

01/2022



SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



Zarobki w cyber security do
35 tys. zł miesięcznie

Infrastruktura sieciowa
Wyzwania, koszty i potrzeby firmy

Blockchain - święty
graal bezpieczeństwa

Komunikacja nowych
technologii w 2022 roku
Trzy największe wyzwania

Bezpieczeństwo
w branży gier online

Blockchain – święty graal bezpieczeństwa	3
Wywiad z Marcinem Białym: Infrastruktura sieciowa. Wyzwania, koszty i potrzeby firmy	11
Bezpieczeństwo w branży gier online	17
HOME OFFICE - wydatki na cyberbezpieczeństwo	22
Komunikacja nowych technologii w 2022 r. Trzy największe wyzwania	30
Jak zabezpieczyć firmę przed kopiowaniem danych przez pracowników?	38
Zarobki w cyber security do 35 000 zł miesięcznie	43
Jak wygląda kontrola UODO w firmie?	48
Czym kierować się podczas wyboru odpowiedniego antywirusa dla Twojego przedsiębiorstwa?	52
Jak skutecznie zarządzać biznesem w 2022 roku?	59

SZANOWNI PAŃSTWO,

W Polsce najbardziej popularną metodą ataku jest phishing. Katalog sposobów ataków wbrew pozorom nie zmienia się znacząco - zmieniają się sposoby wykorzystania, styl komunikacji względem ofiary.

Rozwój technologii stawia coraz większe wyzwania przed firmami, które chcąc rozwijać bądź utrzymać swój biznes. Z drugiej strony cyberprzestępcy mają do dyspozycji coraz to łatwiejsze i wydajniejsze narzędzia, dzięki którym mogą atakować.

Aby skutecznie bronić się przed nimi trzeba mieć świadomość zarówno zagrożeń, ale i możliwości jakie dziś daje nam technologia.

Z wielką przyjemnością oddajemy w Państwa ręce najnowszy numer naszego magazynu, dzięki któremu mogą się Państwo dowiedzieć o nowych trendach w zakresie szerokorozumianego bezpieczeństwa w firmie.

Zapraszam serdecznie do lektury,

Rafał Slepniowski

BLOCKCHAIN – ŚWIĘTY GRAAL BEZPIECZEŃSTWA



Tomasz Szymański
Sygnisoft S.A.

W obecnym dygitalizującym się świecie coraz częściej borykamy się z problemami związanymi z bezpieczeństwem i zaufaniem do informacji prezentowanych w Internecie. Wraz z przenoszeniem usług do sieci i powszechnym ich wykorzystaniem w życiu codziennym, rośnie ilość przestępstw i wyłudzeń. Zagrożenia te istotnie wpływają na dyskusje o przyszłości obecnych rozwiązań i sposobach zabezpieczeń.

PANACEUM NA WSZYSTKIE PROBLEMY

Z jednej strony chcemy ułatwić sobie życie i wykorzystywać zdobycze postępu, z drugiej chcemy mieć pewność bezpieczeństwa w sieci. Coraz to nowsze zabezpieczenia nie nadążają za kreatywnością przestępców, a samo z nich korzystanie znacznie wpływa na wygodę i szybkość wykonywania operacji. Niemniej w ostatnich latach pojawiło się magiczne słowo blockchain, które dla wielu znawców jest świętym graalem bezpieczeństwa i panaceum na wszystkie problemy.

NA CZYM POLEGA FENOMEN BLOCKCHAINA I CO OZNACZA, ŻE JEST ZDECENTRALIZOWANY?

Najlepiej będzie to wytłumaczyć dość prostym przykładem. Weźmy np. komunikat prasowy, który został opublikowany przez spółkę Sygnisoft: „Firma Sygnisoft sprzedała na debiucie 100 000 akcji, nie wchodząc tym samym do grupy najgorszych debiutantów w tym roku” – jest to obiektywnie korzystny komunikat dla inwestorów. Taki komunikat z pe-

wnością będzie powielany przez inne media i może wywołać pozytywny ruch na akcjach.

Jednak czy w rzeczywistości firma Sygnisoft ma kontrolę nad tym komunikatem? Zdecydowanie nie, musi polegać na rzetelności dziennikarzy, którzy występują w roli interpretatora i pośrednika. Jeżeli ktoś chciałby celowo, lub nawet przez pomyłkę, zaszkodzić firmie Sygnisoft, może zmienić tylko jeden wyraz i napisać np. „Firma Sygnisoft nie sprzedała na debiucie 100 000 akcji, wchodząc tym samym do grupy najgorszych debiutantów w tym roku” – ten komunikat z pewnością może wywołać poruszenie wśród inwestorów i spowodować spadek wartości akcji.

Może się tak stać, ponieważ o tym co zostanie wyświetlone w danym medium lub agencji informacyjnej decyduje człowiek – najczęściej redaktor naczelny. Czy to przez ludzki błąd, czy celowe zdarzenie, taka informacja może się pojawić i zanim zostanie skorygowana, może wyrządzić wiele złego.

Czy jest zatem sposób, aby mieć 100% pewność, że dany komunikat będzie niezmienny

i zawsze taki sam, jak stworzył go autor, odporny na błędy ludzkie, te niezamierzone i te celowe? Twierdząca odpowiedź pojawiła się wraz z wymyśleniem rozwiązań opartych o rozproszoną technologię blockchain.

Zasady jej działania postaram się wytłumaczyć na dość obrazowym przykładzie. Wyobraźmy sobie, że każdy wyraz z powyższego przykładu jest zapisany w pudełku - bloku, który składa się z 19 elementów; 17 wyrazów; 1 przecinek; 1 liczba. Bloki są połączone ze sobą w bardzo konkretnym ułożeniu, dzięki temu tworzą komunikat, który chcemy zaprezentować, jak zostało to zademonstrowane na poniższym rysunku.



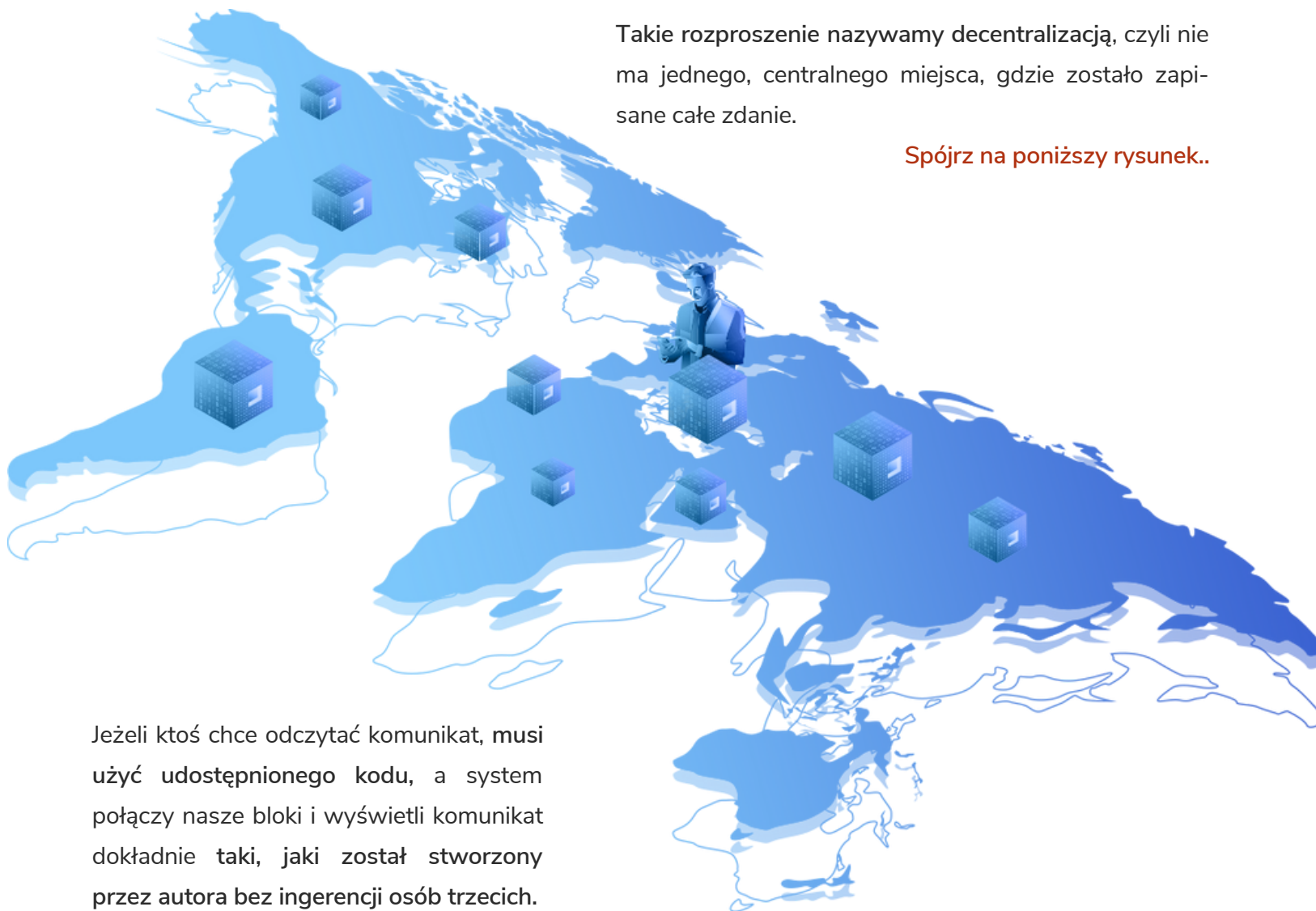
Z jednej strony chcemy ułatwić sobie życie i wykorzystywać zdobycze postępu, z drugiej chcemy mieć pewność bezpieczeństwa w sieci. Coraz to nowsze zabezpieczenia nie nadążają za kreatywnością przestępców, a samo z nich korzystanie znacznie wpływa na wygodę i szybkość wykonywania operacji.

To konkretne ułożenie bloków i sposób ich powiązanie względem siebie możemy zapisać w formie kodu dostępnego dla wszystkich - jeżeli chcesz odczytać komunikat spółki Sygnisoft użyj kodu, który Ci udostępniamy. Teraz wyobraźmy sobie, że te pudełka z poszczególnymi wyrazami zapisywane są na różnych losowo wybranych przez system serwerach zlokalizowanych w różnych częściach świata.

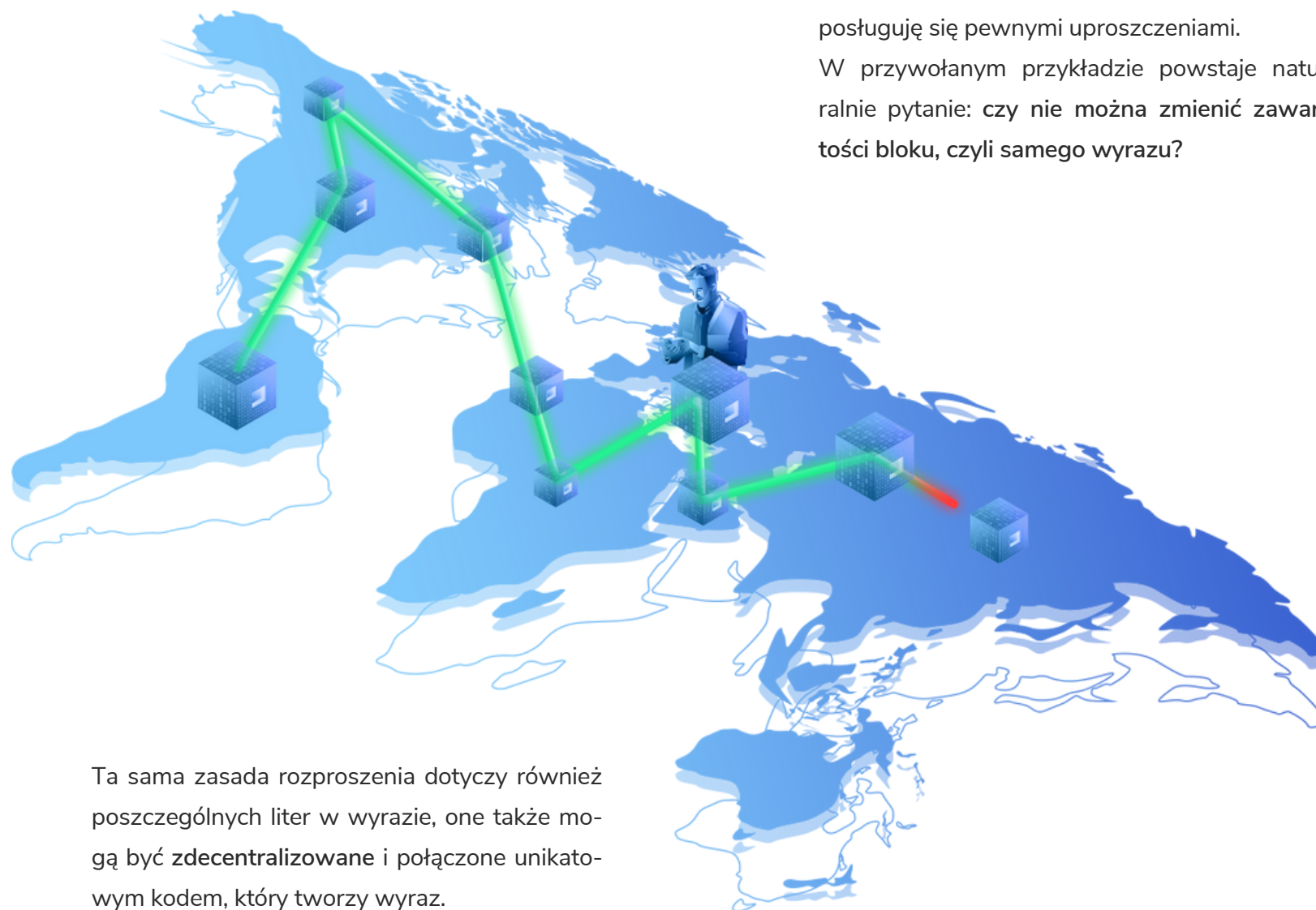
Wyraz „Firma” zapisany jest na serwerach w Argentynie, wyraz „Sygnisoft” w Malezji itd.

Takie rozproszenie nazywamy decentralizacją, czyli nie ma jednego, centralnego miejsca, gdzie zostało zapisane całe zdanie.

Spójrz na poniższy rysunek..



Jeżeli ktoś chce odczytać komunikat, musi użyć udostępnionego kodu, a system połączy nasze bloki i wyświetli komunikat dokładnie taki, jaki został stworzony przez autora bez ingerencji osób trzecich.



Dla zobrazowania zasad działania blockchaina posługuję się pewnymi uproszczeniami.

W przywołanym przykładzie powstaje naturalnie pytanie: czy nie można zmienić zawartości bloku, czyli samego wyrazu?

Ta sama zasada rozproszenia dotyczy również poszczególnych liter w wyrazie, one także mogą być zdecentralizowane i połączone unikatowym kodem, który tworzy wyraz.

Zastosowanie technologii blockchain daje nam 100% gwarancję bezpieczeństwa - **nikt nie może zmienić komunikatu ani nawet go usunąć**. Dzięki zdecentralizowaniu, nie ma jednego miejsca – serwera, gdzie cały komunikat byłby zapisany. Poszczególne elementy są rozproszone w wielu miejscach bez możliwości ich modyfikacji.

Tradycyjnie do przekazania jakiejś informacji możemy użyć kanału telewizyjnego lub portalu internetowego, gdzie wpływ na to co zostanie pokazane odbiorcom mają dziennikarze lub właściciel danego medium. W zdecentralizowanym systemie nie występują pośrednicy – każdy ma dostęp do oryginalnej treści na tych samych zasadach.

KRYPTOWALUTY

Chyba najbardziej flagowym wykorzystaniem blockchained są kryptowaluty. Podobnie jak w wyżej omawianym przykładzie najważniejszymi zaletami jest bezpieczeństwo oraz gwarancja niezmienności – braku wpływu osób trzecich. W tradycyjnych warunkach, szef banku centralne-

go może dowolnie podjąć decyzję o zwiększeniu ilości waluty – czyli **dodrukowaniu**.

Oczywiście, takie działania, szczególnie jeżeli nie mają pokrycia, **powodują obniżenie wartości pieniądza**. Kolejną wadą są oszustwa, podrabianie pieniędzy i inne fałszerstwa.

Świat kryptowalut eliminuje wszystkie te wady. Ilość Bitcoina jest z góry określona i znana, nie ma możliwości technicznych, aby było go więcej, aby ktoś niezależnie podjął decyzję i dodał kolejne miliony.

Dodatkowo, ponieważ jest zdecentralizowany **nie można go zablokować i modyfikować** – w zasadzie nikt nie ma na niego wpływu. Zasady jego działania i ilość jest z góry znana każdemu, pewnikiem jest również niezmiennosc tych elementów.

Te unikalne cechy powodują tak dużą **popularność kryptowalut** w ostatnim czasie i szeroko zakrojoną dyskusję na temat przyszłości tradycyjnych systemów monetarnych.

Zdecydowanie jesteśmy dopiero w początkowej fazie zastosowania rozwiązań blockchain. Kolejne obszary, w których coraz częściej jest wykorzystywany to weryfikacja podpisów umów między innymi przy walnych zgromadzeniach wspólników w spółkach, ksiąg wieczystych, wszelkich aktów notarialnych czy wykorzystanie blockchaina jako alternatywy dla obrotu akcjami czy zabezpieczania danych medycznych obywateli.

Aktualnie rozwiązania oparte o blockchain cierpią ze względu na brak regulacji prawnych i jasności w ich zastosowaniu. Niemniej należy zwrócić uwagę, że nowe pokolenie, które wchodzi w świat biznesu i coraz częściej ma możliwości decyzyjne, zupełnie inaczej podchodzi do otaczającego świata i przyjętych dotąd regulacji. Dla nich fizyczny podpis na kartce jest mało znaczący. Liczy się zaufanie, osoba, która reprezentuje dany projekt lub biznes. Są skłoni to większego ryzyka oraz wierzą, że ich pomysły zmieniają świat na lepszy. W ich opinii problem braku regulacji nie istnieje, ponieważ już dawno zauważyli, że biurokracja została daleko w tyle, a świat napędza odwaga, nawet kosztem większego ry-

zyzka, podejmowanego przy nowych przedsięwzięciach.

Aktualnie rozwiązania oparte o blockchain cierpią ze względu na brak regulacji prawnych i jasności w ich zastosowaniu. Niemniej należy zwrócić uwagę, że nowe pokolenie, które wchodzi w świat biznesu i coraz częściej ma możliwości decyzyjne, zupełnie inaczej podchodzi do otaczającego świata i przyjętych dotąd regulacji.

Bitdefender®



40%
RABATU



KOD RABATOWY:

LUTYBD

**Dla czytelników Security Magazine
mamy 40% rabatu na Bitdefender Internet Security!**

Teraz do końca lutego możesz zakupić roczną ochronę antywirusową dla komputerów z systemem Windows na każdą dostępną ilość stanowisk.

WYWIAD Z MARCINEM BIAŁYM: INFRASTRUKTURA SIECIOWA. WYZWANIA, KOSZTY I POTRZEBY FIRMY



Marcin Biały
Grandmetric Sp. z o.o

**Infrastruktura sieciowa w firmie.
Jakie wyzwania stoją przed firmami?
Jak znaleźć balans pomiędzy koszta-
mi, możliwościami a faktycznymi
potrzebami firmy?
Na te i inne pytania odpowiada
Marcin Biały, Advisory Architect
w Grandmetric.**



CZYM JEST DZISIAJ INFRASTRUKTURA SIECIOWA W FIRMIE. JAK NALEŻY JĄ POPRAWNIE DEFINIOWAĆ?

Mówiąc o infrastrukturze sieciowej trzeba przede wszystkim zdefiniować cel i charakter organizacji, w której taka infrastruktura ma działać. W większości firm infrastruktura sieciowa to nie tylko szereg urządzeń, ale także usługi i aplikacje. Zintegrowane ze sobą zapewniają bezpieczną, skuteczną i niezawodną komunikację użytkowników, aplikacji i systemów biznesowych. W mniejszych organizacjach infrastruktura może w całości sprowadzać się do kilku urządzeń sieciowych takich jak Access Point, przełącznik i Firewall, ale w większych organizacjach infrastruktura sieciowa to setki, a nawet tysiące urządzeń i aplikacji wspomagających i zabezpieczających pracę w sieci.

CO JEST WAŻNE PRZY PROJEKTOWANIU INFRASTRUKTURY SIECIOWEJ W FIRMIE?

Trzy kluczowe aspekty, które należy wziąć pod uwagę to niezawodność, wysoka dostępność

i bezpieczeństwo. Pierwsze dwa uzyskuje się, wykorzystując rozwiązania, które zapewniają ciągłość pracy sieci, nawet przy awarii pojedynczego punktu sieci. Z kolei bezpieczeństwo infrastruktury to bardzo obszerny temat. Mieści się w nim:

- bezpieczny dostęp do sieci przewodowej i bezprzewodowej,
- bezpieczny dostęp zdalny dla pracowników i kontraktorów,
- bezpieczeństwo na styku z Internetem
- zabezpieczenie systemów biznesowych i produkcyjnych.

W każdym z tych punktów powinniśmy dobierać rozwiązania odpowiadające charakterowi danej organizacji. Oprócz tego niezwykle istotny jest charakter ruchu sieciowego i wymagania biznesowe danej organizacji. Inaczej projektuje się sieci dla firm, które przechowują zasoby w chmurze publicznej, a inaczej dla klientów z własnym Data Center. Jeszcze inne podejście stosuje się, kiedy mamy do czynienia z systemami OT w ramach prowadzonej produkcji. Warto nadmienić, że doświadczenie architektów rozwiązań sieciowych pozwala projektować sieci optymalnie biorąc pod uwagę balans wymagań biznesu, jakość oraz koszt takich rozwiązań.

Z JAKIMI WYZWANIAM I MUSZĄ MIERZYĆ SIĘ DZISIAJ FIRMY W ZAKRESIE INFRASTRUKTURY SIECIOWEJ?

Do najważniejszych i najczęstszych wyzwań można zaliczyć trendy technologiczne i społeczne. To one najczęściej wpływają na zmianę podejścia do budowy sieci. Trendy technologiczne, które obecnie obserwujemy są związane z np. z koncepcją Przemysłu 4.0, migracją systemów do rozwiązań chmurowych czy wykorzystaniem na dużą skalę systemów typu SaaS (Software-as-a-Service).

Popularna dzisiaj praca hybrydowa to wyzwanie społeczne, które wymusza często nowe inwestycje i przebudowę obecnej sieci, by umożliwić efektywną komunikację w zespołach znacznie bardziej rozproszonych niż kiedykolwiek.

Drugim obszarem wyzwań jest cyberbezpieczeństwo, które wraz z przesunięciem większości biznesu do Internetu, staje się kluczowym czynnikiem determinującym rozwój systemów IT. Wspomniana już praca hybrydowa czy zdalna wymuszają dodatkowe zabezpieczenia użytkowników, wzrost wydajności takich rozwiązań jak VPNy i Remote Access, bezpieczną komunikację w ramach sieci WAN, a także bezpieczeństwo obszarze workloadów chmurowych.

JAKIE SĄ TRENDY W OBSZARZE INFRASTRUKTURY SIECIOWEJ?

Trendy w infrastrukturze sieciowej są de facto odpowiedzią na trendy technologiczne w IT. Do nich z pewnością możemy zaliczyć wykorzystanie środowisk **Software-as-a-Service**, środowisk chmurowych, wykorzystanie narzędzi takich jak Microsoft 365, pracę hybrydową czy zwiększoną krytyczność komunikacji między oddziałami firmy.

W obszarze infrastruktury sieciowej możemy więc mówić o zaawansowanych rozwiązaniach VPN, w tym bezpieczeństwie z wykorzystaniem rozwiązań typu **Passwordless** czy **Multi Factor Authentication**. W obszarze wsparcia **SaaS** i **Cloud** będzie to trend rozwiązań **Software-Defined WAN**.

W obszarze bezpieczeństwa to z kolei wszelkiego rodzaju rozwiązania **NAC** czy **MDM**. Wreszcie w obszarach **Edge Computing** będzie to chociażby hiperkonwergencja polegająca na łatwym zarządzaniu i skalowaniu środowisk serwerowych i wirtualizacyjnych.

Poza rozwiązaniami opartymi o konkretne technologie, trendem, który przybiera na sile jest potrzeba automatyzacji pracy z sieciami. Wynika to

ze stale zwiększającej się liczby obsługiwanych urządzeń sieciowych, ale również z przeciążenia istniejących zespołów IT pracą, spowodowanego niedoborem specjalistów na rynku. W obu przypadkach przemysłowa automatyzacja pozwala uzyskać przewagę konkurencyjną.

CZY PODEJŚCIE DO TEMATU MOŻE BYĆ INNE DLA FIRM, KTÓRE MAJĄ JEDNĄ ORAZ WIELE LOKALIZACJI?

Często wyzwania i potrzeby nie zależą nawet od samej wielkości firmy czy od liczby oddziałów, ale od usług, które są krytyczne dla jej istnienia. Kiedy firma posiada wiele lokalizacji, najczęściej potrzebuje niezawodnej sieci rozległej (np. **SD-WAN**), by zapewnić odpowiedniej jakości komunikację między oddziałami. W takim przypadku projektuje się lub przebudowuje istniejącą infrastrukturę sieciową zgodnie z wymaganiami biznesowymi klienta. Firma z jedną lokalizacją może mieć zupełnie inne wyzwania np. związane z bezpiecznym dostępem gościnnym czy z pokryciem sygnałem **Wi-Fi** całego zakładu produkcyjnego. Każdy klient to inna historia i inne priorytety.

JAK ZNALEŹĆ BALANS POMIĘDZY KOSZTAMI, MOŻLIWOŚCIAMI A FAKTYCZNYMI POTRZEBAMI FIRMY?

Chciałoby się powiedzieć, że odpowiedź na to pytanie jest łatwa. Doświadczony architekt rozwiązań bierze pod uwagę wymagania biznesowe klienta, specyfikę jego infrastruktury oraz bieżące trendy technologiczne. Potrafi zadać trafne i precyzyjnie skonstruowane pytania, by zważyć ryzyka i pomóc klientowi ich uniknąć. Dopiero wtedy można mówić o proponowaniu dopasowanego rozwiązania.

Co ciekawe, nierzadko zdarza się, że rozwiązanie problemu jest tańsze i prostsze niż się wydawało, tylko klient w ogóle o nim nie pomyślał. W dojrzałym podejściu do budowania oferty kluczowe jest to, by pomóc klientowi, a nie by za wszelką cenę sprzedać.

Jeśli klient pracuje na technologii od konkretnego vendora, nie będziemy mu na siłę przedstawiać wizji migracji do rozwiązania od innego producenta. To samo dotyczy półki cenowej. Jeśli polityka firmy zakłada wykorzystanie urządzeń określonej klasy, integrator powinien to uszanować. Tylko wtedy obie strony mają szansę na transakcję, z której będą zadowolone.



SZUKASZ
EKSPERTA W ZAKRESIE PEŁNIENIA FUNKCJI
INSPEKTORA OCHRONY
DANYCH

W TWOJEJ FIRMIE, KTÓRY BĘDZIE PONOSIŁ
ODPOWIEDZIALNOŚĆ ZA SVOJE DZIAŁANIA?



SPRAWDŹ NASZĄ OFERTĘ

BEZPIECZEŃSTWO W BRANŻY GIER ONLINE



Janis Lasmanis
Evolution



Rozwój gospodarki i technologii, a także wydarzenia wokół nas, zmuszają nas do zmiany myślenia i działania, a Internet odgrywa coraz bardziej kluczową rolę w naszym życiu niż kiedyś. I chociaż przyniósł on ludziom znaczną wygodę, to wygenerował jednocześnie wiele problemów związanych z cyberbezpieczeństwem, w tym ataki hakerskie i wycieki informacji.

KOPALNIA SKARBÓW DLA CYBERPRZESTĘPCÓW

Cyberbezpieczeństwo, szczególnie podczas pandemii, która wymusiła przeniesienie procesów biznesowych do sfery online, jeszcze bardziej zyskało na znaczeniu. Cyberataki nasiliły się w wielu sektorach - ten związany z grami i rozrywką nie jest wcale wyjątkiem. Co więcej, jest on niczym kopalnia skarbów dla cyberprzestępców. Rzeczywistość jest taka, że im więcej dana branża zarabia, tym bardziej narażona jest na tego typu zagrożenia ze strony cyberprzestępców, stąd też nie dziwi fakt, że branża gier, zwłaszcza online – tak popularna i szybko rozwijająca się – wpadła im w oko.

Hakerzy z każdym rokiem stosują coraz bardziej zaawansowane techniki ataków. Rośnie także liczba grup, które tworzą. Mogą przeprowadzać swoje ataki i dokonywać oszustw z dowolnego miejsca na ziemi – w lokalnej kawiarni, biurze czy w domu. Ciekawostką jest fakt, że niektórzy z nich pracują nawet dla firm, które atakują. Zmniejszenie skutków cyberataków i oszustw internetowych ma kluczowe znaczenie dla utrzymania branży gier i rozrywki online, aby zapewnić bezpieczeństwo korzystającym z tych rozwiązań.



WYZWANIA CYBERBEZPIECZEŃSTWA

Głównymi wyzwaniami związanymi z cyberbezpieczeństwem, przed którymi stoją dzisiejsze firmy z branży gier, to:

DDOS

ATAKI TYPU DISTRIBUTED DENIAL OF SERVICE

Wykorzystywane zazwyczaj do pozbawienia usługi dostępu do Internetu.

EXPEDITING I SCRAPING, CZYLI ATAKI OPARTE NA BOTACH

Zautomatyzowane zagrożenie, które polega na użyciu botów do przyspieszenia żmudnych lub czasochłonnych działań, zazwyczaj dla uzyskania jakiegoś rodzaju nieuczciwej przewagi w naruszeniu wyraźnych lub dorozumianych zasad normalnego korzystania z aplikacji i zbierania danych z witryny do złych celów, takich jak odsprzedaż treści, wykorzystywane zazwyczaj do pozbawienia usługi dostępu do Internetu

BOTNET

RODO

NARUSZENIE OCHRONY DANYCH

cyberprzestępcy kradną wszystko, co udało im się znaleźć - kod źródłowy z gier, jak również dane osobowe przechowywane na serwerach usługodawców,

ATAK TYPU RANSOMWARE

Ransomware to złośliwe oprogramowanie zaprojektowane w celu uniemożliwienia użytkownikowi lub organizacji dostępu do plików znajdujących się na ich komputerach i serwerach,

RANSOMWARE

PHISHING

ATAKI TYPU PHISHING I KRADZIEŻ KONT

hakerzy podstępnie nakłaniają ludzi do udostępniania informacji osobistych, takich jak dane uwierzytelniające lub zainstalowania złośliwego oprogramowania na urządzeniu,

ATAKI „ZERO-DAY”

to szeroki termin opisujący niedawno odkryte luki w zabezpieczeniach, które hakerzy mogą wykorzystać do zaatakowania systemów. Termin "zero-day" odnosi się do faktu, że sprzedawca lub deweloper dopiero co dowiedział się o tej luce – co oznacza, że ma "zero dni" na jej naprawienie.

ZERO-DAY

JAK WIĘC ZMNIJSZYĆ PRAWDOPODOBIENSTWO WYSTĄPIENIA CYBERATAKU?

Żaden biznes online nie jest w stu procentach bezpieczny od cyberataków. Oto kilka działań, które możemy podjąć, aby zachować czujność i być przygotowanym na okoliczność cyberataku:

- bądź o krok przed cyberprzestępcami lub przynajmniej biegnij w tym samym tempie co oni,
- zbadaj podatność firmy na cyberataki,
- wykonaj statyczną i dynamiczną analizę kodu,
- przeglądaj swój kod źródłowy,
- regularnie przeprowadzaj wewnętrzne testy penetracyjne i testy podatności,
- upewnij się, że posiadasz najwyższej klasy systemy bezpieczeństwa i ustawienia zabezpieczeń,
- bądź czujny.



sygnisoft

Bądź o krok przed innymi.

W Sygnisoft sprawnie projektujemy, tworzymy
i wdrażamy Twój pomysł.

HOME OFFICE - WYDATKI NA CYBERBEZPIECZEŃSTWO



Redakcja
SECURITY MAGAZINE



Pandemia zmusiła wiele przedsiębiorstw do przejścia na tzw. zarządzanie kryzysowe i wprowadzenie pracy zdalnej. Nie jest ona odkryciem ostatnich dwóch lat, ale skala korzystania z tej formy nigdy nie była tak szeroka. To z kolei zmusiło firmy do inwestycji w ochronę przeciw wyciekom i kradzieżom. Jakie narzędzia polecają? Jak wysokie koszty ponoszą w związku z tym?

BŁYSKAWICZNA ZMIANA MODELU PRACY

W raporcie na temat cyberbezpieczeństwa pracowników zdalnych „2020 Remote Workforce Cybersecurity Report” amerykańska firma Fortinet przeanalizowała wyzwania, przed jakimi stoją podmioty gospodarcze w wyniku przejścia na pracę zdalną, oraz sposób, w jaki planują zabezpieczać swoich pracowników zdalnych na przyszłość. Przeprowadzona została ankieta wśród liderów bezpieczeństwa z różnych branż - z sektora publicznego i prywatnego - w 17 różnych krajach na całym świecie.

Tak jak się spodziewano, szybkie przejście na nowy system pracy nie było łatwe. Prawie 30% firm musiało przenieść ponad połowę siły roboczej do pracy zdalnej praktycznie z dnia na dzień. 83% procent organizacji uznało to przejście za umiarkowane lub bardzo trudne. Największe trudności napotkały w temacie bezpiecznej łączności, później - zapewnienia ciągłości biznesowej i dostępu do aplikacji o znaczeniu krytycznym dla firmy.

Wyzwania są tym większe, że liczba cyberzagrożeń w czasie pandemii gwałtownie wzrosła. Jest to wynik zwiększonego uzależnienia od korzystania z urządzeń osobistych i napływu pracowników poza sieć korporacyjną. Cyberprzestępcy, a szczególnie ci bezwzględni, znaleźli w pandemii sposób na osiągnięcie własnych korzyści.

Raport “Cost of A Data Breach 2020”, opublikowany niedawno przez IBM ujawnił, że średnia wielkość szkody wyrządzona cyberatakami wynosi prawie 3,9 mln dolarów, tj. ok. 15 mln zł.

Przy czym zaznaczyć trzeba, że raport ten publikowany jest nie za cały okres trwania pandemii i jego autorzy oszacowali, że już sama praca zdalna spowodowała ogromne szkody w firmach.

**W ciągu jednego roku trwania
pandemii wzrost wysokości średniej
szkody wzrosła o 137 tys. dolarów,
czyli ponad pół miliona zł.**

PRACA ZDALNA TO RÓWNIEŻ ZAGROŻENIE, ALE FIRMY Z NIEJ NIE REZYGNUJĄ

I tak, według „2020 Remote Workforce Cybersecurity Report”, u 60% podmiotów gospodarczych wzrosła liczba prób naruszeń cyberbezpieczeństwa po przejściu na pracę zdalną. W 34% doszło do rzeczywistych naruszeń.

Z tego jednak powodu firmy nie chcą rezygnować ze zdalnego charakteru pracy swoich podwładnych. Z raportu wynika, że taka opcja odpowiada prawie 30% organizacji.

W związku z tym specjaliści ds. bezpieczeństwa nadal stoją przed wyzwaniem wdrożenia technologii i strategii, które pozwolą dobrze zabezpieczyć telepracę na przyszłość.

Kiedy przeprowadzano ankietę do sporządzenia raportu firmy Fortinet, już wtedy 40% ankietowanych wydawało więcej pieniędzy na wykwalifikowanych pracowników IT. Mieli oni wesprzeć już istniejące działy IT i pracowników zdalnych.

Jednak jak się okazuje, prawie wszyscy przed-

siębiorcy w perspektywie długoterminowej będą inwestować w zabezpieczenie telepracy.

Prawie 60% przedsiębiorstw wyda na ten cel blisko milion złotych w perspektywie najbliższego roku. Ponadto firmy chcą też dokonywać nieplanowanych aktualizacji istniejących systemów, by zabezpieczyć pracę zdalną. Nie wykluczają przy tym wdrażanie nowych technologii, z których wcześniej nie korzystali.



Co warto podkreślić, cyberbezpieczeństwo długo nie należało do priorytetów działań firm dotkniętych ograniczeniami wynikającymi z pandemii.

Dla większości osób zarządzających firmami zmiany wywołane przez covid-19 stanowiły zagrożenie w największym stopniu dla stabilności finansowej przedsiębiorstw, nie dla cyberbezpieczeństwa. Jednak jeśliby wziąć pod uwagę, że zdaniem autorów raportu IBM, ponad 40% szkód wynikających z ataków hakerskich stanowią utracone przychody przedsiębiorstwa, to dotychczasowe podejście musi się zmienić. Ulokowanie cyberbezpieczeństwa na ostatnich miejscach listy priorytetów działań anty-kryzysowych ma też wpływ na brak zastosowania pracy zdalnej do nowych zagrożeń.

W TE NARZĘDZIA INWESTUJĄ FIRMY NA ŚWIECIE

Choć ankieta wykazała, że 65% organizacji miało VPN (wirtualna sieć prywatna, virtual private network - tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy nadawcą i odbiorcą za pośrednictwem publicznej sieci, np.

przez internet) już przed pandemią, to tylko 37% organizacji posiadało uwierzytelnianie wieloskładnikowe (MFA). A przecież sieci VPN odgrywają ważną rolę w zapewnianiu bezpiecznej łączności, są po prostu jednym z elementów zabezpieczania dostępu.

Dodatkowo ponad 70% firm planuje zarówno aktualizację, jak i wdrożenie Network Access Control (NAC) lub rozwiązania do wykrywania zagrożeń na punktach końcowych (EDR). Wdrażając rozwiązania NAC, zespoły IT zyskują lepszą widoczność i kontrolę nad użytkownikami i urządzeniami w swojej sieci. W jaki sposób?

System NAC daje dostęp do zasobów i usług sieciowych na podstawie informacji takich jak:

- uwierzytelniona tożsamość użytkownika lub urządzenia,
- położenie,
- czas,
- aktualny lub historyczny stan zabezpieczeń urządzenia.

Na podstawie tych danych przyznawany jest dostęp.



Narzędzie EDR (Endpoint Detection and Response) z kolei zapewnia zaawansowaną ochronę przed zagrożeniami w czasie rzeczywistym dla punktów końcowych, zarówno przed, jak i po infekcji. Nie koncentruje się ono na identyfikowaniu złośliwego oprogramowania, a na wykrywaniu nieprawidłowych działań.

W przypadku nietypowej aktywności narzędzie generuje alert analitykom bezpieczeństwa, którzy nie tylko mogą zbadać jego przyczynę, ale i właściwie zareagować na określoną nieprawidłowość. Podsumowując, EDR daje stały wgląd w to, co dzieje się w naszej sieci - analizuje uruchomione procesy, usługi, pojawiające się wpisy w rejestrze czy powiązania między procesami.

Okazuje się, że 64% organizacji planuje zaktualizować lub wdrożyć tzw. SD-WAN, ale szczególnie dla domowego biura. Najważniejszą zaletą rozszerzenia bezpiecznej funkcjonalności SD-WAN na indywidualnych telepracowników, zwłaszcza superużytkowników (specjalne konto użytkownika służące do administrowania systemem), jest to, że mają oni zdalny dostęp na żądanie. Cechą tego narzędzia jest też dynami-

cznie skalowalna wydajność niezależnie od dostępności sieci lokalnej.

Secure Access Service Edge (SASE) – to zupełnie nowy model bezpieczeństwa i ochrony danych w chmurze. Nie ma co ukrywać, że migracja do chmury wpłynęła na poprawę produktywności, elastyczności i mobilności pracy. Jednak kontrola bezpieczeństwa jest tu

w przypadku 66% ataków korzystają z błędów przy konfiguracji usług w chmurze, rzadziej uciekają się do kradzieży danych dostępowych. I tak 17% organizacji zainwestowało w SASE już przed pandemią, a 16% - w wyniku pandemii. 58% planuje na przyszłość zainwestować w to rozwiązanie. Choć po raz pierwszy terminu SASE użyto w 2013 roku, to dopiero ostatnio postrzegane jest jako możliwość połączenia

**17% ORGANIZACJI ZAINWESTOWAŁO
W SASE JUŻ PRZED PANDEMIĄ,
A 16% - W WYNIKU PANDEMII.
58% PLANUJE NA PRZYSZŁOŚĆ ZAINWESTOWAĆ
W TO ROZWIĄZANIE.**

niezbędnym elementem funkcjonowania w takim modelu. Organizacje muszą zabezpieczyć dostęp do usług w chmurze i blokować zagrożenia, a także zapobiegać wyciekom danych. Z publikacji „The State of Cloud Security 2020” przygotowanej przez Vanson Bourne wynika bowiem, że cyberprzestępcy

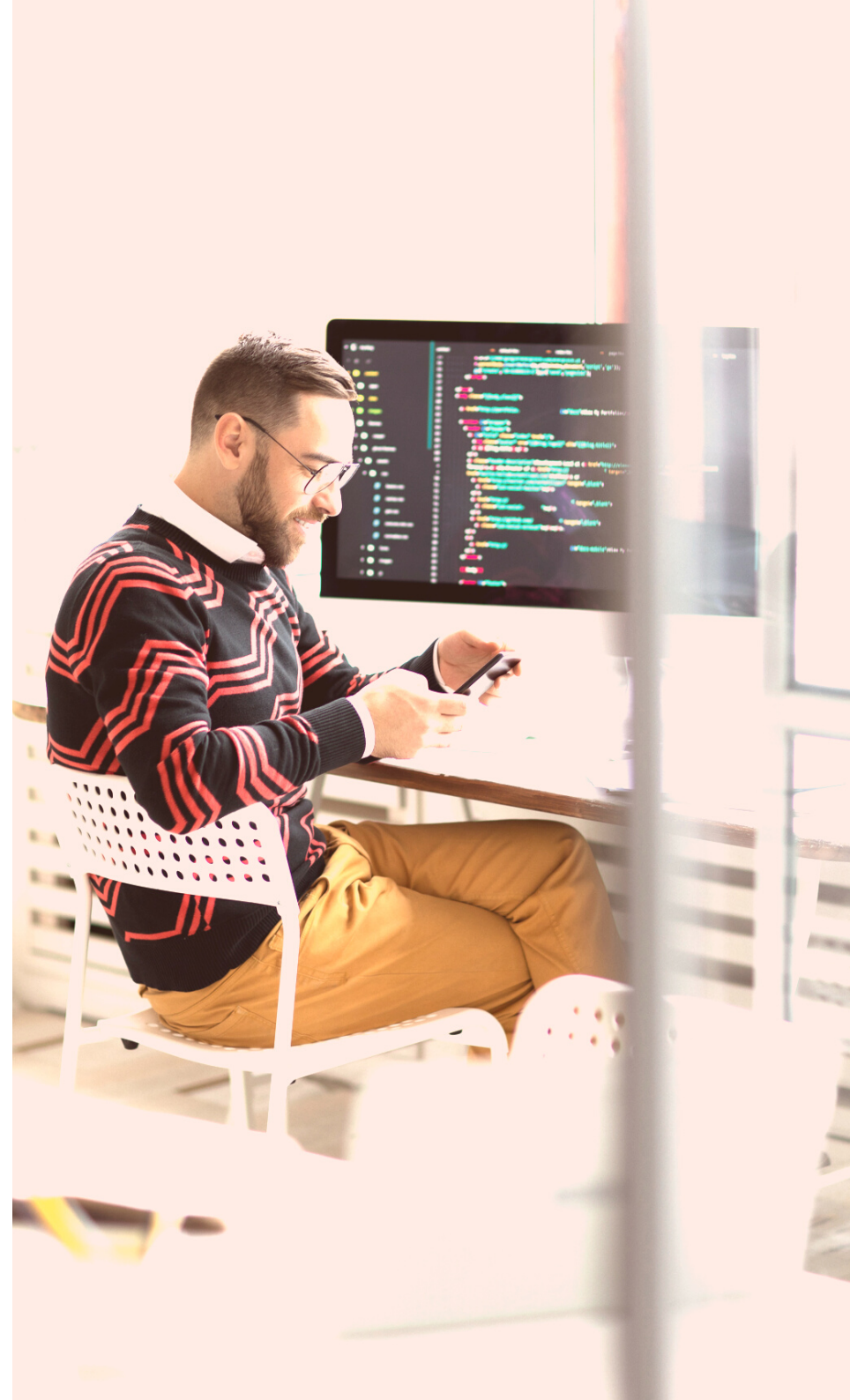
funkcji sieciowych i zabezpieczeń z możliwościami sieci WAN, by zaspokoić wciąż zmieniające się potrzeby współczesnych organizacji w zakresie bezpiecznego dostępu.

SPECJALIŚCI POTRZEBNI NA JUŻ

Musimy jednak pamiętać, że inwestowanie

w narzędzia i drogie rozwiązania to jedno. Najważniejsi są wykwalifikowani specjaliści z zakresu IT.

I tak okazuje się, że na początku pandemii tylko 55% organizacji dysponowało wystarczającą liczbą wykwalifikowanych pracowników IT, którzy mogliby wesprzeć przejście na pracę zdalną. Obecnie 73% organizacji ma zamiar dalszego inwestowania w wykwalifikowanych pracowników IT w ciągu tego roku. To brzmi bardzo obiecująco, choć oczywiście będzie to proces żmudny, jednak potrzebny.



OBSŁUGA PRAWNA E-COMMERCE



KOMUNIKACJA NOWYCH TECHNOLOGII W 2022 ROKU. TRZY NAJWIĘKSZE WYZWANIA



Paulina Fajtek
Come Creations Group



Okres pandemii nie jest łaskawy dla wielu branż. Nie można tego jednak powiedzieć o sektorze technologicznym, który ostatnio wprost rozkwita. Przenoszenie wielu aspektów życia do świata online, wykorzystywanie maszyn w coraz to nowych dziedzinach, czy możliwość oferowania swoich usług na całym świecie – wszystko to sprawia, że firmy technologiczne rozwijają się z niespotykaną dotąd prędkością.

START-UPY A UGRUNTOWANE FIRMY

Jednocześnie prostota zdobywania nowych rynków i docierania do klientów przez przedsiębiorstwa z branży nowych technologii często okazuje się pozorna. Zdarza się, że początkowy entuzjazm w przypadku start-upów lub nawet wieloletnie sukcesy organizacji z większym stażem zderzają się z coraz większymi oczekiwaniami rynku.

Firma CB Insights, zajmująca się m.in. badaniem kondycji start-upów, przeanalizowała ponad 110 firm, które nie poradziły sobie z próbą czasu. Ich założyciele, wśród najczęstszych powodów niepowodzeń wskazywali m.in. brak potrzeby rynku i niedopasowanie produktu do rynku - 35%, a także przegranie z konkurencją wskazane przez 20% respondentów.¹

Pozostając w temacie startupów, wśród początkowych założeń – zarówno właścicieli firm, jak i inwestorów – znajdują się kwestie związane z szybkim zaznaczeniem swojej obecności na rynku poprzez wzrost liczby klientów i wyróżnienie się na tle konkurencji.

Kiedy jednak fundusze od inwestorów zaczynają topnieć, a statystyki pokazują, że kluczowe wskaźniki nie rosną, zaczyna się początek końca.

Z analogiczną sytuacją mamy do czynienia w przypadku firm, które mają ugruntowaną pozycję na rynku. Kiedy organizację dopada stagnacja, a próby dotarcia do użytkowników podejmowane są wyłącznie za pomocą znanych już metod – może się okazać, że nasi klienci już z nich nie korzystają. A w takiej sytuacji działania podejmowane doraźnie i w nieprzemyślany sposób zazwyczaj nie prowadzą do niczego dobrego. Pośpiech nigdy nie jest dobrym doradcą.

ISTOTA PR W DZIAŁALNOŚCI

Wielu z tych kryzysowych sytuacji z pewnością udałooby się uniknąć, gdybyśmy wcześniej mieli przygotowaną spójną strategię budowy wizerunku naszej marki w oczach zarówno potencjalnych, jak i stałych interesariuszy – inwestorów, klientów, czy partnerów biznesowych.

1. Dlaczego startupy upadają? Oto najpopularniejsze powody; mycompanypolska.pl/artikel/dlaczego-startupy-upadaja-oto-najpopularniejsze-powody/7456 [dostęp: 31.01.2022].

Firmy pracujące nad relacjami i lojalnością swoich odbiorców dużo trudniej „pozbyć się” z rynku, ponieważ użytkownicy widzą w oferowanych przez nią rozwiązaniach wartość, której nie znajdują u konkurencji. Dlatego właśnie, prowadzenie działań komunikacyjnych jest tak istotne – pomaga przedsiębiorcom budować tę wartość. Optymistyczne jest jednak to, że przedsiębiorcy dostrzegają potrzebę inwestowania w strategię komunikacyjną – i nie traktują tego jako niepotrzebny wydatek. Według raportu ICCO (Międzynarodowa Organizacja Konsultacyjna ds. Komunikacji) na temat PR 2020-2021 obszar, który odnotował największy wzrost w ciągu ostatnich 12 miesięcy to reputacja firmy (41%). Co więcej, wzrost znaczenia rynku public relations spodziewany jest głównie właśnie dzięki branży IT (63%).²

Prowadzenie optymalnych działań komunikacyjnych nie jest jednak takie proste. Wielość platform, kanałów i narzędzi – a jednocześnie ogromny rozwój technologiczny i potrzeba wyjątkowo szybkiego dostosowania się do wymagań rynku – z tym wszystkim muszą zmierzyć się firmy,

2. Światowy raport ICCO na temat PR 2020-2021; newspoint.pl/blog/swiatowy-raport-icco-na-temat-pr-2020-2021 [dostęp: 31.01.2022].



które chcą przetrwać. Jakie dokładnie wyzwania komunikacyjne czekają na organizacje z sektora nowych technologii?

KOMUNIKACJA ZROZUMIAŁA DLA ODBIORCÓW

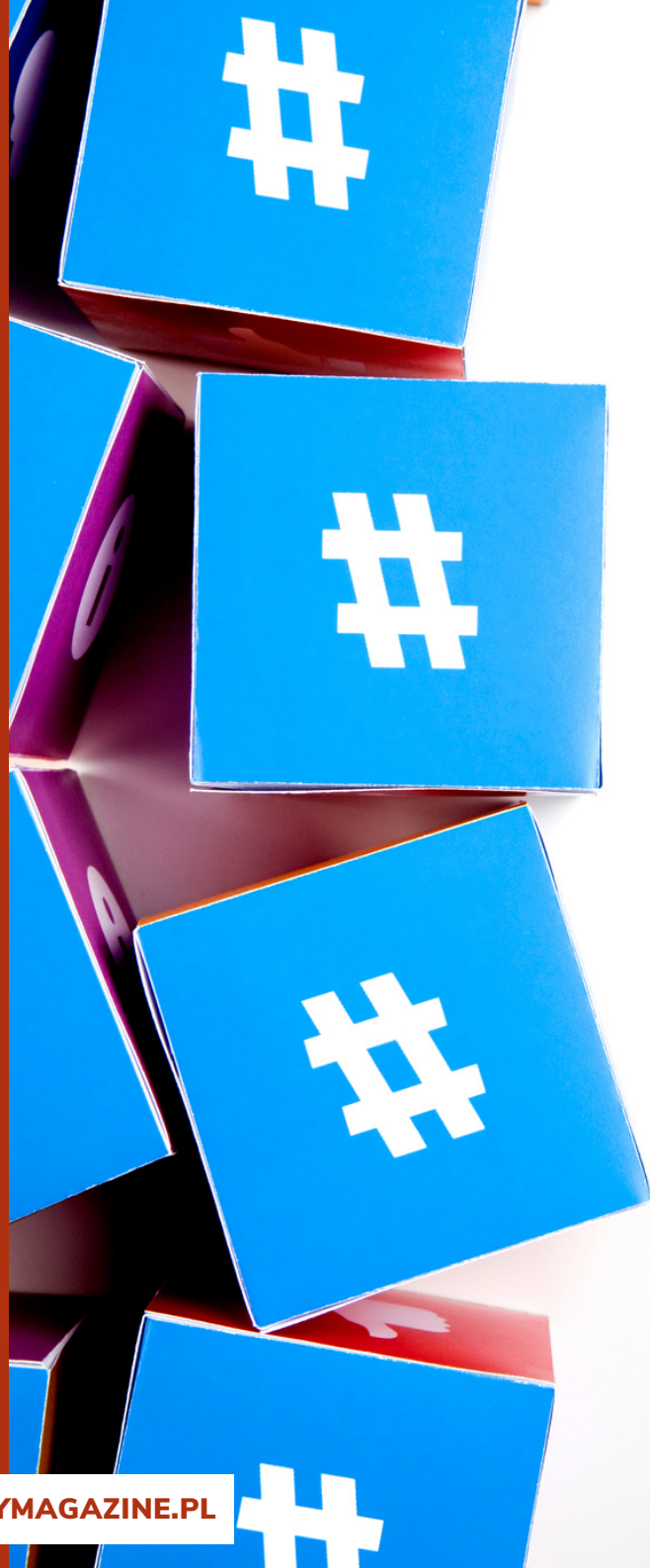
Jednym z pierwszych wyzwań, na jakie natrafiają właściciele firm IT, jest przedstawienie korzyści z użytkowania produktu w taki sposób, aby informacje były zrozumiałe przez grupę docelową. Jest to szczególnie trudne w przypadku, kiedy odbiorcami rozwiązania są osoby słabo zorientowane w tematach technologicznych lub gdy podobna usługa nie była do tej pory obecna na rynku.

W takiej sytuacji musimy przygotować działania oraz opracować komunikaty będące odpowiedzią na potrzeby potencjalnych klientów i partnerów biznesowych. Materiały te mają na celu stworzenie potrzeby korzystania z produktu, budowanie wiarygodności wokół marki, a także zainteresowanie szerokiego grona osób. Powinny więc być jasne i skupiać się na profitach wynikających z użytkowania danej technologii. Jednocześnie przyda się tu odrobina

pasji i wizji – co pozwoli wyróżnić się na tle konkurencji. Dobrze opowiedziana historia może być kluczem do wzbudzenia wiarygodności, przywiązania i zapamiętania.

Opowiadajmy więc o naszym produkcie, nie zominając o **podkreślaniu korzyści**, korzystaniu z różnych dostępnych narzędzi i metod komunikacyjnych. Jednocześnie nie zapominajmy o bardzo ważnej rzeczy – **nadmiar informacji o aspektach technicznych** może przynieść odwrotny skutek do zamierzonego. Lepiej postawić na czytelną stronę internetową, regularnie prowadzone profile w mediach społecznościowych czy też artykuły w mediach, które czytają nasi interesariusze. **Warto zadbać o kanały, z których korzystają najczęściej.** Stwórzmy prostą, ale kolorową opowieść o dużej zmianie.

Jakiś czas temu współpracowaliśmy z klientem, który emitował akcje swojej firmy poprzez jedną z platform equity crowdfundingowych. W tym przypadku trafiliśmy na dwa wyzwania: po pierwsze **pozyskiwanie funduszy** poprzez tego typu platformy w Polsce nie było jeszcze tak bardzo popularne, a po drugie – wśród grupy docelowej tego klienta było wiele osób działają-



cych wyłącznie w przestrzeni offline. Co zrobiliśmy? Zorganizowaliśmy wysyłkę kreatywną do największych polskich portali biznesowych oraz do prasy czytanej przez dużą część interesariuszy. Dotarliśmy dzięki temu z komunikatami zarówno do osób, które były zainteresowane inwestycjami poprzez equity crowdfunding, jak i do tych, które na co dzień nie korzystają z rozwiązań w formie online.

WYBÓR OPTIMALNYCH KANAŁÓW KOMUNIKACJI. NIE ZAWSZE WIĘCEJ TO LEPIEJ

Komunikujemy się poprzez wpisy na blogu, posty w mediach społecznościowych, bierzemy udział w webinarach, publikujemy artykuły w tytułach branżowych, nagrywamy filmy, wysyłamy newslettery... Sporo tego. Jeśli z tych kanałów faktycznie korzystają nasi odbiorcy jest to dobra strategia, ale pod jednym warunkiem – o każdy z tych kanałów należy dbać.

Niestety, analizując komunikację firm często dochodzimy do wniosku, że komunikacja jest chaotyczna i niedopracowana. Przykładowo – posty w mediach społecznościowych pojawiają się nieregularnie, a ich treści są powielane pomimo, że Facebook i LinkedIn wymagają innych komunikatów.

Z kolei materiały publikowane na firmowym blogu pozbawione są słów kluczowych dobranych pod SEO, więc użytkownikom ciężko te wpisy znaleźć.

Kolejna równie ważna kwestia to sprawdzanie skuteczności naszych działań. Które z postów generują najwięcej reakcji? Czy odbiorcy faktycznie klikają w linki przesyłane w newsletterze? Które wpisy na firmowym blogu cieszą się największą popularnością? Przygotowanie odpowiednich komunikatów jest ważne, ale równie ważna jest analiza ich skuteczności i wyciągnięcie z niej wniosków. Na to wszystko potrzeba jednak czasu.

**KLUCZOWE JEST WIĘC
OKREŚLENIE KONKRETNICH
PERSON (INTERESARIUSZY),
DO KTÓRYCH CHCEMY TRAFIĆ
ORAZ WYBÓR KANAŁÓW
I NARZĘDZI, POPRZECZ KTÓRE
POZYSKAMY ICH UWAGĘ.**

Dlatego współpracę z naszymi klientami zawsze rozpoczynamy od przeprowadzenia warsztatów strategicznych. Pozwalają one przeanalizować dotychczasowe aktywności marki i otoczenia konkurencyjnego. Podczas spotkania de-

finiujemy również potrzeby komunikacyjne i tworzymy strategię działania na najbliższe miesiące. Taki konkretny plan oraz harmonogram to pierwszy krok do budowania efektywnej komunikacji.

STRACH PRZED TECHNOLOGIĄ. JAK ZMIENIĆ TO PODEJŚCIE?

Zbyt techniczna komunikacja może wywoływać lęk przed technologią, co okazuje się kolejnym wyzwaniem. Nie trzeba daleko szukać, żeby znaleźć materiały dotyczące obaw odnośnie postępującej robotyzacji, która zabierze nam pracę. Musimy mieć świadomość, że w głowach potencjalnych klientów mogą pojawić się znaki zapytania związane z brakiem zaufania.

Zamiast udawać, że problemu nie ma, lepiej być przygotowanym na trudne pytania ze strony dziennikarzy, klientów lub inwestorów.

Dobrym rozwiązaniem jest sporządzenie przykładowej listy pytań, które mogą się pojawić oraz przygotowanie odpowiedzi na nie i przedyskutowanie ich z kilkoma osobami. Na pewno

pomocne okaże się również prowadzenie komunikacji w oparciu o aspekty edukacyjne dotyczące funkcjonowania naszego rozwiązania i przedstawienie przykładów, w jaki sposób produkt czy usługa pomogła innym firmom.

PODSUMOWANIE

Wyzwań w komunikacji – nie tylko rozwiązań technologicznych – jest całkiem sporo, w tym artykule przedstawiłam, według mnie, najważniejsze z nich. Należy pamiętać, że w przypadku podejmowania jakichkolwiek działań, kluczem do sukcesu jest optymalny wybór narzędzi komunikacyjnych, dostosowanie treści do potrzeb grupy docelowej oraz zaplanowanie poszczególnych aktywności na osi czasu.

Tak przygotowana strategia ma duże szanse na komunikacyjny sukces i wtedy – nawet jeśli zdarzy się jakiś kryzys – nasi odbiorcy dzięki przywiązaniu do marki zostaną z nami na dłużej. A o takich odbiorców warto dbać.

38 podejrzanych połączeń w 15 minut

Tyle wykryliśmy podczas audytu bezpieczeństwa w jednej z firm produkcyjnych.



Standardy, które wykorzystujemy podczas audytów bezpieczeństwa

- **NIST SP800-115:** Technical Guide to Information Security Testing and Assessment
- **OWASP** (Open Web Application Security Project)
- **OWASP MASVS** (Mobile Application Security Verification Standard)
- **OSTTMM** (Open Source Security Testing Methodology Manual)
- **ISSAF** (Information Systems Security Assessment Framework)
- **WASC-TC** (Web Application Security Consortium Threat Classification)
- **PTF** (Penetration Testing Framework)
- **OISSE** (Information Systems Security Assessment Framework)
- **CWE** (Common Weakness Enumeration in Mobile Applications)
- **CVSS** (Common Vulnerability Scoring System)

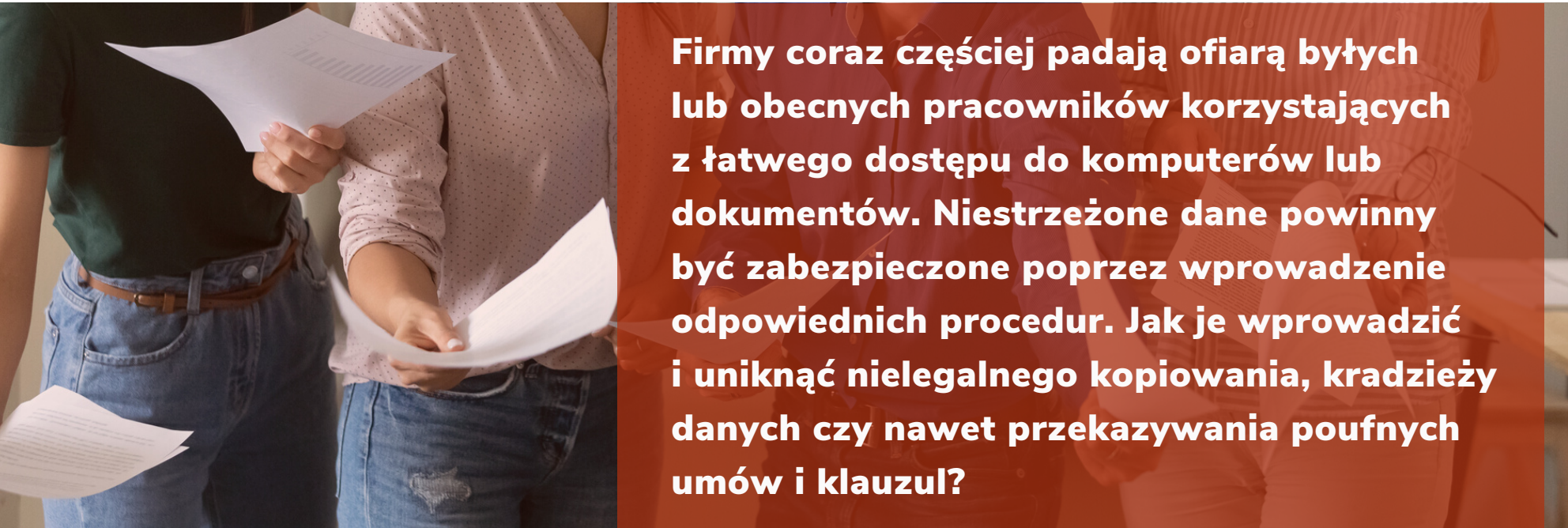


CISCO INNOVATION PARTNER
OF THE YEAR 2021

JAK ZABEZPIECZYĆ FIRMĘ PRZED KOPIOWANIEM DANYCH PRZEZ PRACOWNIKÓW?



Rafał Stępniewski
Rzetelna Grupa



Firmy coraz częściej padają ofiarą byłych lub obecnych pracowników korzystających z łatwego dostępu do komputerów lub dokumentów. Niestrzeżone dane powinny być zabezpieczone poprzez wprowadzenie odpowiednich procedur. Jak je wprowadzić i uniknąć nielegalnego kopiowania, kradzieży danych czy nawet przekazywania poufnych umów i klauzul?

PROCEDURY CHRONIĄCE DANE FIRMOWE

1

W pierwszej kolejności należy zdefiniować, które informacje są poufne i stanowią tajemnicę firmową — to one wymagają szczególnej ochrony.

2

Kolejnym krokiem jest zastosowanie przepisów o ochronie tajemnicy przedsiębiorstwa i zawarcie uregulowań wewnętrznych, dotyczących pracowników.

3

Następnie należy zabezpieczyć przedsiębiorstwo przez wprowadzenie odpowiednich systemów bezpieczeństwa.

Oto kilka ogólnych zasad ochrony:

- unormowanie dostępu do konkretnych danych,
- stosowanie dodatkowych zabezpieczeń do komputerów (w postaci haseł, monitoringu urządzeń USB),
- odpowiednia ochrona przed wirusami i złośliwym oprogramowaniem,
- właściwe zabezpieczenie wewnętrznej sieci

informatycznej, dzięki której pracownicy mogą się ze sobą porozumiewać oraz przysyłać dane (zabezpieczenia to m.in. procesy uwierzytelniania danych, dodatkowe procesy weryfikacyjne, klucze oraz hasła uwierzytelniające).

CO GROZI FIRMIE, W KTÓREJ DOŚZŁO DO WYCIEKU DANYCH?

Gdy dojdzie do incydentu związanego z wyciekiem krytycznych danych, przepisy RODO przewidują obowiązek zgłaszania takiego incydentu organowi ochrony danych. Incydent należy zgłosić w ciągu 72 godzin od stwierdzenia wycieku. Jeżeli istnieje wysokie ryzyko zagrożenia praw i wolności, należy niezwłocznie powiadomić osoby, których dane wyciekły.

Jak można się domyślić, wyciek danych wiąże się z ogromnymi stratami dla przedsiębiorstwa.

WTEDY FIRMA MUSI LICZYĆ SIĘ Z WIELOMA KONSEKWENCJAMI:

- **FINANSOWYMI,**
- **PRAWNYMI,**
- **WIZERUNKOWYMI.**

Jeżeli firma dopuści się poważnych naruszeń, w tym nieprzestrzeganie podstawowych zasad przetwarzania danych osobowych, to RODO przewiduje karę do 20 mln euro lub 4% rocznego obrotu przedsiębiorstwa (art. 5 RODO).

Oprócz kary finansowej, firma powinna liczyć się z osłabieniem reputacji firmy, obniżeniem zaufania, co wiąże się z utratą klientów. Do tego dochodzą straty finansowe spowodowane niższymi obrotami. A to wszystko skutkuje zanikiem przewagi konkurencyjnej i spadkiem wartości przedsiębiorstwa.

Eliminacja wszystkich konsekwencji to wysokie koszty — nałożone kary, kosztowne procesy sądowe mogą warunkować dalsze funkcjonowanie firmy.

Wyżej wymienionych konsekwencji można uniknąć, korzystając z dostępnych na rynku specjalnych rozwiązań i technologii informatycznych. Nowoczesne systemy chronią firmę przed kradzieżą lub przypadkowym wyciekiem krytycznych danych.

OCHRONA PRZED KRADZIEŻĄ LUB WYCIEKIEM DANYCH

Systemy monitoringu IT i aktywności komputera

W dużym uproszczeniu: system monitoringu IT oraz aktywności komputerów użytkowników nagrywa to, co się dzieje na ekranie komputera. Należy pamiętać, że taki sposób kontroli komputera pracownika powinien być legalny i zgodny z przepisami RODO. Oczywiście wspomniane systemy posiadają wiele innych funkcji pozwalających na zapewnienie bezpieczeństwa danych w firmie.

Aby zapobiec wyciekowi danych, istotne są:

- monitoring urządzeń USB,
- alerty w czasie rzeczywistym.

Systemy do wewnętrznej ochrony firmowej sieci internetowej

Wykorzystywanie takich rozwiązań ma na celu eliminację zagrożeń spowodowanych czynnikiem ludzkim. System do wewnętrznej ochrony sieci internetowej zapobiega wyciekom danych osobowych i innych informacji poufnych poza organizację poprzez:

- informowanie o próbie modyfikowania plików i przesyłanie ich pod zmienioną nazwą – poprzez pocztę prywatną (HTTP) – na zewnątrz przez pracowników lub firmy zewnętrzne, serwisantów, osoby trzecie,

- monitorowanie aktywność użytkowników w sieci pracowniczej niezwiązanej z wyznaczonymi zadaniami, a także używanie aplikacji mogących otworzyć drogę do włamań do sieci firmowej.

STANOWISKO PRACY UŻYTKOWNIKA

Żeby skutecznie zabezpieczyć firmę przed wyciekiem i utratą poufnych informacji, należy zadbać o stanowiska pracy użytkowników. Nierzadko w firmach prowadzona jest polityka czystego biurka i na jej przykładzie można wprowadzić tzw. politykę czystego pulpitu, która polega na zapisywaniu na pulpicie jedynie najważniejszych skrótów oraz na wyrobieniu nawyku blokowania ekranu przed odejściem od komputera.

Potencjalnym miejscem, gdzie może dojść do wycieku lub kopiowania danych, jest niezabezpieczona drukarka. Dlatego drukowanie materiałów powinno odbywać się dopiero po autoryzacji na odpowiednim urządzeniu, skąd wydrukowane dokumenty będą mogły być od razu zabrane. Wspomniana autoryzacja może polegać na przydzieleniu specjalnych kodów lub kart magnetycznych — indywidualnych dla każdego pracownika.



OCHRONA DANYCH OSOBOWYCH - CO NA TO KODEKS PRACY?

Co się stanie w wypadku skopiowania danych osobowych przez pracownika, który nie zadbał o dobro firmy?

ZGODNIE Z ART. 100 KODEKSU PRACY (K.P.) JEDNYM Z PODSTAWOWYCH OBOWIĄZKÓW PRACOWNIKA JEST DBANIE O DOBRO FIRMY ORAZ OCHRONA MIENIA. Z TEGO WYNIKA, ŻE ZA NARUSZENIE ZASAD OCHRONY DANYCH PRACOWNIK MOŻE ZOSTAĆ DYSCYPLINARNIE ZWOLNIONY.

Sąd Najwyższy wydał wyrok w sprawie pracownicy, która wbrew uprawnieniom zyskała dostęp do informacji i wykradła część danych osobowych klien-

tów przedsiębiorstwa. Sąd Najwyższy zastosował przepis: art. 52 § 1 k.p.

Pracodawca może rozwiązać umowę o pracę bez wypowiedzenia z winy pracownika w razie:

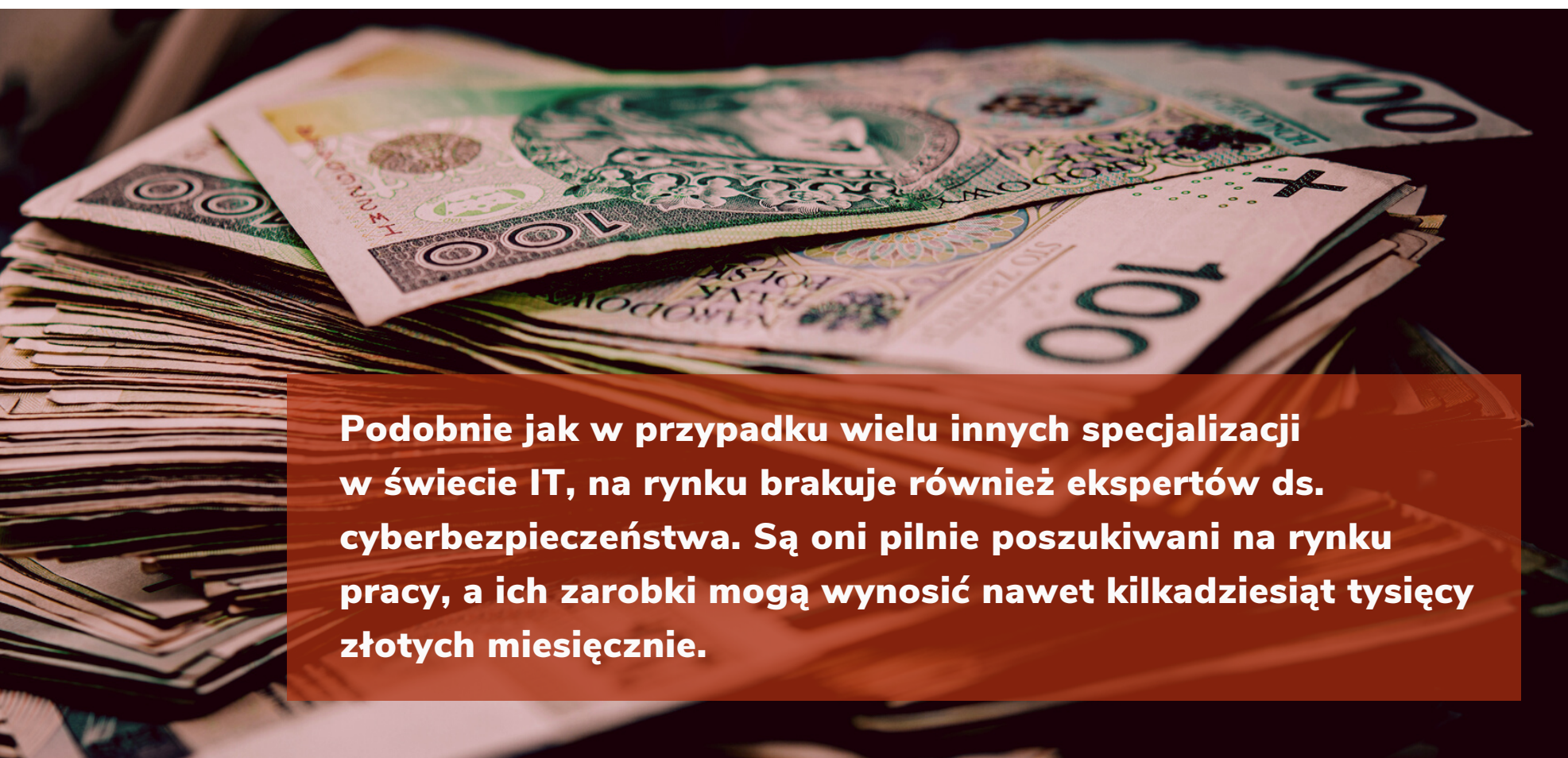
1. ciężkiego naruszenia przez pracownika podstawowych obowiązków pracowniczych,
2. popełnienia przez pracownika w czasie trwania umowy o pracę przestępstwa, które uniemożliwia dalsze zatrudnianie go na zajmowanym stanowisku, jeżeli przestępstwo jest oczywiste lub zostało stwierdzone prawomocnym wyrokiem,
3. zawinionej przez pracownika utraty uprawnień koniecznych do wykonywania pracy na zajmowanym stanowisku.

W ocenie Sądu Najwyższego ciężkim i zawinionym naruszeniem obowiązków pracowniczych jest wykonywanie bez wiedzy i zgody pracodawcy, w miejscu i czasie pracy, przy wykorzystaniu sprzętu i systemu pracodawcy, czynności na rzecz innego podmiotu. Czyn naruszył także obowiązek zachowania tajemnicy o klientach pracodawcy (art. 100 § 2 pkt 4-5 k.p.). Pracownik był upoważniony do dostępu do zbioru, ale wyłącznie w zakresie związanym z pracą wykonywaną na rzecz administratora danych osobowych.

ZAROBKI W CYBER SECURITY DO 35 000 ZŁ MIESIĘCZNIE



Grzegorz Kubera
No Fluff Jobs



Podobnie jak w przypadku wielu innych specjalizacji w świecie IT, na rynku brakuje również ekspertów ds. cyberbezpieczeństwa. Są oni pilnie poszukiwani na rynku pracy, a ich zarobki mogą wynosić nawet kilkadziesiąt tysięcy złotych miesięcznie.

ZAROBKI W IT

No Fluff Jobs, jeden z największych w Europie portali z ogłoszeniami o pracę dla IT i jedyny w Polsce z obligatoryjnymi widełkami w każdym ogłoszeniu, odnotowuje w ostatnich latach wzrosty ofert kierowanych do specjalistów ds. cyberbezpieczeństwa. W stosunku do roku 2019, w roku 2020 było ich więcej o ponad 50 proc., zaś w 2021 - o ponad 90% co pokazuje rosnące zapotrzebowanie na ich usługi. Co więcej, analiza tych ofert pozwala na stwierdzenie, iż specjaliści IT w tej dziedzinie są nie tylko jednymi z najczęściej poszukiwanych, ale również dobrze wynagradzanych przez pracodawców.

Dla przykładu - osoba na stanowisku "Security Architect for Automotive" otrzyma miesięcznie nawet 24 000 zł na umowie o pracę albo do 32 000 zł na kontrakcie B2B. "Cloud Security Specialist" może z kolei liczyć na zarobki rzędu ok. 25 000 zł, "Data Security Engineer" otrzyma co miesiąc przelew w podobnej wysokości, a "Cloud Security Architect" nawet do 35 000 zł miesięcznie.

Firmy, które oferują takie wynagrodzenia, najczęściej pozwalają na pracę z Polski, ale pracują w języku angielskim i realizują prace dla klientów zagranicznych. Znajomość angielskiego jest więc obowiązkowa. Często siedziba danej spółki jest w Warszawie, niemniej w obecnych czasach popularnym rozwiązaniem jest praca zdalna, co oznacza, że przynajmniej w najbliższym czasie, pracy na takim stanowisku możemy szukać z dowolnego miejsca w Polsce.

ZAPOTRZEBOWANIE WIĘKSZE NIŻ KIEDYKOLWIEK

W maju ubiegłego roku Anthony Klotz, psycholog organizacyjny i profesor na Texas A&M University, ukuł termin „wielka rezygnacja”. Określił nim ludzi, którzy odchodzą z pracy z powodu przeciągającej się pandemii koronawirusa. Ta doprowadziła miliony osób do przemysłów w zakresie tego, gdzie, jak, dlaczego i za ile pracują.

I tak tylko w drugiej połowie 2021 r. w USA z pracy odeszło 20 mln ludzi. W Wielkiej Brytanii 4,4 mln osób zrezygnowało z pracy zaledwie

w jednym miesiącu - we wrześniu. Tessian, firma zajmująca się bezpieczeństwem, informuje, że dla prawie trzech czwartych (71%) liderów IT „wielka rezygnacja” doprowadziła do wzrostu ryzyka dotyczącego cyberbezpieczeństwa¹. Dlaczego?

Tessian odkryła, że gdy ludzie rezygnują z pracy, aż jedna trzecia (29%) zabiera ze sobą wrażliwe dane służbowe na nowe stanowiska. Prawie połowa (45%) liderów IT odnotowała wzrost liczby incydentów infiltracji danych w ciągu ostatniego roku. Dane z jednej firmy do drugiej najchętniej zabierają ze sobą przedstawiciele branży marketingowej (63%), a następnie HR i IT (po 37%). Niektórzy nie wiedzą, że to coś złego, ale mnóstwo pracowników (53%) przekonuje, że dane należą do nich, bo nad nimi pracowali. Z kolei 58% ankietowanych jest zdania, że dane z poprzedniej pracy pomogą im w znalezieniu nowej, a 44% chętnie i bez oporu udostępni je nowemu pracodawcy.

Tessian sugeruje, że już ten fakt bardzo zwiększa zapotrzebowanie na specjalistów ds. bezpieczeństwa. Osoby te zaprojektują i zaimple-

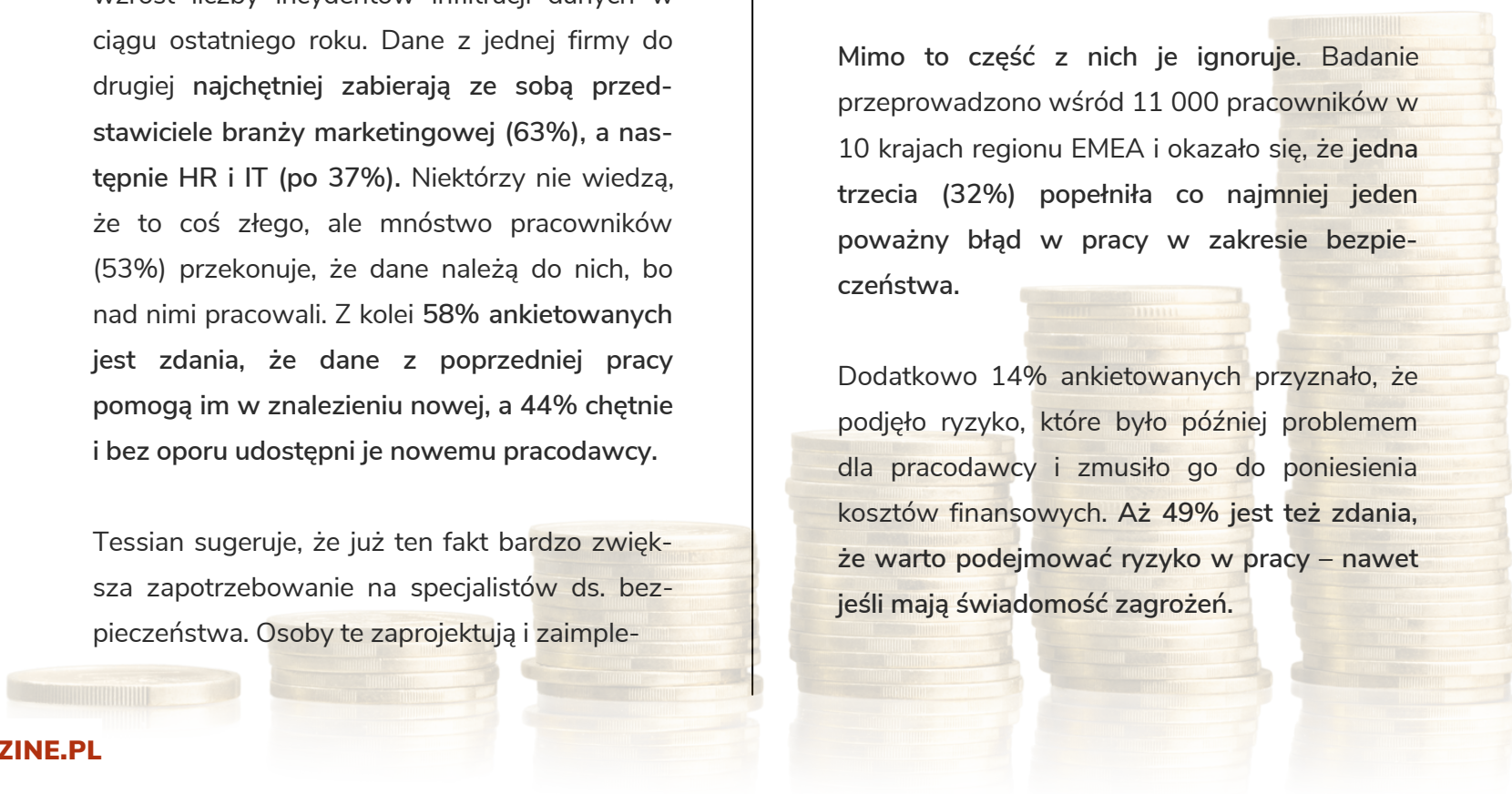
mentują odpowiednie zabezpieczenia i procedury, a także w razie potrzeby zareagują na wszelkie incydenty.

FIRMY ZWIĘKSZAJĄ BUDŻETY

Z innego raportu, przygotowanego przez Iron Mountain, firmy specjalizującej się w zarządzaniu i przechowywaniu dokumentów, wynika z kolei, że pracownicy w całej Europie są świadomi potencjalnych problemów dotyczących bezpieczeństwa².

Mimo to część z nich je ignoruje. Badanie przeprowadzono wśród 11 000 pracowników w 10 krajach regionu EMEA i okazało się, że jedna trzecia (32%) popełniła co najmniej jeden poważny błąd w pracy w zakresie bezpieczeństwa.

Dodatkowo 14% ankietowanych przyznało, że podjęło ryzyko, które było później problemem dla pracodawcy i zmusiło go do poniesienia kosztów finansowych. Aż 49% jest też zdania, że warto podejmować ryzyko w pracy – nawet jeśli mają świadomość zagrożeń.



W firmach ciągle, jak się okazuje, występują wręcz elementarne braki zarówno w edukacji z zakresu bezpieczeństwa, ale też stosowania odpowiednich procedur operacyjnych. Jedna trzecia (34%) badanych nadal używa tego samego hasła na wielu platformach, a jedna piąta (18%) przechowuje hasła dostępne na kartce papieru, trzymając ją na widoku (np. na biurku). Poza tym 36% osób przyznaje, że nie ma zbyt dużej wiedzy o bezpieczeństwie, zwłaszcza w kwestii bezpieczeństwa pracy zdalnej.

Tego rodzaju braki powodują, że firmy zwiększają budżety na zatrudnianie specjalistów ds. bezpieczeństwa. Potwierdza to Międzynarodowa Rada Bezpieczeństwa Neustar (NISC - Neustar International Security Council), która przepytала 302 decydentów ds. IT z różnych organizacji³. I tak, 81% zwiększy budżety na bezpieczeństwo IT w 2022 r., a w prawie jednej czwartej przypadków budżet wzrośnie nawet o 50%. Firmy planują rekrutację nowych członków zespołu, zarówno do wewnątrz, jak i specjalistów zewnętrznych (w ramach outsourcingu).

14% ankietowanych przyznało, że podjęło ryzyko, które było później problemem dla pracodawcy i zmusiło go do poniesienia kosztów finansowych.

Źródła:

1. "How the Great Resignation is Creating More Security Challenges", Tessian, 1.02.2022
2. "Resilience through risk management", Iron Mountain, 9.2021
3. "Cybersecurity Budgets for 2022", Neustar International Security Council, 11.2021; <https://www.nisc.neustar>

ZDARZYŁ SIĘ W TWOJEJ FIRMIE

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC
SPRAWDŹ JAK

JAK WYGLĄDA KONTROLA UODO W FIRMIE?



Redakcja
SECURITY MAGAZINE



Przedsiębiorcy nie lubią być kontrolowani - nie jest to żadna tajemnica. Wizyty kontrolne zaburzają codzienny rytm pracy, stresują pracowników, kończą się zazwyczaj zaleceniami albo sankcjami. Niemniej na taką ewentualność każdy powinien być gotowy. Dotyczy to również kontroli Urzędu Ochrony Danych Osobowych. Kiedy organ rozpoczyna takie postępowanie? Jak wygląda kontrola UODO?

KTO I KIEDY MOŻE ZŁOŻYĆ SKARGĘ?

Skargę składa się do prezesa urzędu - może to zrobić osoba fizyczna, jeżeli nieprawidłowe przetwarzanie dotyczy jej danych osobowych. W przypadku, gdy skarga dotyczy przetwarzania danych osobowych innej osoby, konieczne jest pełnomocnictwo udzielone przez tę osobę do jej reprezentowania w postępowaniu przed prezesem UODO.

Pełnomocnikiem może być zarówno osoba fizyczna, jak i podmiot, organizacja lub zrzeszenie - które nie mają charakteru zarobkowego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą. Skargę można złożyć pisemnie lub elektronicznie.

UODO doradza, by osoby, których naruszenie dotyczy, najpierw kontaktowały się z administratorem danych - jest to dużo szybsza droga, jeśli jednak administrator zaniedbuje swoje obowiązki, po złożonej skardze do urzędu rozpoczyna się kontrola.

PRZED KONTROLĄ

Kontrole UODO są przeprowadzane zgodnie z ich planem albo na podstawie sygnałów, jakie urząd otrzymuje od osób fizycznych czy ich reprezentantów. Informacje o naruszeniu mogą zgłaszać też inne instytucje lub inne organy kontrolujące, np. Komisja Nadzoru Finansowego, Państwowa Inspekcja Pracy czy urząd skarbowy.

Nim przedstawiciele UODO pojawią się u przedsiębiorcy, wysyłana jest mu informacja o kontroli. Musi ona trafić do zainteresowanego na 7 dni przed wizytą. Oczywiście, termin kontroli podlega negocjacjom, natomiast jedynie w przypadku, gdy firma jako administrator danych ma ku temu ważne powody, np. nieobecność inspektora ochrony danych osobowych. Nie są powodami zmian terminu np. inne kontrole mające miejsce na terenie przedsiębiorstwa.

Kiedy kontrolerzy pojawią się w firmie, mają obowiązek okazania legitymacji służbowych i upoważnień. Przedsiębiorca ma z kolei prawo do sprawdzenia, czy ci kontrolerzy skierowani zostali przez UODO. Zwykle zespół kontrolujący

tworzą trzy osoby, w tym jedna to specjalista ds. IT. Kontrola może odbyć się między godziną 6 a 22.

WSPÓŁPRACA PRZEDSIĘBIORCA - UODO

Kontrolerzy informują, co będzie przedmiotem kontroli, choć sam przedsiębiorca może skontaktować się wcześniej z UODO, by zapytać, jakie dokumenty przygotować dla kontrolerów. Podczas samej kontroli sprawdzane są zasady przetwarzania danych i podstawy prawne do przetwarzania danych, a także czy spełniony został obowiązek informacyjny.

Dla kontrolujących istotne jest też, jak realizowane są prawa osób, których dane dotyczą. Urząd kontroluje dokumentację i zabezpieczenia. Kontroli podlegają też dokumenty incydentów oraz informacje o danych do państw trzecich.

Kontrolujący mają prawo zbierać wyjaśnienia od pracowników, a także poruszać się po przedsiębiorstwie, którego kontrola dotyczy. Jednak najczęściej wygląda to tak, że weryfikowana jest ta część działalności podmiotu związana z prze-

twarzaniem danych osobowych w konkretnym postępowaniu.

Do sprawnej kontroli UODO potrzebuje pomieszczenia do pracy, zamykanej szafki na dokumenty, drukarki czy kserokopiarki. Mogą zdarzyć się przesłuchania pracowników, rejestrowanie prowadzonej kontroli za pomocą obrazu lub dźwięku, czasem - gdy przedsiębiorca utrudnia kontrolę - UODO wzywa policję. Warto wiedzieć, że utrudnianie przeprowadzenia kontroli kwalifikuje się też jako wykroczenie podlegające karze.

Efektem kontroli są protokoły częściowe, które przedsiębiorca ma prawo skopiować. Kontrolę kończy protokół z przebiegu kontroli. Przedsiębiorca w ciągu 7 dni musi go podpisać, odmówić podpisania lub wnieść swoje uwagi. W przypadku uwag urząd może się do tego ustosunkować przez uwzględnienie lub odrzucenie zastrzeżeń, przeprowadzenie kontroli uzupełniającej albo od razu ocenić zgromadzony w czasie kontroli materiał.

CO PO KONTROLI?

Kontrola może trwać do 30 dni, zwykle trwa ona około 5 dni. Czas jej trwania zależy od tego, jakiej wielkości jest przedsiębiorstwo oraz jak przebiega współpraca na linii UODO - podmiot kontrolowany. W sytuacji stwierdzenia, że wszystko jest w porządku, kontrola zostaje zakończona. Jeśli przepisy RODO zostały jednak naruszone, UODO wszczyna postępowanie.

Przedsiębiorca może się zgodzić ze stwierdzonymi uchybieniami i od razu poddać się decyzji urzędu. Ten, kończąc sprawę, decyduje albo o umorzeniu postępowania, wydaniu nakazu albo nałożeniu kary. Karą jest ograniczenie lub zakaz przetwarzania danych, nakazanie dostosowania procedur przetwarzania danych do wymogów RODO, cofnięcie certyfikacji, czy nałożenie kary pieniężnej. Natomiast, gdy przedsiębiorca nie zgadza się z decyzją UODO, w ciągu 30 dni może odwołać się do sądu w trybie sądowo-administracyjnym. Nie ma innej możliwości, bo nie przewidziano zaskarżenia decyzji urzędu w innym trybie.



CZYM SIĘ KIEROWAĆ PODCZAS WYBORU ANTYWIRUSA DLA TWOJEJ FIRMY?



Piotr Rozmiarek
Marken -
Bitdefender w Polsce



Skuteczny program antywirusowy jest obecnie niezbędnym elementem struktury sieciowej w każdej firmie. Potencjalne zagrożenie, jakim jest złośliwe oprogramowanie lub phishing może nie tylko poskutkować tym, że stracisz niezbędne pliki lub będziesz musiał wpłacić za nie okup, lecz może się zakończyć także wysoką grzywną za niewłaściwe zadbanie o ochronę krytycznych danych osobowych.

CZYM KIEROWAĆ SIĘ PODCZAS WYBORU OPROGRAMOWANIA ANTYWIRUSOWEGO?

Wielu przedsiębiorców podczas wyboru oprogramowania antywirusowego dla swojej firmy kieruje się wyłącznie ceną produktu. Uważają oni, że każda forma zabezpieczenia przed niebezpieczeństwami jest wystarczająca, nawet ta w pełni bezpłatna. Swoje działania tłumaczą tym, że środki, które zaoszczędzili na ochronie antywirusowej, mogą przeznaczyć na inne cele związane z modernizacją sieci IT. Takie postępowanie z reguły jest krótkowzroczne i może zakończyć się wyjątkowo dotkliwymi konsekwencjami.

Skrajnie innym przypadkiem jest to, że część mikroprzedsiębiorców, chcąc zapewnić sobie najlepszą ochronę, postanawia zainwestować w możliwie najdroższe i najbardziej zaawansowane wersje oprogramowania antywirusowego. W takich wypadkach zdarza się, że zasoby informatyczne takiej firmy nie są wystarczające do tego, aby zapewnić optymalne działanie oprogramowania, co kończy się znaczącym spadkiem wydajności systemów.

Wybór odpowiedniego oprogramowania dla firmy nie jest więc sprawą oczywistą i zawsze powinien być poprzedzony dokładną analizą indywidualnego zapotrzebowania dla danej firmy. Dlatego w następnej części tego artykułu rozważymy cztery czynniki, które warto wykorzystać przy wyborze odpowiedniego oprogramowania antywirusowego.

WIELKOŚĆ FIRMY I RODZAJ ZASOBÓW, KTÓRE CHCEMY CHRONIĆ

Dla niewielkich firm wystarczającym rozwiązaniem mogą okazać się podstawowe wersje pakietów antywirusowych z klasy Biznes. Takie oprogramowania najczęściej umożliwiają pełną ochroną stacji roboczych oraz serwerów.

Antywirusy zawierają również pojedynczą konsolę zarządzającą, która zapewnia kompleksową ochronę stacji roboczych i serwerów, fizycznych lub wirtualnych, a także umożliwia łatwy dostęp do informacji o czynnikach ryzyka, ryzykownych błędach konfiguracyjnych systemu operacyjnego i oprogramowania.

Małe firmy zazwyczaj przeznaczają znacznie mniejszy budżet na zasoby informatyczne niż dużo większe bardziej wymagające przedsiębiorstwa. Z tego też powodu, bardziej zaawansowane mechanizmy ochrony mogą negatywnie wpłynąć na wydajność pracy sprzętu oraz pracowników. Dlatego kluczowym czynnikiem jest to, aby rozwiązanie antywirusowe miało możliwość wyboru modułów ochrony.

Większe przedsiębiorstwa potrzebują bardziej złożonej ochrony, w której skład mogą wchodzić nie tylko podstawowe stacje robocze, lecz także urządzenia mobilne, ochrona poczty na poziomie stacjonarnych serwerów jak Microsoft Exchange, czy ochrona poczty na serwerach Linux. W takim wypadku oprogramowanie antywirusowe powinno zapewniać wielowarstwowe zabezpieczenia najnowszej generacji oraz pozwalać organizacjom włączyć dedykowaną ochronę dla centrów danych, fizycznych punktów końcowych, urządzeń mobilnych i skrzynek pocztowych Exchange z możliwością wyboru usług zabezpieczeń, które chcemy wdrożyć.

W celu zapewniania jak najlepszej ochrony warto rozważyć wdrożenie możliwie jak najskuteczniejszego oprogramowania, dlatego dobrym pomysłem jest sprawdzenie aktualnych wyników testów przeprowa-



dzanych przez niezależne instytuty badawcze, takie jak AV Comparatives. Warto także sprawdzić aktualne trendy na rynku programów antywirusowych. W ostatnich latach niezwykle popularne stały się oprogramowania oparte na uczeniu maszynowym. Tutaj przykładem może być oprogramowanie firmy Bitdefender GravityZone, które łączy uczenie maszynowe i heurystykę z sygnaturami i innymi technikami, aby zapewnić ochronę przed wszystkimi typami złośliwego oprogramowania, a także zagrożeniami, takimi jak phishing, ransomware, exploity i zero-days. Oprogramowanie korzysta także z pionierskich i opatentowanych technologii, takich jak Process Inspector i algorytmy uczenia maszynowego, które są stale rozwijane, szkolone i używane od 2008 roku. Dzięki temu oprogramowanie jest w stanie chronić zasoby użytkownika zarówno przed obecnymi znanymi zagrożeniami, jak i tymi jeszcze nieznanymi.

MODEL PRACY - STACJONARNY CZY ZDALNY?

Obecna sytuacja pandemiczna sprawiła, że w wielu firmach niezbędne okazało się wprowadzenie modelu pracy zdalnej.

Niestety, wiele przedsiębiorstw nie było w pełni przygotowanych do takiej zmiany i w efekcie stały się niemal bezbronna przed atakami cyberprzestępców. Dlatego w kontekście wyboru odpowiedniego oprogramowania dla Twojej firmy powinienś wziąć pod uwagę to, jaki model pracy jest w niej wykorzystywany.

Firmy, które posiadają środowisko wirtualne, mogą rozważyć wdrożenie oprogramowania umożliwiającego zaimportowanie gotowej maszyny wirtualnej do swojego środowiska bez potrzeby zbędnego wgłębiania się w konfigurację poszczególnych elementów systemu.

"WIELE PRZEDSIĘBIORSTW NIE BYŁO GOTOWYCH DO ZMIANY ZWIĄZANEJ Z PANDEMIĄ. W EFEKCIE STAŁY SIĘ NIEMAL BEZBRONNE PRZED ATAKAMI CYBERPRZESTĘPCÓW."



Samo uruchomienie systemu zacznie się do kilku podstawowych czynności i w wielu standardowych instalacjach sprowadzi się do rozpoczęcia automatycznej instalacji i podania klucza licencji.

Drugim rozwiązaniem może być wybór oprogramowania, które posiada wersję systemu opartą w całości o bezpieczną chmurę w swoim środowisku. W takim przypadku system domyślnie umożliwia podłączenia każdego z użytkowników na publicznym adresie do konsoli. Dzięki takiej funkcji każdy użytkownik, bez względu, gdzie się znajduje i gdzie pracuje, będzie pod kontrolą systemu, a tym samym administrator lub osoba zarządzająca bezpieczeństwem może na bieżąco monitorować poziom bezpieczeństwa użytkowników.

RODZAJE ZAGROŻEŃ - NA CO SIĘ PRZYGOTOWAĆ?

Obecnie największym zagrożeniem dla Twojej firmy jest zdecydowanie zainfekowanie złośliwym oprogramowaniem typu ransomware. Dlatego przy wyborze odpowiedniego oprogramowania antywirusowego powinieneś zwrócić uwagę na to, w jaki sposób dane oprogramowanie wykrywa takie wirusy i jak łagodzi jego skutki. Każdy producent oprogramowania przygotował swoje rozwiązanie w tej kwestii. W przypadku produktów z linii GravityZone zostały wprowadzone trzy zaawansowane moduły. Pierwszym z nich jest HyperDetect, czyli moduł, który umożliwia umieszczenie

podejrzanego pliki w kwarantannie i przetestowanie go w bezpiecznych warunkach. Drugim jest Szczepionka Ransomware, której zadaniem jest ukrycie komputera przed atakiem, w taki sposób, że sugeruje on zagrożeniu, że jest już zainfekowany. Co w rezultacie skutkuje tym, że atak pomija maszynę zamaskowaną. Trzecią warstwą ochrony, a właściwie mechanizmem wykorzystywanym po ataku ransomware jest moduł łagodzenia skutków ransomware. Funkcja ta ma za zadanie zrobienia kopii plików, które w wyniku ataku próbują być zaszyfrowane. Po takim ataku system jest w stanie automatycznie przywrócić pliki, które zostały zaszyfrowane.

Skuteczny program antywirusowy powinien zawierać jeszcze moduły, jak zaporę sieciową, ochrona poczty, ochrona przed phishingiem oraz możliwość określenia dostępu do stron internetowych. Warto, aby oprogramowanie zawierało formę zarządzania ryzykiem, która umożliwiłaby administratorowi sieci dostęp do informacji na temat potencjalnie niebezpiecznych zdarzeń oraz możliwość przeprowadzania zdalnych aktualizacji oprogramowania, minimalizując ryzyko włamania się za pomocą exploitów.

KOMFORTOWA PRACA ADMINISTRATORA

Odpowiednie oprogramowanie antywirusowe powinno charakteryzować się nie tylko wysoką skutecznością odpierania ataków, ale i przyjemnym w obsłudze interfejsem. Centrum zarządzania powinno być intuicyjne i przejrzyste, tak by nie wymagało od administratora lub operatora zbyt dużego zaangażowania w pracy z podstawowymi czynnościami, które są niezbędne do prawidłowej pracy oprogramowania.

Konsola powinna być intuicyjna i umożliwić administratorowi łatwy dostęp do wszystkich niezbędnych funkcji. Komfortowe oprogramowanie powinno także posiadać pewną autonomiczność działania. Dzięki temu w pewnym stopniu odciąży administratora. Przykładem takiego działania może być automatyczne wysyłanie próbek potencjalnego zagrożenia do testów przeprowadzonych przez producenta. Kluczowym elementem skutecznego oprogramowania jest to, aby nie był on problematyczny w obsłudze. Przy wyborze odpowiedniego antywirusa dla Twojej firmy zawsze powinienes sprecyzować swoje realne zapotrzebowanie.

ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA

SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



ZAPISZ SIĘ

NEWSLETTER



YOUR EMAIL HERE

SUBSCRIBE

JAK SKUTECZNIE ZARZĄDZAĆ BIZNESEM W 2022 ROKU?



Łukasz Nieborek
Energy Logserver



**Jak zarządzać biznesem?
Monitorując sposoby
wykorzystywania informacji
wrażliwych i prób przekształcenia
ich w przewagę biznesową,
sprawdzając luki w systemach,
dostosowując się do najnowszych
wymagań dotyczących ochrony
danych i szybko reagując w
sytuacji, gdy ma miejsce incydent
cybernetyczny. Jakie jeszcze rady
dla biznesu ma Energy Logserver?**

INCYDENTY BEZPIECZEŃSTWA W 2021 ROKU

Miniony rok stał pod znakiem zmian w sposobie funkcjonowania wielu biznesów. Praca zdalna stała się naturalnym elementem życia organizacji. Jednocześnie zauważalny jest ogromny przyrost naruszeń bezpieczeństwa.

Opinię publiczną poruszały poważne wycieki danych osobowych z tak potężnych organizacji jak Facebook i Amazon, ale jednocześnie warto podkreślić, że te same problemy dotyczą również mniejszych podmiotów.

Zgodnie z raportem przygotowanym przez Computerworld w kooperacji z Polskim Klastrem Cyberbezpieczeństwa #CyberMadeinPoland już jedna trzecia polskich firm była dotknięta naruszeniami bezpieczeństwa IT. To pokazuje, że zagrożenie nie dotyczy wyłącznie dużych organizacji, ale praktycznie każdego, kto gromadzi dane stanowiące wartość biznesową.

W KOGO HAKERZY CELUJĄ NAJCZĘŚCIEJ I DLACZEGO?

Małe i średnie firmy są głównym celem cyberprzestępców. W przeciwieństwie do dużych korporacji, które mają pieniądze i zasoby, aby zapłacić za cyberbezpieczeństwo i ulepszyć swoją sieć, dopasowując się do najnowszych sztuczek hakerskich, małe firmy nie mają tego samego „luksusu” i hakerzy o tym wiedzą. Dlatego około połowa ataków jest wymierzona w mniejsze firmy.



Niemniej jednak wraz z ewolucją technologii pojawiają się ewoluujący hakerzy, a patrząc na powyższe przykłady, możemy zauważyć, że nawet najbogatsze firmy nie są odporne na cyberzagrożenia.

Dlatego każda organizacja, niezależnie od wielkości, musi zrozumieć, jak ważne jest posiadanie potężnego narzędzia, które zapewni ochronę i organizację jej środowiska IT.

DLACZEGO POSIADANIE LOG MANAGEMENT I SIEM SĄ WAŻNE?

Żyjemy w czasach, gdy cyberprzestępczość jest największym zagrożeniem dla każdej firmy na

świecie. Dlatego posiadanie odpowiedniego narzędzia, które może chronić i uporządkować dane, powoli stało się koniecznością. Niestety, ze względu na wysokie koszty, wiele małych i średnich firm wybiera pozostać niechronionymi i narażonymi.

Z tego powodu wiele osób nie odkryło jeszcze, że tego typu rozwiązanie może nie tylko powstrzymać od zagrożeń, ale może również pomagać w podejmowaniu mądrych decyzji, wykrywaniu problemów, odkrywaniu trendów i wzorców oraz w zrozumieniu klientów. Dlatego właśnie wiodące firmy wkładają dużo czasu i wysiłku w zbieranie tych danych. Jest to ich sposób na ciągłe osiąganie sukcesów na obecnym rynku.



Do tej pory praca z gromadzonymi logami i wyciąganie z nich wartościowych informacji było zarezerwowane dla dużych organizacji, które inwestują w rozbudowaną kadrę analityków bezpieczeństwa. Rozwiązania Log Management i SIEM są zbyt drogie, podczas gdy te, które są przyjazne dla budżetu, nie mogą być skalowane do potrzeb większych firm. Dlatego na rynku można znaleźć również i takie oferty, które zachowują właściwy balans doskonałej wydajności oraz przystępnej ceny. Takie rozwiązania mogą uprościć i zrewidować doświadczenie klientów, pokazując, że wszelkie dane mogą być wartościowe.

PRZYSZŁOŚĆ BIG DATA

Rok 2021 był rekordowy pod względem cyberprzestępczości, więc firmy w końcu zrozumiały znaczenie posiadania rozwiązania do zarządzania danymi. Niestety, wiele organizacji nie miało pewności, jak najlepiej wykorzystać swoje dane, aby zachować ochronę, wspierać rozwój i wyprzedzać konkurencję.

W wyniku zmian w środowiskach pracy spowodowanych przez Covid 19 eskalacja danych dostępnych dla firmy sprawiła, że wykorzystanie

sztucznej inteligencji (AI) i uczenia maszynowego (ML) stało się krytyczną przewagą konkurencyjną. Organizacje każdej wielkości będą bardziej aktywnie zwracać się do platform takich jak Energy Logserver, ponieważ zapewniają one funkcje potrzebne do wykrywania, łączenia, integrowania, zarządzania, wykorzystywania i przechowywania zasobów danych, aby umożliwić firmie osiągnięcie celów szybciej i przy zachowaniu mniejszej złożoności w stosunku do poprzednich punktów widzenia.

Niedobór umiejętności w zakresie cyberbezpieczeństwa doprowadzi do większej instrumentacji i automatyzacji. Podczas gdy w zakresie bezpieczeństwa IT/IoT brak siły roboczej już istnieje, niedobór technologii operacyjnych w zakresie bezpieczeństwa (OT) jest znacznie bardziej drastyczny. Niewielu specjalistów i programistów uczelni skupia się na cyberbezpieczeństwie technologii operacyjnych, a rozwiązanie tego problemu zajmie wiele lat. W rezultacie tego przedsiębiorstwa będą musiały polegać na rozwiązaniach do instrumentacji bezpieczeństwa, które zapewniają większą automatyzację wymiany danych i podejmowania decyzji, w tym duży



nacisk będzie kładziony na wysoce zaawansowaną wizualizację i analizę wszystkich dostępnych danych.

Oczekuje się, że przedsiębiorstwa będą próbowały odejść od odosobnionych, samodzielnych rozwiązań cyberbezpieczeństwa na rzecz oprogramowania opartego na platformie lub narzędzi, które mogą zapewnić integrację z wieloma innymi narzędziami.

Technologia analizy Big Data stale ewoluuje, a w 2022 r. pomoże coraz większej liczbie firm być lepiej wyposażonym, podejmować bardziej świadome decyzje i opracowywać skuteczne strategie poprawy ich pozycji na rynku.

JAK ZMAKSYMALIZOWAĆ DANE W 2022 ROKU?

Ogromna część przyrostu Big Data w ciągu ostatnich kilku lat miała postać danych konsumenckich, które są stale połączone z konsumentami podczas korzystania z ich osobistych technologii (takich jak urządzenia do strumieniowego przesyłania danych, urządzenia IoT i media społecznościowe). Rozwiązania AI i ML już same w sobie są futurystyczne, ale automatyzacja

cja i skrócenie przepływu pracy, które umożliwiają, są głównymi czynnikami zmian w grze biznesowej.

Na koniec, naszą radą dotyczącą skutecznego zarządzania biznesem w 2022 roku jest monitorowanie sposobu wykorzystywania informacji wrażliwych, próba przekształcenia ich w przewagę biznesową, sprawdzanie luk w systemach, dostosowywanie się do najnowszych wymagań dotyczących ochrony danych i szybkie reagowanie w sytuacji, gdy ma miejsce incydent cybernetyczny.

W kwestie usprawniania cyberbezpieczeństwa wszyscy jesteśmy zaangażowani, ponieważ transformacja nie jest podróżą do ustalonego punktu końcowego. To sposób myślenia o ciągłym doskonaleniu i rozwoju, co, miejmy nadzieję, jest tym, co rok 2022 przyniesie nam wszystkim.

"TRANSFORMACJA NIE JEST PODRÓŻĄ DO USTALONEGO PUNKTU KOŃCOWEGO. TO SPOSÓB MYŚLENIA O CIĄGŁYM DOSKONALENIU I ROZWOJU."



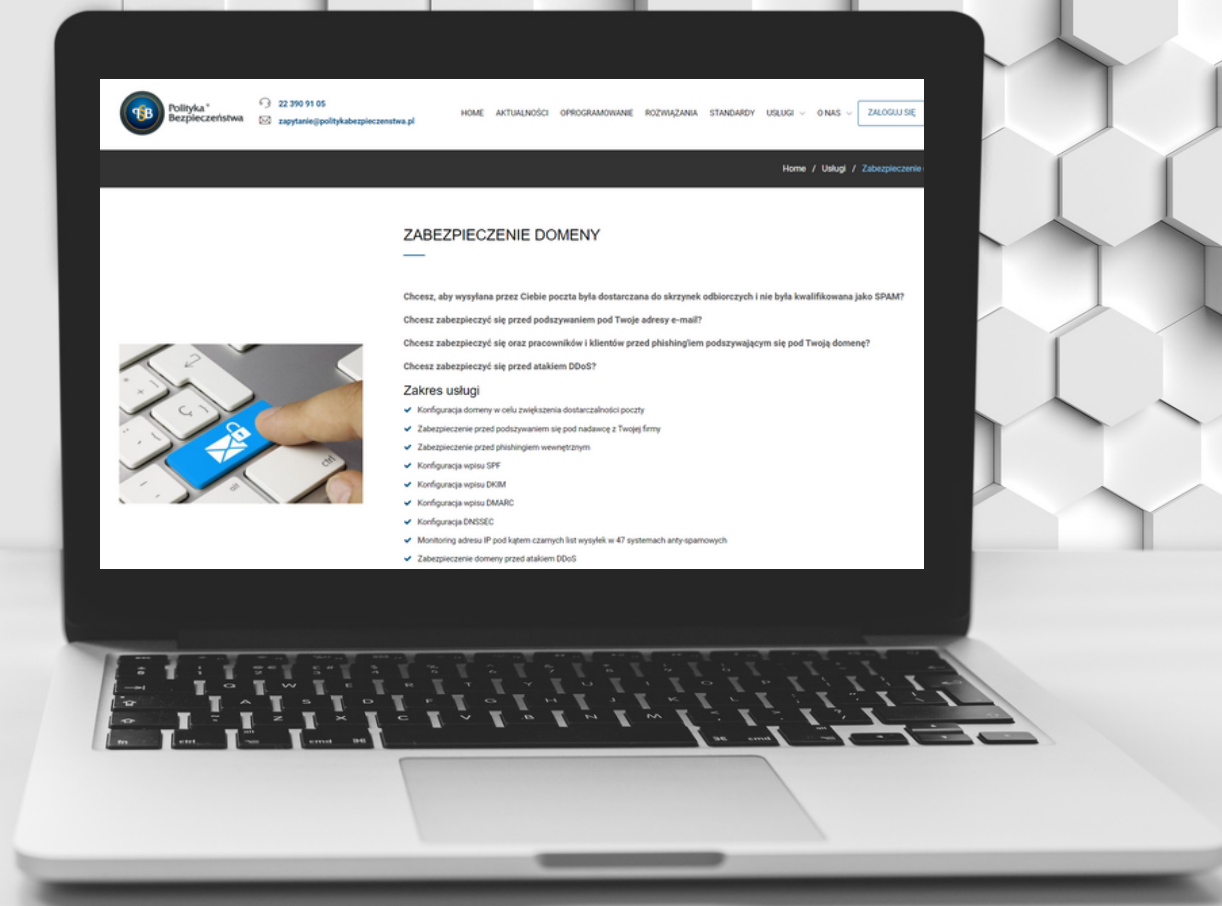
Chcesz, aby wysyłana przez Ciebie poczta była dostarczana do skrzynek odbiorczych i **nie była kwalifikowana jako SPAM?**

Chcesz **zabezpieczyć się przed podszywaniem** pod Twoje adresy e-mail?

Chcesz zabezpieczyć się oraz pracowników i klientów przed phishingiem **podszywającym się pod Twoją domenę?**

Chcesz zabezpieczyć się przed **atakami DDoS?**

ZAPYTAJ O OFERTĘ



TOMASZ SZYMAŃSKI

Prezes zarządu
Sygnisoft S.A.



Przez 20 lat zajmował się wprowadzaniem i rozwojem projektów związanych z digitalizacją. Karierę rozpoczął w międzynarodowych korporacjach w dziale marketingu, następnie tworzył i rozwijał projekty igamingowe oraz aplikacje bankowe, a także wdrażał strategię e-commerce oraz rozwiązania oparte o blockchain.

MARCIN BIAŁY

Advisory Architect
Grandmetric Sp. z o.o



Prowadził projekty transformacji IT w bankowości, sektorze produkcyjnym oraz publicznym. Dziś jego zespół Grandmetric doradza działom IT, jak zwiększyć niezawodność i bezpieczeństwo danych, systemów i użytkowników.

JANIS LASMANIS

Head of Security Department
Evolution AB



Odpowiedzialny za zarządzanie funkcjami bezpieczeństwa związanymi z aplikacjami informatycznymi, komunikacją i usługami komputerowymi w Evolution. Nadzoruje i koordynuje działania związane z bezpieczeństwem w firmie (m.in. technologii informacyjnej, zasobów ludzkich, komunikacji, prawa i innych grup).

PAULNA FAJTEK

PR Director
Come Creations Group



Z Come Creations Group związana od 2019 roku, najpierw jako PR Specialist, następnie awansowała na Team Lidera. Obecnie na stanowisku PR Director. Koordynuje pracę zespołu PR, tworzy plany komunikacyjne dla klientów, głównie z branży IT i nadzoruje ich wykonanie. Wspiera sprzedaż usług agencji.

RAFAŁ STĘPNIEWSKI

Prezes Zarządu
Rzetelna Grupa Sp. z o.o.



Redaktor naczelny serwisu dziennikprawny.pl i Security Magazine. Z branżą e-commerce związany od ponad 15 lat. Manager z 20-letnim doświadczeniem w branżach IT&T i zarządzaniu. Autor wielu publikacji z zakresu prawa e-commerce oraz bezpieczeństwa.

GRZEGORZ KUBERA

Chief Editor
No Fluff Jobs



W No Fluff Jobs jako Chief Editor publikuje teksty na Blogu, ale także rozwija dodatkowy serwis contentowy. W poprzednich latach redaktor naczelny kilku magazynów i serwisów online. Autor bestsellerów biznesowych "Stwórz jednorożca" i "Przeskok".

PIOTR ROZMIAREK

Account Manager
Marken Oficjalny dystrybutor
Bitdefender w Polsce



Magister filologii polskiej o specjalizacji nauczycielskiej oraz językoznawczo-redaktorskiej. Specjalista z zakresu cyberbezpieczeństwa, językoznawstwa, literaturoznawstwa oraz branży OZE. W wolnych chwilach sięga po książkę, gitarę lub teleskop.

ŁUKASZ NIEBOREK

Business Development Manager
Energy Logserver



Od wielu lat związany ze sprzedażą rozwiązań IT security dla rynku prywatnego oraz publicznego. Kieruje zespołem odpowiedzialnym za rozwój kanału sprzedaży systemu Energy Logserver w Polsce oraz na rynkach zagranicznych.

REDAKCJA "SECURITY MAGAZINE" ZAPRASZA DO WSPÓŁPRACY EKSPERTÓW I PRAKTYKÓW

"Naszym priorytetem jest przekazanie czytelnikom merytorycznej, profesjonalnej wiedzy bazującej na doświadczeniu praktyków z Polski i ze świata. Tematy wokół których będziemy się poruszać dotyczą szeroko pojętego bezpieczeństwa w firmach oraz jednostkach publicznych. Chodzi tu nie tylko o bezpieczeństwo fizyczne, ale i - o coraz istotniejsze - bezpieczeństwo IT. Stawiamy na profesjonalizm, rzetelność i wyczerpujące podejście do opisywanych zagadnień. Nasi autorzy również. Dlatego magazyn, mamy nadzieję, stanie się źródłem i inspiracją dla przedsiębiorców, którym zależy na tak kluczowym aspekcie działalności, jak bezpieczeństwo."

Redaktor naczelny, Rafał Stępniewski



KONTAKT: REDAKCJA@SECURITYMAGAZINE.PL

Wydawca:**Rzetelna Grupa sp. z o.o.**

al. Jana Pawła II 61 lok. 212

01-031 Warszawa

KRS 284065

NIP: 524-261-19-51

REGON: 141022624

Kapitał zakładowy: 50.000 zł

Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy

Numer wpisu do sądowego Rejestru dzienników i czasopism PR20362

Redaktor Naczelny: Rafał Stępniewski

Redakcja i korekta: Monika Świetlińska

Projekt i skład: Monika Świetlińska

Wszelkie prawa zastrzeżone.

Współpraca i kontakt: redakcja@securitymagazine.pl

Publikacja w całości jak i każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia Rzetelna Grupa sp. z o.o. z siedzibą w Warszawie. Wszelkie znaki towarowe, nazwy własne, logotypy oraz znaki graficzne i inne treści są chronione prawem autorskim.





SECURITYMAGAZINE.PL