oznacza, że hakerzy chętniej kierują swoją uwagę w kierunku firm posiadających mniejsze zaplecze do walki z cyberatakami.

Udział liczby zarejestrowanych przez firmy incydentów bezpieczeństwa w latach 2019-2020

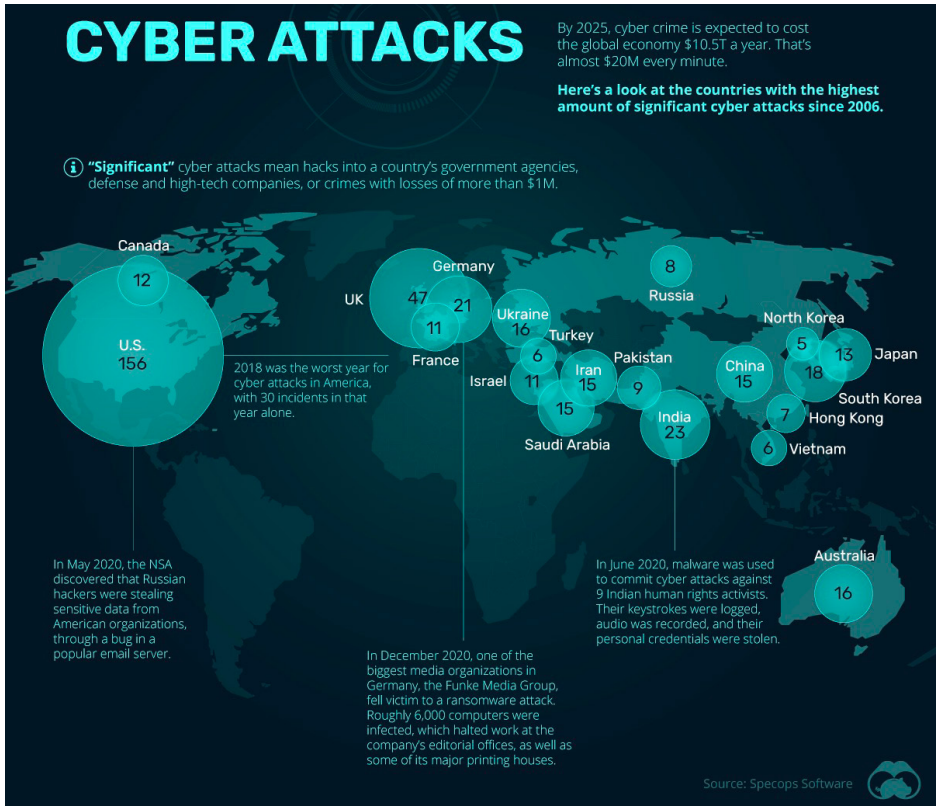


Źródło: KPMG

Polskie organizacje atakowane częściej niż amerykańskie

Z badania „Check Point Research" dotyczącego pierwszego półrocza 2021 roku wynika, że polskie firmy były atakowane częściej niż amerykańskie. O ile ryzyko cyberataku dotyczy każdej branży, to szczególnie jest to dotkliwe w przypadku firm z grupy tzw.nowych technologii. W tym przypadku zanotowano ponad 500 ataków tygodniowo, podczas gdy w USA wynik ten to 443 ataków na organizację tygodniowo. Najwięcej ataków zanotowano w polskim sektorze edukacji i badań, finansach i bankowości, a także militarnym i rządowym.

Kraje o największej liczbie cyberataków skierowanych w strategiczne instytucje w latach 2006-2020



Źródło: Specops Software

Oczywiście w liczbach bezwzględnych skala cyberataków w USA będzie większa, m.in. z powodu różnicy w wielkości obu krajów. Jak podaje serwis visualcapitalist.com, na podstawie danych Specops Software, w latach 2006-2020, Stany Zjednoczone zostały poddane 156 znaczącym cyberatakom. Mowa tutaj o agresji skierowanych na agencje rządowe kraju, firmy obronne lub firmy high-tech. Wliczono w to także cyberprzestępstwa, które wiązały się ze stratami przekraczającymi 1 mln dolarów. Kraj ten jest daleko przed wiceliderem zestawienia - Wielką Brytanią. W pierwszej dziesiątce znajdują się również takie kraje jak Indie, Niemcy, Korea Południowa, Australia, Ukraina, Chiny, Iran i Arabia Saudyjska.

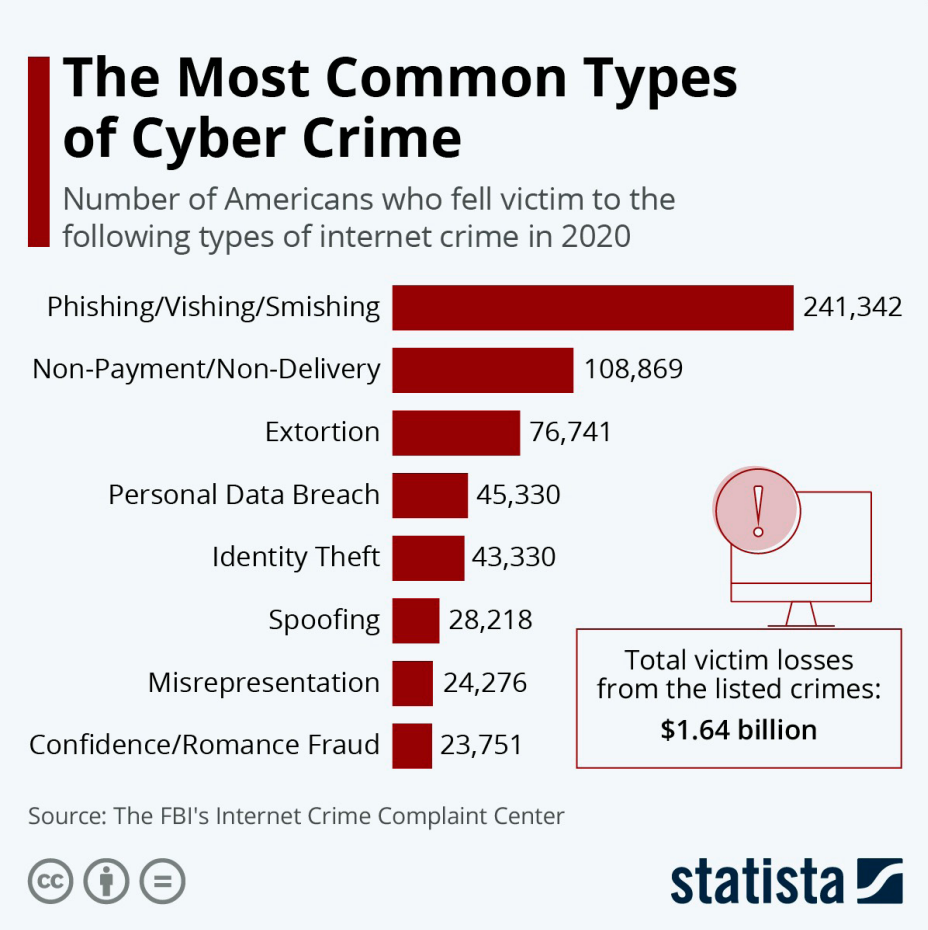
Najpowszechniejsze rodzaje cyberataków

Według ekspertów z grupy Cisco Talos Incident Response, najpoważniejszym cyberzagrożeniem w drugim kwartale 2021 roku były ataki ransomware. Ten rodzaj ataku odpowiadał za około połowę prób hakerskich w tym okresie i występował trzykrotnie częściej niż wicelider tego zestawienia.

Serwis Statista na podstawie danych FBI podaje, że wśród najbardziej powszechnych ataków hakerskich jest phishing. Agencja wskazuje, że w 2020 roku tego typu oszustwom tylko w USA uległo aż 241 tys. osób. Innym często spotykanym typem oszustwa jest brak płatności lub brak dostarczenia zamówionego towaru. Dotyczy to w dużym stopniu zakupów online, których popularność mocno wzrosła w trakcje pandemii COVID-19. Co ważne, mimo iż ten rodzaj przestępstwa znajduje się na drugim miejscu najczęściej stosowanych cyberataków, to od 2017 roku ich częstotliwość się zwiększyła z 84 do prawie 109 tys. poszkodowanych osób w USA. Do innych cyberataków należą

wymuszenia (extortion), kradzież danych osobowych, czy kradzież tożsamości.

Najpopularniejsze typy cyberataków oraz dane o liczbie poszkodowanych z tego tytułu w USA w 2020 roku



Źródło: Statista

Rodzaje cyberataków w podziale na stopień ryzyka wytwarzanego dla organizacji

Źródło: KPMG

Zdaniem ekspertów KPMG, najbardziej rozpowszechnionym sposobem cyberataku, a zarazem jednym z najbardziej niebezpiecznych jest maleware i phishing. Firmy zwracają również

uwagę na zagrożenie związane bezpośrednio z pracownikami, a także możliwość kradzieży lub zgubienia nośników danych. W raporcie KPMG, "Barometr cyberbezpieczeństwa. COVID-19 przyspiesza cyfryzację firm", ankietowani oceniali każde zagrożenie w skali od 0 do 5, z czego cyfra 5 oznacza najwyższe ryzyko.

Negatywne efekty cyberataków

Jeżeli dojdzie do udanego cyberataku, firma musi się przygotować na konsekwencje. W pierwszej kolejności może to być utrudnienie lub uniemożliwienie bieżącej pracy przedsiębiorstwa. Oprócz tego należy się liczyć z ewentualnym wyciekiem danych, a w najgorszym przypadku utraty bazy danych. Kradzież może dotyczyć nie tylko danych osobowych klientów, ale także danych handlowych firmy (kontrahenci, oferty) lub finansowych.

Po negatywnych efektach cyberataku z punktu widzenia funkcjonowania firmy, czas na konsekwencje zewnętrzne, związane z postrzeganiem firmy przez kontrahentów i klientów. Pod tym względem negatywnym efektem dla przedsiębiorstwa może być utrata ważnego kontraktu lub pogorszenie stosunków z partnerem biznesowym, wpływające nie tylko na jeden najbliższy kontrakt, ale długotrwałe relacje. Dodatkowo reputację można stracić również w oczach klientów. To wszystko natomiast będzie skutkowało obniżeniem przychodów firmy.

Trzeba także pamiętać o obowiązku zgłaszania incydentów związanych z kradzieżą danych osobowych. W przypadku nałożenia kary w tym zakresie trzeba liczyć się z grzywną lub nawet z karą ograniczenia wolności.

Słabości firm w kwestii cyberbezpieczeństwa:

- brak strategii w kwestii cyberbezpieczeństwa - część firm nie podchodzi do tego tematu na tyle poważnie, aby stworzyć w tej kwestii odpowiednią infrastrukturę oraz procedury.
- brak zabezpieczenia sieci - daje to hakerom łatwy dostęp do zasobów firmy, a w dalszej kolejności nawet jej urządzeń
- brak bezpiecznych form komunikacji - jeżeli w ramach działalności pracownicy wewnątrz firmy przekazują sobie dane poufne, należy zainwestować w bezpieczną sieć e-mail
- błąd stosowanego systemu - tego typu incydentu nie zawsze można się ustrzec. Z tego powodu warto zabezpieczyć firmę w postaci zaplecza technicznego oraz wykwalifikowanych pracowników
- przestarzałe rozwiązania - wiele firm po zaimplementowaniu systemu bezpieczeństwa przestaje interesować się tym tematem. Natomiast rozwój technologii sprawia, że również kwestie bezpieczeństwa powinny być na bieżąco monitorowane
- nieprzeszkoleni lub niewykwalifikowani pracownicy - według raportu Kaspersky Lab, 90 procent incydentów związanych z naruszeniem bezpieczeństwa związanych jest z błędem ludzkim. Nieumyślne ujawnienie poufnych danych lub nieuważne klikanie na podejrzanych stronach internetowych to tylko niektóre z "grzechów" osób zatrudnionych w firmach.

Źródło: isaca.com

Człowiek najsłabszym ogniwem?

Raport KPMG wskazuje, że dla około połowy firm, barierą dla utrzymania odpowiedniego poziomu bezpieczeństwa jest brak odpowiednio wykwalifikowanych w tym zakresie pracowników. Problem ten zaczął być szczególnie widoczny w 2017 roku, a już w 2019 roku 43 procent firm zadeklarowało trudności w znalezieniu i utrzymaniu wykwalifikowanych pracowników. Z kolei 36 procent wskazań dotyczyło braku wsparcia w temacie bezpieczeństwa najwyższego kierownictwa.

Firmy zwracają uwagę na problem, jaki niesie ze sobą rozpowszechnienie pracy zdalnej. Raport dot. cyberbezpieczeństwa podaje, że dla 51 procent firm konieczność organizacji pracy w trybie zdalnym była wyzwaniem w kontekście zapewnienia bezpieczeństwa, a 25 procent przedsiębiorstw z tego tytułu musiało zwiększyć wydatki na cyberbezpieczeństwo.

Jak znaleźć wykwalifikowanych specjalistów z zakresu cyberbezpieczeństwa?

Powszechna cyfryzacja oraz brak specjalistów IT z zakresu cyberbezpieczeństwa sprawiły, że firmy chwytają się różnych sposobów, aby zapewnić cyberbezpieczeństwo. Oprócz tradycyjnego zatrudnienia własnych specjalistów, pod uwagę należy wziąć usługi zewnętrznej firmy, która zadba o te kwestie.

Podobnie jak w przypadku agencji marketingowej, zatrudnienie firmy, która zadba o cyberbezpieczeństwo pozwala korzystać z jej doświadczenia. Oczywiście, przed podpisaniem umowy należy sprawdzić jej portfolio.

Synology®

Zabezpiecz dane zanim będzie za późno!

ARTYKUŁ PARTNERA

ROZWIĄZANIA CHMUROWE I BACKUP DLA FIRM. DLACZEGO WARTO?

Przemysław Biel
Senior Key Account Manager Poland (Sales Representative), Synology

2

Mam kopię, jestem bezpieczny…

Nikt nie ma chyba cienia wątpliwości, jak ważnym elementem poprawnego funkcjonowania dzisiejszych przedsiębiorstw jest wyposażenie w system backupu, zwany też kopią zapasową, czy kopią bezpieczeństwa. W przeszłości kopia zapasowa danych była swoistą ekstrawagancją. Obecnie dane muszą być chronione bardziej niż kiedykolwiek wcześniej z uwagi na zagrożenia cyberatakami.

Czy jednak zrobienie jednej kopii zapasowej wystarczy, aby firma mogła spać spokojnie?

Z pozoru, wydaje się to proste, robimy kopie, chowamy do sejfu i po sprawie. W praktyce, jednak tak to nie wygląda. Każdy przedsiębiorca powinien sobie zadać pytanie, co się stanie, jeśli moja firma nie będzie w stanie pracować przez 5 minut, godzinę, dzień, tydzień czy miesiąc.

Jakie koszty poniesie właściciel i na ile są one akceptowalne w każdym przypadku. Mając odpowiedź na takie pytania, można się pokusić o opracowanie planu zabezpieczania danych oraz zapewnienia ciągłości biznesowej przedsiębiorstwa. Mimo, iż brzmi to jak dość skomplikowany zabieg, nie musi takie być.

Jeśli mamy już wiedzę, na jak długi okres przerwy w pracy możemy sobie pozwolić oraz jaką część utraconych danych możemy zaakceptować, możemy się zastanowić nad odpowiednim rozwiązaniem.

Chmura, hybryda czy lokalny serwer?

W ostatnich latach, można zaobserwować ogromny rozwój usług chmurowych, które są świetnym rozwiązaniem w wielu obszarach, jednak nie ma rzeczy dobrych do wszystkiego. W odpowiedzi

na zapotrzebowanie rynku pojawiły się rozwiązania hybrydowe, łączące ze sobą elementy chmury publicznej i lokalnych serwerów, określane mianem „edge computing".

Tak jak dobieramy odpowiedni strój do określonej okazji i potrzeb, tak powinno też się wybierać rozwiązania informatyczne do swojej firmy, dzięki temu osiągamy najlepszą efektywność, zarówno kosztową jak i techniczną.

Zasada 3-2-1.

Dobra kopia to skuteczna kopia. Skuteczna kopia to taka, którą jesteśmy w stanie przywrócić w razie potrzeby. Niezawodna kopia to co najmniej 3 kopie.

Zgadza się, niestety, aby móc poczuć się spokojnym o swoje dane, trzeba kopię zapasową robić na wiele sposobów. Każdy sposób, ma swoje zalety i wady, dopiero ich połączenie w spójną całość gwarantuje nam bezpieczeństwo.

Zasada 3-2-1 mówi o tym, aby mieć zawsze 3 kopie, na co najmniej 2 różnych nośnikach, w tym jedna z tych kopii powinna być fizycznie w innej lokalizacji.

Wydaje się to dość ciężkie w realizacji, jednak przy wyborze odpowiednich rozwiązań, może to być bardzo proste.

Serwer NAS oraz usługi chmurowe.

Czym jest serwer NAS? W dużym uproszczeniu to taki wielofunkcyjny komputer z własnym systemem operacyjnym i oprogramowaniem do różnych zastosowań. Jest on dodatkowo zoptymalizowany do pracy ciągłej 24/7, a także pod kątem bezpieczeństwa przechowywanych na nim danych.

Kluczem do sukcesu jest dobranie odpowiedniego rozwiązania do danych potrzeb.

Przy założeniu, że firma ma biuro lokalne i zatrudnia powiedzmy 100 osób, kopię zapasową urządzeń (komputery PC, notebooki, serwer firmowy) możemy wykonać na serwer NAS (modele z serii Plus lub wyższej w zależności od potrzeb). Jeśli w firmie jest wykorzystywany pakiet Microsoft 365, zawartość tej

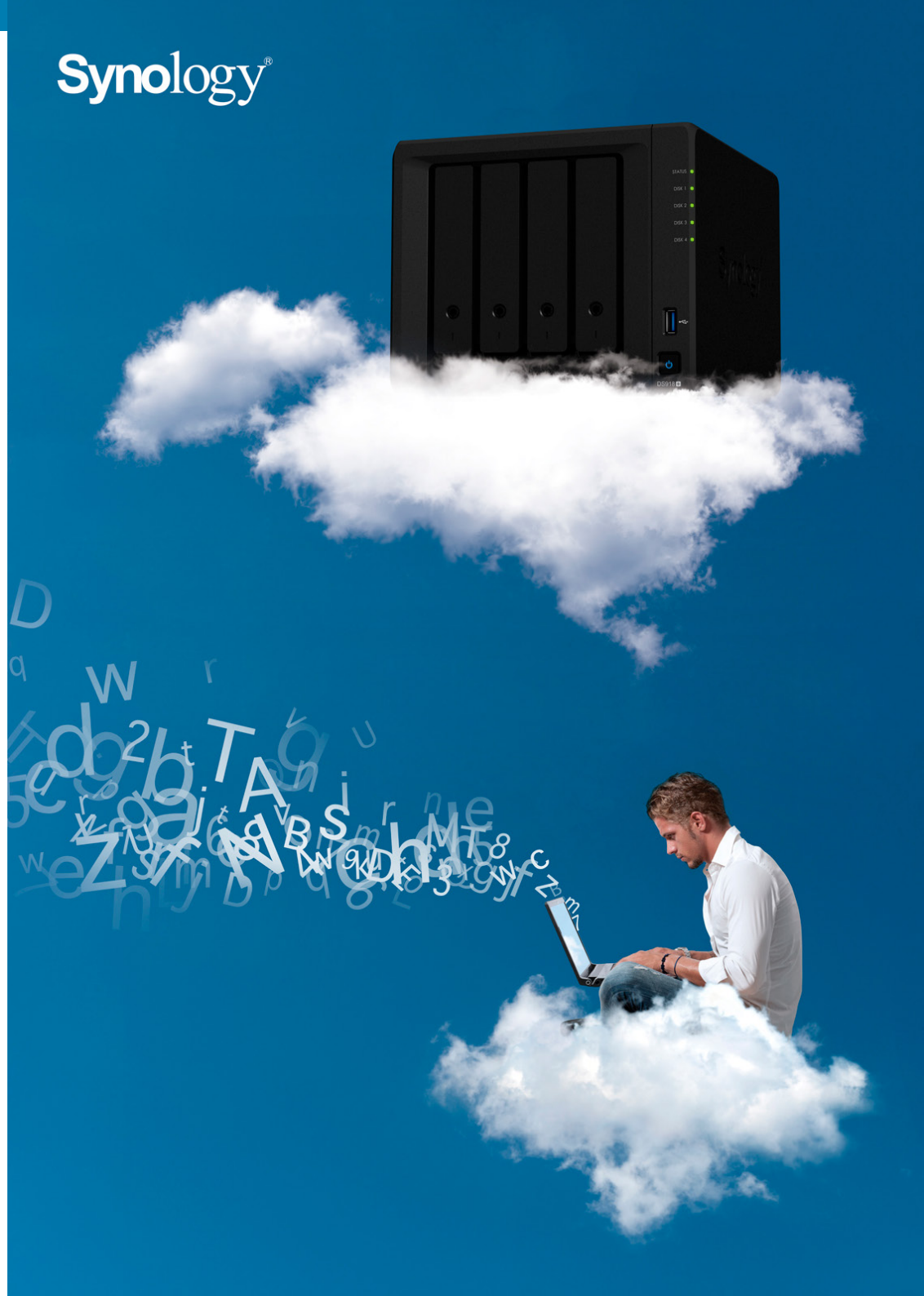
usługi, też można zabezpieczyć na serwerze Synology. Tym sposobem mamy już 1 krok zrobiony w drodze do bezpiecznej kopii.

Drugą kopię należałoby zrobić na inny nośnik, najlepiej, gdyby był odseparowany od sieci firmowej w jakiś sposób lub przeznaczony tylko pod backup i niedostępny dla użytkowników. Może to być też serwer NAS Synology lub inny serwer zgodny z protokołem rsync i tu nie musi być już tak wydajny, jak ten podstawowy serwer kopii zapasowych, gdyż tutaj będziemy robić kopię gotowego archiwum z pierwszego serwera.

Naszą trzecią kopią może być kopia danych firmowych z pierwszego serwera do chmury C2 Storage (może to być też inna usługa obsługiwana przez narzędzie Hyper Backup), dzięki temu mamy załatwiony aspekt kopii w innej fizycznie lokalizacji.

Najlepsze w tym wszystkim jest to, iż wybierając rozwiązanie Synology, nie musimy kupować licencji na oprogramowanie do kopii zapasowych (w przypadku innych producentów, często są to płatne rozwiązania lub z ograniczeniami). Wszystkie aplikacje do kopii zapasowej od Synology są dostępne wraz z urządzeniem (seria Plus lub wyższa).

Innym sposobem na kopię zewnętrzną tzw. off site może być usługa C2 Backup zapowiedziana przez Synology. Pozwoli ona



na robienie kopii urządzeń końcowych (komputerów PC, serwerów) bezpośrednio do chmury. W obecnych czasach, gdzie bardzo wiele osób pracuje z domu, taka forma zabezpieczenia danych, może się okazać kluczowa w całym planie kopii. W przypadku usług kopii bezpośrednio do chmury, trzeba się liczyć z opłatami za subskrypcję, jednak w przypadku C2 Backup nie będzie ograniczeń, jeśli chodzi o ilość urządzeń, płacić się będzie jedynie za określoną pojemność miejsca w chmurze.

Realne koszty skutecznego systemu kopii zapasowych.

Przechodzimy do kolejnego aspektu dobrego rozwiązania do kopii zapasowej, czyli odpowiednia efektywność techniczna i kosztowa.

Na rynku jest wiele rozwiązań do kopii, bardzo często drogich i z dość zagmatwanymi planami licencjonowania. Nie zawsze jednak oferują one odpowiedni poziom wydajności oraz potrzebnych funkcji. Na co zwrócić zatem uwagę?

Przede wszystkim trzeba policzyć koszty w dłuższym okresie i zastanowić się, jaka ilość miejsca na kopie będzie potrzebna przez najbliższe lata. Aby zgodnie z zasadą 3-2-1 zabezpieczyć dane, potrzebujemy zbudować dobrze działający system. Ważne jest, by wszystkie jego elementy ze sobą współgrały.

Jeśli wybieramy serwer NAS pod kopie, warto zwrócić uwagę, czy oferuje on aplikacje do kopii zapasowej naszego całego środowiska firmowego i czy nie jest ona dodatkowo płatna.

Warto sprawdzić, czy takie rozwiązanie do kopii oferuje mechanizm deduplikacji i szyfrowania danych. Pierwsze jest bardzo istotne ze względu na oszczędność na nośnikach danych (deduplikacja może znacząco zmniejszyć wielkość kopii zapasowej), drugie natomiast to obecnie standard, jeśli chodzi o zabezpieczenie danych poufnych i wrażliwych.

Idealną sytuacją jest, jeśli całe rozwiązanie pochodzi od jednego dostawcy, wtedy wszelkie problemy można szybko zdiagnozować i załatwić u źródła. W przypadku, gdy oprogramowanie jest od jednego dostawcy a serwer / pamięć masowa od innego producenta, dość często bardzo trudno jest określić przyczyny problemów.

W przypadku wyboru usług chmurowych, należy zwrócić uwagę za co tak naprawdę płacimy i co gwarantuje dostawca. Istotne jest, aby dane przed wysłaniem do chmury można było zaszyfrować, czasem nawet takie dane są dodatkowo szyfrowane po stronie dostawcy dla zwiększenia bezpieczeństwa. Plany subskrypcji oczywiście obejmują powierzchnię, za którą płacimy, ale bardzo często mają dodatkowe ograniczenia np.: jednocześnie z usługi

może korzystać określona liczba urządzeń, albo za transfer danych lub ich pobranie jest dodatkowa opłata. Takich dostawców unikajmy, gdyż bardzo ciężko jest policzyć realny koszt takiej usługi w dłuższym okresie.

Podsumowując, wybierajmy mądrze i biorąc pod uwagę dłuższą perspektywę czasu. Rozwiązania NAS to nie tylko kopia zapasowa, bardzo często mogą być wykorzystane w wielu innych celach w firmie, warto wziąć to pod uwagę przy zakupie.

Jeśli chodzi o chmurę, unikajmy ograniczeń i ukrytych opłat wybierając dostawców z przejrzystym planem subskrypcji i funkcjami, które naprawdę nam się przydadzą.

JAK CHRONIĆ FIRMĘ PRZED ZAGROŻENIAMI? DLACZEGO PROGRAM ANTYWIRUSOWY NIE WYSTARCZY?

Przemysław Ławrowski
redaktor Interaktywnie.com

pl@interaktywnie.com

3

Przeszkolony personel, najnowsza technologia oraz procedury. Te trzy elementy składają się na skuteczny system zabezpieczeń przed cyberatakami w firmie. Oprócz programu antywirusowego i rozwiązaniu jakim jest VPN, duży wpływ na aspekt bezpieczeństwa ma czynnik ludzki. Z tego względu, gdy nie da się ustrzec zagrożenia, warto zadbać o dodatkową ochronę danych w postaci np. kopii zapasowych.

Dane serwisu tyrantsthem.com pokazują, że 95 procent firm uważa, że ich bezpieczeństwo w sieci nie jest zależne wyłącznie od nich. Trzy czwarte ankietowanych podmiotów stwierdziło natomiast, że chociaż raz doświadczyło próby wyłudzenia poufnych danych, 60 procent było narażonych na ataki w sieci, a 20 procent spotkało się z atakiem Ransomware.

Tymczasem na bezpieczeństwo firmy w sieci składa się wiele czynników, które, gdy ze sobą odpowiednio współgrają, zapewnią odpowiednią ochronę zasobom przedsiębiorstwa. Możemy je podzielić na trzy kategorie:

Czynnik ludzki

Jest to bardzo ważny element systemu cyberbezpieczeństwa. Nawet najlepsze zabezpieczenia sieci na nic się zdadzą, jeżeli pracownik swoim nieświadomym działaniem sprowadzi na system zagrożenie. Tego typu ryzyko dotyczy także nieprawidłowej konfiguracji systemu lub sieci, korzystania z wrażliwych zasobów przy wykorzystaniu publicznej sieci bezprzewodowej, czy stosowania zbyt prostych lub tych samych haseł w kilku miejscach. Na szczęście i z tym problemem mogą poradzić sobie firmy projektujące specjalne systemy zabezpieczające firmy.

Kompleksowe podejście kluczem do bezpiecznej organizacji

Aby skutecznie ochronić firmę przed zagrożeniami trzeba sobie przede wszystkim uzmysłowić, że jest to długotrwały proces. Naszym klientom proponujemy rozpocząć od audytu, podczas którego weryfikujemy istniejące procedury oraz techniczne aspekty bezpieczeństwa. Kluczowym elementem jest również ocena ryzyka organizacji. To dzięki niej dowiadujemy się, co i przed czym chcemy chronić, a następnie określamy, jak należy się zabezpieczyć.

Tak zbudowany System Zarządzania Bezpieczeństwem w organizacji powinien obejmować zarówno aspekty technologiczne, jak i procedury. Aby zapewnić wysoki stopień ochrony, należy zadbać o:

- Bezpieczeństwo infrastruktury – wykorzystywane są między innymi rozwiązania do ochrony sieci, takie jak firewall czy IDS/IPS.
- Bezpieczeństwo stacji końcowych - do ich ochrony tradycyjny antywirus już dawno przestał być wystarczający. Obecnie stosowane są rozbudowane systemy, które oprócz modułów do wykrywania malware posiadają funkcje umożliwiające m.in. szybkie reagowanie na zagrożenie.
- Bezpieczeństwo danych - rozwiązania typu Data Leak Prevention (DLP) umożliwiają monitorowanie i blokowanie wycieku danych.
- Zarządzanie dostępami - systemy klasy IAM oraz PAM pozwalają w sposób zorganizowany zarządzać tożsamością użytkowników oraz ich uprawnieniami. Stosowanie rozwiązań do uwierzytelniania wieloetapowego skutecznie zabezpiecza przed włamaniami związanymi z kradzieżą loginu/hasła (np. ataki phishingowe)
- Reagowanie na incydenty – zadaniem SOC (Security Operation Center), wspartego przez rozwiązania klasy SIEM jest szybkie identyfikowanie i reagowanie na incydenty bezpieczeństwa. Kluczowe jest ciągłe monitorowanie tych systemów, co pozwala zapobiec lub znacznie ograniczyć skutki włamania.

Dawid Jankowski
Cybersecurity Competency Center Manager, Sii Polska

Technologia

Strategia mająca zapewnić firmie cyberbezpieczeństwo musi opierać się na najnowszych rozwiązaniach technologicznych. Stosowanie przestarzałej technologii będzie w tym przypadku mało przydatne ze względu na galopujący postęp. Wśród nich są programy antywirusowe, filtry DNS, programy anti-maleware'owe itd.

Procedury

Element ten związany jest z dwoma poprzednimi kategoriami. Według raportu KPMG, w 2020 roku 64 procent firm odnotowało co najmniej jeden cyberatak. Można stwierdzić, że zabezpieczenia oraz przeszkoleni pracownicy nie są wyłącznym gwarantem skutecznej obrony przed cyberzagrożeniami. W przypadku zagrożenia należy bowiem wiedzieć, jak sobie z nim radzić. W tym celu potrzebne są odpowiednie procedury, który wskażą odpowiednią ścieżkę działania. Będą one również zasadne w codziennej eksploatacji systemu, aby zapobiegać cyberatakom.

Programy antywirusowe. Na co zwrócić uwagę?

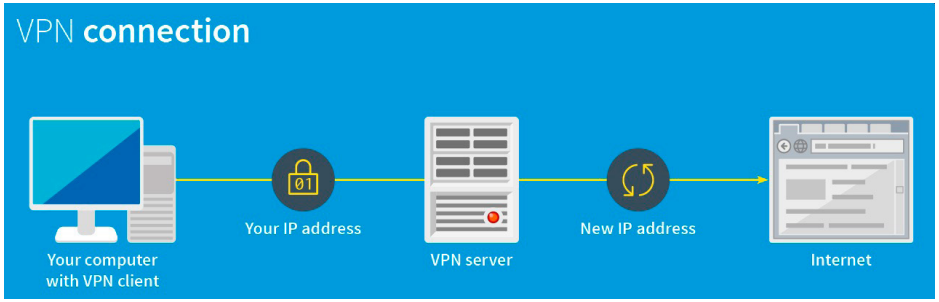
System zabezpieczeń, jakim jest antywirus, już dawno przestał być tylko zwykłym programem chroniącym komputer. Oprócz zapewnienia skutecznej ochrony powinien on zawierać szereg cech:

- dostęp do panelu monitorującego program, pozwalający sprawdzać, a także modyfikować stosowane przez niego zabezpieczenia;
- ochrona urządzeń mobilnych; obry program antywirusowy powinien radzić sobie nie tylko z ochroną komputerów, ale także urządzeń mobilnych;
- częste aktualizacje, tak aby użytkownik programu był pewny, że posiada on najnowsze dane służące do ochrony komputera lub sieci;
- sposób pracy nieobciążający nadmiernie urządzenia, na którym jest zainstalowany;
- raporty informujące administratora o liczbie wykrytych zagrożeń, skanowanych plików czy wykrytych lukach wymagających naprawienia;
- niewymagająca obsługa; rogram antywirusowy nie powinien angażować zbyt wielu zasobów finansowych oraz kadrowych firmy;

VPN, czyli ochrona sieci lokalnej

Posiadając sieć lokalną w firmie warto zainwestować w zintegrowany system zarządzania siecią, na który może składać się oprócz firewalla takie rozwiązanie jak VPN. Z ang. Virtual Private Networks, pozwala na bezpieczne połączenie kanałów pomiędzy użytkownikami pracującymi poza siedzibą firmy, a pracownikami się w niej znajdującymi, lub pomiędzy oddziałami danego podmiotu.

Schemat działania połączenia VPN



Źródło: Gdatasoftware

Rozwiązanie jakim jest VPN uniemożliwia śledzenie danego komputera, na którym jest stosowany. Wówczas komputer łączy sie serwerem VPN za pomocą szyfrowanego połączenia. Przeglądając internet lub korzystając z innych programów wymagających dostępu do sieci, połączenie nawiązuje serwer VPN, a nie komputer. W takiej sytuacji nie są zapisywane dane dotyczące danego komputera, lecz systemu VPN.

W powyższy sposób maskujemy informacje na temat samego użytkownika, a do tego wysyłane i odbierane dane są dodatkowo zabezpieczone. Wysyłanie w ten sposób informacji, można

1login od WP

Wygoda i bezpieczeństwo z 1login od WP

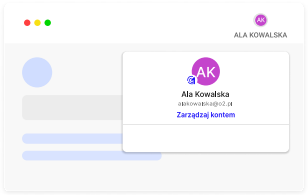
Loguj się za pomocą jednego loginu i hasła do serwisów w polskim internecie (poczta, portale informacyjne, sklepy i usługi).

Loguj się prościej

Dzięki 1login od WP nie musisz za każdym razem wpisywać danych. Wystarczy, że zalogujesz się na konto. Wystarczy, że zalogujesz się na konto, klikając po prostu w przycisk z logo 1login od WP.

Wszystko pod kontrolą

W ustawieniach 1login od WP znajdziesz listę wydarzeń powiązanych z bezpieczeństwem (logowania czy zmiany w ustawieniach). Powiadomimy Cię o każdej próbie logowania się na Twoje konto.



Włącz dodatkową ochronę z aplikacją

Włącz logowanie dwustopniowe i potwierdzaj logowanie w aplikacji 1login od WP na swoim telefonie lub tablecie. Nikt nie zaloguje się na Twoje konto bez Twojej zgody, nawet jeśli pozna hasło.

Docieraj do wszystkich użytkowników

- **9.9 mln** użytkowników korzysta z **Poczty WP i o2** *
- Średnio **30-40%*** ruchu kierowanego z WPM do partnerów to użytkownicy, którzy posiadają już konto pocztowe WP lub o2, czyli użytkownicy, którym potencjalnie **zapewniamy szybszą konwersję.**
- **Użytkownicy zidentyfikowani konwertują** średnio **o 40%** lepiej w porównaniu do użytkowników anonimowych. **
- **Przygotuj swój biznes na ograniczenia 3rd party cookies.** Dzięki **1login od WP** zdywersyfikujesz swój biznes z partnerami innymi niż Google czy Facebook.

Źródło: *dane własne 03-04.2021
** dane własne, 05.2021 na podstawie danych z największych branż fashion, retail i elektroniki.

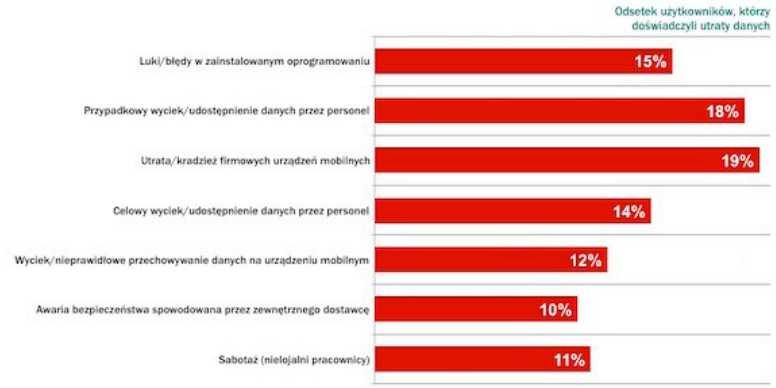
porównać do szyfrowania pliku za pomocą procesu archiwizacji (7z, rar, zip).

Zagrożenia wewnętrzne

Nie tylko osoby z zewnątrz mogą być źródłem potencjalnych cyberataków. Istnieje również szereg wewnętrznych ryzyk, które, jak pokazują dane Kaspersky Lab, nie występują rzadko. Według raportu, aż 21 procent firm borykało się do tej pory z tego typu problemami.

Najwyżej sklasyfikowanym przez Kaspersky Lab jest luka w oprogramowaniu oraz wyciek danych spowodowany przez personel. Szczegółowa klasyfikacja została przedstawiona na wykresie poniżej.

Przypadki utraty danych w wyniku zagrożeń wewnętrznych



Źródło: Kaspersky Lab

Luki w zainstalowanym oprogramowaniu odpowiadają za 15 procent incydentów z zakresu cyberbezpieczeństwa. Z kolei personel oraz spowodowany przez niego wyciek danych odpowiada za 18 procent przypadków naruszenia cyberbezpieczeństwa w firmach. Istotnym czynnikiem jest również kradzież lub utrata urządzeń mobilnych należących do firmy (19 procent), a także, co gorsza, celowe działanie (14 procent). Kaspersky Lab wymienia również takie czynniki jak wyciek danych z urządzeń mobilnych, awarię bezpieczeństwa spowodowaan przez zewnętrznego dostawcę oraz sabotaż.

Metody ochrony danych w firmie

Oprócz firewalla i VPN, w firmie powinny funkcjonować inne zabezpieczenia na wypadek wycieku, utraty lub kradzieży wrażliwych danych. Można zaliczyć do nich:

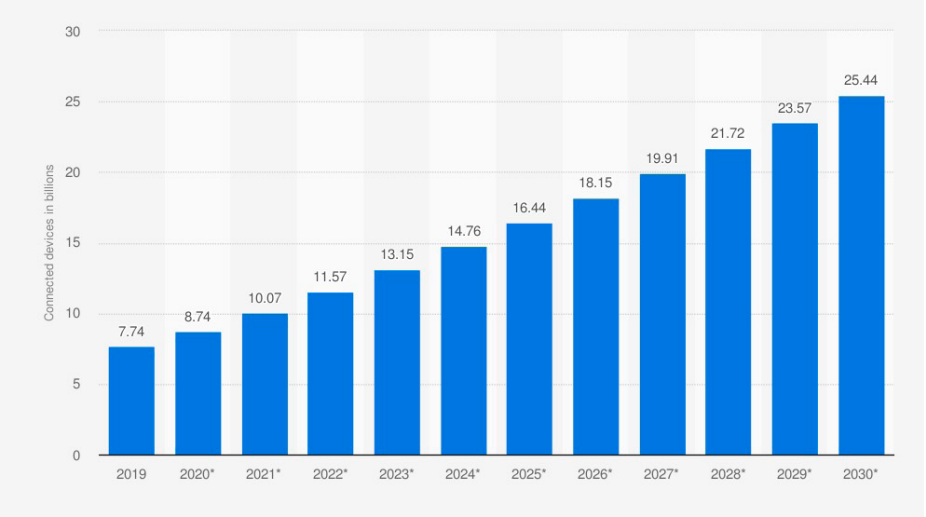
- wykonywanie kopii zapasowych w określonych odstępach czasu;
- podział danych na kilka części i ich osobne szyfrowanie;
- kontrola dystrybucji i procesu zbierania danych;
- szyfrowana transmisja danych.

Dodatkowo w firmie powinna zostać zaimplementowana polityka bezpieczeństwa, procedury postępowania z danymi, ocena ryzyka kradzieży lub zniszczenia bazy danych, przeszkolenie pracowników w zakresie ochrony danych oraz monitorowanie procesów związanych z danymi.

IoT jako potencjalny cel ataku

Rozwój rozwiązań SmartHome oraz SmartCities niesie za sobą ryzyko cyberataków, a tempie rozwoju tego segmentu sprzyja dodatkowo sieć 5G. Według przewidywań serwisu Statista, do 2030 roku, liczba urządzeń podłączonych do sieci w ramach IoT przekroczy 25 mld.

Liczba urządzeń podłączonych do sieci w ramach IoT



Źródło: Statista

Eksperci zwracają uwagę na nadal stosunkowo słabe zabezpieczenie tego typu urządzeń. Stosowana w nich technologia jest podatna na wiele zagrożeń. Wśród słabość możemy wymienić słaby poziom uwierzytelnienia, rozproszony system bezpieczeństwa, korzystanie często z niezabezpieczonej sieci oraz niebezpieczne środowisko przechowywania danych.

Aby stworzyć odpowiedni poziom bezpieczeństwa dla IoT, należy zadbać o kilka elementów:

- fizyczne zabezpieczenie urządzeń;
- dostatecznie zabezpieczony proces identyfikacji i autoryzacji użytkownika;
- zabezpieczenie komunikacji pomiędzy urządzeniami;
- zapewnienie bezpieczeństwa chmurze, w których przechowywane są dane IoT;
- zintegrowanie systemu bezpieczeństwa IoT.

ARTYKUŁ PARTNERA

BLOCKCHAIN JAKO AKCELERATOR TRANSFORMACJI CYFROWEJ W POLSCE

Michał Pierzgalski
Ekspert z Obszaru Rozwoju Systemów i Sektor Publiczny, KIR

4

Niewiele ponad dekadę zajęło blockchainowi przejście od fazy eksperymentalnej do wypracowania opcji praktycznego zastosowania nowej technologii w wielu dziedzinach gospodarki. Zastosowana w 2009 r., na potrzeby obsługi bitcoina rozproszona baza danych, obecnie jest wykorzystywana m.in. w bankowości, finansach, ubezpieczeniach czy logistyce. Systematycznie pojawiają się kolejne potencjalne obszary zastosowania technologii blockchain, a Polska jest jednym z liderów rozwoju inicjatyw, mających na celu akceleracje innowacyjnych rozwiązań blockchainowych.

Blockchain to technologia, która jest wykorzystywana do bezpiecznego przechowywania oraz przesyłania informacji, układanych w sekwencje bloków danych. Jej unikalnymi cechami jest decentralizacja oraz wykorzystanie mechanizmu konsensusu, które wykluczają możliwość dokonywania jakichkolwiek zmian czy ingerencji w zapisanych informacjach w sposób niezauważony przez innych użytkowników. Co więcej, ze względu na brak centralnego serwera przechowującego dane, jest wyjątkowo skutecznie zabezpieczona przed cyberatakami.

Blockchain przestaje być eksperymentem

Korzyści ze stosowania rejestrów rozproszonych pierwszy zauważył sektor finansowy, także poza obszarem tradycyjnie i niesłusznie utożsamianym z blockchainem czyli światem kryptowalut. Branża korzysta już np. z trwałego nośnika - narzędzia opartego na tej technologii, które umożliwia przekazanie dokumentów w wersji elektronicznej w sposób zapewniający ich trwałość i nieusuwalność. W polskim sektorze bankowym, rozwiązanie wykorzystujące trwały nośnik oparty na blockchain i macierzy WORM,

dostarczane przez KIR, stosują już PKO Bank Polski oraz Bank BNP Paribas. Z czasem technologię tę dostrzegły także inne branże - blockchain wykorzystuje się dziś także w ubezpieczeniach, logistyce, opiece zdrowotnej czy kulturze.

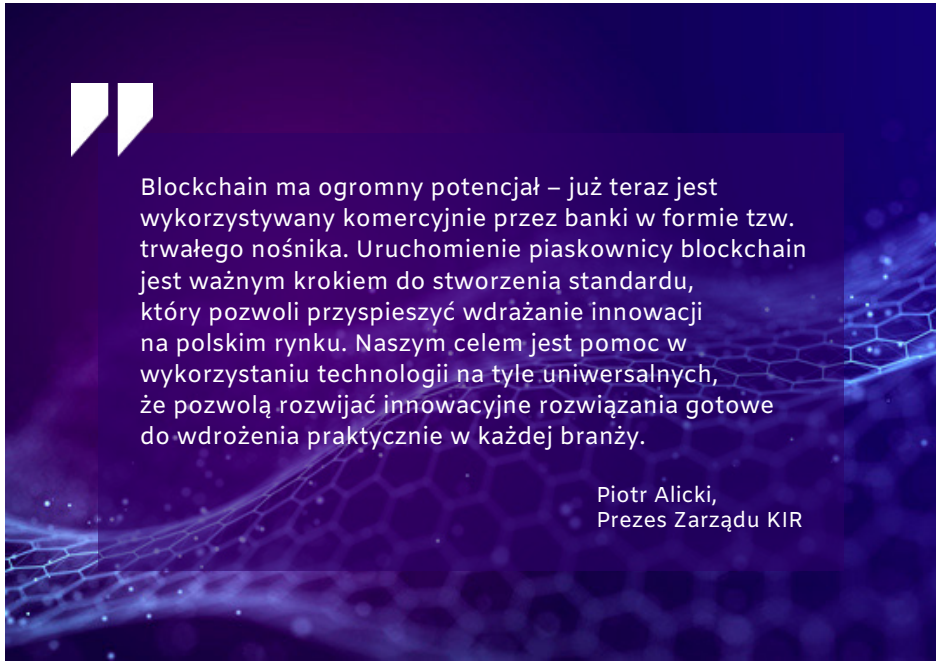
Eksperci prognozują, że w najbliższych latach będziemy obserwować intensywny rozwój blockchain. 55 proc. światowej kadry zarządzającej zaliczyło inwestycje w blockchain do pięciu najważniejszych strategicznie obszarów rozwoju, a tylko 2 proc. ankietowanych uważa, że nie będą mieć one większego znaczenia[1]. 88 proc. uczestników Deloitte's 2020 Global Blockchain Survey uważa, że uniwersalność tego rozwiązania przyczyni się do jego upowszechnienia. Zdaniem 83 proc. ankietowanych, firmy będą wprowadzać blockchain, żeby zachować konkurencyjność. Natomiast wg PwC's Global Blochchain Survey 2018, 84% światowych organizacji rozpoczęło, nawet w niewielkim stopniu inwestycje w ten rodzaj technologii[2].

Polska wyprzedza Europę

Pod koniec 2020 r. KIR wraz partnerami - instytucjami i firmami od lat działającymi na rzecz rozwoju polskiego sektora technologicznego, uruchomił piaskownicę blockchain, czyli platformę technologiczno-biznesową oferującą unikalne rozwiązanie dla firm, w tym startupów, zainteresowanych rozwijaniem biznesu opartego na blockchain. Sandbox Blockchain to pionierski koncept całkowicie bezpłatnego środowiska przeznaczonego do akceleracji innowacyjnych rozwiązań opartych na tej technologii.

We wrześniu ubiegłego roku Komisja Europejska ogłosiła, że do 2022 r. wraz z European Blockchain Partnership (EBP) uruchomi piaskownicę regulacyjną skoncentrowaną na kryptowalutach i blockchainie[3]. Jest to część unijnej strategii Digital Finance, której celem jest m.in. zapewnienie równych warunków działania dostawcom usług finansowych: zarówno tradycyjnym instytucjom bankowym, jak i przedsiębiorstwom technologicznym.

1. https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR proc.202020 proc.20global proc.20blockchain proc.20survey.pdf
2. https://www.pwccn.com/en/research-and-insights/publications/global-blockchain-survey-2018/global-blockchain-survey-2018-report.pdf
3. https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership



Komercjalizacja nowych rozwiązań to wyzwanie

Globalne zainteresowanie blockchainem spowodowało wzrost liczby firm, które budują swoje usługi z wykorzystaniem tego rozwiązania. Tylko w Polsce działa obecnie ponad 40 startupów pracujących wyłącznie nad blockchainem. Liczba ta jest jednak w rzeczywistości znacznie większa, gdyż w raportach nie uwzględnia się przedsiębiorstw, których działalność skupia się także na innych technologiach[4].

Upowszechnianie się usług opartych na blockchainie w gospodarce wymaga dopasowania komercjalizowanych rozwiązań do obowiązujących regulacji. Decydenci twierdzą, że właśnie niepewność regulacyjna to największa trudność we wdrażaniu w organizacjach tego rodzaju technologii[5]. Stanowi to nierzadko wyzwanie, zarówno dla dużych jak i małych podmiotów, które muszą ponosić duże koszty testowania swoich nowych pomysłów biznesowych.

Skuteczność narzędzi typu piaskownica jest od lat obserwowana za granicą – badania przeprowadzone na brytyjskim rynku pokazały, że uczestnictwo w piaskownicy ma pozytywny wpływ na zwiększenie pozyskiwanego kapitału od inwestorów – aż o 15%. Funkcjonowanie środowisk testowych ma znaczenie także dla zmniejszenia asymetrii w zakresie informacji oraz kosztów regulacyjnych. Autorzy badań uznali, że piaskownice mogą stać się kluczowym narzędziem do czerpania korzyści z innowacji finansowych[6].

Wiemy, jak dużym wyzwaniem biznesowym, operacyjnym, technologicznym i kosztowym jest wprowadzenie na rynek nowego rozwiązania. KIR, jako sektorowy hub technologiczny wdrażający innowacyjne narzędzia cyfrowe, ma wieloletnie doświadczenie w tej dziedzinie i chce się nim dzielić. Dlatego w ramach Sandbox Blockchain, wraz z partnerami projektu,

4. https://tracxn.com/explore/Blockchain-Startups-in-Poland
5. https://www.pwccn.com/en/research-and-insights/publications/global-blockchain-survey-2018/global-blockchain-survey-2018-report.pdf
6. https://www.bis.org/publ/work901.htm

oprócz dedykowanego środowiska technologicznego, zapewnia uczestnikom kompleksowe wsparcie w procesie komercjalizacji. Użytkownicy platformy mogą nie tylko testować swoje pomysły pod względem technologicznym, ale również wymieniać się wiedzą oraz doświadczeniami z partnerami projektu.

W budowę Sandbox Blockchain, oprócz KIR włączyli się: PKO Bank Polski, IBM, Chmura Krajowa, UKNF, Fundacja Fintech Poland oraz Fundacja KIR na Rzecz Rozwoju Cyfryzacji Cyberium. W 2021 r. testy swoich rozwiązań w ramach platformy rozpoczęło 19 firm. W tej pierwszej grupie znalazły się przedsiębiorstwa i startupy z branży finansowej oraz spółki zajmujące się energetyką, logistyką, sprzedażą, dostawcy rozwiązań z zakresu bezpiecznego obiegu dokumentów i poufnej komunikacji, firmy związane z obsługą sektora bankowego, a także oferujące usługi i systemy IT dla firm.

Szczegółowe informacje na temat projektu Sandbox Blockchain oraz informacje o możliwości dołączenia do inicjatywy dostępne są na stronie: https://www.sandboxblockchain.pl/.

ROZWIĄZANIA CHMUROWE I BACKUP DLA FIRM. DLACZEGO WARTO?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

5

Według Głównego Urzędu Statystycznego, w 2020 roku z płatnych usług chmurowych korzystało 24,4% przedsiębiorstw w Polsce, a to oznacza wzrost o prawie 7% w porównaniu z rokiem poprzednim. To sporo, ale i sporo mniej niż wynosi europejska średnia.

Polskie firmy przez długie lata do chmury podchodziły sceptycznie, wybierając raczej rozwiązania on premise niż cloud-native, czyli takie, które dostępne są natywnie jedynie w chmurze. Wydaje się jednak, że liczne zalety chmury zaczynają wreszcie przeważać szalę na jej korzyść.

Bo faktycznie wydaje się, że chmura jest lepiej dostosowana do potrzeb współczesnych przedsiębiorstw, zwłaszcza tych, które w 2020 roku w ekspresowym tempie przeszły na model pracy zdalnej. To właśnie rozwiązania chmurowe umożliwiły im skonfigurowanie „wirtualnego biura", ale później, wiele z nich stworzyło już pełną, świadomą, chmurową strategię, wybierając podejście multi-cloud, w którym - do wykonywania różnych zadań - sięgają po różne platformy, redukując w ten sposób ryzyka, towarzyszące trzymaniu się jednego tylko dostawcy.

Jakie zalety przekonują firmy do rozwiązań chmurowych?

Chmura to bynajmniej nie tylko narzędzia takiej Teams, Slack czy Zoom. To cały model, w którym zamiast kupować usługi, niejako je wypożyczamy, ograniczając w ten sposób koszty aktualizacji, utrzymania i rozwoju systemów oraz wsparcia technicznego. Dzięki temu organizacja może szybko skalować - w górę lub w dół - potrzeby w zakresie wykorzystania infrastruktury tak, by dopasować je do zmieniających się potrzeb i możliwości.

Czy nasze dane są bezpieczne?

Decyzję o zabezpieczaniu danych powinna ułatwić nam świadomość ilości zagrożeń, jakie na nie czyhają. Do utraty danych może dojść z wielu przyczyn, np. awaria sprzętu, działanie użytkownika, kradzież, a także pożar lub zalanie. Coraz częściej użytkownicy narażeni są na ataki z zewnątrz, ogromnym zagrożeniem są wirusy szyfrujące.

Jak się zabezpieczyć?

Produkty Synology gwarantują ochronę danych, zapewniając przy tym szereg dodatkowych funkcji. Do wyboru mamy rozwiązania obsługujące od jednego, aż do 180 dysków. Jednak nawet 2-dyskowy model serii Plus obsłuży wszystkie opisywane tutaj funkcje.

Przy wyborze serwera NAS nie możemy bazować jedynie na dobrej specyfikacji sprzętowej. Bardzo ważne jest zoptymalizowane oprogramowanie oraz to, jak producent podchodzi do kwestii zabezpieczeń. Serwerem Synology zarządza system DSM. Jego najważniejsze cechy to intuicyjność, wydajność i przede wszystkim bezpieczeństwo. Możliwość logowania dwuelementowego zapewnia usługa SignIn, dodatkową ochroną będzie urządzenie mobilne lub klucz sprzętowy. Automatyczne blokowanie i zapora sieciowa chronią przed atakami z zewnątrz. Automatycznie mogą instalować się także ważne aktualizacje.

Ochrona infrastruktury IT

Zanim dane trafią na bezpieczny serwer, musimy je tam przetransportować. Z pomocą przychodzi narzędzie Active Backup Suite, które zabezpieczy nasze komputery, serwery fizyczne, serwery plików, maszyny wirtualne Hyper-V i VMware, a także środowiska Microsoft 365 i Google Workspace. To wszystko w cenie urządzenia, bez dodatkowych opłat. Dzięki deduplikacji zaoszczędzimy miejsce, szyfrowanie zapewni dodatkowe bezpieczeństwo, a funkcja kopii bare-metal pozwoli na szybkie przywrócenie danych.

Dostępny jest także pakiet Synology Drive, służący do stworzenia prywatnej chmury. Znajdziemy tam rozbudowany system uprawnień i obsługę wersjonowania. Synology Drive pozwala na synchronizację danych i współpracę wielu użytkowników, obsługuje również kopię plikową. Oprócz aplikacji klienckiej, do dyspozycji mamy portal dostępny przez przeglądarkę oraz aplikacje mobilne.

Ochrona serwera NAS

Przed skutkami potencjalnej awarii dysków chroni nas system RAID. Nad zapisem i przechowywaniem danych czuwa nowoczesny system plików Btrfs. Chroni on przed tzw. cichym uszkodzeniem danych, wykorzystując do ich naprawy sumy kontrolne. Kolejny element to migawki, które zapamiętują stan naszych plików. Dane możemy przywrócić w każdej chwili, np. po ich przypadkowym usunięciu lub po ataku wirusa szyfrującego.

Zgodnie z zasadą 3-2-1, jedna kopia to za mało. Rozwiązaniem jest aplikacja Hyper Backup, obsługująca deduplikację i wersjonowanie, która pozwoli na skopiowanie naszych danych z Synology do innych lokalizacji, zarówno fizycznych jak i chmurowych, w tym do Synology C2 Storage.

Dla środowisk wymagających maksymalizacji pracy bez przestojów dostępne jest narzędzie Synology High Availability. Z dwóch takich samych serwerów (nawet dwudyskowych) stworzymy klaster wysokiej dostępności, synchronizujący się w sposób ciągły. W przypadku awarii wszystkie usługi przełączą się automatycznie, a dane będą dostępne niemal natychmiast.

Bądź bezpieczny przed szkodą

Koszty ratowania danych po awarii znacząco przewyższają koszty wdrożenia systemu kopii zapasowej. Tylko od nas zależy, czy będziemy należeć do osób robiących regularne kopie, czy do grupy, która dopiero będzie je robić. Stawką są nie tylko nasze nerwy, ale przede wszystkim bezpieczne funkcjonowanie naszej firmy.

Tomasz Iwańczuk
Synology Solution Engineer

Synology®

Chmura oznacza też bezpieczeństwo. Oczywiście, nie daje 100-proc. gwarancji, że usługi hostowane na infrastrukturze gigantów takich jak Google czy Amazon nigdy nie ulegną czy to awarii, czy klęsce żywiołowej, ale w tym przypadku - oprócz tego, że jest to dużo mniej prawdopodobne ze względu na skalę i jakość używanych zabezpieczeń - nie ma obaw o ciągłość działania.

Przechowywanie danych w chmurze zapewnia bowiem tworzenie ich kopii zapasowych i ochronę w bezpiecznej lokalizacji. A możliwość szybkiego ponownego uzyskania dostępu do danych pozwala prowadzić działalność w zwykły sposób, minimalizując przestoje i spadki produktywności.

Te i inne zalety sprawiły, że Polska pod względem wykorzystania rozwiązań chmurowych nie wlecze się już w ogonie Europy (teraz są to Grecja, Rumunia i Bułgaria). Wciąż jednak daleko nam do czołówki, którą tworzą kraje skandynawskie (Finlandia, Szwecja i Dania). Potencjał wzrostu przed polskim rynkiem jest więc ciągle jeszcze spory, ale - mimo niewątpliwych zalet chmury - przed migracją, warto zdać sobie sprawę również z jej wad i zrozumieć ryzyko.

Czy migracja do chmury wiążą się z ryzykiem?

Co jest więc kluczowe? Przede wszystkim - zawarcie odpowiednich umów z dostawcami usług. Powinny one zawierać zapisy regulujące poziom usług (SLA). Dokładna analiza umowy SLA oraz upewnienie się, że każda ze stron rozumie własne zobowiązania, to punkt wyjścia. Warto jednak zastanowić się również, jak dane będą przechowywane i zabezpieczone podczas outsourcingu. Zapisy o tym, kto ma dostęp do danych i jakie środki bezpieczeństwa zostaną przedsięwzięte, by je chronić, również powinny znaleźć się w umowie.

Przed podjęciem decyzji należy też sprawdzić, gdzie przechowywane - fizycznie - będą dane oraz jakie przepisy dotyczące prywatności i bezpieczeństwa będą miały do nich zastosowanie. Znajomość wymogów prawnych i regulacji obowiązujących w danej lokalizacji geograficznej ma bowiem ogromne znaczenie.

W maju 2020 roku, Microsoft poinformował o zamiarze wybudowania pierwszego w Europie Środkowo-Wschodniej data center w Warszawie. Microsoft zainwestuje miliard dolarów, a część tej kwoty zostanie przeznaczona na programy wsparcia transformacji cyfrowej.

Jednak to nie obiektywne czynniki, a raczej brak kompetencji jest główną przeszkodą, która stoi na drodze rozwiązaniom chmurowym, wynika z badań serwisu Computerworld.

Czy nadal warto trzymać kopie danych lokalnie?

Bezpieczeństwo systemów IT oraz zapewnienie ciągłości dostępu do usług wymaga złożonych i kosztownych rozwiązań. Kopia zapasowa potrzebuje urządzeń do składowania danych, zasad ich weryfikacji, przechowywania w bezpieczny sposób czy procedur wynoszenia poza organizację.

Znacznie wygodniej stworzyć kopię danych w chmurze, dlatego wielu klientom Sii polecamy usługi MS Azure. Dzięki nim możemy zbudować rezerwowe centrum danych, które nie wymaga zakupu sprzętu i oprogramowania, wynajmu powierzchni czy złożonej konfiguracji. A do tego automatycznie uruchomi nasze aplikacje, gdy nastąpi awaria lub pozwoli nam odtworzyć kopie, gdy stracimy dostęp do serwerowni czy laptopa.

Azure Backup to usługa, której zadaniem jest wykonanie i przechowywanie kopii naszych danych w chmurze. Może chronić serwery wirtualne, bazy danych i wybrane foldery na naszych serwerach. Konfiguracja jest bardzo prosta, usługa posiada też centralny panel zapewniający monitoring, system raportowania i alerty. Kopie w chmurze są odpowiednio szyfrowane, a klucz szyfrujący nie opuszcza naszego serwera.

Azure Site Recovery to druga usługa, która wykonuje kopie naszego środowiska w chmurze. W odróżnieniu od Backupu przechowuje tylko 24 kopie co godzinę, ale zapewnia bardzo szybki proces przywrócenia środowiska. Sam proces odtworzenia danych można zautomatyzować i jest on znacznie krótszy niż odzyskiwanie danych z kopii zapasowych.

Obie usługi doskonale się uzupełniają. Azure Site Recovery zapewni niski czas utraty danych i przywrócenia środowiska, Azure Backup - dostęp do archiwalnych danych. Co ważne, płacimy jedynie za rzeczywiste wykorzystanie tych rozwiązań, więc ich koszt jest znacząco niższy niż tradycyjnych kopii danych realizowanych lokalnie.

Krzysztof Polewiak
Cloud Solutions Architect w Sii Polska

Brakuje zarówno specjalistów, którzy potrafią zaprojektować infrastrukturę chmurową i procesy migracji zasobów, jak i osób, które mogłyby zarządzać tym procesem od strony prawnej. Aż 43% firm przebadanych w ankiecie Computerworld przyznało, że ich organizacje dopasowały rozwiązania chmurowe do poziomu posiadanych kompetencji. I pewnie też dlatego wiele firm wciąż jeszcze wybiera produkty w tradycyjnym modelu, który wymaga zakupu infrastruktury, oprogramowania i usług.

A jest to model z całą pewnością nieprzystający do dzisiejszego, ciągle zmieniającego się świata. Wymaga inwestycji, które zwrócą się w najlepszym razie w ciągu kilku lat i wydatnie ogranicza zwinność modelów biznesowych.

Sztuczna inteligencja w cyberbezpieczeństwie

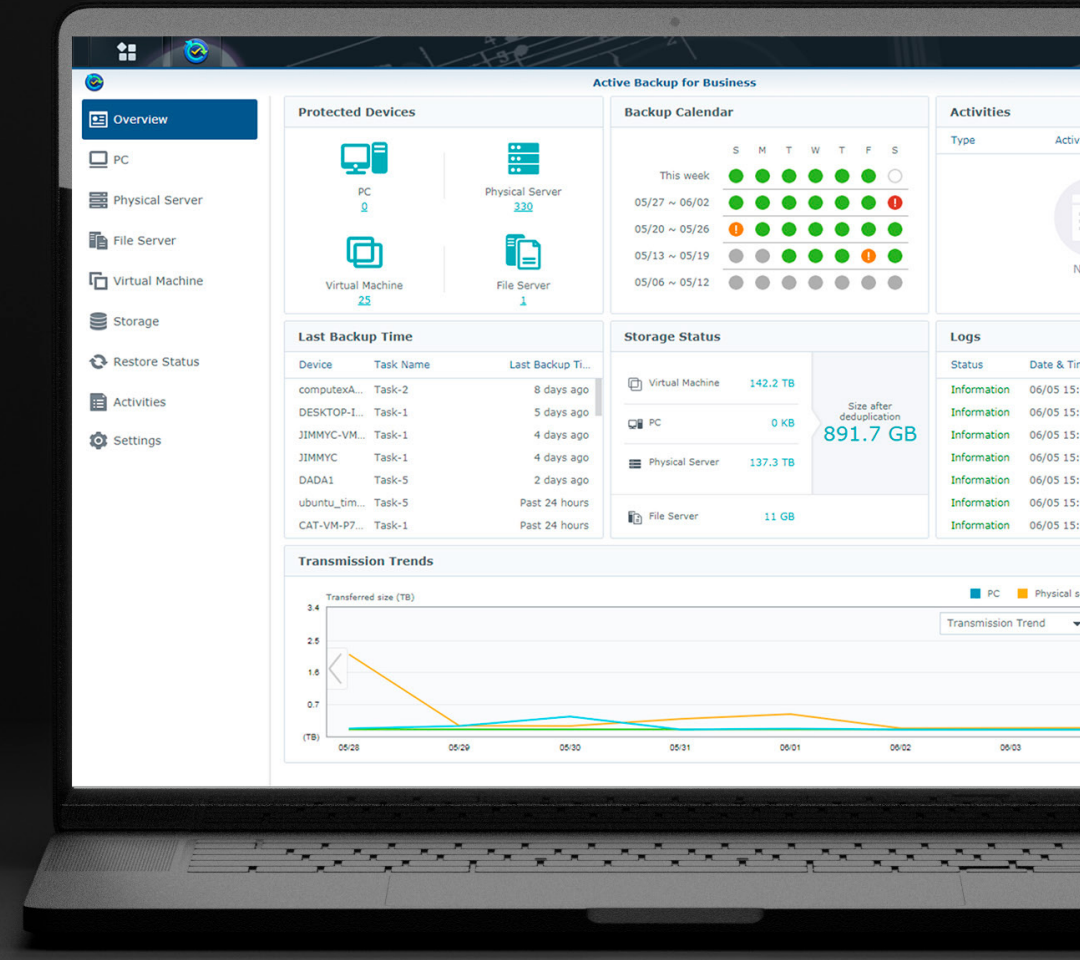
Według TechRepublic, średniej wielkości firma codziennie otrzymuje alerty o ponad 200 000 cybernetycznych zdarzeń i nietrudno nie domyślić się, że żaden zespół ekspertów ds. bezpieczeństwa nie będzie w stanie manualnie ich przetworzyć. I tutaj wkracza sztuczna inteligencja, która może ich wspierać w tej nierównej walce.

Sztuczna inteligencja i uczenie maszynowe stają się obecnie niezbędne dla bezpieczeństwa informacji, ponieważ technologie te są w stanie szybko analizować miliony zestawów danych i śledzić szeroką gamę zagrożeń cybernetycznych, od zagrożeń

Synology®

Backup danych i ciągłość biznesowa

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



Uzyskaj kompleksową kopię zapasową dla:

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

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

50% firm pozostaje nieprzygotowanych na katastrofę

złośliwym oprogramowaniem po podejrzane zachowania, które mogą skutkować atakiem. Technologie te nieustannie się uczą i ulepszają, stale czerpiąc wiedzę z przeszłych doświadczeń i teraźniejszości, aby wskazać i przewidzieć nowe odmiany ataków, które mogą nastąpić.

Sztuczna inteligencja może być wykorzystywana do wykrywania cyberzagrożeń i potencjalnie złośliwych działań tam, gdzie tradycyjne systemy nie nadążają. Systemy AI, „szkolone" pod kątem wykrywania konkretnych wzorców i zachowań, to zupełnie inna historia. Dzięki temu, że samodzielnie gromadzą dane i uczą się każdego dnia - pozwalają reagować szybciej i działać prewencyjnie. Może bowiem dostarczyć informacji o wszystkich wykrytych anomaliach, porównać je z dostępnymi danymi i w ten sposób zidentyfikować nowe zagrożenie.

Jak wykorzystać AI w cyberbezpieczeństwie?

Walka z botami

Boty są dzisiaj prawdziwą plagą, z którą bez sztucznej inteligencji właściwie nie sposób sobie poradzić. AI pomaga zrozumieć, czy ruch, który trafia na stronę jest organiczny, czy sztucznie generowany.

Przewidywanie ryzyka naruszenia

Systemy AI mogą też określić, które elementy danej infrastruktury są potencjalnie narażone na ataki, dzięki czemu można zawczasu zaplanować strategię obrony i np. przydzielić większe zasoby do obszarów o największej podatności.

AI może obsłużyć ogromny ruch

Nawet w firmie średniej wielkości, przepływ danych - w tym danych wrażliwych - bywa na tyle duży, że zespół ds. cyberbezpieczeństwa nie może analizować całego ruchu pod kątem możliwych zagrożeń. AI to rozwiązanie, które pomoże wykryć wszelkie zagrożenia maskowane pod pozorem normalnej aktywności.

Według Capgemini Research Institute, wzmocnienie strategii cyberbezpieczeństwa za pomocą sztucznej inteligencji jest „pilne" dla nowoczesnych przedsiębiorstw. Sztuczna inteligencja jest zwyczajnie szybsza w reakcjach, a rodzaje zagrożeń zmieniają się zbyt często, by to lekceważyć.

TBMS DIGITAL MARKETING AGENCY

MARKETING DLA IT

STRONY INTERNETOWE, KAMPANIE GENERUJĄCE LEADY B2B, CONTENT MARKETING W MEDIACH BIZNESOWYCH

Skorzystaj z doświadczenia agencji specjalizującej się w promocji firm technologicznych

O AGENCJI

TBMS
| DIGITAL MARKETING AGENCY

SPÓŁKA SPECJALIZUJE SIĘ W DIGITAL MARKETINGU DLA FIRM TECHNOLOGICZNYCH,
ALE PRZYGOTOWUJE TAKŻE EVENTY ORAZ KAMPANIE
W MEDIACH KLASYCZNYCH

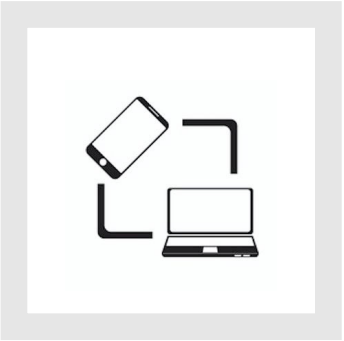
- Agencję stworzyli współtwórcy sukcesów największych w Polsce portali ekonomicznych.
- Eksperci spółki mają ponad 15-letnie doświadczenie w marketingu internetowym.
- Firma realizowała działania promocyjne dla największych firm z branży IT, które operują w Polsce i za granicą. Wśród nich są m.in:

- IBM,
- Comarch,
- Asseco,
- Salesforce,
- Sygnity.

NASZA SPECJALNOŚĆ TO DIGITAL MARKETING, A W SZCZEGÓLNOŚCI:

REKLAMA W INTERNECIE

Realizujemy kompleksowo kampanie reklamowe w sieci. Od koncepcji, poprzez realizację i zakup mediów, do raportowania efektów, a nawet monetyzacji. Media kupujemy także w modelu programmatic



STRONY INTERNETOWE

Wdrażamy nowoczesne witryny, przygotowane do pozycjonowania, dostosowane do urządzeń mobilnych, podążające za światowymi trendami. Od prostych landing page'y, przez wizytówki, aż do skomplikowanych projektów e-commerce

SEM - SEO I PPC, CONTENT MARKETING, LEAD GENERATION

… a także public relations i szkolenia oraz event marketing - agencja TBMS oferuje promocję typu 360 stopni

PROWADZIMY KAMPANIE REKLAMOWE GENERUJĄCE LEADY I BUDUJĄCE WIZERUNEK

WYSOKI ZWROT Z INWESTYCJI (ROI), PONADPRZECIĘTNA KONWERSJA

Oferujemy
m.in. kampanie:

- w wynikach wyszukiwania Google (Google Ads),
- reklamy tekstowe i graficzne w Google Display Network,
- display na najwiekszych portalach wertykalnych i horyzontalnych (m.in.: Onet, WP, Interia, Gazeta.pl),
- e-mail marketingowe,
- content marketingowe,
- natywne,
- w social media,
- typu lead generation,
- remarketingowe,
- w mediach kupowanych w modelu programmatic (m.in. RTB).

107

leadów B2B pozyskanych zaledwie w 30 dni dla Klienta wdrażającego rozwiązania infrastrukturalne IT

CONTENT MARKETING - REKLAMA NATYWNA - OFERUJEMY NIESTANDARDOWE FORMY PROMOCJI

Nasze
kampanie promocyjne:

- są natywne,
- konstruowane są w oparciu o potrzeby internautów, co sprawia, że nie tylko rozwiązują ich problemy, ale także budują zaufanie do promowanej marki,
- to nowoczesna forma promocji, uwzględniająca nie tylko oczekiwania sprzedażowe Klienta, ale łącząca multichannelowo także inne jego potrzeby marketingowe, np.: employer branding, public relations, CSR,
- mogą zostać połączone także z działaniami SEO oraz marketingiem szeptanym,
- obejmują m.in. tworzenie,

  - poradników,
  - e-booków (white paper),
  - artykułów eksperckich,
  - wideo,
  - webinarów,
  - infografik.

250

portali i blogów znajduje się w naszej stałej ofercie reklamowej. Z uznanymi wydawcami mamy wynegocjowane konkurencyjne ceny dla naszych Klientów

WP | onet

GAZETA.PL | Newsweek

BUSINESS INSIDER POLSKA | RZECZPOSPOLITA

Puls Biznesu | Forbes

TBMS

DIGITAL
MARKETING
AGENCY

ZAPRASZAMY

DO WSPÓŁPRACY

TBMS Sp. z o.o.
tbms.pl, kontakt@tbms.pl, tel.: 71 302 75 35

BLOCKCHAIN - MODA CZY ABSOLUTNA KONIECZNOŚĆ?

Kaja Grzybowska
redaktor Interaktywnie.com

kg@interaktywnie.com

7

Zainteresowanie tematem blockchainu - mimo towarzyszących tej technologii jeszcze niedawno kontrowersji - nieustannie rośnie. Z ciekawością przyglądają się jej nie tylko branża finansowa, ale również ta związana z nieruchomościami, medyczna, a nawet rozrywkowa. I choć nie brakuje opinii, że to ryzykowny wybór, nawet giganci skłonni są takie ryzyko podejmować, bo to się opłaca.

Zaledwie przed kilkoma dniami zrobił to TikTok, ogłaszając, że nawiąże współpracę z Audius, jedną z pierwszych platform streamingowych, działających na blockchainie. Partnerstwo ma mu ułatwić zarządzanie swoją rozległą wewnętrzną biblioteką audio. Dlaczego jednak zdecydował się na platformę opartą na blockchainie?

Co to jest blockchain?

Zacznijmy od definicji. Mimo że blockchain najbardziej kojarzy się z bitcoinem, to jest to technologia o dużo szerszym potencjale. To zdecentralizowany, niezmienialny rejestr operacji, do którego dostęp i wgląd mają wszyscy użytkownicy danej sieci.

System zbudowany jest z wielu równorzędnych elementów, które przechowują dane o wszystkich zatwierdzonych zmianach. Technicznie nie ma więc jednego „centrum zarządzania"; tę rolę pełnią bowiem wszystkie elementy systemu. I właśnie brak elementu centralnego jest kluczowy: wymiana informacji (również danych transakcyjnych) może bowiem dokonywać się wyłącznie na linii nadawca - odbiorca.

W sieci blockchain można śledzić i np. kupować bądź sprzedawać wszystko, co ma jakąś wartość - rzeczy materialne (dom, samochód, gotówka, grunt) i niematerialne (własność intelektualna, patenty, prawa autorskie, branding).

Ten model odróżnia Audius od platform, które wykorzystują bardziej popularne, „nieblockchainowe" serwisy takie jak Spotify czy Apple Music. Artyści korzystający z Audius

samodzielnie zarządzają swoją własnością, decydując, jak ją monetyzować i promować (mogą np. decydować, jakich stawek oczekują od słuchaczy za odtworzenie). W Spotify i Apple Music nie ma o tym mowy, co sprawia, że o prawdziwych zyskach mogą mówić jedynie największe gwiazdy.

I choć blockchainowi, jak już wspomnieliśmy, towarzyszą kontrowersje - w tym wypadku polegają one na tym, że Audius rozlicza się z artystami za pomocą własnej kryptowaluty - to zgoda co do tego, że technologia ta może być sposobem na zwiększenie przejrzystości przetwarzania danych, nie tylko danych finansowych, jest raczej powszechna.

Jakie branże mogą wykorzystać technologię blockchain?

Wydaje się jednak, że żadnej nagłej rewolucji nie będzie; stopniowe zmiany jednak - jak najbardziej. Decentralizacja sposobu rejestrowania danych, może zmienić strukturę współczesnej gospodarki, bo jej fundamentem jest informacja. Metody, które zapewniają natychmiastowy i dokładny przepływ informacji są obecnie testowane niemal we wszystkich branżach.

Czym jest blockchain i jak firmy mogą wykorzystywać tę technologię?

Blockchain to technologia, która zapewnia niezaprzeczalność zapisywanych za jej pomocą informacji. Znajduje zastosowanie wszędzie tam, gdzie niezbędna jest 'twarda' gwarancja zaufania. W przypadku rozwiązań cyfrowych to zaufanie może opierać się na odpowiedniej infrastrukturze umożliwiającej decentralizację baz danych, kontrolę rejestru wprowadzanych zmian i wgląd w chronologię.

W KIR uważamy, że blockchain to kolejny krok w ewolucji usług opartych na przesyłaniu lub współdzieleniu danych. W czasach przyspieszonej cyfryzacji, możliwość bezpiecznej wymiany informacji w trybie, który nie pozwala w nie ingerować bez wiedzy innych użytkowników, jest konkretną korzyścią biznesową dla wielu sektorów gospodarki. Dlatego w ramach Sandbox Blockchain, wraz z partnerami projektu, oprócz dedykowanego środowiska technologicznego, zapewniamy uczestnikom dodatkową wartość w postaci kompleksowego wsparcia w komercjalizacji innowacyjnych rozwiązań biznesowych.

Technologia blockchain jest obecnie w kręgu zainteresowań wielu sektorów komercyjnych - jak chociażby sektora energetycznego. Szczególna dynamika zmian na tym rynku, w tym zachodzących zwłaszcza w sektorze energii odnawialnej (rozwój mikroinstalacji PV, zmiany legislacyjne idące w kierunku modelu prosumenckiego), znacząco poszerza perspektywy praktycznego zastosowania tej technologii. Połączenie z komplementarnymi technologiami, takimi jak np. IoT, może istotnie przyspieszyć jej rozwój i umożliwić osiągnięcie zupełnie nowej jakości. Stąd, następnym krokiem po uruchomieniu piaskownicy Sandbox Blockchain, jest udostępnienie klientom KIR produkcyjnego rozwiązania blockchain, zaprojektowanego właśnie dla sektora energetycznego.

Małgorzata Ignaczewska
Biuro Inicjatyw i Projektów KIR

SANDBOX BLOCKCHAIN

Sandbox Blockchain - pierwsza w Polsce platforma do bezpłatnego testowania biznesowych pomysłów opartych na blockchain.

Twoja firma rozwija produkty lub usługi w oparciu o blockchain? Szukasz wsparcia biznesowego, sposobu na obniżenie kosztów infrastruktury i skrócenia „time to market”?

Poznaj platformę biznesowo-technologiczną Sandbox Blockchain i sprawdź:

- czy Twój pomysł na blockchainowy biznes ma szansę na wsparcie największego banku w Polsce;
- jak i gdzie aplikować do udziału w Sandbox;

KIR · Bank Polski · IBM · chmura krajowa · FIN TECH POLAND · KIR Fundacja Cyberium · INNOVATION HUB KNF

www.sandboxblockchain.pl

Blockchain pozwala śledzić zamówienia, płatności, rachunki w bardziej przejrzysty i tańszy - dzięki eliminacji pośredników - sposób. Dlatego też jest - zaraz po sztucznej inteligencji - uznawany za jeden z najbardziej perspektywicznych kierunków rozwoju, zarówno przez europejskich inwestorów, jak i przedsiębiorców.

Największe zainteresowanie implementacją technologii opartej na rozproszonych rejestrach na razie wykazuje branża finansowa. I nie, nie chodzi o kryptowaluty. Ze względu na ogromne przepływy dynamicznie zmieniających się danych, instytucje finansowe testują różne sposoby ich przetwarzania. Przykładów nie brakuje. Nasdaq współpracował z dostawcą infrastruktury blockchainowej - Chain.com - by ulepszyć sposób przetwarzania i walidacji transakcji finansowych; Bank of America, JPMorgan, New York Stock Exchange, Fidelity Investments i Standard Chartered testują, czy blockchainowe rozwiązania sprawdzą się jako zamiennik tradycyjnego przetwarzania transakcji w wybranych obszarach; a bank Kanady testuje cyfrową walutę zwaną monetą CAD dla przelewów międzybankowych.

Polskie instytucje finansowe także dostrzegają zalety blockchaina. PKO BP zdecydował się na współpracę z Coinfirm, by pracować nowymi rozwiązaniami weryfikującymi autentyczność danych, a GPW już zapowiedziała uruchomienie Private Market, która łączyć ma spółki poszukujące kapitału z inwestorami na rynku niepublicznym.

Zastosowanie tematem blockchaina nie ogranicza się jednak do finansów.

Właściciele praw autorskich wykorzystują łańcuchy bloków do ochrony utworów objętych prawem autorskim, w nadziei, że blockchain uchroni ich przed nieautoryzowanym udostępnianiem i pomoże w kontrolowaniu wysokości tantiem. Już dzisiaj istnieje wiele firm, które koncentrują się na tworzeniu nowych sposobów rejestracji i ochrony praw autorskich, w tym Binded, Pixsy, TinEye, Ascribe, Mediachain i Proof of Existence.

Ta sama zasada dotycząca blockchaina może pozwolić tej technologii znaleźć zastosowanie w opiece zdrowotnej. Rozproszone rejestry mogą umożliwić lekarzom i pracownikom służby zdrowia bezpieczny i łatwy dostęp do dokumentacji medycznej, niezależnie od wybranej placówki.

Blockchain może też być użyteczny w sektorze administracji oraz branży prawniczej. Dzięki niemu systemy głosowania byłyby bardzo trudne do sfałszowania, a działania związane ze zbieraniem podatków, zmianami w aktów własności, wpisów do ksiąg wieczystych, zostałyby uproszczone bez uszczerbku na bezpieczeństwie.

Pozostając przy temacie ksiąg wieczystych, blockchain testowany jest także przez branżę nieruchomości. Systemy oparte na tej technologii mogą bowiem zredukować i uprościć procesy

money.pl impact

Nagroda money.pl

Rusza III edycja Nagród money.pl.

Nagrody money.pl trafią do **najbardziej innowacyjnych firm i ludzi,** którzy w nieschematyczny, otwarty i nowoczesny sposób patrzą na biznes, wyznaczając jego trendy.

O nagrodzie

Nagroda money.pl to prestiżowe wyróżnienie przyznawane od 2019 roku. **W tym roku po raz trzeci wręczymy statuetki w październiku na uroczystej gali razem z Impactem**. Wyboru laureatów nagrody dokonuje kapituła złożona z prezesów największych polskich firm, doświadczonych menadżerów, a także przedstawicieli redakcji money.pl oraz Wirtualnej Polski. **Zgłoszenie do udziału w konkursie jest darmowe i może to zrobić każdy.**

- **Człowiek roku**
- **Firma roku**
- **Technologia roku**

związane z obiegiem dokumentów transakcyjnych. A dzięki tzw. inteligentnym kontraktom (takim, które zostaną „wykonane" automatycznie dopiero po spełnieniu określonych warunki, w tym finansowych) uproszczona zostanie procedura przeniesienia własności np. mieszkania. Pośrednictwo notariusza zostałoby bowiem wyeliminowane.

Czy blockchain jest bezpieczny?

Apologeci rozwiązania podkreślają jego przewagę nad tradycyjnymi metodami: według nich dużo łatwiej łatwo włamać się do jednego, centralnego rejestru danych, niż zhackować ten rozproszony, który, siłą rzeczy, wydaje się dużo większą barierą, tym bardziej, że zabezpieczony jest dwojako - kluczem szyfrującym i tzw. kluczem konsensów (historia transakcji musi zostać zatwierdzona przez wszystkie węzły, zanim zostanie zapisana).

Przeciwnicy zauważają jednak, że są odnotowywane skuteczne włamania na platformy kryptowalutowe. W czasie jednego z najgłośniejszych, w 2016 roku, przestępcy ukradli 50 mln z funduszu inwestycyjnego The DAO. I faktycznie, na razie blockchaina trudno uznać za remedium na wszystkie problemy związane z cyberbezpieczeństwem. Bo choć idea decentralizacji zasobów faktycznie eliminuje ryzyko pojedynczych ataków, to implementacja platform opartych o blockchain wciąż jeszcze nie jest idealna.

Z dużym prawdopodobieństwem można jednak stwierdzić, że przed blockchainem rysuje się obiecująca przyszłość, bo zwyczajnie ma potencjał, by zredukować koszty operacyjne, przy jednoczesnym zwiększeniu ich wydajności.

RAPORTY INTERAKTYWNIE.COM 2021

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: www.interaktywnie.com/biznes/artykuly/raporty-interaktywnie-com

Wykorzystane do raportu zdjęcia pochodzą z banku zdjęć Pixabay.