1(22)/2024

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Dlaczego potrzebujemy Identity Security?

Jak zabezpieczyć dane osobowe zgodnie z RODO?

Bezpieczne przechowywanie kopii zapasowych

Zabezpieczanie firmowych aplikacji i platform e-commerce przed cyberatakami

SPIS TREŚCI

SZANOWNI PAŃSTWO,

witamy w 2024 roku, który zwiastuje kolejny etap w obszarze bezpieczeństwa i tego cyfrowego, i fizycznego.

2023 był świadkiem znaczących przełomów w dziedzinie cyberbezpieczeństwa, a błyskawiczny rozwój technologii AI pokazał, jak szybko może ewoluować wirtualna rzeczywistość i jak głęboko wpływa na nasze codzienne życie. W tym kontekście, rozpoczęty właśnie rok zapowiada się jako okres, w którym jeszcze bardziej zintensyfikują się wyzwania związane z ochroną przed cyberatakami.

W naszym magazynie nadal chcemy skupiać się na dostarczaniu Wam aktualnych i przystępnych informacji, które pomogą w starciu z tymi wyzwaniami, dostarczą informacji, rozwiązań, polecą wsparcie najlepszych specjalistów z dziedziny bezpieczeństwa IT, jak i tego fizycznego.

Niezmiennie, od niemal 2 lat, na łamach "Security Magazine" eksperci z różnych dziedzin bezpieczeństwa dzielą się swoimi spostrzeżeniami i radami, jak skutecznie chronić się przed nowymi zagrożeniami. Naszym celem jest też inspirowanie do aktywnego działania w celu zwiększenia bezpieczeństwa osobistego i zawodowego.

Oddajemy w Wasze ręce to noworoczne wydanie, mając nadzieję, że stanie się ono cennym źródłem informacji i inspiracji. Zapraszamy do lektury i życzymy bezpiecznego oraz owocnego roku 2024.

Rafał Stępniewski

SZCZEGÓŁY STR. 88

RAPORT ATS2023

Owocem 10. jubileuszowej edycji konferencji Advanced Threat Summit jest raport „Sztuczna inteligencja – wróg czy sojusznik cyberbezpieczeństwa?" Jest on źródłem wiedzy o przyszłości cyberbezpieczeństwa i sztucznej inteligencji. Ten unikalny materiał pozwala spojrzeć w przyszłość technologii, przedstawiając najnowsze trendy, wyzwania i innowacje w dziedzinie cyberbezpieczeństwa i AI. Analizuje wpływ AI zarówno z perspektywy obronnej, jak i ofensywnej. Przedstawia rozwój rynku sztucznej inteligencji w cyberbezpieczeństwie, podkreślając zarówno wyzwania, jak i możliwości wynikające z integracji tych technologii.

Jego mocną stroną jest kompleksowe podejście do tematu, obejmujące technologiczne, etyczne i praktyczne aspekty wykorzystania AI. Dostarcza cennych informacji dla profesjonalistów, jak i dla osób zainteresowanych szerszym kontekstem technologicznym i społecznym AI.
Polecamy jego lekturę dla uzyskania głębszego zrozumienia obecnych i przyszłych trendów w cyberbezpieczeństwie oraz roli, jaką AI odegra w kształtowaniu tej dziedziny. Można go pobrać **TUTAJ**.

SZKOŁA DOKTORSKA W NASK

1 października 2024 roku pierwsi doktoranci rozpoczną kształcenie w Szkole Doktorskiej NASK-PIB! Dyrektor NASK Wojciech Pawlak podpisał zarządzenie oficjalnie powołujące szkołę, która będzie tworzyć w NASK SCIENCE środowisko badań nad AI i zagadnieniami cyberbezpieczeństwa. Szczegóły już niebawem.

Zapraszamy do dzielenia się z nami newsami (do 500 zzs) z Twojej firmy, organizacji, które mają znaczenie ogólnopolskie i globalne.

Zachęcamy do przesyłania newsów na adres redakcja@securitymagazine.pl do 20. dnia każdego miesiąca.

Redakcja "Security Magazine"

AI ACT DLA UNII EUROPEJSKIEJ

AI Act to innowacyjna inicjatywa regulacyjna Unii Europejskiej, która ma na celu ustanowienie jasnych zasad korzystania z sztucznej inteligencji (AI). Ostatnie porozumienie w sprawie AI Act spotkało się z entuzjazmem, choć nadal istnieją zagadnienia wymagające wyjaśnienia, a finalizacja prac może zająć kilka miesięcy. Komisarz UE Thierry Breton ogłosił, że Europa jest pierwszym kontynentem z jasnymi zasadami dotyczącymi AI, mimo obaw niektórych państw o hamowanie rozwoju rynku AI.

Najważniejsze aspekty AI Act obejmują m.in. systemy rozpoznawania twarzy, zdalną biometrię i egzekwowanie prawa. AI Act ma stanowić rewolucję w biznesie, a jego jasność i pewność są istotne dla uniknięcia dezorientacji rynku i utrudnień w inwestycjach. Akt nie został zmieniony o 180 stopni, zachowując podział na kategorie ryzyka użycia AI. Uregulowano status wydajnych modeli AI oraz obowiązek rozliczania się producentów z danych, na których systemy AI były trenowane.

REKRUTACJA DO CYBERWOJSKA

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, powołane w 2022, rozpoczęło drugą edycję kampanii rekrutacyjnej dla studentów technicznych. DKWOC, poszukujące kandydatów do służby w cyberprzestrzeni, skupia się na młodych talentach z umiejętnościami analitycznymi, kreatywnością i zainteresowaniem kryptologią czy technologią. Szczegółowe informacje dostępne są online oraz na uczelniach. Więcej informacji o karierze w WOC można uzyskać pod numerem infolinii 509-677-777.

Zapraszamy do dzielenia się z nami newsami (do 500 zzs) z Twojej firmy, organizacji, które mają znaczenie ogólnopolskie i globalne.

Zachęcamy do przesyłania newsów na adres redakcja@securitymagazine.pl do 20. dnia każdego miesiąca.

Redakcja "Security Magazine"

PATRONAT
SECURITY MAGAZINE

8. edycja InfraSec Forum, wyjątkowe wydarzenie poświęcone bezpieczeństwu i ochronie technicznej infrastruktury operacyjnej odbędzie się 28-29 lutego w Warszawie. Konferencja stanie się miejscem dyskusji o zagrożeniach fizycznych i cyberbezpieczeństwie.

8. EDYCJA InfraSEC FORUM
ICS SCADA OT IIOT

InfraSec Forum 2024 to platforma spotkań i dialogu dla przedstawicieli sektorów i branż stanowiących krytyczne elementy w funkcjonowaniu nowoczesnych społeczeństw.

Dlaczego warto uczestniczyć?

- **Eksperci i prelegenci.** Wystąpienia ekspertów z bogatym doświadczeniem na rynkach polskim i zagranicznych.
- **Zróżnicowany program.** Precyzyjnie dobrane zagadnienia, wyłonione na podstawie rozmów z przedstawicielami środowiska.
- **Praktyczne warsztaty.** Możliwość dogłębnego przepracowania wybranych zagadnień z prowadzącymi specjalistami.
- **Networking.** Spotkania z przedstawicielami branży, wymiana doświadczeń i nawiązywanie kontaktów.

Dla kogo?

Wydarzenie adresowane jest do kadry zarządzającej, managerów i ekspertów z obszarów IT, automatyki, (cyber)bezpieczeństwa, infrastruktury krytycznej z branży przemysłowej i przesyłowej, sektora utilities, energii, gazu, paliw oraz dużych firm produkcyjnych, przetwórczych i wydobywczych.

Zainteresowani uczestnictwem mogą zgłosić udział poprzez stronę **InfraSec Forum**. W razie pytań, możliwy jest kontakt: **weronika.warpas@evention.pl**

Dołącz do InfraSec Forum 2024 i bądź na bieżąco z najnowszymi trendami oraz rozwiązaniami w dziedzinie cyberbezpieczeństwa OT!

SZCZEGÓŁY I REJESTRACJA

ORGANIZUJESZ KONKURS DLA SWOICH KLIENTÓW? ZRÓB TO ZGODNIE Z PRAWEM

Aneta Grala
Rzetelna Grupa

Jako organizator konkursów, masz obowiązek chronić dane osobowe uczestników. Dowiedz się, jak zorganizować bezpieczny konkurs zgodny z RODO, budując zaufanie i zapewniając uczestnikom ochronę ich danych. Czy Twoje procedury są zgodne z RODO i innymi przepisami o ochronie danych?

ZBIERANIE DANYCH OSOBOWYCH W KONKURSACH I ZAGROŻENIA Z TYM ZWIĄZANE

Przeprowadzanie wszelkiego rodzaju konkursów czy to stacjonarnie, online, w mediach społecznościowych wiąże się z przetwarzaniem danych osobowych. Uczestnicy konkursów, aby wziąć w nich udział najczęściej muszą przekazać do organizatora swoje dane osobowe już w momencie złożenia zgłoszenia, np. imię, nazwisko, adres e-mail, numer telefonu. Ponadto z uwagi na rodzaj konkursu może wystąpić konieczność gromadzenia większej ilości danych niezbędnych do zaklasyfikowania uczestników do udziału w konkursie, np. wiek, miejsce zamieszkania, zajmowane stanowisko, wykształcenie itp. W przypadku zwycięzców konkursu może być to jeszcze większa ilość danych, gdyż mogą się one powiększyć o dane niezbędne do wydania nagród, np. dokładny adres, numer konta bankowego.

W związku z tym uczestnik konkursu może być zobligowany do przekazania dużej ilości danych osobowych. Świadomość tego jak ważna jest ochrona swoich danych osobowych jest coraz wyższa i determinuje uczestników to zadania sobie pytania – czy jest to w ogóle bezpieczne?

Trzeba mieć na względzie, że organizator może okazać się oszustem i wykorzystać wyłudzone dane osobowe uczestników w innych celach niż zostały zebrane, np. do czynności przestępczych takich jak zawarcie jakiejś umowy bez wiedzy uczestnika. Warto zatem wybierać konkursy, w których do wzięcia udziału niezbędna jest mała ilość danych osobowych, np. imię i adres e-mail. **Bezwzględnie nigdy nie należy podawać danych dostępowych do konta czy karty bankowej!**

Ważne jest zatem uprzednie zweryfikowanie organizatora konkursu, czy jest to sprawdzony podmiot, podający prawdziwe dane, a najlepiej korzystać z oficjalnych stron czy profili w mediach społecznościowych. Natomiast ze strony organizatora konkursu istotne jest, aby uprawdopodobnił rzetelność firmy i to, że działa zgodnie z prawem w sposób przejrzysty, a podane przez uczestników dane osobowe będą bezpieczne.

PRZESTRZEGANIE RODO PODCZAS PRZETWARZANIA DANYCH OSOBOWYCH

Organizator konkursu, który zbiera dane osobowe uczestników musi przetwarzać te dane zgodnie z obowiązującymi przepisami, w tym przede wszy-

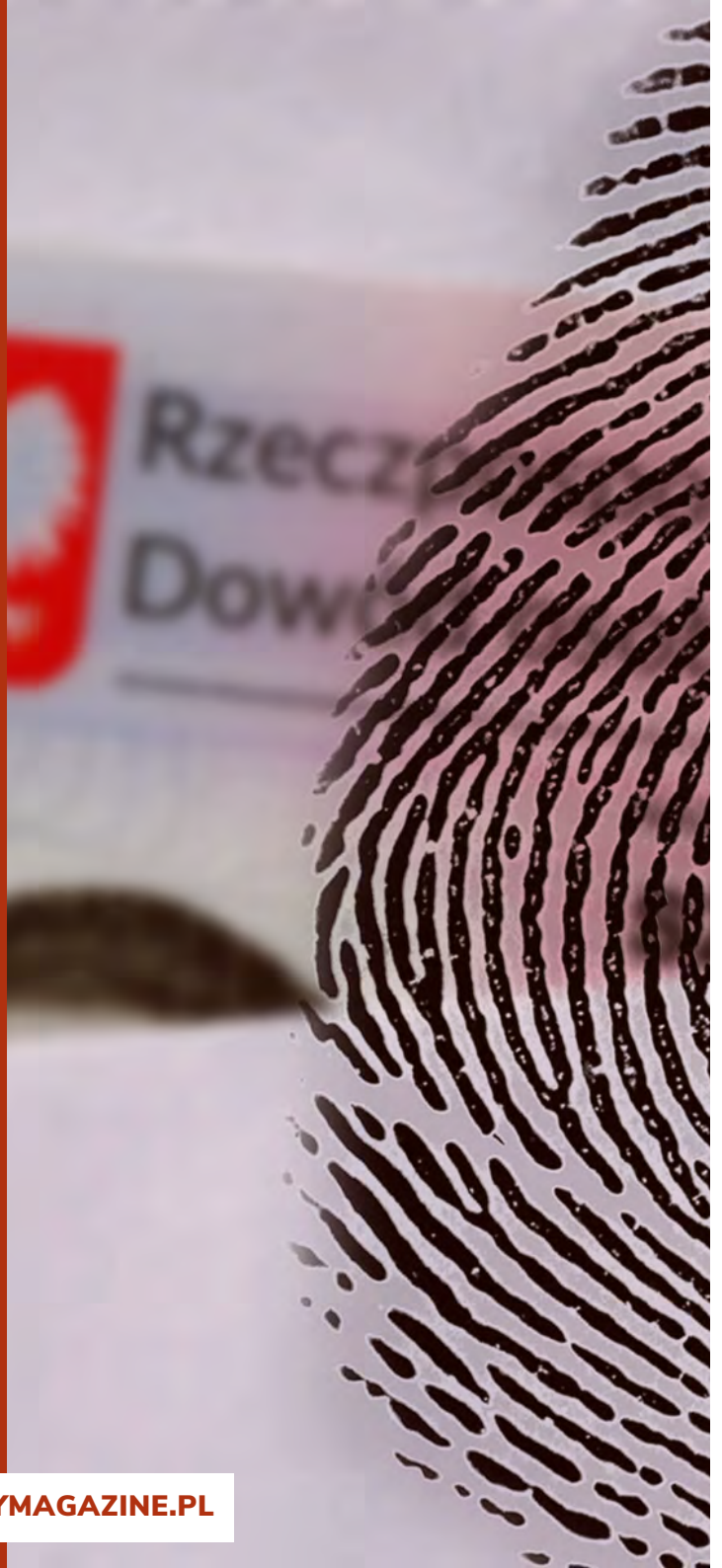
stkim RODO.

Mając na uwadze przepisy RODO - zgodnie z art. 13 RODO, organizator konkursu ma obowiązek przekazać uczestnikowi informacje, w jaki sposób będzie przetwarzał jego dane osobowe. Obowiązek informacyjny powinien być przekazany uczestnikowi w momencie pobierania od niego danych osobowych, oznacza to, że w chwili złożenia zgłoszenia do konkursu powinna być możliwość zapoznania się z treścią obowiązku informacyjnego (treść może być częścią regulaminu konkursu). Art. 13 RODO wskazuje enumeratywnie jakie informacje należy zamieścić w treści obowiązku informacyjnego.

W szczególności należy mieć na względzie, aby organizator konkursu przestrzegał zasad przetwarzania danych osobowych wskazanych w art. 5 RODO. Między innymi zasadę minimalizacji danych i zasadę ograniczonego celu, mówiące o tym, że dane osobowe muszą być ograniczone do tego, co niezbędne do celów, w których są przetwarzane oraz zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Innymi słowy, dane osobowe mogą być wykorzystywane tylko na potrzeby konkursu oraz tylko w minimalnym zakresie jaki jest niezbędny.

Niedozwolone jest przekazywanie danych osobowych uczestników konkursu do innych podmiotów ani ujawnianie ich. Dopuszczalne jest jedynie przekazanie danych osobowych, które jest niezbędne do obsługi konkursu, np. przekazanie danych do przelewu – do instytucji bankowej, przekazanie danych uczestnika konkursu na potrzeby złożenia zgłoszenia online czy korespondencji e-mail – do firmy, która świadczy usługi hostingu czy dane adresowe w celu dostarczenia nagrody – do firmy świadczącej usługi kurierskie. Informacje te powinny być wskazane w obowiązku informacyjnym.

Na etapie zgłoszenia zwykle niezbędna jest mniejsza ilość danych osobowych – organizator konkursu powinien pobierać tylko dane osobowe niezbędne do weryfikacji prawidłowości zgło-



szenia i organizator konkursu nie ma podstawy prawnej na tym etapie, aby pobierać od uczestnika konkursu większą ilość danych osobowych. Dopiero po wytypowaniu zwycięzców, organizator ma podstawę prawną, aby pobrać od tych zwycięzców dane osobowe potrzebne do wydania nagrody.

TWORZENIE I WDRAŻANIE REGULAMINU KONKURSU

Ważną kwestią jest także klarowność warunków wzięcia udziału w konkursie oraz zasad jego przeprowadzania, powinny być one uregulowane w regulaminie konkursu.

Organizację konkursu od strony formalnej należy rozpocząć od utworzenia regulaminu konkursu, w którym będą uregulowane wszystkie kwestie dotyczące warunków uczestnictwa, wskazanie nagród, zasady rozstrzygnięcia konkursu, tryb wyłonienia zwycięzców i przyznania nagród oraz kwestie postępowania reklamacyjnego.

W momencie zgłoszenia do konkursu uczestnik powinien mieć możliwość zapoznania się z regulaminem konkursu. Następnie do wzięcia udziału w konkursie niezbędna jest akceptacja treści regulaminu konkursu przez uczestnika konkursu. W przypadku formularzy internetowych pole akceptacji nie może być wcześniej zaznaczone, gdyż uczestnik konkursu musi wyrazić świadomą i dobrowolną zgodę.

Jeśli organizatorów konkursu jest kilku jednocześnie i mają dostęp do danych osobowych uczestników, wówczas trzeba przeanalizować, czy są oni współadministratorami myśl w RODO i powinni zawrzeć umowę o współadministrowaniu, która ureguluje obowiązki współadministratorów.

W przypadku jeśli drugi podmiot wykonuje tylko określone czynności zlecone przez organizatora konkursu, np. dokonuje jedynie dostarczenia nagrody, dochodzi wtedy do powierzenia przetwarzania danych osobowych w celu dostarczenia nagrody w zakresie ograniczonym tylko do danych osobowych niezbędnych do wykonania zleconej czynności. Każde przekazanie danych do innego podmiotu należy analizować indywidualnie.

Przetwarzanie danych osobowych następuje zwykle na każdym etapie konkursu, od złożenia zgłoszeń, wyboru zwycięzców, do wydania nagrody, ale i po zakończeniu konkursu. Organizator konkursu posiada prawnie uzasadniony interes, aby przechowywać dane osobowe uczestników oraz zwycięzców przez określony czas, a następnie ma obowiązek je usunąć zgodnie z czasem retencji danych jaki został wskazany w obowiązku informacyjnym przekazanym uczestnikom konkursu.

Dane te powinny być przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane. Należy uwzględnić w tym długość całego procesu rozstrzygnięcia konkursu oraz postępowania reklamacyjnego.

Masz pytania i potrzebujesz wsparcia w organizacji konkursu, w tym przygotowania profesjonalnego regulaminu konkursowego zgodnego z prawem?

Skontaktuj się z nami:
Agnieszka Zboralska,
agnieszka.zboralska@rzetelnagrupa.pl
tel.: +48 506 947 431

-20%

SECURITY MAGAZINE

NOWOROCZNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

WAŻNY DO

30.01.2024

KONTAKT I SZCZEGÓŁY:

redakcja@securitymagazine.pl

+48 518 609 987

DLACZEGO POTRZEBUJEMY IDENTITY SECURITY?

Grzegorz Brol
Integrity Partners

Krzysztof Andrian
Integrity Partners

Jakie korzyści wynikają z wdrożenia rozwiązań Identity Security, nie tylko dla dużych korporacji, ale także dla mniejszych firm? Dlaczego coraz więcej firm decyduje się na połączenie sił z partnerami specjalizującymi się w obszarze Identity Security, aby zaoferować klientom kompleksowe rozwiązania cyberbezpieczeństwa? Na ten temat rozmawiamy z Grzegorzem Brolem i z Krzysztofem Andrianem z Integrity Partners.

Czym są rozwiązania Identity Security i jaka jest ich rola w zarządzaniu bezpieczeństwem firm?

Krzysztof Andrian: Rozwiązania Identity Security pozwalają na weryfikację tożsamości i zarządzanie dostępem do fundamentalnych zasobów w firmie. Dziś ich rola jest ważna z dwóch powodów. Po pierwsze organizacje zmieniły swój sposób działania, coraz częściej funkcjonują w środowisku hybrydowym i rozproszonym, pracownicy łączą się więc z systemami i aplikacjami z przeróżnych miejsc, w różnym czasie. Zabezpieczenie tego procesu jest wyjątkowo ważne. Po drugie – rośnie aktywność cyberprzestępców, a przejęcie danych uwierzytelniających pracowników jest często początkiem udanego cyberataku.

Zatem narzędzia Identity Security pełnią ważną rolę w zapewnieniu bezpieczeństwa w organizacjach rozproszonych. I to nie tylko tych dużych. Coraz więcej firm średniej wielkości zaczyna myśleć o implementacji takich rozwiązań. To słuszne podejście, ponieważ tak naprawdę każda firma, która chce działać sprawnie i utrzymać ciągłość działania, powinna zwrócić uwagę na Identity Security.

Jakie firmy i sektory powinny rozważyć wdrożenie narzędzi z obszaru Identity Security?

Grzegorz Brol: Jeszcze kilka lat temu rozwiązaniami Identity Security interesowały się przede wszystkim największe instytucje finansowe czy publiczne. Działo się tak, ponieważ odpowiednich zabezpieczeń wymagały od nich zewnętrzne regulacje. Prekursorem, taką awangardą rynkową była branża finansowa, która po prostu musiała wprowadzać nowoczesne na-

rzędzia chroniące dane i użytkowników. Rynek jednak dojrzewa i ewoluuje. Dziś elementem skłaniającym firmy do zabezpieczania tożsamości są nie tylko regulacje, ale i realne zagrożenia, których doświadczają. Rośnie świadomość firm w zakresie zachowania ciągłości działania oraz skutków, jakie pociąga za sobą cyberatak. Skutków wielowarstwowych, bo przecież cyberatak to nie tylko problem z działaniem infrastruktury, ale też przestoje w działalności, utrata zaufania kontrahentów i inwestorów, straty wizerunkowe, ogromne koszty związane z przywracaniem działań operacyjnych czy z koniecznością zapłacenia kar.

To dlatego na rozwiązania klasy Identity Security decydują się coraz mniejsze przedsiębiorstwa, także wytwórcze, usługowe, z bardzo różnych sektorów. Co więcej, różnego rodzaju regulacje dotyczą coraz mniejszych firm i coraz szerszego spektrum branż. Spójrzmy na przykład na NIS 2 – grupa podmiotów uznanych za ważne i istotne, czyli objętych tą dyrektywą, jest naprawdę szeroka.

Jakich korzyści mogą się spodziewać firmy wdrażające u siebie systemy Identity Security? Czy chodzi tylko o bezpieczeństwo danych?

K.A.: Rzeczywiście, historycznie źródłem zainteresowania systemami Identity Security była potrzeba zwiększenia bezpieczeństwa danych, zmniejszenia ryzyka wycieku czy naruszeń polityk bezpieczeństwa. Dziś firmy dostrzegają coraz szersze korzyści z zastosowania rozwiązań tej klasy. Benefity te dotyczą pięciu istotnych obszarów. Pierwszym i najbardziej oczywistym jest bezpieczeństwo. Drugim compliance, czyli zgodność z regulacjami. Trzecim – produktywność. W tym zakresie Identity Security pomaga w procesie onboardingu – przydzielania dostępów, wyznaczania ról, ale i offboardingu, czyli odbierania uprawnień pracownikom odchodzącym. W tym punkcie warto również podkreślić, że narzędzia Identity Security eliminują błędy, jakie mogą się pojawić w tych procesach, gdy zarządzają nimi

ludzie. Błędy, które mogą firmę sporo kosztować.

I skoro już przy kosztach jesteśmy – czwartym obszarem są oszczędności. Z jednej strony w postaci uwolnienia zasobów – rozwiązania Identity Security automatyzują pracę, dzięki czemu odciążeni pracownicy mogą zająć się bardziej zaawansowanymi zadaniami, nie ma potrzeby rozszerzania zespołów. Z drugiej – w postaci sprawniejszego działania service desków. Wdrożenie Identity Security zmniejsza liczbę zgłoszeń serwisowych, pozwala również na wprowadzenie mechanizmów self-service. Rozwiązania klasy IAM, czyli Identity Access Management, dają takie możliwości. Wtedy to użytkownicy zarządzają wieloma procesami, odciążany jest więc zespół serivce desku.

I w końcu piątym elementem jest skalowalność. Identity Security żyje razem z firmą. Nawet jeśli organizacja połączy się z inną czy podzieli, zatrudni wielu nowych pracowników, rozbuduje infrastrukturę IT – to narzędzie dostosuje się do zmian i pomoże w ich przeprowadzeniu.

Innym słowem – rozwiązania Identity Security to nie jest zabawka dla działów IT. To jest narzędzie dla firm, które rozszerzają działalność, wchodzą w kanały cyfrowe, zatrudniają pracowników, potrzebują działać wydajnie, zwinnie, chcą być wiarygodne. I nie chcą tracić zasobów w związku z cyberatakami.

Jak wygląda proces integracji rozwiązań Identity Security z wykorzystywanymi już przez przedsiębiorstwa technologiami. Na co powinny się nastawić firmy, decydując się na wdrożenie IS?

G.B.: W przypadku wdrażania rozwiązań Identity Security ważna jest współpraca z odpowiednim partnerem technologicznym. Nie chodzi bowiem o samą implementację systemu, ale o jego odpowiednią integrację ze wszystkimi komponentami, w szczególności z aplikacjami. Nieodpowiednie wdrożenie i zintegrowanie narzędzia IS kończy się tym, że mimo wysiłku, mimo wprowadzenia kolejnej technologii firma działa tak samo, nie zyskuje wielu korzyści.

Dlatego warto postawić na współpracę z integratorem, który ma szerokie kompetencje w tym obszarze. Bo choć oczywiście samo wdrożenie systemu IS jest coraz bardziej zautomatyzowane, mamy coraz więcej wtyczek, narzędzi, które ułatwiają cały proces, to jednak dynamika tworzenia nowych aplikacji w firmach, rozwój środowisk DevOps rodzą

wyzwania. A to oznacza, że wsparcie integratora jest potrzebne nie tylko podczas wdrożenia, ale także po nim, w momencie, gdy pojawiają się nowe rozwiązania firmy, które trzeba także objąć ochroną.

K.A.: Bardzo ważne jest odpowiednie przygotowanie firmy do wdrożenia rozwiązania klasy Identity Security. Samo wdrożenie rzeczywiście ma charakter integracyjny. Partner technologiczny nie wyrzuca żadnych systemów po stronie klienta, ale łączy je z platformą. I są to systemy, z których korzystają różne działy, nie tylko IT. To są na przykład działy HR czy infrastruktura Active Directory. Kompleksowe podejście do wdrożenia daje również szansę na weryfikację i poprawienie procesów biznesowych. Sprawdzenie, czy na pewno są optymalne, czy dają firmie to, czego potrzebuje. Warto pamiętać, że wiele procesów zostało zaimplementowanych przed laty i było dostosowanych do sytuacji firmy na danym etapie rozwoju. Wdrożenie Identity Security pozwala zweryfikować, czy dziś też odpowiadają na oczekiwania przedsiębiorstwa. Np. proces wprowadzania nowych pracowników i nadawania im uprawnień do systemów.

Z drugiej strony to jest najlepszy moment na wyczyszczenie i poprawienie jakości danych w systemach. Chodzi o konta duchy lub konta nieprzypisane do żadnej tożsamości. Pracownicy odeszli z firmy, a konta zostały. Albo pracownicy odeszli, a mimo to nadal mają dostępy do wewnętrznych systemów. To niebezpieczne sytuacje podnoszące ryzyko nieuprawnionego .

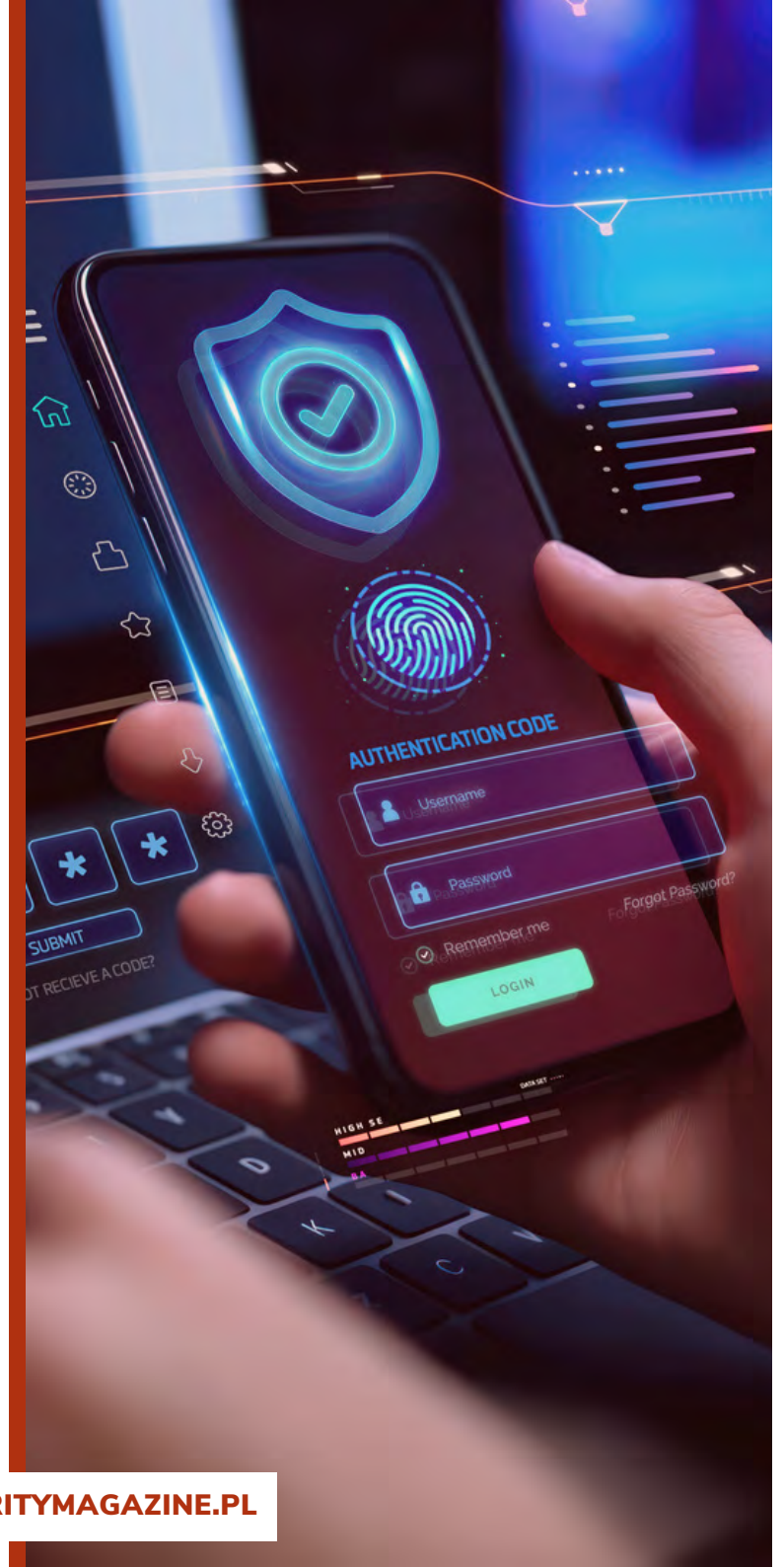
dostępu do danych. Dzięki wdrożeniu Identity Security można automatycznie zidentyfikować i wyczyścić tego typu rekordy.

Tylko firma, która dobrze przygotuje się do wdrożenia, obejmie nim wszystkie systemy i zrozumie, co może dać jej rozwiązanie Identity Security, będzie w stanie w pełni wykorzystać potencjał tego narzędzia. A ten potencjał jest ogromny i obejmuje wiele obszarów, działów i pracowników, nie tylko technicznych, ale przede wszystkim biznesowych.

Potrzeby firm w obszarze rozwiązań do zarządzania tożsamością i dostępem rosną. W jakim kierunku idzie dziś rynek?

G.B.: Na rynku można zauważyć kilka istotnych trendów. O pierwszym już wspomnieliśmy – po rozwiązania Identity Security sięgają coraz mniejsze firmy. Także takie, które nie mają swoich własnych zespołów kompetencyjnych i wielkich budżetów, nie są też związane z sektorami regulowanymi. One szczególnie muszą liczyć na wsparcie konsultantów zewnętrznych. I co ważne – mogą skorzystać z coraz szerszej oferty usług zarządzanych oraz rozwiązań w modelu SaaS, także w obszarze Identity Security. Takich wdrożeń opartych na technologii chmurowej jest dziś coraz więcej i ten trend moim zdaniem będzie się rozwijał.

Drugą tendencją, o której warto wspomnieć, jest zbliżanie się do siebie zagadnień ochrony tożsamości użytkowników i tożsamości uprzywilejowanej. Kiedyś to były dwie zupełnie niezależne warstwy ochrony.



Dziś rynek idzie w kierunku podejścia kompleksowego – Identity Security dotyczy nie tylko uprawnień administratora czy pracowników, ale wszystkich użytkowników biznesowych.

I trzecia rzecz – rośnie zainteresowanie wykorzystaniem rozwiązań Identity Security w środowiskach DevOps. Te środowiska są bardzo dynamiczne, jest w nich dużo zmian, którymi trudno zarządzać ręcznie, sekretów, które należy chronić. Żeby robić to skutecznie, potrzebna jest automatyzacja. Zatem firmy, które tworzą własne aplikacje na potrzeby wewnętrzne, też coraz częściej wdrażają narzędzia Identity Security.

Jakich nowości możemy się spodziewać w zakresie Identity Security w perspektywie kilku następnych lat?

K. A.: Na pewno możemy spodziewać się coraz większego odejścia od haseł. Świat idzie w kierunku passwordless, w kierunku używania biometrii jako drugiego czynnika uwierzytelniania i to się nie zmieni. Będziemy też zabezpieczać coraz więcej tożsamości non-human. Firmy powszechnie korzystają z robotów, z urządzeń IoT, IIoT, z botów – one wszystkie także łączą się z Internetem, komunikują ze sobą i świadomość tego, że tę komunikację trzeba odpowiednio zabezpieczyć, także rośnie.

Upowszechniać się będzie także adaptacja filozofii Zero Trust, czyli podejścia, które zakłada brak zaufania do każdego, kto próbuje dostać się do naszych zasobów. Zatem istotne jest uwierzytelnienie każdej próby dostępu do firmowego środowiska, szcze-

gólnie w organizacjach złożonych, hybrydowych, wykorzystujących rozwiązania chmurowe.

Możemy też spodziewać się w Identity Security połączenia biometrii z zachowaniami użytkownika, czyli weryfikowanie tożsamości poprzez np. odczytanie linii papilarnych w połączeniu z konkretnym schematem zachowania.

Integrity Partners połączył siły z Concept Data między innymi po to, by rozszerzyć swoją ofertę i kompetencje o rozwiązania Identity Security. W firmie był już pion cybersecurity. Skąd więc taki ruch?

G.B.: Rozwiązania zarządzania tożsamością były kiedyś odległe od klasycznego cybersecurity zarówno w wymiarze organizacyjnym właścicieli systemów, jak i w wymiarze integracji. Te dziedziny jednak w ostatnich latach bardzo się zbliżyły.

W związku z tym także rozwiązania, które oferujemy w Integrity Partners i Concept Data, stały się bardzo silnie komplementarne i wzajemnie się uzupełniają. Razem tworzą szczelną ochronę przedsiębiorstw i użytkowników. W związku z czym nasze organizacje w naturalny sposób się zbliżyły.

Dodatkowo część klientów, z którymi Integrity Partners współpracuje od wielu lat, których jest zaufanym doradcą i partnerem, korzysta też z rozwiązań oferowanych wcześniej przez Concept Data. Dzięki połączeniu możemy wykorzystać wspólne kompetencje do bardziej kompleksowej obsługi klienta.

Jaką pozycję na rynku chcą Państwo teraz zająć? Jakie nowe możliwości daje połączenie?

Dlaczego potrzebujemy Identity Security?

G.B.: Identity Partners od lat budował pozycję lidera w kilku kategoriach rynkowych. Bardzo mocno postawiliśmy na cybersecurity i cloud. Rozwijamy usługi zarządzane. Concept Data wyspecjalizował się w Identity Security. Działając wspólnie, możemy stać się liderem w zakresie szeroko pojętego cybersecurity na polskim i regionalnym rynku. Zwłaszcza w obszarze tak dziś ważnej i zyskującej na znaczeniu ochrony i zarządzania tożsamością.

K.A.: Mamy ambicję stać się doradcą przedsiębiorstw, trusted advisor, partnerem, który rozumie potrzeby firmy i przekłada je na rozwiązania wspierające biznes. Chcemy zająć silną pozycję między Wielką Czwórką a małymi integratorami. Wspólnie mamy odpowiednią skalę, ponad 130-osobowy zespół, szerokie know how i dostęp do narzędzi największych firm technologicznych na świecie. Dzięki temu możemy doradzać, wdrażać, ale też proponować usługi MSP tym firmom, które potrzebują skutecznych zabezpieczeń, ale którym brakuje kompetencji własnych oraz dużych budżetów.

Polityka®
Bezpieczeństwa

ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE...

POMOŻEMY

agnieszka.zboralska@rzetelnagrupa.pl
+48 506 947 431

SECURITYMAGAZINE.PL

CYBERATAKI W IV KWARTALE 2023 ROKU

Redakcja
SECURITY MAGAZINE

W ostatnim kwartale minionego roku spokojnie nie mogła spać nawet rodzina królewska. Na celowniku cyberprzestępców znalazły się także m.in.: czeski rząd, brytyjska biblioteka, linie lotnicze Air Europa, a w Polsce - ALAB. Do jakich cyberataków doszło jeszcze w czwartym kwartale 2023 roku?

Ostatni kwartał 2023 roku obfitował w wiele cyberataków, od których wolna nie była nawet rodzina królewska. Początkiem października Royal.uk, oficjalna strona monarchów, była nieaktywna przez około 90 minut. Gdy witryna znów zaczęła działać, wprowadzono moduł sprawdzania adresów IP, aby upewnić się, że osoby uzyskujące dostęp do witryny nie są botami. W poście na Telegramie dotyczącym cyberataku KillNet stwierdził, że przeprowadził go w ramach *„ataku na pedofilów”*, który miał nawiązywać do zarzutów o wykorzystywanie seksualne nieletniej postawionych księciu Andrzejowi, księciu Yorku.

6 października firma biotechnologiczna 23andMe ujawniła, że padła ofiarą naruszenia bezpieczeństwa danych. Celem cyberataku byli najprawdopodobniej użytkownicy pochodzenia żydowskiego. Cyberprzestępca występujący pod pseudonimem „Golem” twierdził, że w poście na forum hakerskim BreachForums przesłał bazę danych 1 miliona osób pochodzenia żydowskiego.
„Golem” oferował na sprzedaż pakiety danych, które, jak twierdził, zawierały „dostosowane do potrzeb grupy etniczne, zindywidualizowane zbiory danych, dokładne szacunki pochodzenia, informacje o fenotypie, zdjęcia, linki do setek potencjalnych krewnych i, co najważniejsze, surowe profile danych”.

Cyberprzestępca przekazał także, że ukradł dane należące do *„najbogatszych ludzi mieszkających w USA i Europie Zachodniej”*, w tym brytyjskiej rodziny królewskiej, Rockefellerów i Rothschildów. Informacje te jednak nie zostały potwierdzone. Ceny zestawów danych wahały się od 10 do 1 dolara, w zależności od tego, ile profili byli skłonni kupić potencjalni nabywcy. Naruszenie skłoniło firmy zajmujące się testowaniem DNA do domyślnego korzystania z loginów uwierzytelnianych dwuskładnikowo.

ATAK NA LINIE LOTNICZE AIR EUROPA

Z kolei Air Europa doświadczyła naruszenia bezpieczeństwa danych, w wyniku którego ujawniono informacje dotyczące płatności swoich klientów. 10 października linia lotnicza wysłała e-mail do dotkniętych atakiem klientów, informując ich, że podczas cyberataku, przestępcy mogli uzyskać dostęp do ich danych dotyczących płatności. Według linii lotniczej incydent wykryto, gdy zauważono podejrzane aktywności w jednym z jej systemów. Numery kart kredytowych, daty ważności i kody CCV klientów zostały ujawnione, mimo że przechowywanie kodów CCV jest niezgodne z przepisami Payment Card Industry Data Security Standard (PCI DSS).

Ze względu na charakter ujawnionych danych Air Europa wezwała wszystkie osoby, które korzystały z karty kredytowej do płacenia za loty, do anulowania karty, chociaż linia lotnicza stwierdziła również, że nie ma dowodów na to, że naruszenie zostało „*ostatecznie wykorzystane do popełnienia oszustwa*".

NAJWIĘKSZE W HISTORII ATAKI DDOS

Dostawcy infrastruktury internetowej Google Cloud, Cloudflare oraz AWS zgłosili 10 października największe w historii ataki DDoS, w którym liczba żądań na sekundę (rps) osiągnęła najwyższą wartość ponad 398 milionów, co stanowi siedem i pół raza więcej niż poprzedni rekordowy Atak DDoS. CSO Cloudflare Grant Bourzikas napisał w poście na blogu Google, że „kluczowe" jest zrozumienie, że atak mógł być przeprowadzony z użyciem „*botnetu skromnej wielkości, składającego się z około*

20000 maszyn." Co więcej, dane osobowe 815 milionów mieszkańców Indii, najwyraźniej wydobyte z bazy danych ICMR dotyczącej testów na Covid, zostały wystawione na sprzedaż w DarkNecie na początku tego miesiąca. Według firmy ochroniarskiej Resecurity, która odkryła wpis, dane obejmowały imię i nazwisko ofiary, wiek, płeć, adres, numer paszportu i numer Aadhaar (12-cyfrowy rządowy numer identyfikacyjny).

FAŁSZYWE INFORMACJE O ERUPCJI WULKANU WE WŁOSZECH

Natomiast we Włoszech doszło do ataku, którego celem było rozsyłanie nieprawdziwych informacji do obywateli na temat rzekomych erupcji wulkanu. Badacze z włoskiej firmy D3-Labs zajmującej się cyberbezpieczeństwem odkryli, że przestępcy wykorzystywali usługę IT-Alert – nowy publiczny system ostrzegania, używany przez włoski rząd do udostępniania obywatelom informacji o zagrożeniach m.in. tych, dotyczących erupcji wulkanu.

Cyberprzestępcy stworzyli witrynę udającą IT Alert, na której widniała informacja „*w związku z możliwymi erupcjami wulkanu może wystąpić ogólnokrajowe trzęsienie ziemi*", a następnie kazano czytelnikom pobierać aplikację. Gdy ofiara kliknęła przycisk, pobierany był plik o nazwie IT-Alert.apk zawierający złośliwe oprogramowanie SpyNote. Monitując użytkownika w tle, przestępcy mogli uzyskać pełną kontrolę nad smartfonem ofiary, umożliwiając jej na przykład kradzież danych logowania do aplikacji bankowych i mediów społecznościowych.

NA CELOWNIKU CZECHY I BIBLIOTEKA BRYTYJSKA

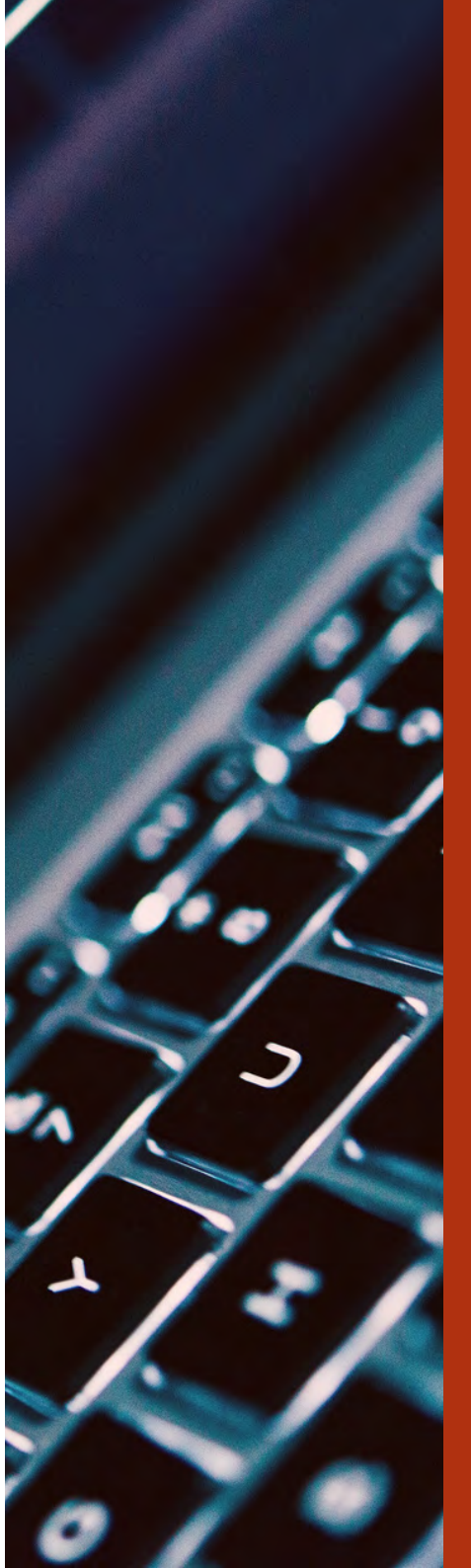
Ostatni kwartał 2023 roku pod kątem cyberbezpieczeństwa nie był łaskawy również dla Czechów, ponieważ zaatakowano ich strony rządowe oraz serwisy internetowe policji i lotniska w Pradze, a także stronę internetową Platformy Krymskiej, międzynarodowego szczytu odbywającego się tego dnia w Pradze. Ataki zakłócały działanie stron na około dwie godziny. Różne źródła podają, że za ataki odpowiedzialni byli hakerzy NoName057. Od marca 2022 r. ugrupowanie to stoi za szeregiem cyberataków na agencje rządowe i media w USA i Europie, których celem są przede wszystkim podmioty, które uważa się za wrogów Rosji.

Z kolei w Wielkiej Brytanii cyberataku doświadczyła Biblioteka Brytyjska. Przestępcy zakłócili działanie strony internetowej, systemów internetowych, publicznej sieci Wi-Fi oraz usługi telefoniczne. Obie placówki w Londynie i Yorkshire dotknięte były, jak sama biblioteka określiła, „*poważną awarią technologiczną*". „*W odpowiedzi na atak podjęliśmy ukierunkowane środki ochronne, aby zapewnić integralność naszych systemów. Przy wsparciu Narodowego Centrum Cyberbezpieczeństwa i specjalistów ds. cyberbezpieczeństwa podejmujemy również dochodzenie prokuratorskie*" – napisała w komunikacie do pracy Biblioteka Brytyjska. Do ataku przyznali się operatorzy oprogramowania ransomware Rhysida.

ZAATAKOWANA POPULARNA APLIKACJA RODZICIELSKA

W ostatnim kwartale 2023 roku cyberprzestępcy zaatakowali także popularną aplikację rodzicielską Kid Security, która pozwala rodzicom monitorować i kontrolować bezpieczeństwo swoich dzieci w Internecie. Aplikacja udostępniała dzienniki aktywności użytkowników w Internecie przez ponad miesiąc za pośrednictwem źle skonfigurowanych instancji Elasticsearch i Logstash. Badacz bezpieczeństwa Bob Diachenko z SecurityDiscovery po raz pierwszy zidentyfikował ujawnione informacje w październiku. Według CyberNews naruszonych zostało ponad 300 milionów rekordów danych, w tym 21 000 numerów telefonów i 31000 adresów e-mail. Ujawniono także niektóre dane kart płatniczych.

Badacze z Aqua Nautilus odkryli Kubernetes Secrets – obiekty zawierające niewielkie ilości wrażliwych danych, takich jak hasła, tokeny czy klucze – dotyczące setek organizacji wystawionych na działanie Internetu w publicznych repozytoriach GitHub. Wśród poszkodowanych znalazła się firma SAP SE. Badacze odkryli dane uwierzytelniające, które zapewniły dostęp do 95 592 696 artefaktów, a także uprawnienia do pobierania i niektóre operacje wdrażania.



Powiadomiono firmę SAP SE, która zareagowała „w najbardziej profesjonalny i skuteczny sposób", rozwiązując problem, rozpoczynając dochodzenie i utrzymując komunikację z Aqua Nautilus.

Ponadto pod koniec 2023 roku ujawniono, że TmaxSoft, firma informatyczna z Korei Południowej, od ponad dwóch lat udostępnia w Internecie 2 TB danych za pośrednictwem pulpitu nawigacyjnego Kibana. Dane zawierają ponad 56 milionów rekordów. Większość wyciekających danych to informacje o firmie i e-maile, ale obejmują nazwiska pracowników, numery telefonów, numery umów o pracę i e-maile, a także załączniki do e-maili, metadane i inne wrażliwe informacje, które mogą zostać wykorzystane w atakach na łańcuch dostaw.

NA POLSKIM PODWÓRKU

W ostatnim kwartale 2023 roku doszło również do głośnego cyberataku w Polsce. Chodzi ogólnopolską sieć laboratoriów medycznych ALAB. Jak podają polskie media, wyciek jest skutkiem ataku grupy ransomware. W wyniku ataku, w sieci znalazły się dane co najmniej kilkudziesięciu tysięcy Polek i Polaków, którzy od roku 2017 do 2023 wykonywali badania medyczne w sieci ALAB Laboratoria.

Co więcej, nieznana grupa ransomware RA World opublikowała na swoim blogu nie tylko informację o skutecznym włamaniu do firmy ALAB, ale także próbkę wykradzionych danych, a w niej między innymi wyniki ponad 50 tysięcy badań medycznych. Hakerzy domagali się okupu od firmy za to, że nie ujawnią wszystkich przejętych danych. Chcieli, aby pieniądze trafiły na ich konta do końca roku. Ostatecznie cyberprzestępcy opublikowali 100 GB danych jeszcze przed świętami.

Polityka ®
Bezpieczeństwa

SZKOLENIA
Z OCHRONY DANYCH OSOBOWYCH

SPRAWDŹ OFERTĘ

MASZ PYTANIA?

michal.wolinski@rzetelnagrupa.pl
+48 508 554 285

CHMURA OBLICZENIOWA. KLUCZ DO BEZPIECZNEJ PRZYSZŁOŚCI?

Wiesław Sokół
UNICARD SA

Czy chmura jest bezpieczna? Mimo coraz nowszych rozwiązań technologicznych, wiele firm wciąż ma opory przed przeniesieniem danych poza własne, fizyczne środowisko IT. Postawmy więc na fakty. Przywołując case studies i statystyki rozwieję wątpliwości na temat bezpieczeństwa chmury obliczeniowej.

Czy chmura jest bezpieczna? Mimo coraz to nowszych rozwiązań technologicznych, wiele firm wciąż ma opory przed przeniesieniem danych poza własne, fizyczne środowisko IT.

Postawmy zatem na fakty. Przywołując case studies i statystyki postaram się rozwiać wątpliwości na temat bezpieczeństwa chmury obliczeniowej, na które wpływ mają ochrona dostępu do danych, fizyczne zabezpieczenia, jakość działania chmury czy ochrona pod kątem utraty danych.

POLSKA W NIECHLUBNYCH RANKINGACH

Analiza raportów i badań niestety nie pozostawia złudzeń – zdecydowana większość polskich firm z pewną dozą nieufności podchodzi do technologii chmurowych.

Według statystyk:

- tylko 7% firm w Polsce uważa swoją dojrzałość w chmurze za wysoką (PwC);
- jedynie 38% firm w Polsce wdrożyło chmurę we wszystkich lub większości swojej działalności (PwC);
- wydatki firm na usługi świadczone w modelu chmurowym stanowią aktualnie około 15% budżetów (Chmura obliczeniowa w Polskim e-biznesie, 2023).

Opór przed przeniesieniem poza własne, fizyczne środowisko IT wynika głównie z obaw o powierzenie wrażliwych danych zewnętrznej firmie oraz komplikacje związane z potencjalną zmianą dostawcy usług chmurowych – na takie powody zwróciło uwagę aż 32% badanych z wyżej wymienionego raportu.

Czy słusznie? Jak pokazują **badania**, w niemal 90% przypadków winę za naruszenia bezpieczeństwa chmury ponosi... błąd ludzki, a nie dostawcy chmury.

CORAZ BARDZIEJ WYRAFINOWANE ATAKI

Jak widać, polskie firmy mają spore obawy związane z możliwością przedostania się ich prywatnych danych w niepowołane ręce. Jednak niestety często nie idzie to w parze z należytą dbałością o cyberochronę.

Kilka tygodni temu głośno zrobiło się na temat ataku ransomware na ogólnopolską sieć ALAB Laboratoria. Hakerzy RA World udostępnili wrażliwe dane medyczne i personalne kilkudziesięciu tysięcy Polaków i Polek. To niestety jednak dopiero przedsmak ich planów – grupa zapowiada, że jeśli nie otrzyma okupu (którego wielkość wynosi rzekomo kilkaset tysięcy dolarów), na swoim blogu udostępni kolejne wrażliwe informacje.

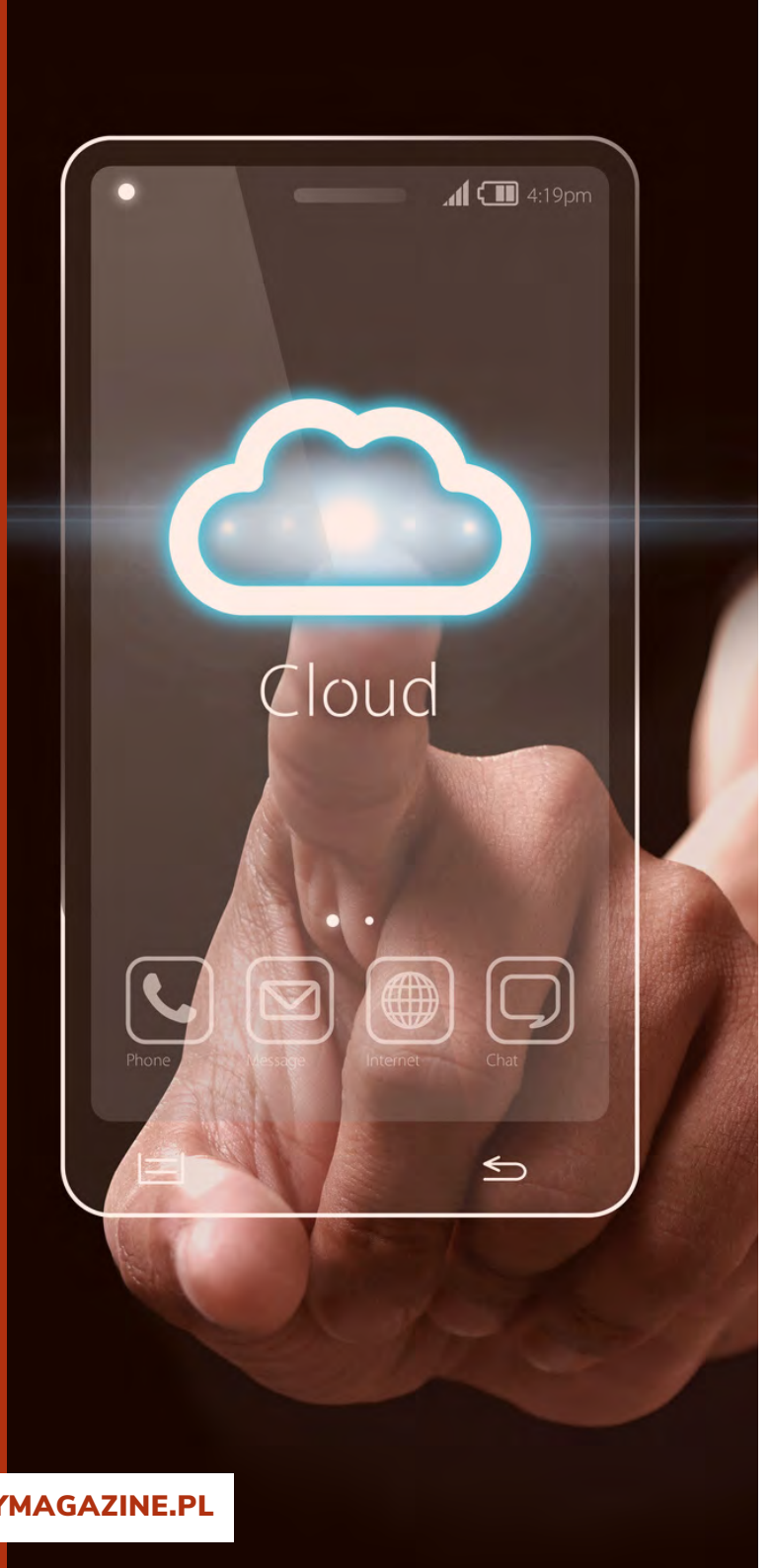
Z kolei pod koniec zeszłego roku światło dzienne ujrzała szokująca informacja – chińska grupa Chimera, niezauważona przez ponad dwa lata, infiltrowała sieć holenderskiego giganta półprzewodników. Naruszenie pozostało niewykryte do końca 2019 roku, tym samym narażając firmę na ogromne straty finansowe oraz wizerunkowe.
Jak widać, ataki cybernetyczne stają się nie tylko coraz bardziej śmiałe, ale niestety też skuteczne.

W ciągu ostatnich lat w Polsce hakerzy byli realnym zagrożeniem dla takich firm jak m.in.:

- Castorama;
- mBank;
- Allegro;
- Orange.

Incydenty dotknęły nawet instytucji rządowych jak Krakowa Rada Komornicza. W 2022 włamano się też na witrynę internetową polskiego Sądu Najwyższego.

Kto ponosi odpowiedzialność za te ataki? Trudno w takiej sytuacji nie oczekiwać od zhakowanych firm, aby z maksymalną uważnością dbały o bezpieczeństwo danych swoich klientów, pracowników, użytkowników czy pacjentów. Jednak, jak wynika z badań przeprowadzonych przez KPMG, w 2022 roku nawet **58% firm w Polsce doświadczyło ataku hakerskiego**. W tym samym roku do CERT Polska zgłoszono aż o 176% więcej ataków w porównaniu z rokiem 2021.



To pokazuje, że cyberataki stały się jednym z największych zagrożeń dla polskiego biznesu, który często nie jest gotowy na to, aby móc się przed nimi chronić.

PKO BANK POLSKI, POLSAT: GIGANCI PRZECIERAJĄ SZLAKI

Na szczęście dobre praktyki w kwestii bezpieczeństwa są coraz częściej wybierane i promowane przez topowe marki. Kilka miesięcy temu największy pod względem aktywów bank w Polsce – PKO Bank Polski – udowodnił swoje zaufanie do publicznej chmury obliczeniowej, przenosząc tam swoje zasoby IT.

Współpraca PKO BP z Chmurą Krajową zaowocowała migracją danych, zapewnieniem wsparcia oraz monitorowania przeniesionego systemu. Dzięki temu bank zaimplementował innowacyjne i efektywne technologie, osiągając wyższy poziom bezpieczeństwa oraz redukując koszty związane z utrzymaniem i modernizacją swojej infrastruktury.

Kluczowe jest, że terminale używane przez personel banku podczas interakcji z klientami służą jedynie jako punkty dostępowe, gdyż wszelkie obliczenia i transakcje odbywają się w chmurze. To upraszcza zarządzanie dużą liczbą sprzętu i obniża koszty zużycia energii elektrycznej. Jednak, co najważniejsze, taka konfiguracja znacząco wzmacnia bezpieczeństwo i ochronę przetwarzanych danych.

Na transformację cyfrową postawiła też Grupa Polsat. Co więcej, wykorzystywane przez nią rozwiązania są zasilane zieloną energią! W ramach współpracy z Polsat, Google podpisze swoją pierwszą w Polsce umowę na zakup czystej, ekologicznej energii elektrycznej.
- *Inwestycje w rozwój czystych, odnawialnych źródeł energii to praktyczna realizacja naszej strategii ESG* – mówi **Piotr Żak, wiceprzewodniczący Rady Nadzorczej Grupy Polsat Plus**.

Swoje usługi na chmurze opierają też takie marki jak Netflix, Airbnb, Spotify, Twitter, a nawet zaawansowane systemy bezpieczeństwa jak kontrola dostępu **impero 360**, przechowywana na Microsoft Azure, z którego korzysta aż 95% firm z listy Fortune 500, m.in. Audi czy Bosch.

Podjęcie decyzji o przejściu "do chmury" być może wielu polskich firmom ułatwi niedawne posunięcie Microsoftu, który kilka miesięcy temu otworzył pierwsze w Polsce (a nawet Europie Środkowo-Wschodniej) centrum przetwarzania danych w chmurze. To aż trzy niezależne lokalizacje w rejonie Warszawy, a każda z nich zawiera jedno lub więcej centrów danych. Co więcej, wszystkie lokalizacje zapewniają najwyższą jakość w kwestii prywatności, bezpieczeństwa oraz przechowywania danych zgodnie z obowiązującymi w Polsce przepisami.

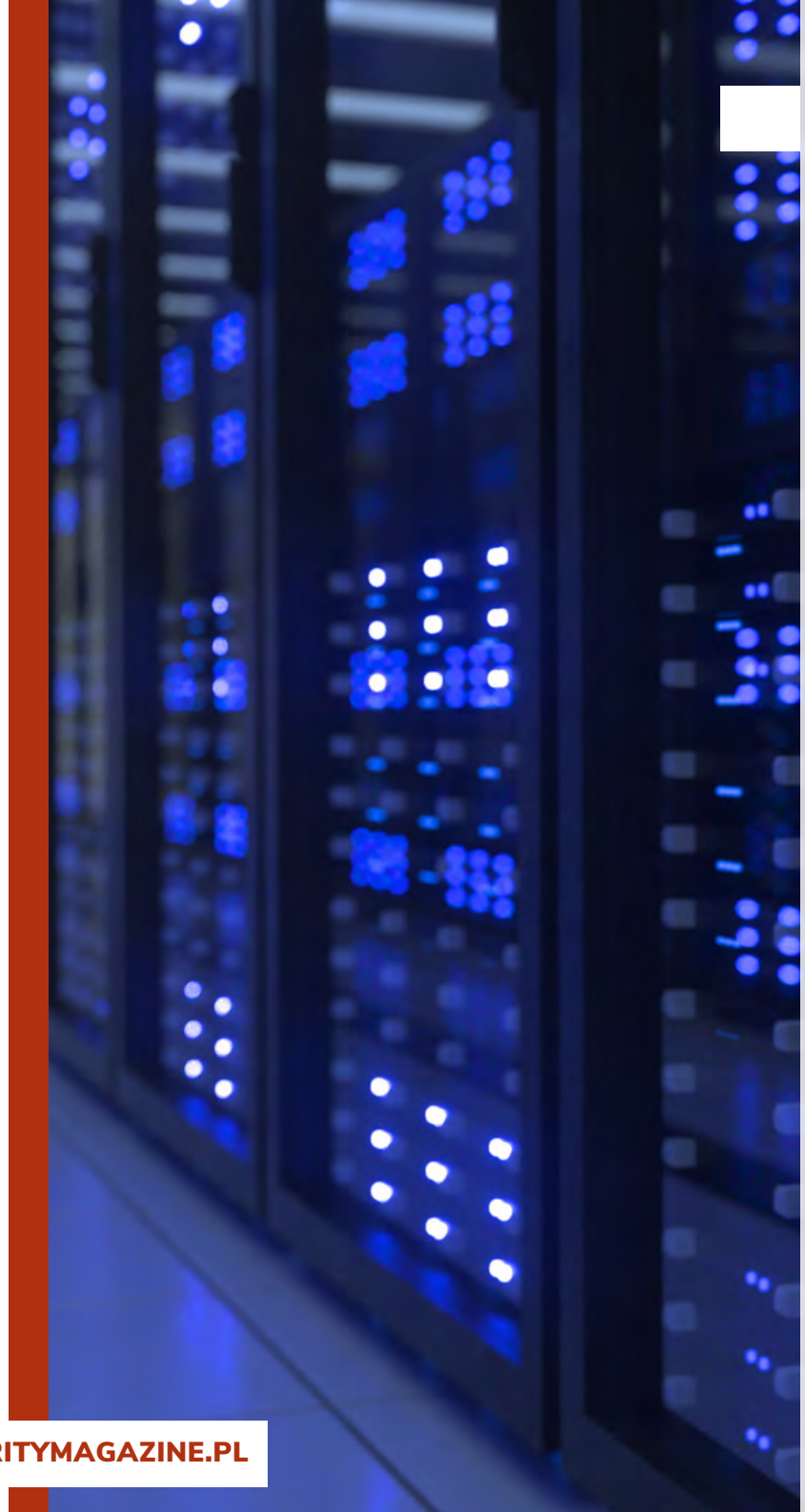
DYREKTYWA NIS2 ZMIENI WSZYSTKO?

Dyrektywa NIS2 (Network and Information Systems Directive 2) to aktualizacja unijnej regulacji z 2016 roku mającej na celu zwiększenie poziomu cyberbezpieczeństwa w Unii Europejskiej.

NIS2 rozszerza zakres obowiązków dla dostawców kluczowych usług i firm cyfrowych, w tym firm chmurowych, platform cyfrowych i dostawców usług internetowych. Zmierza do:

- ujednolicenia standardów bezpieczeństwa na poziomie europejskim,
- wprowadzenia rygorystycznych wymogów w zakresie zarządzania ryzykiem i zgłaszania incydentów,
- zwiększenia odpowiedzialności i przejrzystości działań firm w kontekście cyberbezpieczeństwa.

Dyrektywa nie wymusza bezpośrednio stosowania rozwiązań chmurowych.



Jej głównym celem jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych, wykorzystywanych przez podmioty kluczowe dla gospodarki i społeczeństwa. Oznacza to, że organizacje muszą stosować odpowiednie środki bezpieczeństwa, ale sposób ich wdrożenia zależy od indywidualnej oceny ryzyka i specyfiki danej organizacji.

Jednakże, w praktyce, wiele organizacji może uznać, że wykorzystanie rozwiązań chmurowych od renomowanych dostawców może pomóc w spełnieniu wymogów bezpieczeństwa określonych w dyrektywie NIS2. Chmury obliczeniowe często oferują zaawansowane narzędzia bezpieczeństwa, które mogą być trudne lub kosztowne do zaimplementowania we własnej infrastrukturze.

ZATEM... CZY CHMURA JEST BEZPIECZNA?

Wróćmy jednak do kluczowego pytania o bezpieczeństwo chmury obliczeniowej.
Po wielu latach pracy ze środowiskiem Microsoft Azure – w tym jako dostawca rozwiązania opartego o tę technologię – mogę śmiało wyrazić swoje zaufanie do chmury. Wynika ono nie tylko z zaawansowanych, wielowarstwowych zabezpieczeń, stałego backupu danych oraz redundacji środowiska, ale też faktu, że rozwiązanie jest ciągłe monitorowanie przez setki specjalistów Microsoftu.

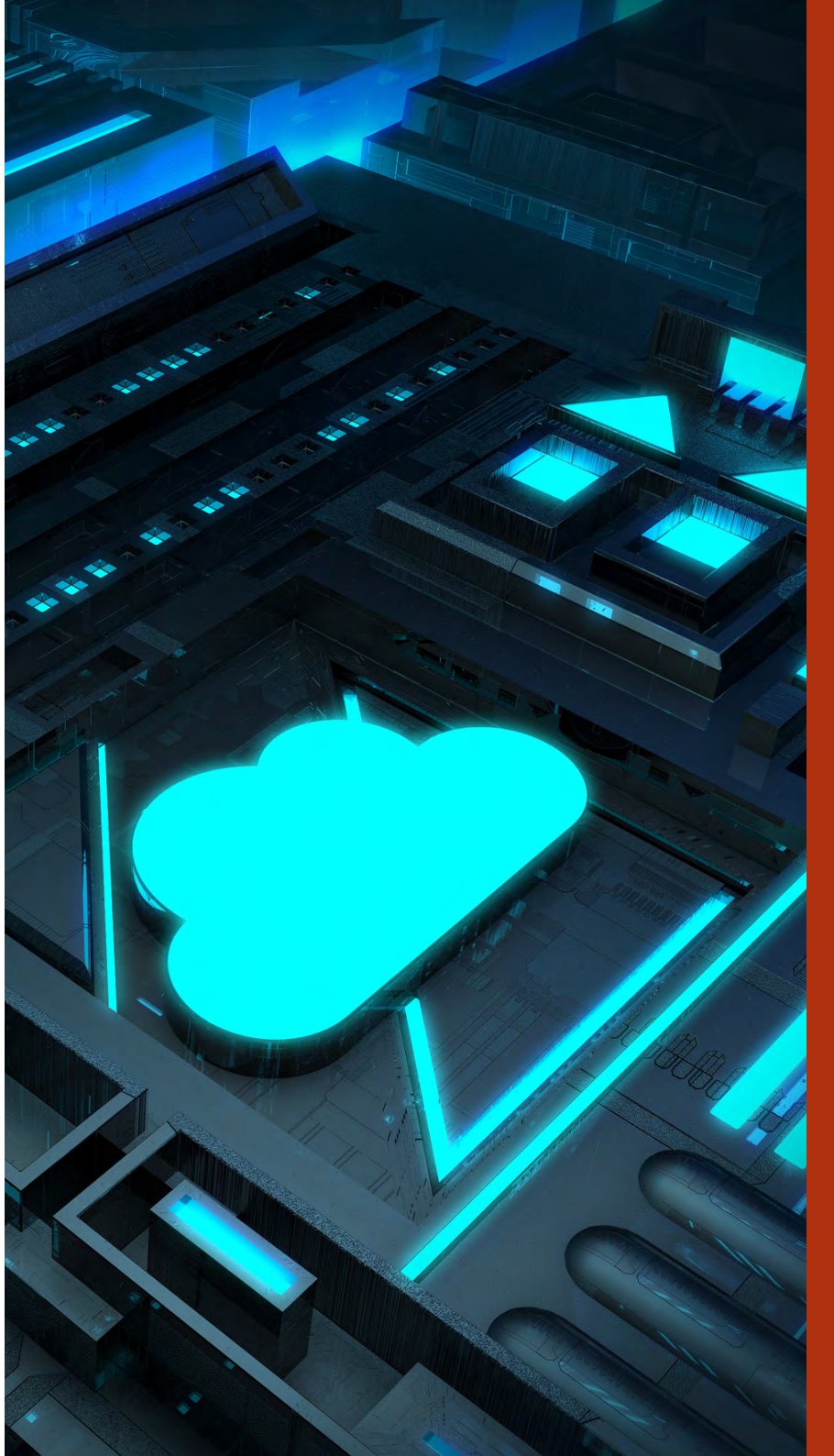
Nie można też pominąć dodatkowych zalet, jak:

- **ekologia** – chmura dynamicznie dzieli zasoby pomiędzy aplikacje, co powoduje maksymalne wykorzystanie zasobów. Dostawcy chmury dbają też o to, aby jak najwięcej zużywanej energii elektrycznej pochodziło ze źródeł odnawialnych. Pozwala to m.in. na obniżenie śladu węglowego.

Wybierając chmurę, dołączamy do grona firm, które kreują przyszłość kolejnego pokolenia oraz promują świadomość ekologiczną;

- **elastyczność** – klient nie ponosi nakładów na zakup infrastruktury i w każdej chwili może ograniczyć lub zrezygnować z części rozwiązania;
- **zawsze aktualna wersja oprogramowania** – użytkownicy chmury nie muszą dbać o aktualizację oprogramowania systemowego i aplikacji oraz nie ponoszą kosztów takiej usługi;
- **zgodność z przepisami prawa** – zmiany prawa mogą wymuszać zmiany w aplikacji. W przypadku chmury to producent zawsze odpowiada za tę kwestię;
- **bezpieczna kopia danych** – korzystając z chmury nie trzeba się martwić, że dane zostaną utracone lub backup się nie uda;
- **stały dostęp do zasobów i wydajność** – środowisko chmurowe jest w pełni wydajne bez względu na to, ile osób na nim pracuje.

Jak wynika z raportu Cybersecurity Insiders z 2023 roku o bezpieczeństwie chmury, inne czynniki, które skłaniają do rozważenia rozwiązań opartych na chmurze, obejmują zwiększoną skalowalność (54% respondentów), przyspieszony czas wdrożenia (52%) oraz oszczędność kosztów (41%).



Warto też pamiętać, że we wielu przypadkach na poziom bezpieczeństwa środowiska chmurowego ogromny wpływ ma sam użytkownik. Błędna konfiguracja czy niedostateczna ochrona danych uwierzytelniających mogą sprawić, że rozwiązanie będzie podatne na złośliwe działania lub incydenty czy naruszenia nie zostaną wykryte odpowiednio szybko.

Jednak najnowsze technologie w kwestii bezpieczeństwa, nowe oficjalne dyrektywy, a przede wszystkim – decyzje topowych firm, jak wspomniany PKO Bank Polski – pokazują, że rewolucja w stronę chmury jest nieunikniona. Im szybciej firmy zdecydują się na ten krok, tym lepiej dla środowiska i nich samych.

Polityka® Bezpieczeństwa

ZAMÓW
AUDYT BEZPIECZEŃSTWA
I PRZEKONAJ SIĘ, JAK MOŻEMY WZMOCNIĆ OCHRONĘ TWOICH DANYCH I SYSTEMÓW. NIE RYZYKUJ

POZNAJ SZCZEGÓŁY

POROZMAWIAJMY

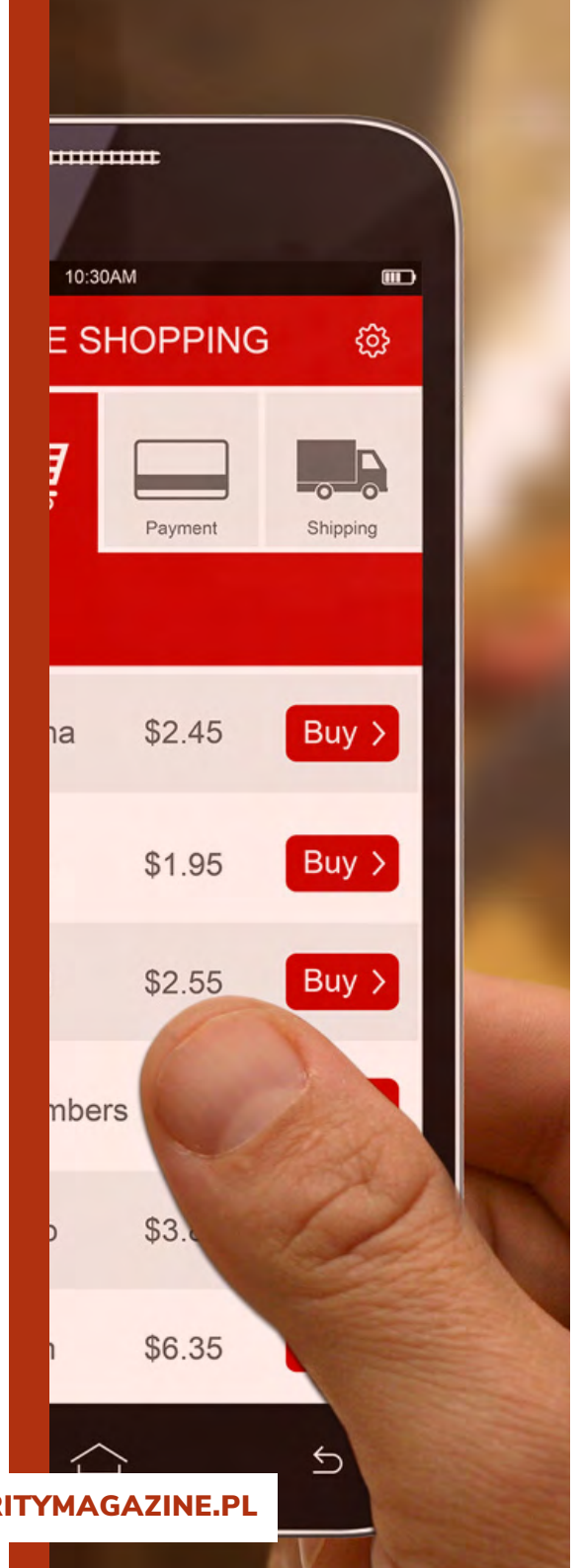
agnieszka.zboralska@rzetelnagrupa.pl
+48 506 947 431

ZABEZPIECZANIE FIRMOWYCH APLIKACJI I PLATFORM E-COMMERCE PRZED CYBERATAKAMI

Redakcja
SECURITY MAGAZINE

Bezpieczeństwo, szczególnie danych i transakcji, to podstawa w e-handlu. Brak zabezpieczeń to ryzyko nie tylko utraty reputacji wśród klientów, ale także pieniędzy. Jak zatem chronić swoje aplikacje i platformy e-commerce przed cyberatakami?

Zabezpieczanie firmowych aplikacji i platform e-commerce przed cyberatakami



PODSTAWA NOWOCZESNEGO BIZNESU

Dziś handel elektroniczny stał się podstawą nowoczesnego biznesu, zapewniając komfort zarówno firmom, jak i konsumentom. Jednak wraz ze wzrostem liczby transakcji internetowych, rośnie potrzeba lepszej i skuteczniejszej ochrony platform e-commerce oraz aplikacji, dzięki którym można robić e-zakupy.

Dowodem na to niech będą, chociażby amerykańskie badania z 2021 roku, które potwierdzają, że konsumenci na całym świecie przywiązują dużą wagę do bezpieczeństwa podczas zakupów online. W szczególności w Stanach Zjednoczonych, Meksyku i Australii, gdzie około dziewięciu na dziesięciu respondentów uważało, że bezpieczeństwo ma kluczowe znaczenie podczas dokonywania zakupów online. Co więcej, respondenci uważają, że nawet mały błąd związany z bezpieczeństwem danych i trakcji jest dla nich równoważny z utratą zaufania na długie lata.

KONIECZNOŚĆ PRZESTRZEGANIA STANDARDÓW

Ale niechęć klientów to niejedyna konsekwencja takiego błędu. Firma, która zajmuje się e-handlem, zobligowana jest także do przestrzegania standardów, takich jak Ogólne Rozporządzenie o Ochronie Danych (RODO) oraz Standard Bezpieczeństwa Danych Branży Kart Płatniczych (PCI DSS), które zapewniają, że dane klientów są traktowane z najwyższą starannością. Nieprzestrzeganie przepisów grozi nie tylko zniechęceniem klientów, ale także konsekwencjami prawnymi i wysokimi karami finansowymi. Dlatego firmy, które zajmują się e-handlem, muszą dokładać wszelkich starań, aby chronić swoje platformy i aplikację przed cyberatakami.

Jak więc to robić skutecznie? Na początku warto rozważyć wdrożenie szyf-

rowania Secure Socket Layer (SSL) wraz z wymuszaniem odpowiedniej wersji Transport Layer Security (TLS). Protokoły te szyfrują dane pomiędzy przeglądarką użytkownika a serwerem internetowym, zapewniając, że wszelkie przesyłane dane, takie jak numery kart kredytowych lub dane osobowe, pozostaną poufne. Dla konsumentów znakiem rozpoznawczym szyfrowania, jest kłódka, która pojawia się w pasku przeglądarki. Ta mała ikonka sprawia, że przekazując swoje dane, użytkownik czuje się bezpieczniej, co przekłada się na częstsze zakupy. Dodatkowo większość przeglądarek będzie ostrzegać użytkownika w przypadku połączeń nieszyfrowanych SSL, co w przypadku zakupów online równa się niemal z 100% ucieczką klienta z takiej strony internetowej.

Kolejna zasada bezpieczeństwa, o której w firmie warto pamiętać, dotyczy silnych haseł. Tę kwestię powinno się skutecznie egzekwować zarówno od pracowników, jak i od klientów. Wymuszanie wręcz na klientach długich haseł, z wielkimi i małymi literami oraz znakami specjalnymi jest konieczne, ponieważ zmniejsza podatność konta na ataki typu brute-force.

REGULARNE AKTUALIZACJE

Aby dobrze chronić swoje aplikacje i platformy e-commerce, potrzebna jest także regularna aktualizacja oprogramowania. Dlaczego? Bo nieaktualne i złośliwe oprogramowanie to kopalnia złota dla cyberprzestępców. Firmy mogą łatać luki w zabezpieczeniach i unikać potencjalnych prób exploitów, regularnie aktualizując swoje e-platformy, wtyczki i inne oprogramowanie systemowe.

Ciekawą, ale dość kosztowną, opcją na ochronę jest korzystanie z pomocy firm, które specjalizują się w cyberbezpieczeństwie. Zwykle tacy specjaliści oferują testy penetracyjne, oceny podatności i monitorowanie 24 godziny na dobę, 7 dni w tygodniu, w celu szybkiego wykrywania i reagowania na zagrożenia.

Nim skorzystamy z wyrafinowanych narzędzi dających bezpieczeństwo, warto zadbać o podstawy, tj. regularną aktualizację wiedzy pracowników o cyberbezpieczeństwie. Szkolenia najlepszych praktyk, rozpoznawania prób phishingu i utrzymywania integralności danych, to zawsze dobra inwestycja, która realnie wpływa na bezpieczeństwo w firmie.

OCHRONA TRANSAKCJI PŁATNICZYCH

Odpowiednich zabezpieczeń wymagają także transakcje płatnicze w sklepach internetowych. Godna zaufania bramka płatnicza jest niezbędna do zapewnienia płynnych transakcji i ochrony wrażliwych informacji finansowych przed potencjalnymi zagrożeniami. Gdy klienci podają dane swojej karty kredytowej, ufają, że platforma e-commerce będzie obchodzić się z ich danymi w sposób odpowiedzialny.

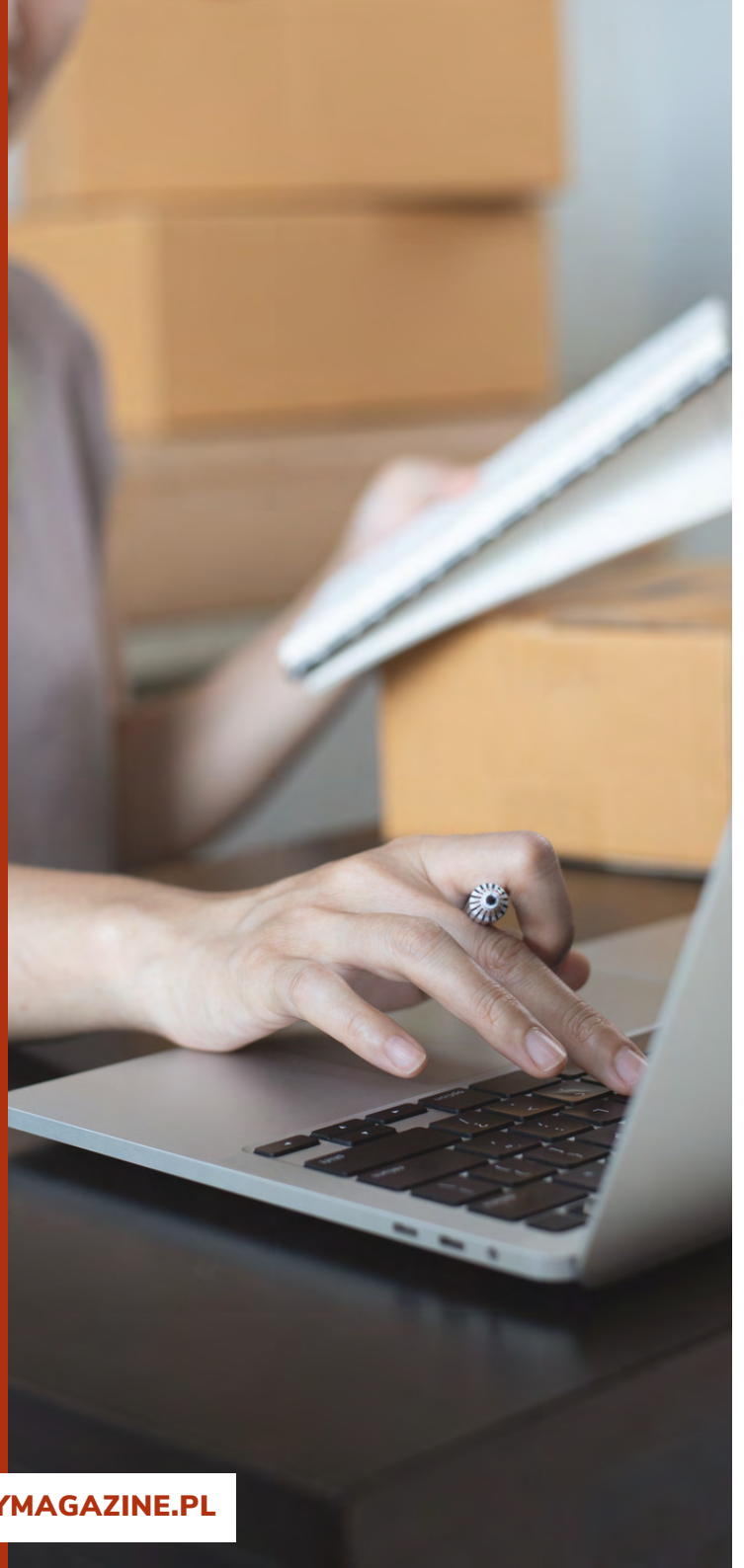
Aby pod tym względem zapewnić bezpieczeństwo aplikacjom oraz platformom e-commerce, należy stosować tzw. standard bezpieczeństwa danych kart płatniczych (PCI DSS), czyli zestaw rygorystycznych standardów bezpieczeństwa opracowanych w celu zapewnienia, że wszystkie firmy akceptujące, przetwarzające, przechowujące lub przesyłające informacje o kartach kredytowych zachowują bezpieczne środowisko. Przestrzeganie tych standardów gwarantuje klientom, że dane ich kart kredytowych są przetwarzane z zachowaniem najwyższych standardów bezpieczeństwa, minimalizując ryzyko naruszeń.

Kolejną opcją na ochronę jest tzw. tokenizacja danych kart płatniczych. Ta nowoczesna funkcjonalność pomaga chronić numer karty i jej datę ważności, zastępując te informacje danymi niewrażliwymi w postaci unikalnego ciągu cyfr, jakim jest tzw. token, który w przypadku naruszenia nie ma żadnego wartościowego znaczenia.

JAK JESZCZE MOŻNA ZABEZPIECZYĆ SWOJE PLATFORMY I APLIKACJĘ?

Dobrą ochronę zapewniają także:

- **regularne audyty bezpieczeństwa** są niezbędne w przypadku platform e-handlu. Audyty te identyfikują luki w systemie, czy to w oprogramowaniu, infrastrukturze, czy w punktach dostępu użytkownika. Zajmując się tymi problemami proaktywnie, firmy mogą zapobiec potencjalnym naruszeniom.
- **uwierzytelnianie dwuskładnikowe,** które wymusza na użytkowniku drugą formę identyfika-



cji, często w postaci jednorazowego kodu wysyłanego na zarejestrowany numer telefonu lub adres e-mail. To sprawia, że nieautoryzowany dostęp jest znacznie trudniejszy.

- **należyta staranność w sprawdzaniu dostawcy**. Firmy zajmujące się handlem elektronicznym często integrują usługi stron trzecich w celu przetwarzania płatności, zarządzania relacjami z klientami lub śledzenia stanów magazynowych. Konieczne jest dokładne sprawdzenie tych dostawców i upewnienie się, że przestrzegają rygorystycznych protokołów bezpieczeństwa. W końcu łańcuch jest tak mocny, jak jego najsłabsze ogniwo.
- **stosowanie protokołu HTTPS.** „S” w HTTPS oznacza, że dane przesyłane między serwerem internetowym a przeglądarką są szyfrowane. Szczególnie istotny w przypadku stron realizacji transakcji, protokół HTTPS jest obecnie uważany za podstawowy standard na każdej platformie e-commerce.
- **regularne tworzenie kopii zapasowych** gwarantuje, że w przypadku utraty danych lub ataku oprogramowania ransomware firmy będą mogły przywrócić swoje systemy do ostatniego stanu bez znaczącej utraty danych lub przestojów.
- **zapora aplikacji internetowej (WAF)** działa jak tarcza między serwerem witryny internetowej a połączeniem danych, odfiltrowując złośliwe boty i próby hakerów, chroniąc w ten sposób platformę przed zagrożeniami.
- pamiętaj, że **tylko niektórzy pracownicy potrzebują dostępu do wszystkich części systemu**. Firmy mogą minima-

lizować ryzyko związane z zagrożeniami wewnętrznymi lub przeoczeniami, przyznając prawa dostępu na podstawie ról i okresowo przeglądając te uprawnienia.

Wdrożenie tych najlepszych praktyk tworzy kompleksową osłonę przed większością zagrożeń, wzmacniając cyfrowe operacje firmy w celu ochrony danych klientów i zwiększając zaufanie klientów do marki.

BEZPIECZEŃSTWO JEST NAJWAŻNIEJSZE!

Cyberprzestępcy nie śpią. Przeglądając interenet, co chwilę można trafić na informację, że doszło do wycieku danych lub kradzieży potężnych sum pieniędzy. Dlatego przy prowadzeniu biznesu, zwłaszcza takiego, jak e-commerce, dobre zabezpieczenia to podstawa.

O kompleksową ochronę swoich aplikacji oraz platform sprzedażowych należy w szczególności zadbać w okresach wzmożonych zakupów, np. podczas noworocznych wyprzedaży. Duża liczba zamówień, zmęczenie, walka z czasem, aby terminowo zrealizować zamówienie, roztargnienie osłabiają naszą czujność, co w konsekwencji sprawia, że stajemy się łatwym celem cyberprzestępców. Niestety, ale ataki w tych najbardziej gorących okresach bolą najbardziej, ponieważ wtedy straty są największe.

Rzetelny Regulamin®

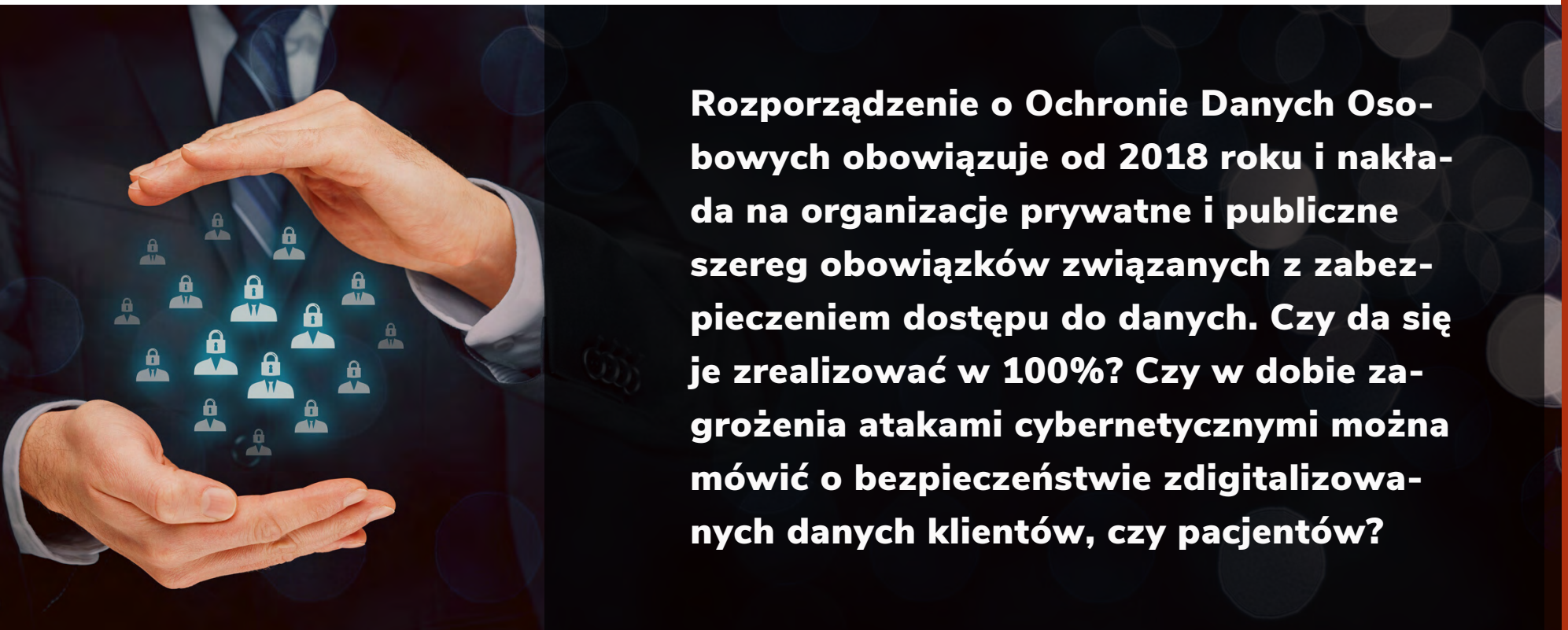
POZNAJ SZCZEGÓŁY

anna.wesolowska@rzetelnagrupa.pl
+48 501 291 432

Kompleksowa obsługa prawna Twojego e-commerce

JAK ZABEZPIECZYĆ DANE OSOBOWE ZGODNIE Z RODO?

Łukasz Zajdel
Perceptus Sp z o. o.



Rozporządzenie o Ochronie Danych Osobowych obowiązuje od 2018 roku i nakłada na organizacje prywatne i publiczne szereg obowiązków związanych z zabezpieczeniem dostępu do danych. Czy da się je zrealizować w 100%? Czy w dobie zagrożenia atakami cybernetycznymi można mówić o bezpieczeństwie zdigitalizowanych danych klientów, czy pacjentów?

RODO to nie tylko ochrona gromadzonych danych, zarządzanie nimi, ale też zabezpieczenie przed ich utratą. Istnieją narzędzia, które mogą ułatwić właściwe przygotowanie tych procesów.

OPROGRAMOWANIE DO ZARZĄDZANIA DANYMI W ORGANIZACJI

Myśląc o skutecznej ochronie danych gromadzonych przez organizację, także danych osobowych, warto poznać dwa systemy ukryte pod skrótami DLP i PAM.

DLP to oprogramowanie Data Loss Prevention, czyli technologia przeznaczona do monitorowania i zarządzania danymi, w celu zapobiegania ich nieautoryzowanemu ujawnieniu. Została ona zaprojektowana w celu zapobiegania utracie, wyciekowi lub nieautoryzowanemu dostępowi do danych. Działa poprzez monitorowanie, wykrywanie i blokowanie potencjalnych incydentów związanych z przesyłaniem danych, w oparciu o ich rodzaj.

PAM z kolei pozwala na Privileged Access Management, czyli zarządzanie dostępem do określonych obszarów infrastruktury IT, w tym baz danych, czy systemów. Dzięki temu systemowi można wybrać, które dane są w zasięgu pracowników określonych szczebli, działów, stanowisk.

JAK OPROGRAMOWANIE DLP ORAZ PAM WSPIERAJĄ ZARZĄDZANIE DANYMI W ORGANIZACJI ZGODNIE Z RODO?

Rozwiązania DLP odgrywają kluczową rolę w pomaganiu organizacjom w spełnianiu wymogów dotyczących ochrony danych. Pomagają firmom w identyfikacji i klasyfikacji informacji przechowywanych w ich zasobach. Dzięki temu odpowiednie struktury w organizacji mogą łatwiej zarządzać tymi danymi i dbać o ich odpowiednie zabezpieczenie.

Pozwalają też na monitoring ruchu w sieci. Oprogramowanie DLP wykorzystuje zaawansowaną technologię i dzięki temu może zablokować transmisję danych osobowych, które nie są autoryzowane do przesyłania poza organizację (Data leak prevention). Jest to zaawansowana ochrona przed wyciekami informacji. Oprogramowanie DLP pomaga też w szyfrowaniu danych, zapewniając, że są one chronione przed nieautoryzowanym dostępem. Wspiera wykrywanie i blokuje próby dostępu do danych przez nieautoryzowane osoby czy

systemy.

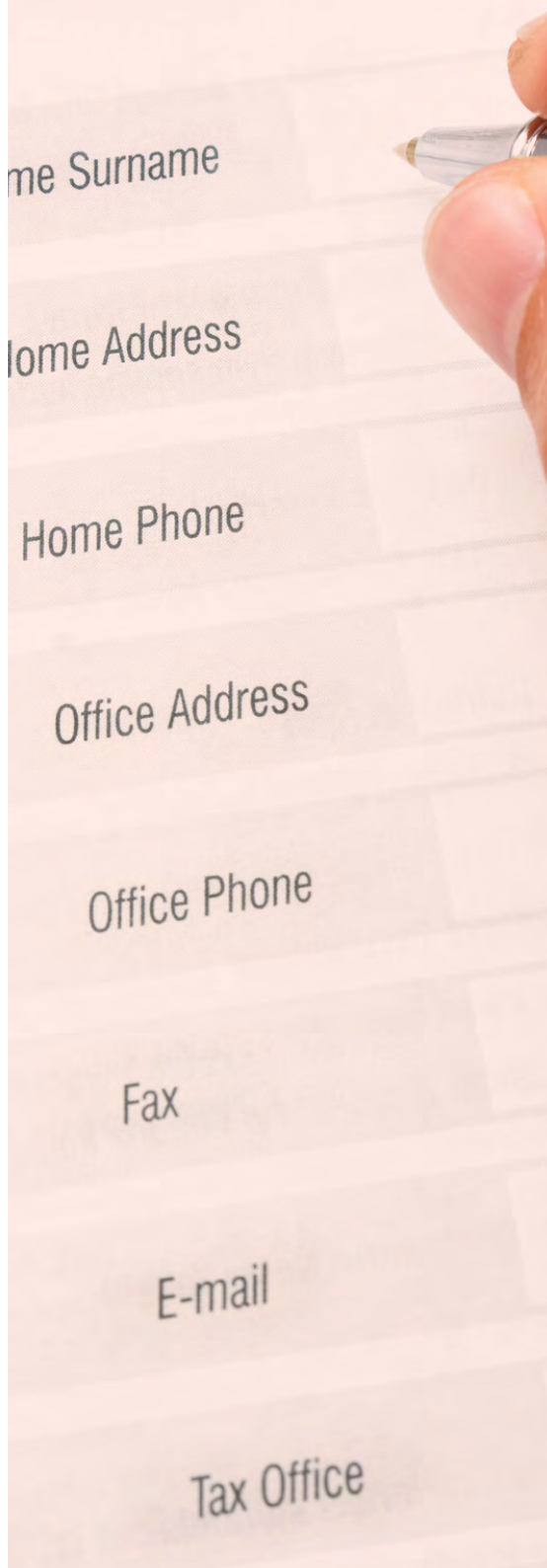
Jedną z zasad wprowadzonych przez RODO jest zbieranie minimalnej ilości danych, niezbędnych do danego celu, aby firmy przechowywały jedynie te dane, które są niezbędne do celów, dla których zostały zebrane. Oprogramowanie DLP może pomóc organizacjom w monitorowaniu i usuwaniu zbędnych danych.

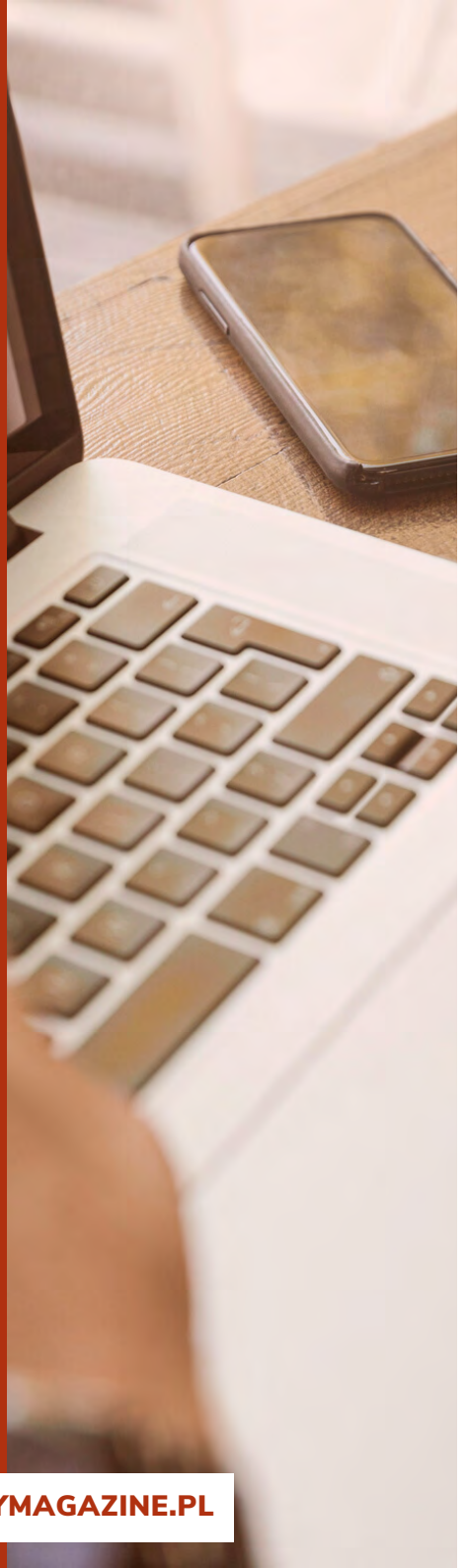
PAM z kolei umożliwia ustalenie ścisłych zasad ograniczenia fizycznego dostępu do danych, co stanowi ich najlepsze zabezpieczenie przed użytkownikami, którzy nie powinni ich poznać. Pozwala na zdefiniowanie wielopoziomowych autoryzacji, które są potrzebne do uzyskania dostępu do danych osobowych. To oznacza, że nie każdy użytkownik ma automatyczny dostęp do wszystkich danych, co jest zgodne z zasadą minimalizacji danych RODO.
Dodatkowo PAM pozwala na kontrolowanie sesji użytkowników i ich aktywności w czasie rzeczywistym. To umożliwia szybką reakcję na niepożądane zachowania lub próby naruszenia zabezpieczeń.

ZGŁASZANIE NARUSZEŃ, A SYSTEM OCHRONY PRZED WYCIEKIEM DANYCH FIRMOWYCH

Zgłoszenie naruszenia danych osobowych jest wymagane przez Urząd Ochrony Danych Osobowych. Naruszeniem jest zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do tej kategorii informacji, które zaszły w skutek złamania zasad bezpieczeństwa danych. Dokładna procedura zgłaszania takiego naruszenia oraz formularz zgłoszenia znajdują się **POD TYM ADRESEM.**

W przypadku potencjalnego naruszenia danych, zarówno oprogramowanie DLP jak i PAM generują powiadomienia i raporty, które pomagają organizacjom w szybkiej reakcji na incydent oraz w skutecznym raportowaniu do organów nadzorczych. Jest to ważne w kontekście szybkiego powiadamiania o naruszeniach.





POLITYKI OPARTE NA TREŚCI – REGUŁY BLOKUJĄCE UDOSTĘPNIANIE DANYCH OSOBOWYCH

Szczególnie przydatne w kontekście RODO są polityki oparte na treści. Oprogramowanie DLP umożliwia tworzenie złożonych reguł opartych na treści, które reagują na konkretne typy informacji. Na przykład organizacja może ustawić politykę, która blokuje wysyłanie e-maili zawierających numery identyfikacyjne obywateli lub numerów kart kredytowych. Takie funkcje skutecznie pozwalają zadbać o to, by żadne gromadzone dane wrażliwe nie wyciekły z organizacji.

OCHRONA PRZED DOSTĘPEM TO JEDNO - A CO Z UTRATĄ DANYCH?

Ostatnim elementem, który uzupełnia zabezpieczenie danych jest backup, czyli bezpieczna kopia danych, która zabezpiecza ich utratę nawet w sytuacji, kiedy oryginalny nośnik zostanie zaszyfrowany lub fizycznie uszkodzony w efekcie ryzyka losowego (np. pożar) lub celowego działania osób z organizacji lub spoza jej szeregów. Ważne, by kopia danych była przechowywana w odseparowanej lokalizacji. Dzięki temu szansa na zachowanie danych w niezmienionej postaci jest zdecydowanie większa. Bardzo ważne, by backup był wykonywany w systemie migawkowym. Dzięki temu organizacja może przywrócić swoje dane do wcześniejszego stanu, wybierając którą kopię chce przywrócić. „Wracając" do odpowiedniego momentu np. sprzed określonej godziny lub dnia (...w którym potencjalnie nastąpiła infekcja złośliwym oprogramowaniem), w zależności od tego, jak często robimy migawki i jak długo je przechowujemy, może przywrócić kopię czystą od wszelkich infekcji.

Perceptus od 15 lat zabezpiecza dane firm komercyjnych oraz publicznych. Wśród naszych klientów są takie instytucje jak prokuratura, policja, ministerstwa, szpitale i duże organizacje e-commerce. Szukasz partnera, który pomoże Ci w zabezpieczeniu Twoich danych? Porozmawiajmy.

CHCESZ PODZIELIĆ SIĘ WIEDZĄ I DOŚWIADCZENIEM NA ŁAMACH LUTOWEGO WYDANIA “SECURITY MAGAZINE”?

Skontaktuj się z nami

redakcja@securitymagazine.pl

+48 22 390 91 05
+48 518 609 987

Deadline:
wydanie lutowe: do 22.01

SECURITYMAGAZINE.PL

OCHRONA MAILA, CHMURY I EDUKACJA PRACOWNIKÓW W OBSZARZE CYBERBSECURITY

Redakcja
SECURITY MAGAZINE

#SECURITY
#STARTUP

Cyberzagrożenia są coraz powszechniejsze i poważniejsze. Jeśli prowadzisz firmę – musisz dbać o to, aby jak najbardziej minimalizować ryzyko wystąpienia incydentów. Jak jednak zaadresować tak szerokie wyzwanie, jak cyberbezpieczeństwo? Na szczęście z pomocą przychodzą startupy.

ABNORMAL SECURITY – OCHRONA MAILI

Startup Abnormal Security to organizacja oferująca nowoczesne rozwiązania w dziedzinie ochrony e-maili. Platforma spółki oparta na chmurze walczy z zaawansowanymi atakami ukierunkowanymi, chroniąc organizacje korzystające z programów takich jak Office 365, G-Suite, Outlook, Mi'crosoft Teams, Gmail, Slack czy Zoom.

Jedną z najważniejszych funkcji platformy jest wykrywanie włamań na konta e-mail oraz blokowanie ataków phishingowych i złośliwych wiadomości. Abnormal Security wykorzystuje sztuczną inteligencję, aby analizować zachowanie użytkowników i wykrywać potencjalne zagrożenia, co pozwala szybko reagować na incydenty. Mowa tutaj o tzw. analizie behawioralnej.

Rozwiązanie to wspomaga ochronę we wcześniej wspomnianych programach, ulepszając już istniejące opcje zabezpieczeń. Dzięki temu jest to dodatkowa warstwa ochrony przed zaawansowanymi cyberatakami na twoją organizację.

Co więcej – dodatkowym aspektem jest również blokowanie szerokiego spektrum ataków. Od socjotechnik po ataki generowane przez narzędzia AI. Platforma Abnormal Security skupia się na wykrywaniu i zatrzymywaniu różnorodnych zagrożeń, zapewniając tym samym kompleksową ochronę.

Mowa tutaj o takich zagrożeniach jak ataki typu BEC, ataki związane z oszustwami finansowymi, czy próby przejęcia kont e-mailowych w celu rozprowadzania złośliwego oprogramowania.

Krótko mówiąc – Abnormal Security oferuje rozwiązania, które idą znacznie dalej niż standardowe opcje cyberbezpieczeństwa. Ich platforma skupia się na wykrywaniu, blokowaniu i reagowaniu na zaawansowane zagrożenia, zapewniając organizacjom bezpieczne środowisko pracy w dobie coraz bardziej wyrafinowanych cyberataków.

LACEWORK – AUTOMATYZACJA BEZPIECZEŃSTWA CHMURY

W ostatnich latach usługi chmurowe są ważnym miejscem działalności dla wielu firm, oferując zaawansowane rozwiązania i skalowalność. Jednak jak to bywa ze wszystkim, co popularne – pojawiło się tu dużo zagrożeń.

Odpowiedzią na nie jest Lacework – startup sku-

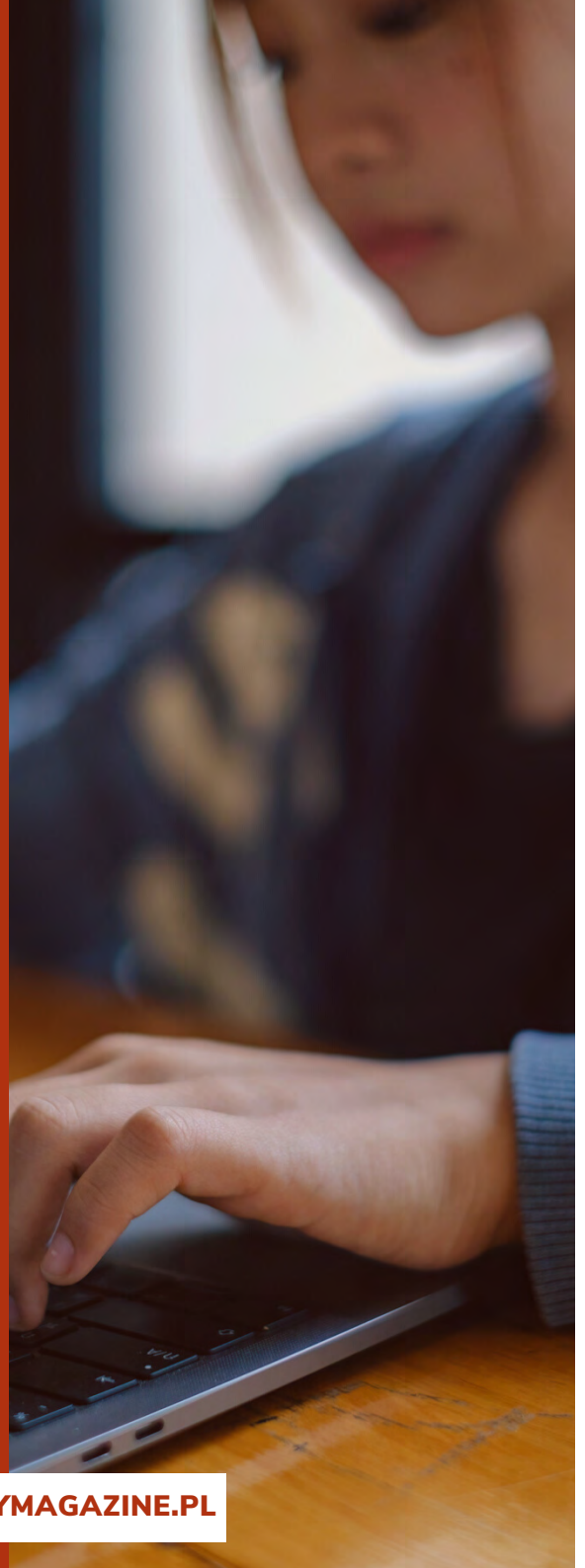
piający się na automatyzacji bezpieczeństwa w chmurze. Ich platforma oferuje ocenę konfiguracji, wykrywanie zagrożeń oraz zapewniania zgodności w środowiskach wielochmurowych. Co więcej – startup dostarcza też rozwiązania w zakresie monitorowania zachowań, wykrywania anomalii czy wykrywania włamań do hosta w różnych platformach chmurowych.

Jednym z istotnych atutów Lacework jest jej wszechstronność – oprogramowanie to integruje się z różnymi środowiskami, w tym z AWS, Azure, Google Cloud i Kubernetes.

Platforma Lacework wyróżnia się automatyzacją w zakresie każdego aspektu cyberbezpieczeństwa, co obejmuje nie tylko ocenę konfiguracji czy monitorowanie zachowań, lecz także wykrywanie zagrożeń, badanie incydentów oraz zapewnienie ciągłego monitorowania wszystkich komponentów chmury.

Dodatkowo oprogramowanie to pomaga w wykrywaniu zagrożeń, wyszukiwaniu podejrzanych komunikatów i zapewnieniu bezpieczeństwa w szerokim spektrum różnorodnych środowisk chmurowych.

Lacework wydaje się obiecującym rozwiązaniem. Pozwala firmom na rozwijanie swojego biznesu w sposób bezpieczny i efektywny. Najważniejszym aspektem okazuje się automatyzacja i zapewnienia ciągłego cyberbezpieczeństwa w środowisku chmurowym. Co stanowi istotną wartość dla coraz większej liczby przedsiębiorstw decydujących się na usługi chmurowe.



HOXHUNT – PLATFORMA E-LEARNINGOWA DLA PRACOWNIKÓW

Najsłabszym ogniwem w kontekście cyberbezpieczeństwa zawsze jest człowiek. W końcu to ataki socjotechniczne stanowią największą część wszystkich incydentów cyfrowych. Dlatego tak ważne jest dbanie o odpowiednią edukację pracowników.

I tu pojawia się HoxHunt, startup oferujący platformę zwiększającą świadomość w zakresie zagrożeń cyfrowych. Podejście organizacji skupia się na podnoszeniu świadomości pracowników poprzez symulowanie różnorodnych ataków jak phishing czy spear phishing oraz nagradzanie za zgłaszanie potencjalnych problemów związanych z bezpieczeństwem.

Platforma HoxHunt wykorzystuje sztuczną inteligencję, naukę behawioralną i zaawansowaną automatyzację, aby kompleksowo zarządzać ryzykiem ludzkim. Jej głównym celem jest wykształcenie wzorca zachowań pracowników w obszarze cyberbezpieczeństwa, co przyczynia się do zwiększenia możliwości ochrony, wykrywania i reagowania na zagrożenia, minimalizując tym samym ryzyko.

Platforma ta skutecznie symuluje ataki, które są dostosowane do języka, roli i lokalizacji użytkowników. Dzięki temu są one bardziej realistyczne i skuteczne w podnoszeniu świadomości. Symulacje te są oparte na aktualnych informacjach o zagrożeniach, co umożliwia użytkownikom nauczenie się rozpoznawania i reagowania na potencjalne incydenty.

Startup chwali się, że ich rozwiązanie pomaga ograniczyć skuteczne ataki phishingowe o 70%.

Dodatkowo, platforma umożliwia reakcję na rzeczywiste ataki. Grupuje zduplikowane raporty w pojedyncze zdarzenia, przyspieszając tym samym reakcję na zagrożenia oraz eliminację potencjalnych incydentów.

W kontekście współczesnego środowiska biznesowego, gdzie bezpieczeństwo danych jest priorytetem, podejście HoxHunt jest zdecydowanie skuteczne. Skupienie na zmianie zachowań pracowników i edukacji w zakresie cyberbezpieczeństwa stanowi istotny krok w kierunku bardziej świadomej i bezpiecznej pracy w środowisku online.

To przykłady tylko niektórych spółek technologicznych, które dostarczają rozwiązań z zakresu cyberbezpieczeństwa. Grunt to dostosować rozwiązanie do swoich potrzeb i możliwości finansowych. Jednak jak pokazują liczne przykłady – na bezpieczeństwie (w tym cyberbezpieczeństwie) naprawdę nie warto oszczędzać.

WYRÓŻNIJ SIĘ W BRANŻY BEZPIECZEŃSTWA

- **Publikuj artykuły sponsorowane w "Security Magazine", prezentując swoje produkty lub usługi tysiącom czytelników**
- **Buduj zaufanie wśród potencjalnych klientów**
- **Wzmacniaj pozycję swojej marki w branży**

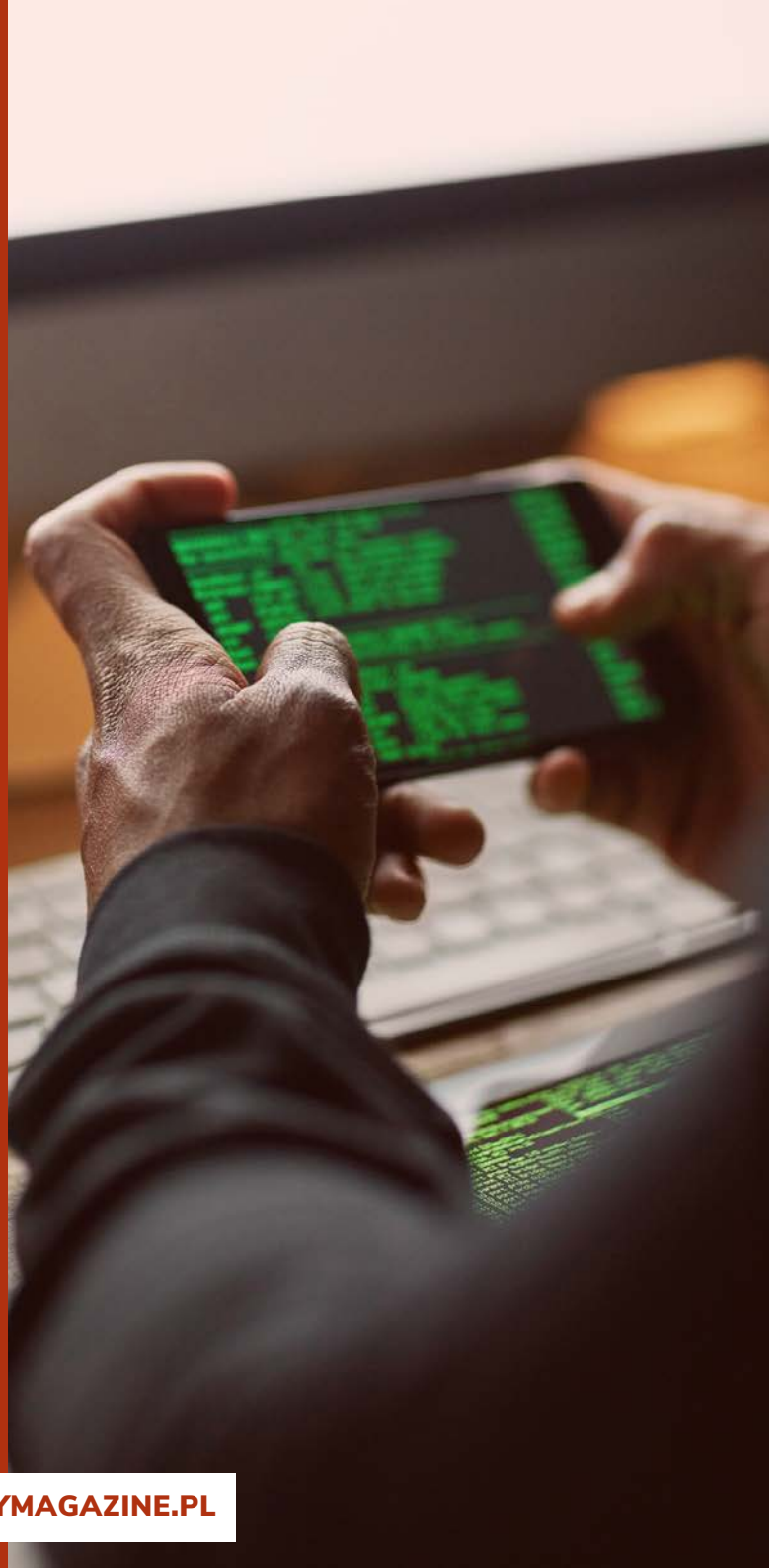
redakcja@securitymagazine.pl
+48 518 609 987

www.securitymagazine.pl

JAK NIS 2 KSZTAŁTUJE PRZYSZŁOŚĆ CYBERBEZPIECZEŃSTWA W ORGANIZACJACH

Oleksii Doroshenko
Redsaber Security

Dyrektywa NIS 2 (Network and Information Systems Directive 2) jest istotnym elementem wzmocnienia cyberbezpieczeństwa w Unii Europejskiej. Uaktualnienie poprzedniej dyrektywy NIS odpowiada na rosnące potrzeby ochrony kluczowych infrastruktur i usług cyfrowych przed coraz bardziej wyrafinowanymi atakami.



WAŻNE ZMIANY W DYREKTYWIE NIS 2

Dyrektywa NIS 2, jako ewolucja poprzedniej dyrektywy NIS, wprowadza znaczące zmiany mające na celu wzmocnienie cyberbezpieczeństwa w Unii Europejskiej. Te zmiany uwzględniają doświadczenia i wyzwania napotkane podczas implementacji NIS 1, a także dynamiczny rozwój technologii i zagrożeń cyfrowych.

Ważnym aspektem nowej dyrektywy jest rozszerzenie zakresu sektorów objętych regulacją, obejmujące teraz nowe obszary krytyczne dla gospodarki i społeczeństwa, w tym usługi pocztowe i kurierskie. To rozszerzenie odpowiada na rosnące znaczenie komunikacji cyfrowej i logistyki w codziennym życiu, podkreślając potrzebę większej ochrony w tych sektorach.

NIS 2 wprowadza bardziej rygorystyczne wymogi dotyczące raportowania incydentów, zwiększając odpowiedzialność organizacji. Organizacje teraz muszą poinformować odpowiednie organy w ciągu 24 godzin od wykrycia incydentu. Wymaga to od firm wdrożenia bardziej zaawansowanych systemów do wykrywania i reagowania na incydenty, co ma na celu szybsze identyfikowanie i minimalizowanie potencjalnych szkód. Dyrektywa stawia także nacisk na bezpieczeństwo łańcucha dostaw, wymagając od organizacji dokładnej analizy i zarządzania ryzykiem związanym z dostawcami usług teleinformatycznych. Wymusza to nie tylko ocenę obecnych dostawców, ale również wdrażanie nowych wymogów cyberbezpieczeństwa w umowach.

W odpowiedzi na ograniczoną skuteczność kar finansowych w poprzedniej dyrektywie, NIS 2 znacząco zwiększa wysokość kar za naruszenia, które mogą sięgać do 10 milionów euro lub 2% całkowitego rocznego obrotu dla podmiotów kluczowych. Podkreśla to powagę, z jaką Unia Europejska traktuje zagadnienia cyberbezpieczeństwa. Dodatkowo, dyrektywa wprowadza pojęcie "poważnych incydentów", które obejmuje zarówno zakłócenia operacyjne, jak i potencjalne straty finansowe oraz wpływ na osoby fizyczne lub prawne, dając pełniejszy obraz skutków incydentów.

Podkreślając znaczenie międzynarodowego wymiaru cyberbezpieczeństwa, dyrektywa NIS 2 inicjuje znacznie większą współpracę i wymianę informacji między państwami członkowskimi Unii Europejskiej. To podejście ma na celu stworzenie bardziej zintegrowanej i skoordynowanej reakcji na zagrożenia cybernetyczne, które coraz częściej mają charakter transgraniczny.

Współpraca międzynarodowa w ramach NIS 2 jest istotna, aby skutecznie stawić czoła wyzwaniom w dynamicznie zmieniającym się środowisku cybernetycznym, co przyczynia się do wzrostu ogólnego poziomu bezpieczeństwa cyfrowego na terenie całej Unii Europejskiej.

ANALIZA RYZYKA I WYMOGI RAPORTOWANIA W KONTEKŚCIE NIS 2

W dobie rosnących zagrożeń cybernetycznych, dyrektywa NIS 2 stawia przed organizacjami nowe wyzwania w zakresie analizy ryzyka i raportowania incydentów. Istotne jest, aby podejście do tych zagadnień było kompleksowe, uwzględniając zarówno aspekty techniczne, jak i biznesowe. Wynikają z tego następujące wnioski, zaimplementowane w nowych przepisach:

- **Analiza ryzyka cybernetycznego** w kontekście NIS 2 wymaga kompleksowego podejścia. Organizacje muszą rozszerzyć zakres swojej analizy ryzyka, aby obejmo-

wała nie tylko zagrożenia zewnętrzne, ale także wewnętrzne słabości systemów i procedur. Ta holistyczna analiza powinna wziąć pod uwagę wszystkie aspekty działalności organizacji, do technicznych po operacyjne i biznesowe, oceniając, jak cyberzagrożenia mogą wpływać na kluczowe operacje biznesowe i ciągłość działania.

- Kluczowe jest zrozumienie roli i odpowiedzialności organizacji w społeczeństwie. Analiza ryzyka powinna również skupić się na usługach krytycznych z punktu widzenia państwa i obywateli. Na przykład, dla elektrowni ważne będzie dostarczanie prądu, natomiast dla banków kluczowym aspektem będzie zapewnienie dostępu do usług bankowości elektronicznej.
- Raportowanie incydentów wymaga nowego podejścia. NIS 2 nakłada na organizacje wymóg szybkiego raportowania incydentów, w ciągu 24 godzin od ich wykrycia. Działy IT i bezpieczeństwa muszą efektywnie wykrywać i reagować na incydenty oraz potrafić rozróżnić, które z nich są "poważne" i wymagają raportowania. Ponadto, istotne jest zrozumienie potencjalnego wpływu incydentów na społeczeństwo i państwo, co wymaga systemów zdolnych do oceny skali oraz wpływu incydentu w szerszym kontekście społecznym i gospodarczym.

ROLA CYBERBEZPIECZEŃSTWA W ŁAŃCUCHU DOSTAW

W kontekście dyrektywy NIS 2, rola cyberbezpieczeństwa w łańcuchu dostaw nabiera nowego wymiaru, stając się ważnym obszarem, na którym organizacje muszą się skoncentrować. Nowe wymagania dotyczą zarówno zabezpieczenia własnych systemów organizacji, jak i tych należących do dostawców usług i technologii. Organizacje są zobowiązane do przeprowadzania regularnych audytów bezpieczeństwa swoich dostawców, by upewnić się, że spełniają one narzucone wymogi w zakresie cyberbezpieczeństwa.

Istotne w tym procesie jest nie tylko weryfikowanie certyfikacji bezpieczeństwa firm, z którymi współpracujemy, ale też negocjowanie klauzul bezpieczeństwa w umowach. Aktywne zarządzanie ryzykiem wymaga ciągłego monitorowania i oceny poziomu cyberbezpieczeństwa dostawców usług teleinformatycznych, co stanowi nieodłączny element zabezpieczania całego łańcucha dostaw.

W tym kontekście coraz większe znaczenie mają testy penetracyjne, które powinny wykraczać poza samo sprawdzenie jednolitego systemu. W nowym paradygmacie, testy te powinny obejmować analizę szeregu integracji z innymi środowiskami, na przyk-

ład w systemach księgowo-płatniczych oraz innych krytycznych systemach, w których aplikacje są nierozerwalnie powiązane z różnorodnymi kanałami komunikacji. To podejście demonstruje, jak rozległy i kompleksowy charakter mają testy penetracyjne, obejmując w swoim zakresie nie tylko pojedyncze aplikacje, ale całe złożone systemy, sprawdzając ich zabezpieczenia w różnych scenariuszach i kontekstach.

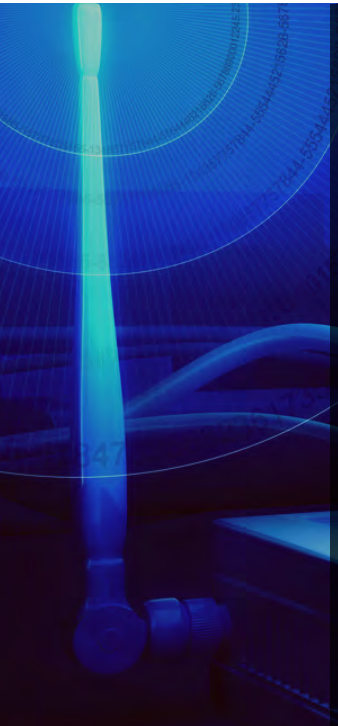
Równie istotne stają się testy socjotechniczne, zwłaszcza w sytuacji, gdy firma współpracuje z licznymi dostawcami. Te testy wykorzystują wyrafinowane metody, aby sprawdzić, na ile pracownicy są podatni na różnego rodzaju manipulacje, które mogą prowadzić do naruszenia bezpieczeństwa. Przeprowadzanie takich testów w firmach o rozległej sieci dostawców pozwala na identyfikację potencjalnych luk w świadomości bezpieczeństwa i procedurach, jak również na zwiększenie ogólnej odporności organizacji na ataki socjotechniczne. Przykładem mogą być symulowane ataki phishingowe czy inżynieria społeczna, które testują, na ile pracownicy są przygotowani do rozpoznawania i odpowiedniego reagowania na próby wyłudzenia informacji czy dostępu do wrażliwych danych.

Cyberbezpieczeństwo nie jest już opcją, ale kluczowym elementem każdej organizacji działającej w cyfrowym świecie. Dyrektywa NIS 2 podkreśla ten fakt, stawiając nowe wymagania i wyznaczając nowe standardy. Organizacje, które zrozumieją i zaadaptują się do tych zmian, będą lepiej przygotowane na wyzwania przyszłości.

Redsaber Security pomaga firmom dostosować się do dyrektywy NIS 2 zarówno instytucjom publicznym jak w sektorze prywatnym, oferując kompleksowe testy socjotechniczne dla pracowników jak i testy penetracyjne systemów internetowych, w celu poprawienia świadomości cyberzagrożeń oraz eliminacji podatności systemów.

JAK ZABEZPIECZYĆ FIRMOWĄ SIEĆ WI-FI PRZED NIEAUTO-RYZOWANYM DOSTĘPEM?

Redakcja
SECURITY MAGAZINE



Wydajna sieć bezprzewodowa jest dziś podstawą funkcjonowania środowiska pracy, zapewniając nie tylko nieograniczony dostęp do internetu, ale i umożliwiając efektywną komunikację i współpracę. Jednak razem z powszechnym stosowaniem sieci bezprzewodowych, pojawia się coraz większa potrzeba skupienia uwagi na bezpieczeństwie tych połączeń. Niezabezpieczona sieć Wi-Fi w firmie może stanowić podatny obszar na nieautoryzowany dostęp.

DLACZEGO SILNE HASŁA SĄ WAŻNE?

Silne hasło definiuje się jako takie, które jest wyzwaniem dla cyberataków, zwłaszcza tych opartych na próbach brute force. Polegają one na systematycznym testowaniu różnych kombinacji znaków, a słabe hasła, jak np. "password" czy "123456", stają się łatwym celem dla hakerów, umożliwiając nieautoryzowany dostęp do konta.

Podobnie jest z hasłami przewidywanymi np. P@ssw0rd. Hasło zawiera duże i małe litery, znak specjalny i liczbę, ale jest powszechnie znane i mimo swojej złożoności może być łatwo złamane podczas próby uzyskania dostępu.

Stosowanie słabych haseł grozi poważnym zagrożeniem dla bezpieczeństwa danych, szczególnie jeśli przechowują one ważne informacje, takie jak dane finansowe czy korespondencja e-mail. Dlatego zaleca się korzystanie z różnych kombinacji znaków, które zawierają duże i małe litery, cyfry i symbole.

Dodatkowo, unikanie użycia łatwo dostępnych informacji, np. imienia czy daty urodzenia, jest istotne w kreowaniu hasła. Długość hasła także ma znaczenie – im dłuższe, tym trudniejsze do złamania. Zaleca się, aby hasło miało minimum 8 znaków, jednak preferowane są dłuższe kombinacje. Inne ważne praktyki to unikanie używania tych samych haseł do różnych kont oraz regularna ich zmiana. Rozważenie korzystania z menedżera haseł, który pomaga w generowaniu silnych kombinacji może również ułatwić sprawę.

UTWORZENIE ODDZIELNEJ SIECI GOŚCINNEJ (GUEST NETWORK)

Utworzenie oddzielnej sieci gościnnej (Guest Network) w firmie jest ważnym krokiem w zabezpieczaniu infrastruktury sieciowej, który pozwala na fizyczne lub wirtualne oddzielenie ruchu internetowego gości od głównej sieci firmowej. Dzięki temu odwiedzający i pracownicy, którzy nie potrzebują dostępu do wrażliwych zasobów firmy, mogą korzystać z internetu bez ryzyka przypadkowego lub złośliwego dostępu do poufnych danych. Taka izolacja ruchu sieciowego znacząco zwiększa bezpieczeństwo, minimalizując ryzyko, że malware lub wirusy przenikną z urządzeń gości do firmowej sieci. Nowoczesne routery umożliwiają łatwe ustawienie sieci gościnnej, co pozwala na ustalenie innego hasła dla tej sieci i jego regularną zmianę bez wpływu na główną sieć firmową. Można również ograniczyć dostęp do określonych usług lub aplikacji, co jest dodatkowym zabezpieczeniem.

Sieć gościnna umożliwia także monitorowanie i kontrolowanie podłączonych urządzeń, co pozwala na szybką reakcję w przypadku wykrycia podejrzanej aktywności. Jest to również wygodne rozwiązanie dla odwiedzających, którzy mogą potrzebować dostępu do Internetu, bez konieczności uzyskiwania dostępu do bardziej zabezpieczonej, firmowej sieci. Dodatkowo, w niektórych przypadkach, oddzielna sieć gościnna może pomóc w spełnieniu wymogów prawnych dotyczących ochrony danych, zapewniając, że dostęp do poufnych informacji jest ściśle kontrolowany.

WYŁĄCZANIE NADAWANIA SSID

Zabezpieczenie sieci Wi-Fi Twojej firmy jest podstawą ochrony poufnych danych i zapobieganiu cyberbezpieczeństwa. Jednym ze sposobów na zwiększenie bezpieczeństwa sieci jest wyłączenie nadawania SSID (z ang. Service Set Identifier), co sprawia, że nazwa sieci Wi-Fi nie jest widoczna dla osób niepowiązanych. Choć ta metoda bywa czasem kwestionowana pod kątem skuteczności, ma ona swoje zalety w kontekście bezpieczeństwa.

CO TO JEST SSID I JAK WYŁĄCZYĆ WIDOCZNOŚĆ?

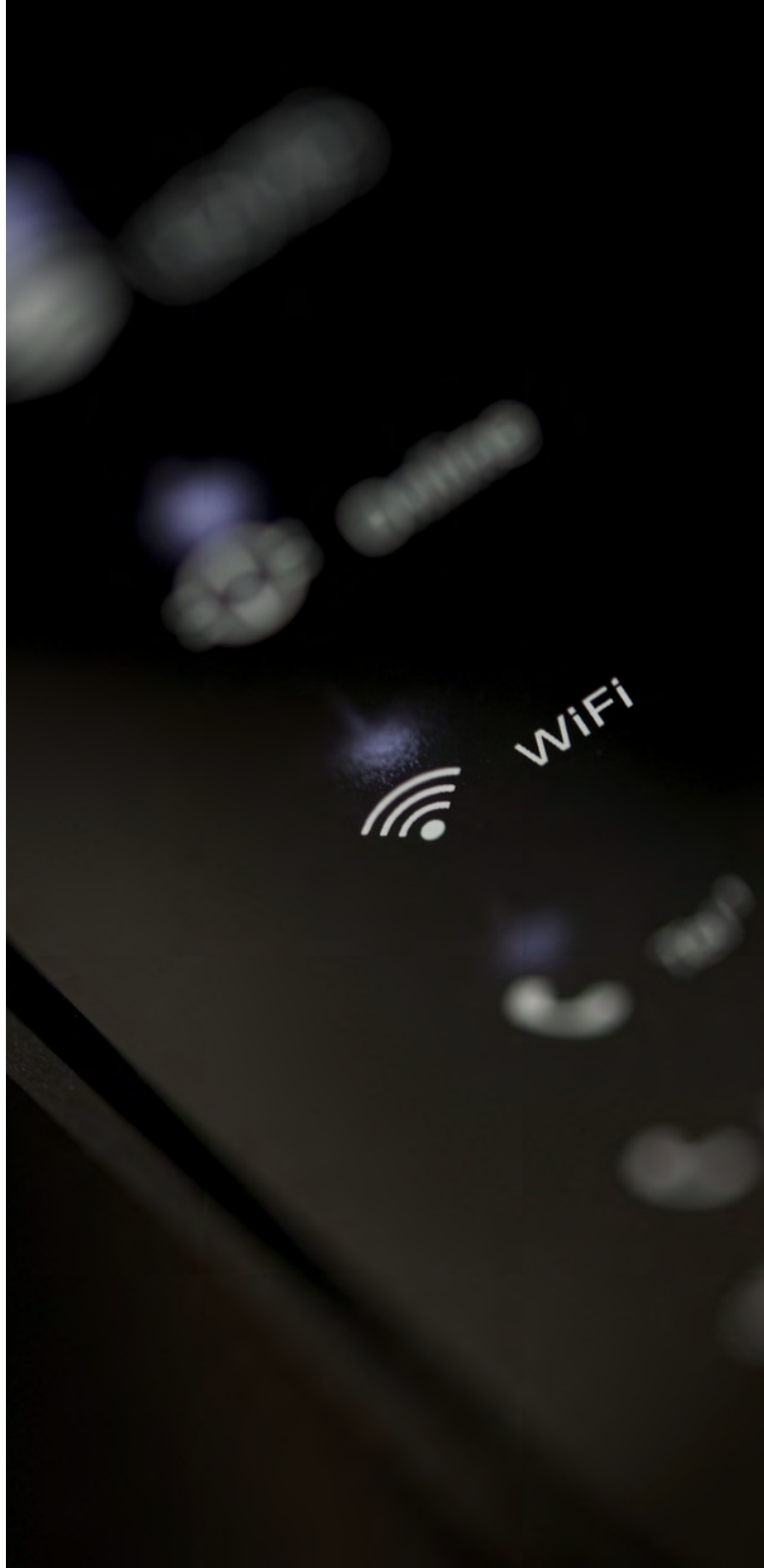
SSID to nazwa sieci bezprzewodowej, która umożliwia urządzeniom identyfikację i połączenie się z odpowiednią siecią Wi-Fi. Kiedy nadawanie SSID jest wyłączone, nazwa sieci nie pojawia się na liście dostępnych sieci Wi-Fi, co może utrudnić potencjalnym atakującym lokalizację i atak na Twoją sieć.

Wyłączenie nadawania SSID jest zazwyczaj prostym procesem, który można wykonać poprzez panel administracyjny routera. Należy zalogować się do panelu, znaleźć ustawienia sieci Wi-Fi i wybrać opcję ukrycia nazwy sieci.

Mimo że ukrycie SSID może wydawać się dobrym pomysłem, nie należy traktować tego jako jedynego środka ochrony. To nie gwarantuje całkowitego bezpieczeństwa. Atakujący o większym doświadczeniu potrafią pokonać to zabezpieczenie.

FILTROWANIE ADRESÓW MAC

Kolejnym ze sposobów na wzmocnienie bezpieczeństwa Twojej firmowej



sieci jest wykorzystanie filtrowania adresów MAC (unikalny adres karty sieciowej, podobnie jak adres IP), która pozwala na połączenie z siecią tylko dla adresów MAC wprowadzonych na listę routera. Chociaż ta metoda ma swoje zalety, ważne jest, aby zrozumieć jej ograniczenia i właściwie ją implementować.

Filtrowanie adresów MAC umożliwia dostęp do sieci wyłącznie zatwierdzonym urządzeniom. Dzięki temu, przedsiębiorcy mogą skutecznie kontrolować, które jednostki mogą łączyć się z ich siecią. Takie działanie zwiększa bezpieczeństwo wrażliwych danych i całej infrastruktury.

Jednakże, filtracja adresów MAC nie jest pozbawiona ograniczeń. Choć może skutecznie odstraszać mniej doświadczonych atakujących, którzy poszukują łatwych celów, nie stanowi niezawodnej bariery dla bardziej zaawansowanych cyberprzestępców. Adresy MAC mogą być bowiem fałszowane przez doświadczonych hakerów, co oznacza, że filtracja adresów MAC nie zawsze jest wystarczającym środkiem ochrony. Dodatkowo, zarządzanie listą dozwolonych urządzeń może być czasochłonne, szczególnie w dynamicznie rozwijających się firmach, gdzie regularnie dodawane są nowe urządzenia.

WŁĄCZANIE ZABEZPIECZEŃ WPA3

WPA3, czyli Wi-Fi Protected Access 3, to protokół zabezpieczeń sieci bezprzewodowych, który oferuje znacznie lepszą ochronę niż jego poprzednik, WPA2. Jest obecnie standardem dla urządzeń certyfikowanych przez Wi-Fi Alliance i stanowi ważny krok w kierunku zabezpieczania danych przesyłanych przez sieci Wi-Fi.

Czym jednak jest WPA3? To trzecia iteracja standardu certyfikacji bezpieczeństwa opracowanego przez Wi-Fi Alliance. Zapewnia lepszą ochronę danych przesyłanych przez osobiste i firmowe sieci Wi-Fi.

Jedną z głównych zalet WPA3 jest zwiększona ochrona dla prostych haseł. W środowisku biznesowym, gdzie prostota dostępu często idzie w parze z potrzebą bezpieczeństwa, WPA3 oferuje rozwiązanie, które chroni nawet proste hasła przed atakami. Dzięki temu, pracownicy mogą korzystać z łatwiejszych do zapamiętania haseł, nie narażając przy tym bezpieczeństwa sieci.

WPA3 zapewnia również lepsze szyfrowanie dla sieci osobistych i otwartych. To szczególnie ważne w miejscach, gdzie pracownicy lub klienci mogą korzystać z publicznych hotspotów Wi-Fi. WPA3 gwarantuje, że nawet w tych mniej kontrolowanych środowiskach, dane przesyłane przez sieć są odpowiednio zabezpieczone.

Bezpieczeństwo na poziomie przedsiębiorstwa to kolejna istotna cecha WPA3. Ten standard oferuje zaawansowane protokoły szyfrowania, które są niezbędne w dużych, złożonych sieciach firmowych. Zapewnia to ochronę wrażliwych danych.

Ochrona przed szczególnie trudnymi i wzmożonymi cyberatakami to kolejna istotna cecha WPA3. Ten standard chroni przed próbami odgadnięcia haseł offline, wymagając od użytkowników bezpośredniej interakcji z urządzeniem Wi-Fi przy każdej próbie odgadnięcia hasła. To znacząco utrudnia potencjalne ataki.

Mimo tych wszystkich zalet, WPA3 nie jest wolny od ograniczeń. Na przykład, istnieje ryzyko, że atakujący w zasięgu ofiary może uzyskać hasło do sieci Wi-Fi, co pozwala na odczyt i kradzież danych. Dlatego też, choć WPA3 jest znaczną poprawą w stosunku do WPA2, nie jest on odporny na wszystkie rodzaje ataków.

Zabezpieczanie firmowej sieci Wi-Fi staje się ważnym elementem utrzymania płynności działania przedsiębiorstwa w dynamicznym środowisku biznesowym. Nie tylko zapewnia ona niezbędny dostęp do Internetu, ale również umożliwia efektywną komunikację i współpracę. Ważne jest, aby pamiętać, że bezpieczeństwo sieci Wi-Fi wymaga kompleksowego podejścia i nieustannej uważności.

DLACZEGO DANE CIĄGŁE CZYTAJĄ SIĘ WOLNIEJ OD POFRAGMENTOWANYCH?

Paweł Kaczmarzyk
Serwis komputerowy Kaleron

Przywykliśmy, że dane zapisane w sekwencji kolejnych sektorów powinny czytać się szybciej od pofragmentowanych. Szczególnie jest to widoczne w dyskach twardych, gdzie jeżeli dane są pofragmentowane, głowica traci czas na odnajdywanie kolejnych fragmentów pliku. Stąd w ich przypadku defragmentacja danych jest często zalecaną czynnością optymalizującą pracę komputera. Ale nie zawsze tak jest. Dlaczego niekiedy dane pofragmentowane czytają się szybciej od zapisanych liniowo?

ADRESACJA LOGICZNA A FIZYCZNA

Kiedy obserwujemy rozmieszczenie plików i oceniamy ich fragmentację, posługujemy się adresacją LBA (Logical Block Addressing). Choć ten poziom adresacji jest często postrzegany jako sektory fizyczne, w rzeczywistości jest to adresacja logiczna pozwalająca na zachowanie kompatybilności pomiędzy nośnikami danych, protokołami komunikacyjnymi i systemami plików. W tej adresacji posługujemy się 512-bajtowymi sektorami, którym nadajemy kolejno numery od 0 aż do ostatniego.

Wprawdzie sektory LBA mogą nam się kojarzyć z sektorami dysków twardych, ale obecnie jest to już tylko zaszłość historyczna. Współczesne dyski twarde posługują się sektorami liczącymi 4 kB, które odpowiadają 8 sektorom logicznym. Jeszcze bardziej złożona jest sytuacja w przypadku nośników NAND-owych. Układy NAND nie rozumieją sektorów, a adresują dane w blokach (minimalna jednostka kasowania) i stronach (minimalna jednostka programowania i odczytu). Dodatkowo algorytmy rozpraszania danych powodują, że kolejne sektory logiczne mogą trafiać do różnych fizycznych jednostek alokacji.

Za przeliczanie adresów LBA na adresację fizyczną odpowiada część oprogramowania układowego nośnika – podsystem translacji. Podsystem translacji jest bardzo wrażliwy na błędy i jego problemy są częstą przyczyną awarii zarówno dysków twardych, jak i nośników półprzewodnikowych. Więcej możesz o tym przeczytać w Security Magazine nr **9(18)/2023** i **11(20)/2023.**

ROZMIESZCZENIE SEKTORÓW LBA W DYSKACH TWARDYCH

Do połowy lat ‘80 sektory w dyskach twardych były adresowane bezpośrednio w adresacji fizycznej CHS (C - *cylinder*, czyli grupa ścieżek o tym samym promieniu, H – *head*, głowica jednoznacznie identyfikująca powierzchnię talerza i S – *sector*, sektor będący fragmentem wybranej ścieżki).

Rosnąca w tamtym czasie liczba producentów oraz modeli dysków o zróżnicowanych parametrach przy jednoczesnym upowszechnianiu techniki komputerowej, która zaczęła masowo trafiać w ręce nietechnicznych użytkowników wymusiły standaryzację urządzeń. I to mające na celu zapewnienie kompatybilności dysków twardych oraz uproszczenie ich obsługi standardy ATA oraz SCSI wprowadziły adresację LBA.

Dlaczego dane ciągłe czytają się wolniej od pofragmentowanych?

Ale od samego wprowadzenia nowej adresacji stara przecież nie zniknęła. Dyski wewnątrz nadal adresują konkretne fizyczne sektory na konkretnych ścieżkach i konkretnych powierzchniach talerzy. Muszą też odpowiednio zarządzać uszkodzonymi sektorami, aby nie były one zagrożeniem dla bezpieczeństwa danych. Do tego przy przypisywaniu fizycznym sektorom adresów logicznych producenci kierują się chęcią uzyskania nośników o jak najlepszych parametrach wydajnościowych i gęstości zapisu.

Logicznym jest, by kolejne numery adresów nadawać kolejnym sektorom na ścieżce, a następnie przechodzić na sąsiednią ścieżkę. Ponieważ nawet przepozycjonowanie głowicy na sąsiednią ścieżkę wymaga czasu, numery sektorów nadaje się z odpowiednim przesunięciem tak, by kolejny sektor nie uciekł w tym czasie spod głowicy, ale podjechał pod nią we właściwym momencie. Ale z której strony zacząć? Od środka, czy od zewnętrznej krawędzi?

Z pomocą w podjęciu decyzji przychodzi nam wzór na długość okręgu = $2\pi r$. Łatwo wtedy zauważymy, że wraz z promieniem rośnie także długość okręgu, a więc zewnętrzne ścieżki są znacznie dłuższe od wewnętrznych. A ponieważ adresacja LBA pozwoliła producentom ukryć wewnętrzną adresację fizyczną przez światem zewnętrznym, zyskali oni swobodę zróżnicowania liczby sektorów na ścieżkę. Dzięki temu na zewnętrznych ścieżkach mogą oni umieścić więcej sektorów niż na wewnętrznych, co pozwala nie tylko uzyskać większą gęstość zapisu, ale też wyższą wydajność. I takich stref o różnej liczbie sektorów na ścieżkę na powierzchni talerza może być nawet kilkadziesiąt.

Jeśli na zewnętrznych ścieżkach umieścimy więcej sektorów, będziemy mogli w czasie jednego obrotu talerza przeczytać więcej danych. Dlatego pierwsze numery LBA przypisywane są sektorom na zewnętrznych ścieżkach. Od czasu do czasu numeracja przechodzi na kolejne powierzchnie talerzy, by stopniowo w miarę równomiernie zbliżać się do środka.

Możemy to zaobserwować na wykresie skanu powierzchni talerza, gdzie bez trudu zauważymy, że początkowe sektory odczytywane są nawet trzy razy szybciej od końcowych. Dlatego pofragmentowane dane położone w początkowych sektorach LBA mogą się czytać szybciej od danych ciągłych zapisanych pod koniec dysku.

ZARZĄDZANIE DEFEKTAMI

Na potrzeby tego artykułu możemy defekty na dysku podzielić na dwie kategorie. Fabryczne – ujawnione na etapie testów fabrycznych oraz eksploatacyjne – powstałe lub ujawnione w trakcie eksploatacji dysku. I odpowiednio mamy dwie listy defektów. Listę podstawową (lista P) dla defektów fabrycznych oraz przyrostową (lista G) dla defektów eksploatacyjnych. Rzeczywiste rozwiązania zarządzania defektami bywają dużo bardziej skomplikowane, ale na nasze potrzeby to uproszczenie nam wystarczy.

Nadając sektorom numery LBA możemy wykorzystać listę P i po prostu omijać uszkodzone sektory. Dlatego jeśli na ścieżce trafi się defekt fabryczny, głowica musi jedynie zaczekać na kolejny cały czas pozostając nad ścieżką. Natomiast w przypadku uszkodzeń eksploatacyjnych takie podejście jest niepraktyczne, gdyż wymagałoby przenumerowania wszystkich kolejnych sektorów, a ze względu na spójność adresowania logicznego, także przenoszenia ich zawartości.

Dlatego w przypadku defektów eksploatacyjnych stosuje się inne podejście. Część ścieżek pozostawia się bez nadanych numerów LBA jako rezerwę i jeśli zostanie ujawniony uszkodzony sektor, jest on wpisywany na listę G, a jego numer LBA jest mu odpierany i przypisywany któremuś z sektorów rezerwowych. Operację tę nazywa się remapowaniem lub realokacją.

Dla ograniczenia negatywnych skutków dla wydajności dysku, grupy ścieżek rezerwowych tworzy się przy każdej strefie ścieżek. Tym niemniej w przypadku realokacji sektorów zrywana jest fizyczna ciągłość zapisu i głowice muszą w czasie odczytu poszukać takiego remapowanego sektora, a następnie wrócić nad pierwotną ścieżkę. To też wpływa na na czas odczytu danych.

SEKTORY NIESTABILNE

Przy współcześnie uzyskiwanej gęstości zapisu niemożliwym jest uzyskiwanie bezbłędnych zapisów i odczytów. Warunki masowej produkcji talerzy nie pozwalają na pełną powtarzalność ich wykonania i nawet na powierzchni jednego talerza mogą występować różnice w jakości warstwy magnetycznej. Dlatego stosowane są złożone algorytmy kodowania i dekodowania danych pozwalające na korekcję błędów bitowych.

Jednak nawet przy wykorzystaniu tych rozwiązań liczba błędów bitowych może przekroczyć ich możliwości. Gdyby w takiej sytuacji za każdym razem sektor był uznawany za uszkodzony i podlegał remapowaniu, szybko wyczerpalibyśmy pulę sektorów rezerwowych. Z tego powodu dysk podejmuje kolejne próby odczytu takiego sektora.

Zazwyczaj takich prób jest kilkanaście, do ok. 20 i dopiero jeśli nie przyniosą one rezultatu, dysk wystawia komunikat o błędzie. Każda kolejna próba, to czas, w którym musimy zaczekać na kolejny obrót talerza.

BUFOROWANIE

W niektórych przypadkach dane są buforowane i kiedy je odczytujemy, nie musimy ich wyszukiwać na dysku, tylko możemy je odczytać szybciej z bufora. Zwykle buforowanie sprzyja szybszemu odczytywania danych ciągłych. Tak jest np. w przypadku odczytu wyprzedzającego. Polega on na tym, że jeśli żądamy od dysku odczytana sekwencji adresów LBA, dysk może na wszelki wypadek odczytać i umieścić w buforze kolejne sektory nie czekając na polecenie ich odczytania. Jeśli będziemy chcieli odczytać właśnie te sektory, będą już czekać przygotowane w buforze. Jeżeli będziemy chcieli przeczytać inne, opróżnienie bufora jest znacznie szybsze od odnalezienia i fizycznego odczytania tych danych z talerza.

Ale producenci, szukając możliwości poprawy wydajności, stosują też inne sposoby buforowania. Takim rozwiązaniem były np. dyski SSHD wyposażone w bufor NAND, w którym umieszczano najczęściej odczytywane sektory. Również bufor Media Cache w przypadku dysków niewykorzystujących technologii SMR jest wykorzystywany do przyśpieszenia odczytu najczęściej odczytywanych sektorów. Oprócz tego mogą być też wykorzystywane bufory zewnętrzne, jak np. zmiennofazowy (zajrzyj do **nr 3(12)/2023 Security Magazine**) bufor Optane.

W tych przypadkach na czas odczytu pliku większy wpływ może mieć umieszczenie go w buforze, niż to, czy jest on pofragmentowany, czy nie.

SMR

Artykuł o dyskach SMR został opublikowany w nr **6(15)/2023 Security Magazine.** W tych dyskach z uwagi na dwupoziomowy podsystem translacji adresów logicznych na fizyczne dochodzi do zerwania wcześniej względnie stałego przywiązania adresów LBA do sektorów fizycznych.

Szczegóły rozwiązań pozwalających poradzić sobie z utratą swobodnego dostępu do sektora fizycznego podczas zapisu są różne dla dysków różnych producentów, jednak w każdym z tych przypadków nie możemy już oczekiwać, że kolejne sektory w adresacji LBA będą fizycznie umieszczone w bliskim sąsiedztwie.

Podobnej sytuacji możemy spodziewać się w dyskach z zapisem przeplotowym (IMR – *Interlaced Magnetic Recording*), których jeszcze wprawdzie nie ma na rynku, ale zapewne niebawem się pojawią. Będą to dyski wykorzystujące technikę częściowego nadpisywania ścieżek podobną do znanej z dysków SMR w połączeniu z techniką zapisu wspomaganego energetycznie. W założeniu rozwiązanie to ma poprawić możliwą do uzyskania gęstość zapisu oraz uprościć podsystem translacji adresów logicznych na fizyczne, jednak jeśli nawet w końcowym efekcie zapis przeplotowy będzie prostszy od gontowego, to i tak będzie bardziej skomplikowany od zapisu konwencjonalnego.

Dlaczego dane ciągłe czytają się wolniej od pofragmentowanych?

Podane wyżej przykłady pokazują, że o ile faktycznie w większości przypadków odczyt plików ciągłych jest szybszy od odczytu danych pofragmentowanych, to w pewnych konkretnych sytuacjach właśnie dane pofragmentowane mogą być odczytane szybciej.

Wpływ na to ma szereg czynników związanych z fizycznym rozmieszczeniem danych na powierzchni dysku lub w buforze. Prędkość odczytu danych zależy także od stanu technicznego nośnika i jakości jego namagnesowania, a także od rozwiązań oprogramowania układowego.

BEZPIECZNE PRZECHOWY-WANIE KOPII ZAPASOWYCH DANYCH. WSKAZÓWKI

Redakcja
SECURITY MAGAZINE

Kopie zapasowe to podstawa w zdigitalizowanym biznesie. I zgodnie z danymi organizacji Acronis 90% firm robi kopie zapasowe. Jednak tylko 41% tworzy je codziennie. Dlaczego kopie zapasowe są istotne i tak ważne jest ich wykonywanie?

DLACZEGO KOPIE ZAPASOWE SĄ WAŻNE?

W cyfrowym świecie kopie zapasowe są niezwykle istotne. W końcu mnóstwo danych i informacji przechowujemy obecnie w chmurach, urządzeniach mobilnych i na lokalnych dyskach. Niestety – ciągle nie każdy to rozumie. Jak pokazują dane organizacji Acronis – prawie 50% respondentów uważa, że backupy nie są potrzebne.

I to pomimo tego, że 42% firm zgłosiło, że w tym roku utracili dane, co skutkowało przestojami, a 41% wskazało, że przez to straciło pieniądze lub zmalała ich produktywność. W końcu aż 68% firm nadal traci dane w wyniku przypadkowego usunięcia, awarii sprzętu lub oprogramowania albo nieaktualnej kopii zapasowej.

Ponadto ciągle mało specjalistów IT (20%) stosuje zasadę tzw. hybrydowych kopii zapasowych, tzn. przechowując je zarówno w chmurze, jak i na lokalnych nośnikach. Większość organizacji polega obecnie na chmurach. A niekoniecznie jest to dobre rozwiązanie. To, że mocno przywykliśmy do usług chmurowych sprawia, że presja na infrastrukturę IT po stronie usługodawców jest olbrzymia. I niekoniecznie zawsze im sprostają.

Owszem, zewnętrzni dostawcy są nierzadko bardzo skuteczni, mowa tutaj o największych firmach, jak Droppbox, OneDrive, Mega, Apple czy Google. Jednak poleganie wyłącznie na usługach chmurowych może skutkować utratą danych w przypadku chociażby awarii po ich stronie.

RODZAJE KOPII ZAPASOWYCH

Należy pamiętać, że w przypadku backupu mówimy o różnych typach strategii ich tworzenia. Mamy tu na myśli:

- **Pełne kopie zapasowe** – backupy polegające na skopiowaniu wszystkich danych z systemów lub urządzeń. Jest to najbardziej czasochłonny proces, ale uwzględnia dosłownie wszystko;
- **Przyrostowe kopie zapasowe** – backupy, w których koncentrujemy się tylko na danych ulegających zmianie od ostatniej kopii zapasowej. To szybsza metoda i obejmuje tylko najistotniejsze zmiany;
- **Różnicowa kopia zapasowa** – to rodzaj backupu uwzględniający jedynie dane, które uległy zmianie od ostatniej pełnej kopii zapasowej.

Wybór zależy od możliwości i potrzeb organizacji. Na pewno nie ma sensu przeprowadzania codziennie pełnego backupu, do czego jeszcze wrócimy.

DOBRE KOPIE ZAPASOWE TO CZĘSTE KOPIE ZAPASOWE

Jednak hybrydowość tworzenia backupów to nie wszystko. Istotną kwestią jest zwiększenie częstotliwości ich tworzenia. W najlepszym przypadku byłoby wykonywanie ich kilka razy dziennie albo przynajmniej raz. Jednak jak pokazuje badanie Acronis – to wcale nie jest reguła. Tylko 15% firm tworzy kilka kopii zapasowych dziennie, a raz dziennie wykonuje je 26% organizacji. Reszta robi to rzadziej – 28% raz na tydzień, a 20% raz na miesiąc.

Tworzenie kopii zapasowych oczywiście wymaga nieco czasu, zasobów i uważności. Dlatego w tym obszarze warto postawić na inteligentne formy lub automatyzację. I oczywiście – ważne jest zwiększenie częstotliwości dokonywania backupów. Sytuacje jak wyżej opisane, czyli robienie kopii raz na miesiąc, absolutnie nie mogą mieć miejsca. Zwłaszcza, jeśli mówimy o kopiach przyrostowych czy różnicowych.

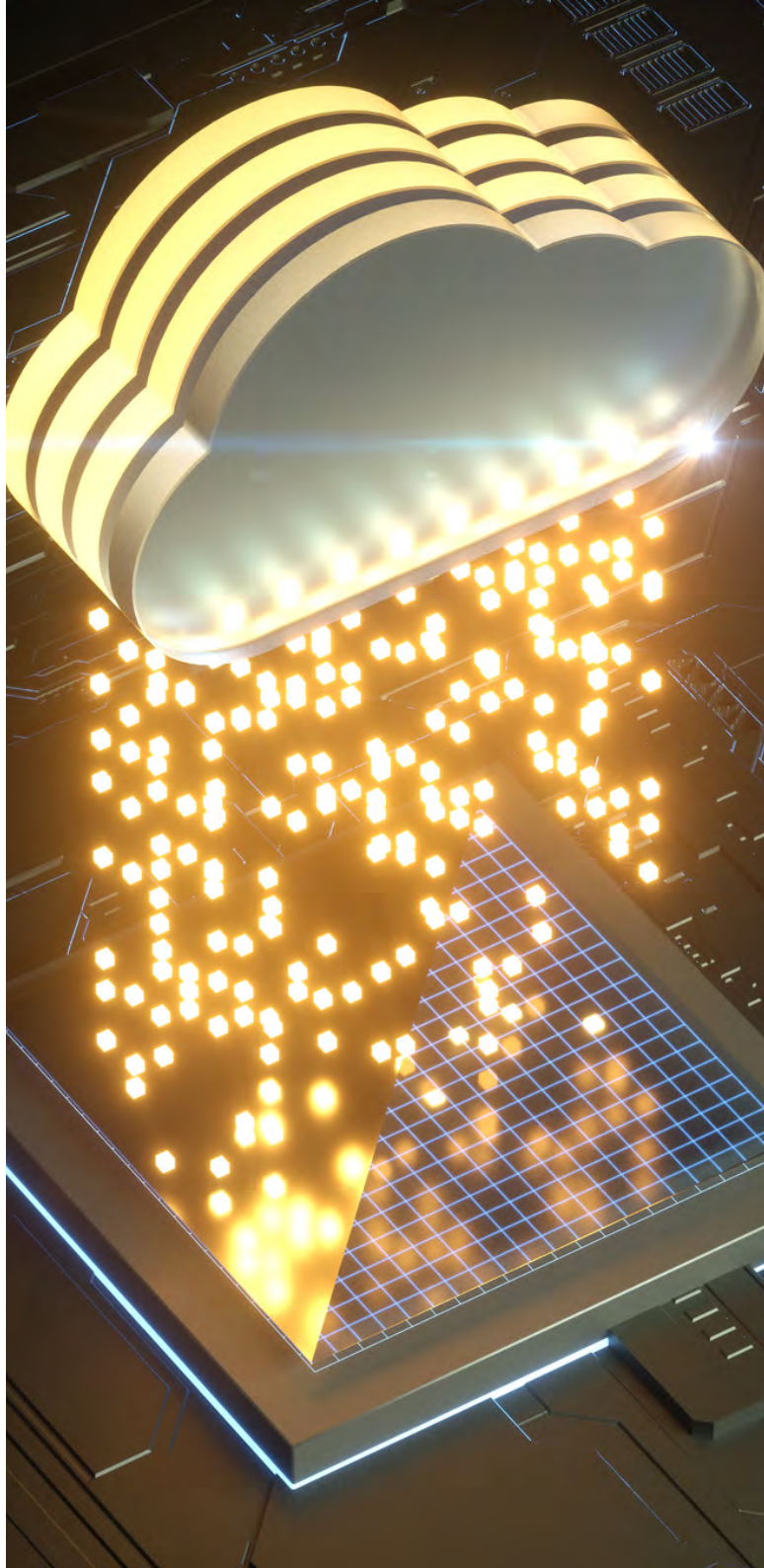
Dodatkowo warto zainteresować się tzw. przyrostowym kopiom zapasowym na poziomie bloku (BLI), które umożliwiają szybkie ich tworzenie, przechowując jedynie zmienione bloki danych. To skuteczne podejście, które zapewnia szybkie i częste tworzenie backupów.

STRATEGIA – DLACZEGO TO WAŻNE?

W kontekście tworzenia kopii zapasowych nie można zapomnieć też o strategii. Prawda jest taka, że trudno jest (zwłaszcza mniejszym organizacjom) wykonywać backupy kilka razy dziennie bez priorytetyzacji. Przede wszystkim, jeśli mowa o lokalnych nośnikach, jak zewnętrzne dyski, które trzeba fizycznie podpiąć. Dodatkowo nierzadko jest tak, że firmy korzystają z wielu różnych aplikacji, na których pojawiają się jakieś dane lub informacje.

Dlatego najważniejsze to ustalić, co musi być kopiowane w pierwszej kolejności i gdzie, a także przez kogo. Bez odpowiedniego zarządzania takim projektem, nie ma co liczyć na regularność. Priorytetem musi być ustalenie kluczowych, krytycznych danych, które muszą mieć backup.

W kontekście strategii istotne jest też ustalenie, kto ma dostęp do backupów i codziennych danych, a nie tylko kto nimi zarządza.



ZASADA 3-2-1

W kontekście kopiowania danych istotna jest jeszcze tzw. zasada 3-2-1. Jest to rzecz jasna powiązane ze strategią tworzenia kopii zapasowych. Rzeczona zasada podkreśla, że organizacje powinny przechowywać trzy pełne kopie swoich danych. Dwie muszą mieć charakter lokalny, ale na różnych nośnikach. W idealnej sytuacji byłoby też, gdyby były przechowywane w różnych lokalizacjach. Np. na wypadek kradzieży, pożaru czy klęski żywiołowej.

Rzecz jasna, jeśli coś takiego jest niemożliwe, to można uznać, że drugi nośnik przechowywanych danych, nie będzie fizyczny, a np. chmurowy. To szczególnie istotne w dzisiejszym, scyfryzowanym świecie, a może być bardzo pomocne dla organizacji działających zdalnie, bez stałej siedziby. Ważne jednak, aby usługodawca chmurowy dbał tutaj o cyberbezpieczeństwo. Tak, aby nie było łatwo usunąć kopii danych w wyniku chociażby cyberataku.

I jeśli już mówimy o chmurach, to należy zwrócić uwagę na to, jak działają i dokładnie przekalkulować ich wartość. Może się bowiem okazać, że jeśli mamy sporo danych do przechowywania np. 50, 100, 200 TB, to rozwiązanie lokalne (czyli fizyczne nośniki) okażą się bardziej opłacalne finansowo. W końcu nie będzie trzeba płacić za miejsce co miesiąc, czy co roku. Tyczy się to jednak przeważnie organizacji, które mają naprawdę sporo danych.

Decydując się na chmurę warto też sprawdzić, czy dany usługodawca zapewnia np. odzyskiwanie danych (DRaaS), dba o standardy cyberbezpieczeństwa (należy przejrzeć, czy miały miejsce jakieś wycieki w ostatnim czasie lub czy klienci tracili swoje dane) itd.

Przechowywanie starych danych jest niepotrzebne
Na początku pisaliśmy o tym, że warto robić kopie zapasowe codziennie. Ma to jednak też znaczenie w kontekście nie korzystania z kopii jako formy przechowywania danych. Odzyskiwanie powinno się tyczyć najnowszej kopii, a nie takiej sprzed kilku miesięcy ani tym bardziej lat. Zasada jest prosta – im więcej danych w takiej kopii, tym trudniej się nią zarządza i odnajduje to, co jest niezbędne.

Kopie muszą się przede wszystkim nadpisywać, nie ma sensu magazynowania w nich nieaktualnych informacji, plików itd. itp. Odchudzanie tego procesu i zapisywanie jedynie najpotrzebniejszych rzeczy znacząco przyspiesza i ułatwia przywracanie.

Pliki, które nie są aktualne, ale mogą się jeszcze przydać powinny być poddawane archiwizacji, a nie przetrzymywane w kopiach zapasowych jako magazyny.

WDRAŻANIE ZAPOBIEGANIA UTRATY DANYCH

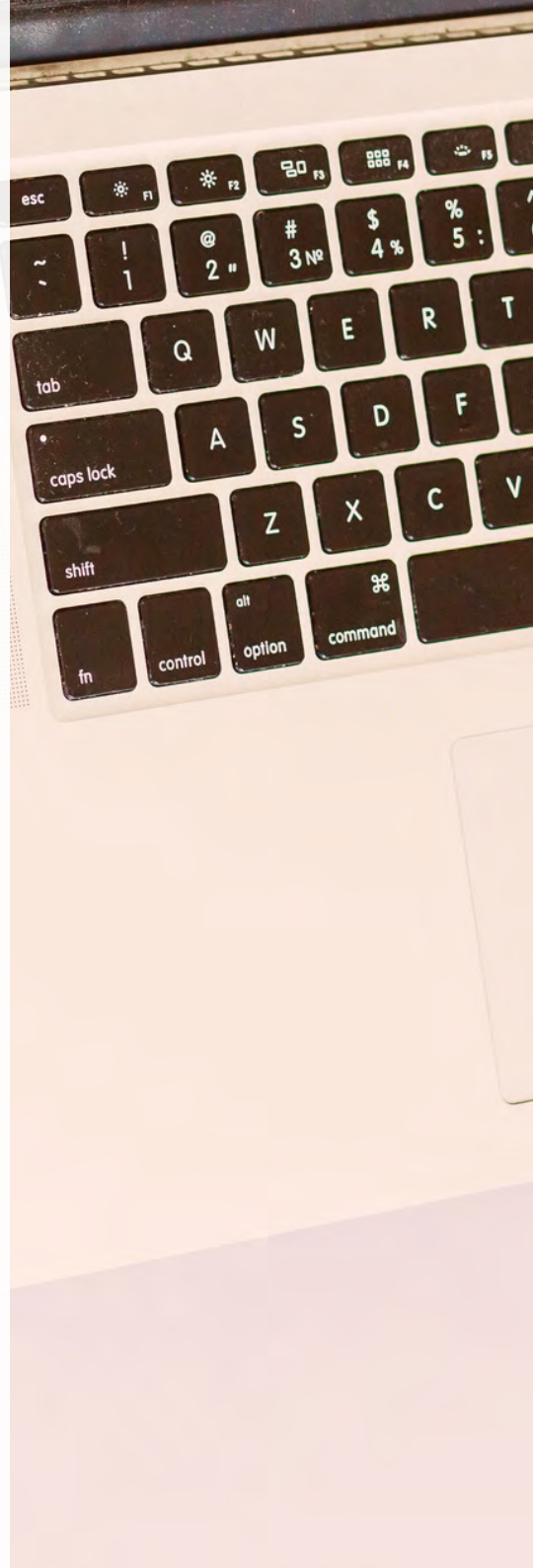
Mówiąc o backupach nie możemy też zapomnieć, że ważne jest, aby zapobiegać utratom danych. Kopie zapasowe to opcja B, opcją A zawsze powinno być cyberbezpieczeństwo.
A zapobieganie utracie danych to zestaw strategii i narzędzi, stosowanych by uniknąć kradzieży lub utraty ważnych informacji. Firmy stosują różne środki, aby chronić informacje oraz zabezpieczyć swoje systemy.

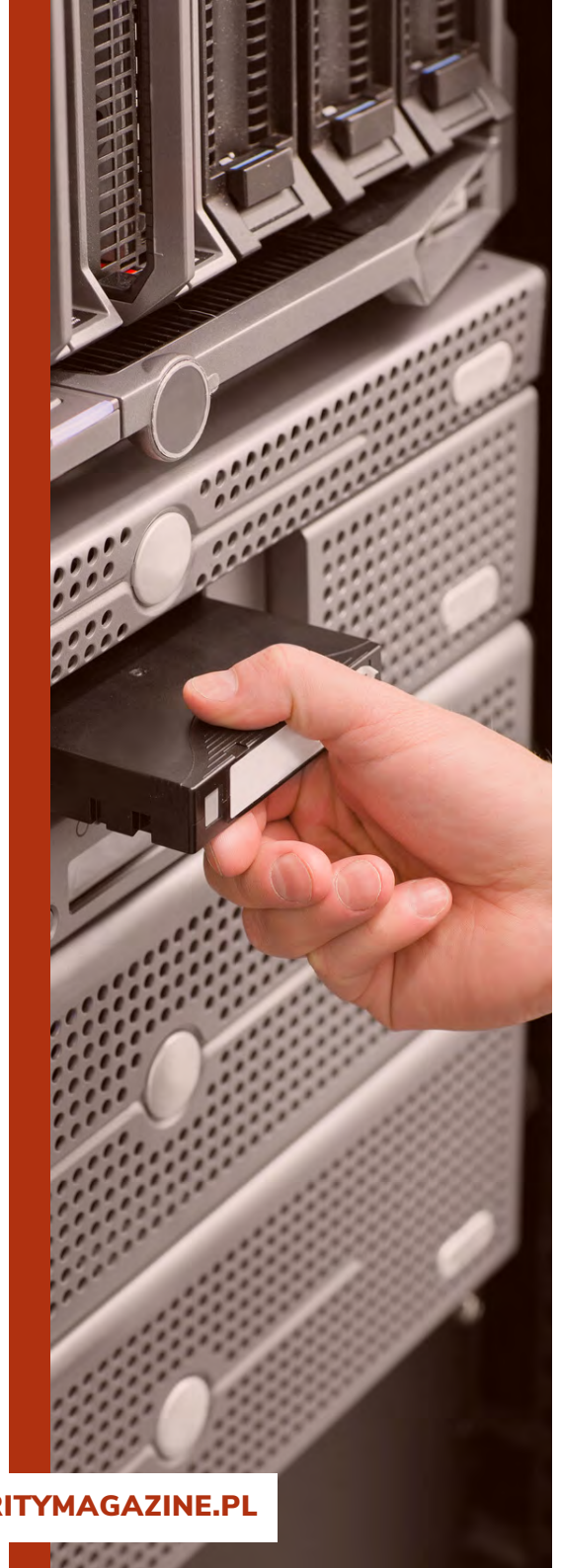
Ważne jest podejmowanie odpowiednich decyzji, jeśli chodzi o ochronę danych. Wybór właściwego rozwiązania do zapobiegania utracie danych (DLP) dla firmy jest niezwykle istotny. DLP pomaga ekspertom ds. cyberbezpieczeństwa w uzyskiwaniu aktualizacji zabezpieczeń danych, które są istotne dla kadry kierowniczej.

EDUKACJA PRACOWNIKÓW I OCHRONA

Ostatnią kwestią jest dbanie o samo cyberbezpieczeństwo. Nawet jeśli regularnie wykonujesz backupy i sprawdzasz swoich usługodawców, to zawsze istnieje szansa, że coś się wydarzy. Nierzadko ze względu na czynnik ludzki. Wszyscy popełniamy błędy, nikt nie jest idealny, a świat pędzi do przodu.

Dlatego dbając o kwestie tworzenia kopii zapasowych, nie można pominąć wątku związanego z szerzeniem świadomości o cyberzagrożeniach wśród swojego zespołu (i to cały, a nie tylko dział IT). Pracownicy powinni być regularnie szkoleni z cyberbezpieczeństwa i umieć rozpoznać chociażby ataki socjotechniczne. Dzięki temu minimalizujemy ryzyko problemów, jakie cyberataki mogą wywołać w kontekście utraty danych.





Należy też dbać o aktualizację oprogramowań, korzystanie z dodatkowych zabezpieczeń, jak filtry antyspamowe, uwierzytelnianie wieloskładnikowe czy programy antywirusowe. To w końcu kolejna bariera, którą cyberprzestępca będzie musiał pokonać, jeśli chce naruszyć czyjeś dane.

PLAN AWARYJNY – A CO JEŚLI?

Zawsze istnieje ryzyko, że w jakiś sposób utracimy dane. W takiej sytuacji musimy mieć plan awaryjny. Odzyskiwanie po awarii to taka metoda, która pomaga w odtworzeniu systemów i oprogramowania potrzebnego do funkcjonowania firmy. To o wiele więcej niż tylko robienie kopii zapasowych. Wszystkie firmy powinny mieć taki plan. Podczas tworzenia planu odzyskiwania, ważne jest uwzględnienie dwóch rzeczy: docelowego punktu przywracania (RPO) i docelowego czasu odzyskiwania (RTO).

RPO mówi nam, jak często tworzone są kopie zapasowe danych i ile możesz stracić danych w przypadku awarii. Natomiast RTO mówi nam, jak długo zajmie odzyskanie danych po awarii. To ma na celu zapewnienie, że w przypadku problemów z danymi, firma może wrócić do normalnego funkcjonowania w możliwie krótkim czasie.

Tak prezentuje się kwestia związana z backupami. Reasumując, kopie zapasowe powinny być częste, zwłaszcza, jeśli mówimy o ważnych czy zmieniających się informacjach. Jednocześnie nie może to być po prostu archiwum, w którym przechowywane są nieaktualne, niepotrzebne dane. Warto dbać o to, aby kopie były na co najmniej dwóch różnych nośnikach fizycznych i trzecim – np. chmurowym. Ewentualnie na fizycznym (chociażby zewnętrznym dysku) i chmurowym. W końcu dbając o regularne kopie zapasowe, minimalizujemy ryzyko strat, jakie z tego tytułu możemy ponieść – zarówno finansowych, jak i wizerunkowych.

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

GRZEGORZ BROL
CEO
Integrity Partners

Z branżą technologiczną związany od 1995 r., a z Grupą Altkom od 2005 r. W 2010 objął kierownictwo i udziały w powołanej w Grupie Altkom Integrity Solutions Sp. z o.o. Od 2015 r. pod marką Integrity Partners współtworzy jedną z czołowych polskich firm eksperckich w zakresie Cloud & CyberSecurity. Wcześniej zarządzał sprzedażą w w Jtt Computer SA oraz Computer Service Support SA (obecnie Comp SA).

KRZYSZTOF ANDRIAN
Identity Security BU Director
Integrity Partners

Działa na rynku ICT od ponad 20 lat. W firmie Integrity Partners dyrektor pionu Identity Security. Wcześniej był dyrektorem wykonawczym w Concept Data, a także zarządzał zespołami i projektami oraz realizował strategie sprzedaży dla spółek IT: Softbank, IBM Polska, Tieto Poland. W latach 2011-2014 zbudował i kierował nowym działem usług IT Contracting w Hays Polska.

PAWEŁ KACZMARZYK
Prezes Zarządu
Serwis komputerowy Kaleron

Prezes i technik w serwisie komputerowym Kaleron sp. z o. o. Specjalizuje się w odzyskiwaniu danych i naprawach elektronicznych urządzeń komputerowych, a także prowadzi szkolenia w tym zakresie.

ANETA GRALA
Specjalistka ds. ochrony danych osobowych
Rzetelna Grupa Sp. z o.o.

Prawniczka specjalizująca się w ochronie danych osobowych. W spółce Rzetelna Grupa zajmuje się kompleksową obsługą w zakresie ochrony danych osobowych, m.in. naruszeniami ochrony danych osobowych, bezpieczeństwem, kontaktem z UODO, doradztwem w zakresie zgodności z RODO biznesu e-commerce.

EKSPERCI WYDANIA

WIESŁAW SOKÓŁ
Dyrektor Działu Rozwoju
UNICARD

Od ponad 20 lat związany z branżą IT. Aktualnie Dyrektor Działu Rozwoju w UNICARD SA, gdzie stoi na czele zespołów programistycznych, które rozwijają produkty kontroli dostępu (impero 360), rejestracji czasu pracy, P&R oraz Małopolskiej Karty Aglomeracyjnej.

ŁUKASZ ZAJDEL
Dyrektor Sprzedaży
Perceptus Sp z o. o.

Dyrektor Sprzedaży w Perceptus Sp z o. o. Od roku 2016 związany jest z branżą cybersecurity. Z sukcesem realizuje komplementarne projekty i wdrożenia rozwiązań związanych z bezpieczeństwem IT, zarówno dla klientów komercyjnych jak i publicznych.

OLEKSII DOROSHENKO
Business Development Manager
Redsaber Security

Specjalista w dziedzinie cyberbezpieczeństwa, współzałożyciel Redsaber Security - firmy oferującej kompletne rozwiązania w zakresie pentestingu, testów socjotechnicznych i operacji red team. Nasza misja to wzmacnianie poziomu cyberbezpieczeństwa w każdej organizacji, zarówno w prywatnym sektorze, jak i publicznym.

ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ

Wydanie 2/2022
POBIERZ

Wydanie 3/2022
POBIERZ

Wydanie 4/2022
POBIERZ

Wydanie 5/2022
POBIERZ

Wydanie 6/2022
POBIERZ

Wydanie 7/2022
POBIERZ

Wydanie 8/2022
POBIERZ

Wydanie 9/2022
POBIERZ

Wydanie 1(10)/2023
POBIERZ

Wydanie 2(11)/2023
POBIERZ

Wydanie 3(12)/2023
POBIERZ

Wydanie 4(13)/2023
POBIERZ

Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

Wydanie 7(16)/2023
POBIERZ

Wydanie 8(17)/2023
POBIERZ

Wydanie 9(18)/2023
POBIERZ

Wydanie 10(19)/2023
POBIERZ

Wydanie 11(20)/2023
POBIERZ

Wydanie 12(21)/2023
POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

ul. Nowogrodzka 42 lok. 12
00-695 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
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

Redaktor prowadząca: Monika Świetlińska

Redakcja: Damian Jemioło, Joanna Gościńska, Katarzyna Leszczak

Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL