09/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Metaverse a bezpieczeństwo

Technologizacja branży security Oszczędności a rosnąca presja płacowa

Zagrożenia dla e-sklepów opartych na licencji open source

Jak skutecznie usunąć zbędne dane?

2023 rok w branży cybersecurity

SPIS TREŚCI

SZANOWNI PAŃSTWO,

Kończy się rok pełen wyzwań oraz bardziej lub mniej oczekiwanych zdarzeń - tych, które na zawsze zmieniły sposób postrzegania bezpieczeństwa w ogóle. Na bezpieczeństwo patrzymy dziś inaczej. Jesteśmy wyczuleni na nietypowe incydenty, ale również przyglądamy się tym, co do których (z pozoru) nie powinniśmy mieć wątpliwości.

Nowa rzeczywistość każe nam kontrolować zarówno przestrzeń online, jak i tę offline. Bo bezpieczeństwo dotyczy również miejsc pracy, miejsc publicznych, jednostek zdrowia, obiektów nauki oraz rozrywki. Nie bez powodu po raz kolejny przedłużone zostały alarmy BRAVO i CHARLIE-CRP.

"Rozsądek i czujność" - słyszymy niemal na każdym kroku i motto to mogło nam już nieco spowszednieć. Pamiętajmy jednak, że to właśnie my - ludzie, jesteśmy najsłabszym ogniwem, kiedy chodzi o ataki w sieci i w realnym świecie.

Dlatego z okazji zbliżających się świąt i Nowego Roku 2023 życzę wszystkim naszym Czytelnikom właśnie "rozsądku i czujności", spokoju i bezpiecznej podróży przez kolejne 12 miesięcy. byśmy tego czasu nie przespali, a uczyli się stawiać czoła wyzwaniom i wyciągali wnioski z wydarzeń, które zmieniły nasze postrzeganie bezpieczeństwa.

W imieniu całego zespołu redakcyjnego życzę Państwu rodzinnych świąt Bożego Narodzenia i dobrego 2023 roku.

Rafał Stępniewski


ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA
SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy
SECURITY MAGAZINE
ZAPISZ SIĘ
NEWSLETTER
YOUR EMAIL HERE
SUBSCRIBE

TECHNOLOGIZACJA BRANŻY SECURITY. OSZCZĘDNOŚCI A ROSNĄCA PRESJA PŁACOWA

Tomasz Wojak
Seris Konsalnet

Rozwój nowych technologii, digitalizacja, zmiany wywołane przez pandemię i wzrost kosztów dla przedsiębiorców spowodowały duże zmiany na rynku usług. Szczególnie dotknęły one branżę security.

Technologizacja branży security. Oszczędności a rosnąca presja płacowa

Coraz więcej firm w ramach szukania oszczędności skłania się ku inwestycjom w nowe technologie obok zatrudniania nowych pracowników fizycznych. Czy monitoring, zdalny nadzór obiektów i szeroko pojęta technologizacja jest przyszłością sektora bezpieczeństwa?

Przed marcem 2020 roku branża security notowała wzrosty rok do roku (według Frost& Sullivan nawet 7-9% rocznie). Jednak pandemia i dynamiczny wzrost nowych technologii diametralnie zmieniły sytuację – w zaledwie pół roku od jej rozpoczęcia aż 77% spółek tego sektora dotknęły poważne cięcia. Zwłaszcza firmy z branży handlowej, transportowej i związane z edukacją ograniczały koszty związane z zabezpieczeniem.

Co więcej, eksperci przewidują, że w najbliższym czasie sytuacja nie tylko nie zmieni się, ale że firmy security będą szukać kolejnych oszczędności. Innymi słowy, niewiele wskazuje na to, że rynek z 2019 roku będzie możliwy do odbudowania. Na popularności zyskują natomiast rozwiązania zdalne oraz pomagające zabezpieczyć pracę zdalną.

Wyzwaniem stały się przede wszystkim rosnące koszty utrzymania firmy i presja płacowa. Oszczędzanie na ochronie i systemach bezpieczeństwa staje się wyjątkowo trudne także z innego powodu. Wraz z rozwojem technologii rośnie zuchwałość sprawców. Dotyczy to nie tylko drobnych kradzieży w sklepach, ale przede wszystkim poważnych zdarzeń, takich jak włamania i przywłaszczenie mienia

w większym zakresie. Istnieje jeszcze inny aspekt, do którego przyczyniła się pandemia: rozwój technologiczny i wysyp nowych narzędzi IT dla branży security.

OCHRONA TECHNICZNA W NOWEJ RZECZYWISTOŚCI

Obserwacja w czasie rzeczywistym, zdalny nadzór obiektów, czy monitoring wideo zapewniają firmom dostęp do informacji o bezpieczeństwie w wygodny i prosty sposób. Jednak technologizacja branży security staje się odpowiedzią także na rosnącą presję płacową.

Aktualnie branża ochrony osób i mienia dotkliwie odczuwa skutki sytuacji gospodarczo-ekonomicznej w Polsce. Galopująca inflacja, czy waloryzacja wynagrodzenia minimalnego wymuszają na firmach zajmujących się bezpieczeństwem zmiany. Przedsiębiorstwa branży security podnoszą stawki za swoje usługi, ale jednocześnie poszukują nowych rozwiązań. **Wśród nich jest przejście od ochrony fizycznej do technicznej.** Jak wskazują badania, ochrona techniczna na koniec 2020 roku uzyskała poziom 40-50% rynku ochrony fizycznej (dla porównania przed 2016 rokiem miała szczątkowy udział w ochronie mienia).

Według prognoz udział ochrony technicznej będzie tylko wzrastał, a już na koniec 2025 roku znacząco przewyższy udział klasycznej ochrony fizycznej. Wśród przyczyn jest między innymi oszczędność finansowa.

Pracownicy ochrony fizycznej to często osoby, które zarabiają najniższą krajową. To powoduje, że nadchodzące wraz z nowym rokiem podwyżki płacy minimalnej mocno uderzą w firmy security. Szacuje się, że w efekcie pracę może stracić nawet 25 tys. osób, zwłaszcza, że rozwój nowych technologii daje coraz większe możliwości wykorzystania rozwiązań smart w branży security.

FIRMY INWESTUJĄ W ROZWIĄZANIA SMART SECURITY

Nowe technologie mają istotny wpływ na całe nasze życie: od pracy i nauki, aż po wsparcie w codziennych czynnościach. Pojawia się więc pytanie, dlaczego w branży security miałoby być inaczej? Tym bardziej, że systemy zdalnego monitoringu sprawdzają się w wielu organizacjach – szczególnie w firmach o regularnych godzinach pracy lub w takich, które nie wymagają obecności fizycznej w da-

nej lokalizacji (na przykład zamknięte place budowy, hurtownie, składy budowlane, magazyny czy salony samochodowe).

To powoduje, że z roku na rok rośnie popularność usług ochrony w postaci monitoringu i zdalnego dozoru obiektów. Firmy decydują się na usługi monitoringu w oparciu, na przykład, o systemy telewizji przemysłowej czy systemy sygnalizacji włamania. Poza rosnącymi wynagrodzeniami tendencja ta jest efektem wzrostu cen za usługi ochrony. Te z kolei wynikają z rosnących kosztów ochrony fizycznej oraz z wprowadzania nowych, tańszych rozwiązań technologicznych. Wydaje się, że inwestycja w rozwój zwiększający potencjał centrum monitorowania staje się nieunikniona dla większości przedsiębiorstw.

W branży security zwrot w kierunku nowych technologii jest szczególnie zauważalny. Po zmianach wywołanych pandemią zwiększyło się zainteresowanie rozwiązaniami technologicznymi jako wsparciem obecności człowieka przy chronionej osobie czy w obiekcie.

Coraz częściej przedsiębiorcy wybierają rozwiązania ze zdalnym nadzorem wideo, zastosowaniem nowoczesnych technologii również w kontroli dostępu, nadzorze wideo czy detekcji ruchu.

Co więcej, zwrot z inwestycji w monitoring może nastąpić zaledwie po kilku miesiącach użytkowania..

SZTUCZNA INTELIGENCJA, CHMURY I DRONY W SŁUŻBIE BRANŻY SECURITY

Nieoceniona w nowoczesnych narzędziach do monitorowania, nadzoru i zapewniania bezpieczeństwa okazuje się być sztuczna inteligencja. Pozwala ona, na przykład, na rozpoznanie ruchomych obiektów, takich jak człowiek, zwierzę czy pojazd. Ponadto umożliwia rozróżnienie fałszywych alarmów, które mogą zostać wywołane przez obiekty, takie jak ruchome gałęzie, liście, zwierzęta, nagłe zmiany poziomu oświetlenia, cienie, opady atmosferyczne i wiele innych.

Jednym z filarów transformacji branży security w stronę nowych technologii jest wykorzystanie rozwiązań chmurowych.

W Polsce jak dotąd narzędzie to nadal traktowane jest przez przedsiębiorców branży ochroniarskiej ostrożnie, choć, jak wskazują prognozy, istnieje duża szansa, że ulegnie to zmianie. Rozwiązania chmurowe doskonale sprawdzą się w komunikacji marketingowej, obsłudze klienta czy jako wsparcie grup i patroli interwencyjnych. To nowoczesne narzędzie umożliwia również zastosowanie automatyzacji żmudnych oraz czasochłonnych procesów, a tym samym oszczędność

czasu. Na szybką i skuteczną weryfikację fałszywych alarmów pozwolą również drony, obsługiwane przez odpowiednio przeszkolony personel. Urządzenia te umożliwiają także sprawne patrolowanie nawet rozległego terenu przy niewielkich kosztach operacyjnych.

Firmy z branży security, które chcą zoptymalizować rozwiązania, z których korzystają, a także przygotować się na wyzwania, jakie niesie przyszłość, już teraz mogą rozważyć zastosowanie innowacyjnych technologii, które pozwolą stworzyć skuteczne systemy zabezpieczenia technicznego.

Przy tym należy pamiętać, że nowe technologie, choć niosą ogromną wartość dla branży security, nie zastąpią w pełni człowieka, który często podejmuje trudne decyzje i odpowiada za działania wedle procedur i przepisów prawa.

Szczególne znaczenie ma to w sytuacjach nagłych, kiedy trzeba na przykład przeprowadzić ewakuację, udzielić pierwszej pomocy, czy też użyć środków przymusu bezpośredniego.

Walutomat®

Wymieniaj walutę online - korzystnie i bezpiecznie 24/7

Największa platforma wymiany walut w Polsce

Korzyści:

- Szybkie i korzystne przelewy zagraniczne **do ponad 50 krajów**
- Przelew natychmiastowy w **EUR - SEPA Instant**
- Szybka wpłata kartą płatniczą, QR kodem, BLIK lub PayPal
- Intuicyjna **aplikacja mobilna**

Dowiedz się więcej na **www.walutomat.pl**

Zeskanuj kod i odbierz rabat

Kupon ważny w terminie 20.09.2022 - 31.01.2023

10 LAT EUROPEJSKIEGO MIESIĄCA CYBER-BEZPIECZEŃSTWA

Katarzyna Koletyńska
PIB-NASK

W tym roku Europejski Miesiąc Cyberbezpieczeństwa obchodził swoje 10. urodziny, a pierwsza edycja odbyła się w 2012 r. Obecnie kampania stanowi integralną część działań krajów Europy mających na celu wdrożenie przepisów unijnego aktu o cyberbezpieczeństwie. Dotyczą one zwiększania świadomości i edukacji.

OCHRONA UNII EUROPEJSKIEJ

Europejski Miesiąc Cyberbezpieczeństwa (ECSM – European Cybersecurity Month), to ogólnoeuropejska kampania organizowana przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z inicjatywy Komisji Europejskiej.

Kampania trwała przez cały październik, a jej celem była popularyzacja wiedzy, zwiększanie świadomości i wymiana dobrych praktyk z zakresu cyberbezpieczeństwa, żeby wyposażyć obywateli w umiejętności, które pomogą im stawić czoła zagrożeniom cyberzagrożeniom. W Polsce koordynatorem kampanii był Państwowy Instytut Badawczy NASK (NASK-PIB).

- *Europejski Miesiąc Cyberbezpieczeństwa to sztandarowy projekt, który stanowi część naszych wysiłków mających ułatwić obywatelom i innym zainteresowanym podmiotom w UE bezpieczne poruszanie się w internecie. Podejmujemy wiele różnych działań mających na celu ochronę UE i potrzebujemy świadomych obywateli, którzy będą stanowić element unii bezpieczeństwa. Tegoroczna kampania pozwoliła każdemu poznać i zrozumieć sposoby chronienia się na co dzień przed nowymi zagrożeniami, takimi jak np. oprogramowanie szantażujące* – powiedział Margaritis Schinas, wiceprzewodniczący Komisji Europejskiej do spraw promowania europejskiego stylu życia.

PHISHING I RANSOMWARE

Jak co roku, kampania koncentrowała się na tematach przewodnich, które są uzgadniane ze wszystkimi państwami członkowskimi. Tegoroczna edycja ECSM skupiona była na dwóch zagrożeniach, na które obecnie najczęściej są narażeni są użytkownicy internetu tj.:

- wyłudzanie informacji (phishing),
- oprogramowanie szantażujące (ransomware).

Do każdego z bloków tematycznych opracowano szereg różnorodnych materiałów zawierających porady i wskazówki, jak się chronić przed tego typu zagrożeniami.

Dodatkowo na stronie znajduje się interaktywna mapa, na której zaznaczone są instytucje i organizacje funkcjonujące w danym kraju, do których można zgłaszać się w sytuacji, kiedy staliśmy się ofiarą cyberprzestępstwa.

Tegoroczna edycja była skierowana szczególnie do osób pracujących w wieku 40-60 lat, ze wszys-

kich sektorów gospodarki, zwłaszcza małych i średnich przedsiębiorstw oraz osób, które w swojej pracy na co dzień wykorzystują nową technologię i narzędzia cyfrowe.

– *Liczbę udanych ataków dokonywanych przez internet można by znacznie zmniejszyć, gdyby więcej osób znało sposoby ich wykrywania oraz odpowiedniego reagowania na nie. Temu właśnie służą działania podejmowane w trakcie Europejskiego Miesiąca Cyberbezpieczeństwa (...). Budowa Europy, w której cyberprzestrzeń jest bezpieczna i godna zaufania, oznacza również pomoc wszystkim przedsiębiorstwom w rozwijaniu działalności w bezpiecznym otoczeniu cyfrowym* – powiedział **Juhan Lepassaar, dyrektor wykonawczy ENISA.**

W ramach kampanii ENISA i państwa członkowskie zorganizowały szereg wydarzeń m.in. konferencje, warsztaty, sesje szkoleniowe, webinaria i quizy.

ECSM W POLSCE

Również w Polsce odbyło się wiele inicjatyw, które miały na celu podniesienie świadomości uczestników w zakresie cyberbezpieczeństwa i cyberhigieny, korzystania z cyfrowych narzędzi oraz umiejętne wykorzystanie wiedzy i doświadczenia w życiu codziennym.

Temu właśnie służy Europejski Miesiąc Cyberbezpieczeństwa – unijna inicjatywa, która doskonale się sprawdziła w ciągu ostatniej dekady. W Polsce w ostatnich trzech latach obserwujemy wzrost zainteresowania kampanią – od 2019 jesteśmy liderem wśród państw członkowskich w liczbie zgłaszanych inicjatyw. Pozwala to wysnuć wniosek, że społeczeństwo staje się coraz bardziej świadome, a co za tym idzie bardziej odporne na zagrożenia w cyberprzestrzeni.

Jak co roku, także i teraz w kampanii uczestniczyły różne podmioty: urzędy, w tym ministerstwa, fundacje, instytuty, firmy, osoby prywatne no i oczywiście szkoły. W ramach kampanii zgłoszono 73 różne inicjatywy, z czego:

- 44 - skierowane do dorosłych użytkowników internetu (ekspertów i specjalistów z zakresu cyberbezpieczeństwa, innych dziedzin powiązanych z nowymi technologiami i innowacjami, pracowników firm, instytucji oraz zainteresowanych),
- 29 – to inicjatywy edukacyjne - skierowane do uczniów i wychowanków szkół i placówek oświatowych (od dzieci w wieku przedszkolnym po uczniów szkół średnich) nauczycieli, edukatorów, a także rodziców

Aktywności, jakie zgłaszali uczestnicy kampanii przybierały różnorodne formy: od konferencji i spotkań z ekspertami, szkoleń, kampanii informacyjnych w mediach społecznościowych po zajęcia edukacyjne, warsztaty, webinary, testy wiedzy.

W ramach kampanii ECSM powstały także różnego rodzaju materiały w postaci podcastów, publikacji, artykułów, infografik, dotyczące bezpiecznego korzystania z internetu i cyberhigieny.

Inicjatywy, w tym większość edukacyjnych, odbywały się stacjonarnie, natomiast te skierowane do dorosłych użytkowników miała w dużej mierze formułę online, co umożliwiło udział w nich większej liczbie uczestników.

Wszystkie informacje o zgłoszonych inicjatywach oraz materiały z tej edycji i poprzednich są dostępne na polskiej stronie kampanii oraz na stronie europejskiej, a także w mediach społecznościowych.

W tym roku polską edycję 10. jubileuszową kampanię Europejskiego Miesiąca Cyberbezpieczeństwa patronatem honorowym objęli:

Fundacja Bezpieczna Cyberprzestrzeń, Komendant Główny Policji, Komisja Nadzoru Finansowego, Krajowy Związek Banków Spółdzielczych, Ministerstwo Edukacji i Nauki, Ośrodek Rozwoju Edukacji, Polskie Towarzystwo Informatyczne, Związek Pracodawców Branży Internetowej IAB Polska.

Honorowy patronat objął - Pełnomocnik rządu ds. Cyberbezpieczeństwa Janusz Cieszyński.

Już teraz zapraszamy do aktywnego udziału w kolejnej edycji kampanii ECSM 2023. Jednocześnie zachęcamy do śledzenia naszych mediów społecznościowych i strony internetowej, bo u nas bezpieczny miesiąc trwa cały rok, bo – „Cyberbezpieczeństwo to nasza wspólna odpowiedzialność."

10 EUROPEJSKI MIESIĄC
lat CYBER BEZPIECZEŃSTWA

PRZEZ TO, ŻE ZESPÓŁ BY FEHU ŁAMIE SCHEMATY, NASZA WIZJA WYPRZEDZA! WIEDZA O SEO, UX, UI, SXO, AI, RWD DAJE NAM PEWNOŚĆ, ŻE STRONY I SKLEPY KTÓRE TWORZYMY, SĄ TECHNOLOGICZNIE ZAAWANSOWANE, ZAUTOMATYZOWANE, GOTOWE DO DZIAŁANIA BY FEHU

MOŻESZ TU ZACZĄĆ

ALARM BOMBOWY W FIRMIE. ZASADY POSTĘPOWANIA

Redakcja
SECURITY MAGAZINE

insp. dr Mariusz Ciarka
Komenda Główna Policji

Policja nie ujawnia szczegółów działań związanych z alarmami bombowymi, bo ma świadomość, że sprawcy zwłaszcza fałszywych alarmów mogliby z takich informacji korzystać. Wie też, że zależy im na nagłaśnianiu ich poczynań. To nie oznacza, że do takich zdarzeń nie dochodzi, zwłaszcza od czasu wybuchu wojny na Ukrainie. Warto więc wiedzieć, jakie są zasady postępowania, kiedy w skrzynce firmowej pojawi się wiadomość, że na terenie przedsiębiorstwa znajduje się bomba.

Alarmy bombowe zdarzają się nie tylko w urzędach miast, sądach, szpitalach, szkołach i uczelniach wyższych. Dotyczą też firm prowadzonych przez prywatne podmioty, w tym głównie supermarketów, stacji paliw, kin, hoteli, przedsiębiorstw produkcyjnych, czy też gigantów bez względu na branżę. Bez względu na to, do jakiego podmiotu wysłany zostanie mail lub SMS o tym, że w jego siedzibie znajduje się ładunek wybuchowy, zasady postępowania są te same.

ZAGROŻENIE TERRORYSTYCZNE

Najczęściej spotykaną formą działań terrorystycznych, zmierzających do wywołania dużego oddźwięku medialnego, a zwłaszcza politycznego jest zamach bombowy, w którym ofiarami są przede wszystkim osoby przypadkowe będące w miejscach powszechnie dostępnych. To miejsca dużych skupisk ludzi, jak np. imprezy masowe, targowiska, dworce, przystanki komunikacyjne, duże sklepy czy środki komunikacji.

Często zdarza się, że zanim nastąpi eksplozja bomby zostanie ona w taki lub inny sposób ujawniona. W związku z takimi sytuacjami specjaliści wprowadzili do użytku termin "incydent bombowy". Właściwe zachowanie w przypadku wystąpienia takiego incydentu jest niezwykle ważne dla prawidłowej reakcji specjalistów z różnych służb i zapobieżeniu ewentualnym skutkom. Przede wszystkim, informacji o zagrożeniu bombowym nie wolno bagatelizować ani lekceważyć.

Zawiadamiając Policję o incydencie bombowym, należy podać informacje:

1. rodzaj zagrożenia i źródło informacji o zagrożeniu (informacja telefoniczna, ujawniony podejrzany przedmiot)
2. treść rozmowy z osobą informującą o podłożeniu ładunku wybuchowego
3. numer telefonu, na który przekazano informację o zagrożeniu oraz dokładny czas jej przyjęcia
4. adres, numer telefonu i nazwisko osoby zgłaszającej
5. opis miejsca i wygląd ujawnionego przedmiotu.

ZASADY POSTĘPOWANIA

Eksperci z Biura Operacji Antyterrorystycznych Komendy Głównej Policji opracowali zasady postępowania w przypadku incydentu bombowego, zwłaszcza, jeżeli jesteś osobą, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego lub ujawniła przedmiot niewiadomego pochodzenia, co do którego istnieje podejrzenie, że może on stanowić zagrożenie dla osób i mienia.

Fakt ten należy zgłosić:

- służbom odpowiedzialnym za bezpieczeństwo w danym miejscu,
- administratorowi terenu, na którym zdarzenie ma miejsce,
- Policji lub Straży Miejskiej.

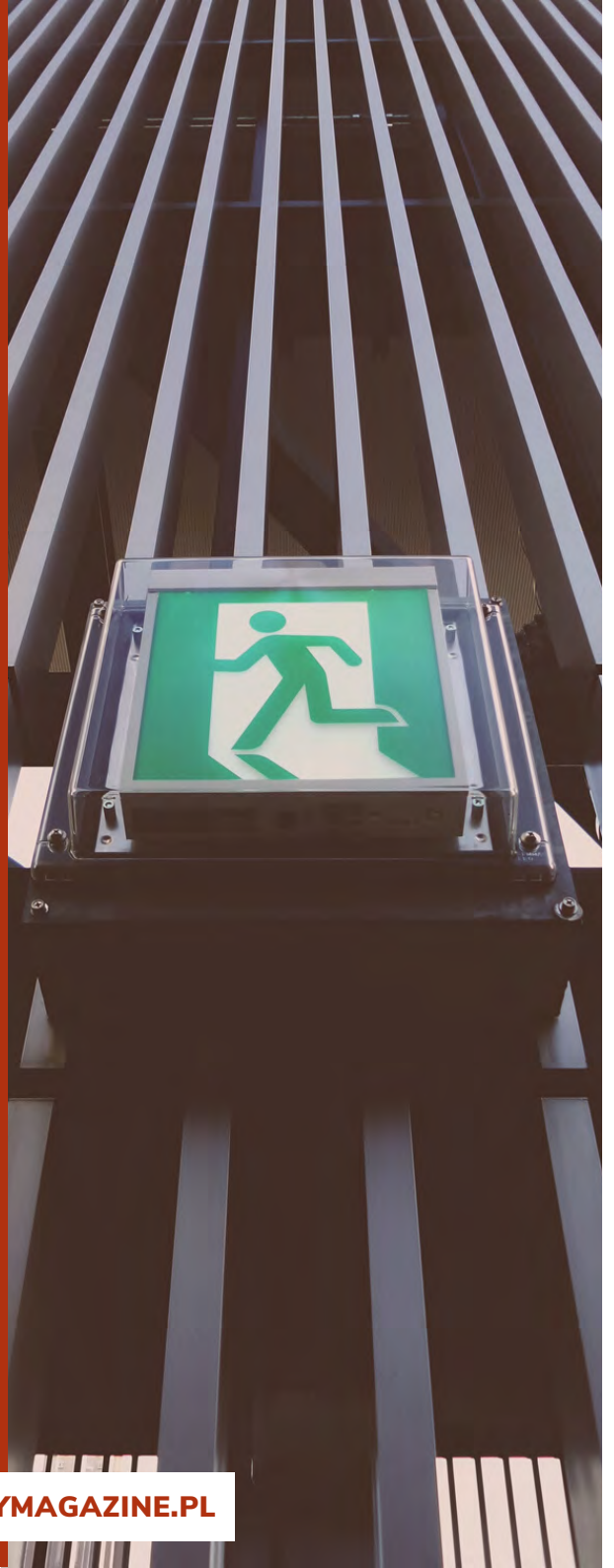
Informacji takiej nie należy przekazywać niepowołanym osobom - jej niekontrolowane rozpowszechnienie może doprowadzić do paniki i utrudnić przeprowadzenie sprawnej ewakuacji.

ODPOWIEDZIALNOŚĆ ADMINISTRATORA

Działania podejmowane przed przybyciem na miejsce służb koordynowane są przez administratorów obiektów, którzy – w wielu przypadkach – prawidłowo szacują ryzyko prowadzenia ewakuacji (na przykład w placówkach medycznych) i uciążliwość dezorganizacji funkcjonowania instytucji spowodowanej odwoływaniem zaplanowanych na dany dzień zadań i obowiązków.

Co powinni zrobić administratorzy budynku po uzyskaniu informacji, że w obiekcie może znajdować się ładunek wybuchowy?

O otrzymaniu zgłoszenia lub odnalezieniu podejrzanego przedmiotu należy niezwłocznie powiadomić Policję. Można dzwonić na numer alarmowy 997 lub 112. Do czasu przybycia na miejsce Policji, administrator obiektu (terenu) lub osoba odpowiadająca za jego bezpieczeństwo kieruje całą akcją.



CO POWINIEN ZROBIĆ ADMINISTRATOR PRZED PRZYBYCIEM SŁUŻB?

1. Jeżeli w informacji o podłożeniu "bomby" nie wskazano konkretnego miejsca, na polecenie kierownika (administratora) obiektu użytkownicy poszczególnych pomieszczeń (pracownicy) powinni sprawdzić swoje miejsca pracy i bezpośrednie otoczenie, pod kątem ujawnienia przedmiotów „podejrzanych” - nieznanego pochodzenia, których dotychczas tam nie było.

2. Na miejsce zagrożenia incydentem bombowym należy wezwać służby pomocnicze, takie jak: pogotowie ratunkowe, straż pożarną, pogotowie gazowe, pogotowie wodno-kanalizacyjne, pogotowie energetyczne.

3. Pomieszczenia ogólnodostępne (korytarze, klatki schodowe, windy, toalety, piwnice, pomieszczenia gospodarcze, strychy) oraz najbliższe otoczenie zewnętrzne obiektu, sprawdzają osoby wyznaczone przez administratora obiektu lub służby ochrony odpowiedzialne za bezpieczeństwo w danego podmiotu.

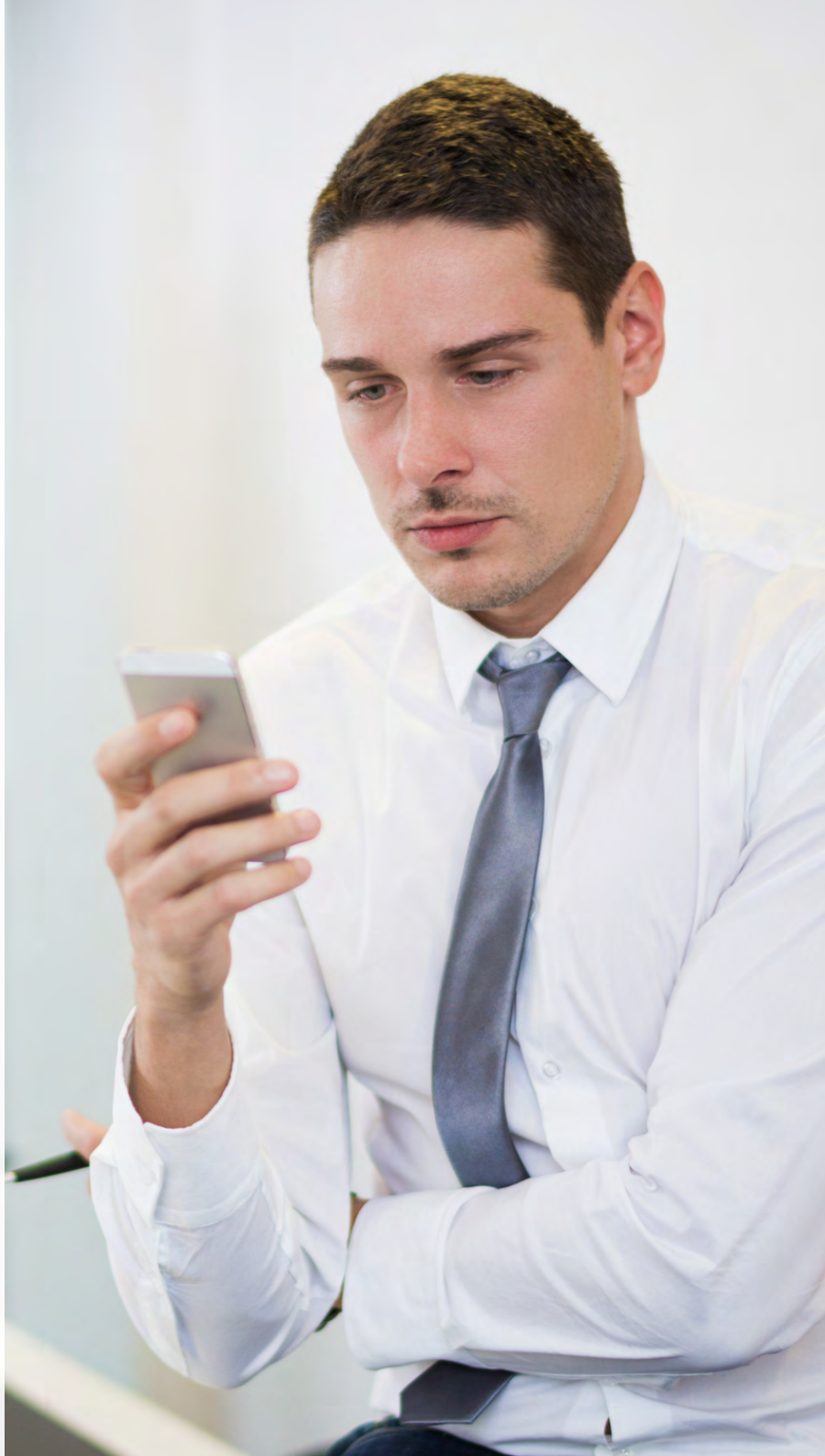
4. W przypadku ujawnienia podejrzanego przedmiotu nie należy zbliżać się bezpośrednio do niego ani dotykać go. Natychmiast informację o odnalezieniu przedmiotu przekazać trzeba administratorowi obiektu lub osobom (służbom) odpowiadającym za bezpieczeństwo na tym terenie. Należy dążyć do ustalenia ewentualnego właściciela ujawnionego przedmiotu.

5 Administrator może ogłosić ewakuację z budynku. Jeśli tak zdecyduje, należy zachować spokój, sprawnie opuszczać wskazany teren, zabierając rzeczy osobiste. Jeśli o ewakuacji nie zdecyduje, to warto wiedzieć, że dla każdego zgłoszenia powstaje m. in. specjalna rekomendacja funkcjonariuszy Centralnego Biura Śledczego, którzy określają, czy konieczne będzie przygotowanie ewakuacji osób znajdujących się w miejscu zagrożonym.

Po przybyciu Policji na miejsce incydentu bombowego przejmuje ona dalsze kierowanie akcją.

Administrator, zawiadamiając Policję o informacji z możliwością podłożenia „bomby" powinien podać następujące dane:

- rodzaj wskazanego w otrzymanym zgłoszeniu zagrożenia (na przykład „ma wybuchnąć bomba"),
- źródło informacji o zagrożeniu (informacja telefoniczna, ujawnienie podejrzanego przedmiotu – na przykład pozostawionej walizki),
- w przypadku zgłoszenia telefonicznego o podłożeniu „bomby" treść rozmowy ze zgłaszającym, w przypadku informacji otrzymanej drogą elektroniczną – treść komunikatu,
- numer telefonu, na który przekazano informację o zagrożeniu oraz dokładny czas jej przyjęcia lub adres mailowy (pocztowy) na który wpłynął komunikat,
- w przypadku odnalezienia niepokojącego przedmiotu - opis miejsca jego odnalezionego oraz opis przedmiotu, adres, numer telefonu i nazwisko osoby przekazującej otrzymaną informację.



Dyżurny Policji, potwierdzając przyjęcie zgłoszenia, może pozostawać w kontakcie z przedstawicielem instytucji przekazującym zgłoszenie, aby poinformować o tym, jaka rekomendacja funkcjonariusza Centralnego Biura Śledczego została wydana w zakresie przeprowadzania ewakuacji. Identyfikacją zagrożenia związanego z odnalezieniem podejrzanego przedmiotu oraz jego ewentualną neutralizacją zajmują się wyłącznie wyspecjalizowane jednostki Policji.

FAŁSZYWE ALARMY. KONSEKWENCJE

W większości alarmy bombowe - incydenty bombowe - okazują się fałszywe. - *Kodeks karny zabrania takich zachowań. Kto wiedząc, że zagrożenie nie istnieje, zawiadamia o zdarzeniu, które zagraża życiu lub zdrowiu wielu osób podlega karze pozbawienia wolności od 6 miesięcy do lat 8 lat* - przypomina **insp. Mariusz Ciarka, rzecznik prasowy Komendanta Głównego Policji,** dodając, że anonimowy telefon o podłożeniu ładunków wybuchowych uruchamia całą lawinę działań Policji oraz innych służb zaangażowanych w zabezpieczenie miejsca rzekomego podłożenia ładunku.

To również koszty dla podmiotów - firm oraz instytucji - które na czas trwania działań służb muszą m.in. przerwać pracę i zapewnić bezpieczeństwo osobom przebywającym w budynku. Takimi kosztami są najczęściej zakłócenia normalnego toku pracy (odwołanie odlotów, wyjazdów, produkcji), utrudnienia w załatwieniu codziennych spraw (zamknięcie urzędu czy firmy, wyproszenie interesantów czy klientów, odwoływanie spotkań, wydarzeń, które często poprzedzone są długą organizacją i zainwestowanymi środkami). Nie mówiąc o zainteresowaniu mediów sprawą, które niejednokrotnie generuje kryzysy wizerunkowe.

Dobra informacja jest jednak taka, że autorzy takich żartów są jednak ustalani i pociągani do odpowiedzialności karnej.

- Pamiętajmy, że oprócz odpowiedzialności karnej, takie osoby muszą się liczyć także z odpowiedzialnością cywilnoprawną, możliwością obciążenia kosztami przeprowadzonej akcji, czy np. odszkodowaniami za straty spowodowane wstrzymaniem działalności danej instytucji - przypomina **insp. Mariusz Ciarka.**


home.pl
TYLKO DLA CZYTELNIKÓW SECURITY MAGAZINE
Najlepszy Hosting PrestaShop dla Twojego e-sklepu
SSD
Do 8x szybsze ładowanie sklepu internetowego*
Hosting specjalnie dopasowany do PrestaShop
Szybkie dyski SSD NVMe
Wydajne procesory AMD EPYC
Zamów hosting specjalnie dopasowany do oprogramowania PrestaShop **30% taniej** z kodem rabatowym: **SM30**
Pośpiesz się! Liczba hostingów objętych promocją z kodem rabatowym: 30
Odbierz rabat na Hosting PrestaShop
*W stosunku do poprzedniej (działającej do 7.11.2022 r.) wersji infrastruktury usługi Hosting PrestaShop w home.pl

ZAGROŻENIA DLA E-SKLEPÓW OPARTYCH NA LICENCJI OPEN SOURCE

Rafał Jakacki
home.pl

PrestaShop i WooCommerce to w Polsce anno Domini 2022 najpopularniejsze rozwiązania typu open source dla sklepów internetowych. Ułatwiają życie sprzedawcom i pozwalają elastycznie rozwijać e-biznes niezależnie od branży. Warto mieć na uwadze kwestie bezpieczeństwa tych rozwiązań technologicznych. Czy do takiego sklepu cyberprzestępca może wejść tylnymi drzwiami, w łatwy sposób? Jak zabezpieczyć się przed zagrożeniem?

W świecie technologii obserwujemy próbę upraszczania wielu procesów. Tak samo jest w dziedzinie tworzenia witryn internetowych.

Niegdyś serwisy www były tworzone w żmudny sposób, odręcznie. Pisano je właściwie linijka po linijce. Mało zautomatyzowane procesy powodowały ryzyko wielu ludzkich błędów i to zarówno z zakresu stabilności, jak i bezpieczeństwa takich witryn. Z czasem to się zmieniło.

Na początku 2000 roku świat technologii zaczął interesować się systemami zarządzania treścią, czyli CMS-ami (ang. Content Management System) na licencji open source. Twórcy takiego oprogramowania założyli, że każdy może ingerować w kod źródłowy technologii i dostosowywać ją do swoich potrzeb, otrzymując jednocześnie solidne podstawy dla własnej strony internetowej. Z założenia CMS-y stały się więc mocno otwarte na społeczność, która wspólnie mogła przyczyniać się do ich rozwoju. Było to strzałem w dziesiątkę i już na zawsze odmieniło sposób tworzenia stron internetowych i zarządzania witrynami.

SYSTEMY ZARZĄDZANIA TREŚCIĄ WYWRACAJĄ ŚWIAT IT DO GÓRY NOGAMI

W 2002 roku pojawia się pierwsze wydanie słynnego WordPressa, najpopularniejszego dziś systemu zarządzania treścią dla witryn internetowych na świecie. Niedługo później, bo w 2005 roku dołącza do niego Joomla. Z biegiem czasu pojawi się jeszcze co najmniej kilkadziesiąt ciekawych silników witryn opartych na podobnych założeniach. Tymi założeniami są usprawnienie procesu tworzenia witryny oraz łatwiejsze zarządzanie jej treścią.

Początkowo CMS-y służyły do tworzenia prostych i dynamicznych stron internetowych, takich jak blogi. Większość ludzi borykała się z problemem niedostatecznej wiedzy i umiejętności potrzebnych do stworzenia własnej witryny.

Blog o ulubionym hobby? Strona dla pasjonatów elektroniki? Na początku XXI wieku nie było to takie proste. Systemy CMS odpowiedziały więc na palącą potrzebę i zyskały dużą popularność. Pozwalały przeciętnemu użytkownikowi stworzyć własną stronę, wywołując swoją drogą niemałą frustrację u web developerów, którzy w dużej mierze potrakto-

wali to rozwiązanie jako konkurencyjne dla ich dotychczasowego sposobu tworzenia stron.

Systemy CMS oparte na open source rozwijały się przez kolejne lata i oferowały coraz ciekawsze automatyzacje i funkcje. Z czasem najsłynniejszy z nich, **WordPress**, zaczął być wykorzystywany również dla stron typowo wizytówkowych, niekoniecznie mających być blogami. Pozwoliła na to **baza dodatków, zwanych wtyczkami**. Dzięki nim pojawiły się możliwości dodania interaktywnego kalendarza, galerii zdjęć czy systemu rejestracji.

E-COMMERCE TEŻ CHCE MIEĆ Z GÓRKI. DEBIUT CMS-A DLA HANDLOWCÓW

Internetowi sprzedawcy bacznie obserwowali rozwój rozwiązań typu open source. Szybko dostrzegli, że intuicyjny silnik do tworzenia witryny i zarządzania nią może świetnie przysłużyć się sklepom internetowym. Do tej pory utworzenie e-sklepu wiązało się z ogromnymi kosztami – konieczne było kodowanie specyficznych rozwiązań sklepowych z uwzględnieniem tak istotnych kwestii jak płatności czy koszyk zakupowy. W tamtych czasach, gdy płatności online dopiero raczkowały, było to wyjątkowo wymagające i żmudne, a sama wizja, że właściciel

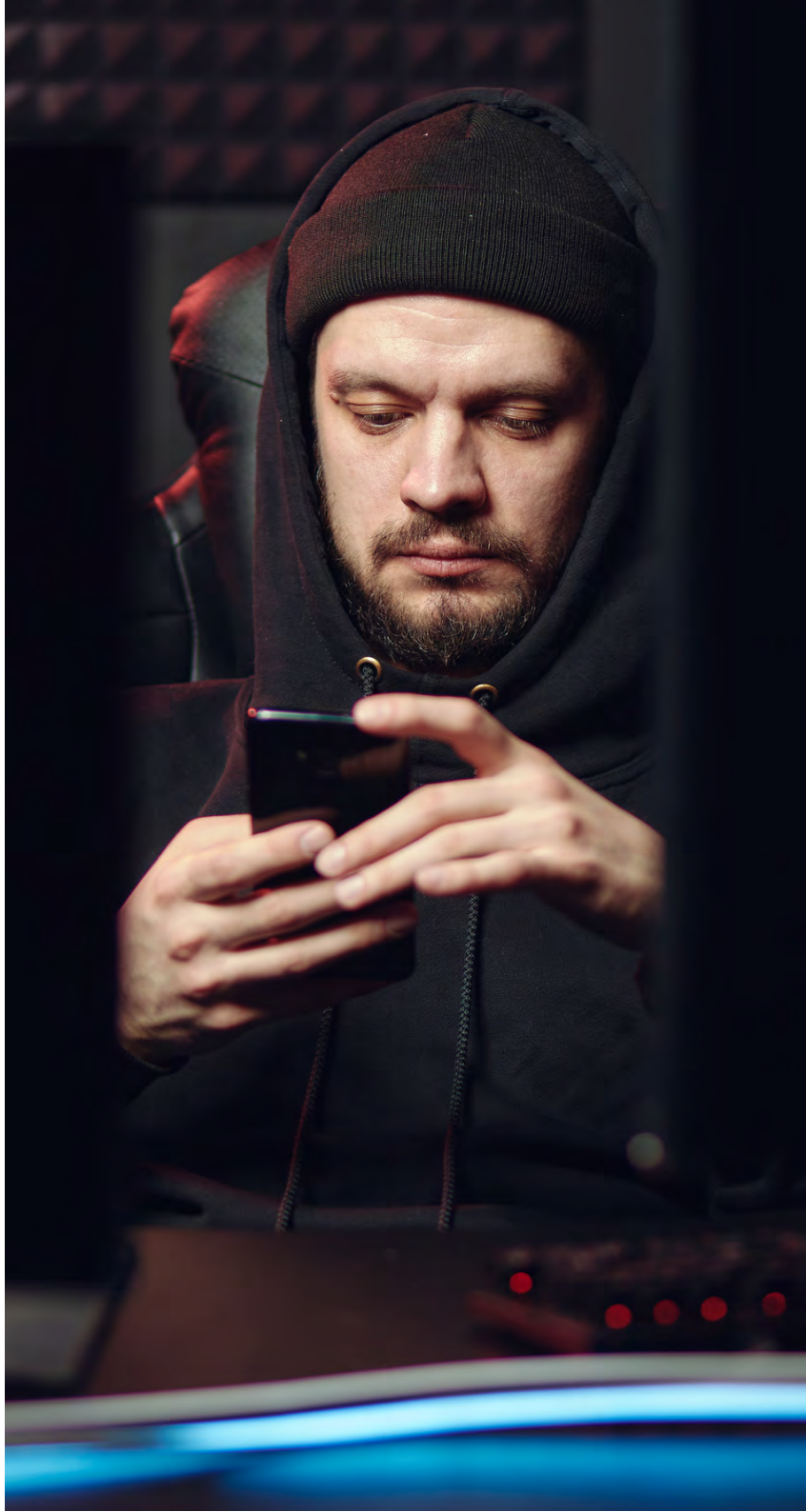
e-sklepu mógłby zarządzać zamówieniami z poziomu intuicyjnego panelu sklepowego w swoim komputerze, była niczym marzenie.

Głównie dzięki takiemu marzeniu zadebiutował w 2007 roku PrestaShop rozwijany do tej pory. W pierwszych latach istnienia oferował on wszystkie najważniejsze funkcje pozwalające intuicyjnie utworzyć swój sklep internetowy i zarządzać nim w sieci. Nie zapominajmy też o wspomnianym wcześniej WordPressie. To jego topowa pozycja wśród oprogramowania open source sprawiła, że społeczność użytkowników utworzyła wtyczkę WooCommerce – obecnie najpopularniejszy system sklepu internetowego na świecie.

W 2022 roku, według statystyk BuiltWith, PrestaShop i WooCommerce są najpopularniejszymi silnikami open source dla sklepów internetowych w Polsce. Łącznie z ich wykorzystaniem działa w naszym kraju ponad 40 tysięcy e-biznesów.

DLACZEGO STRONY I SKLEPY WYKORZYSTUJĄCE OPEN SOURCE INTERESUJĄ CYBERPRZESTĘPCÓW?

Wszystkie CMS-y oparte na open source mają wspólny mianownik. Łączy je sposób, w jaki są rozwijane poprzez społeczność z całego świata. Deweloperzy dodają własne wtyczki i motywy do ogólnodostępnego repozytorium, z którego mogą korzystać inni użytkownicy. Na takich dodatkach opiera się większość funkcjonalności i struktura blogów, sklepów i innych stron. Jest to nieocenioną zaletą CMS-ów, ale ma też swoją ciemną stronę. Wtyczki i motywy nie zawsze są



bez wad. Bardzo często włamania na strony internetowe odbywają się przy wykorzystaniu ich luk bezpieczeństwa.

Biorąc pod uwagę, że łącznie w Polsce jest ponad **pół miliona stron** CMS, skala zagrożenia wydaje się naprawdę istotna. Jeśli przestępca potrafi zidentyfikować lukę bezpieczeństwa we wtyczce, np. wykorzystywanej przez sklep internetowy, to kolejnym krokiem jest jego umyślne działanie w celu wyrządzenia szkody. Najczęściej jest to przejęcie dostępu nad sklepem. To już furtka do pozyskania częściowo zakodowanych poświadczeń z bazy danych – loginów czy haseł. **Często przestępcy wstrzykują własny złośliwy kod lub ustawiają przekierowania**, aby nieświadomy użytkownik skorzystał z linków dających przestępcom zysk.
W tym czasie swój obrót traci oczywiście prawowity właściciel sklepu internetowego lub strony.

W przypadku CMS-ów o charakterze blogowym atak objawia się często w ten sposób, że w ramach strony masowo publikowane są spamerskie artykuły, wyrządzające duże szkody dla SEO danej witryny. Przestępca może nawet pójść krok dalej i zaprojektować atak phishingowy. Powstanie wtedy bliźniaczo podobny do oryginalnego serwis z fałszywą stroną logowania, mający na celu wyłudzanie danych klientów.

W przypadku dużych e-commerce'ów, magazynów blogowych czy stron znanych firm, znane są przypadki, że przestępcy żądają okupu za odzyskanie strony internetowej. I nie zdarza się to rzadko, co potwierdzają liczne raporty firm badających bezpieczeństwo w sieci.

AKTUALIZACJE: CZY TO KONIECZNE?

Ze statystyk wiemy, że piętą achillesową CMS-ów w zakresie cybersecurity są wspomniane wtyczki, motywy i dodatki, które możemy doinstalować do swojej strony. Więc niezależnie, czy mowa o CMS WordPress, czy PrestaShop – wszystkie wymagają od użytkownika, by dbał o aktualizacje. Mówimy tu o aktualizacji silników stron, ale również wtyczek oraz motywów. Niestety, zdarza się, że właściciele stron internetowych nawet nie mają pełnego dostępu do kokpitów administracyjnych swoich stron. Najczęściej wynika to z tego, że stronę tworzył im zewnętrzny specjalista, który po zakończeniu prac tymi dostępami się nie podzielił.

Z drugiej strony są także użytkownicy, którzy mają dostępy, ale w ogóle nie wchodzą w swój panel administracyjny.

Bywa tak, że w momencie publikacji wersja premierowa strony działa świetnie. Często z upływem czasu okazuje się, że zaczynają się z nią dziać niepokojące rzeczy.

Pojawiają się dziwne fragmenty tekstu, przekierowania na niebezpieczne zewnętrzne witryny, a strona zaczyna długo się ładować. To wszystko wynika często z wprowadzenia złośliwego kodu przez osobę o złych zamiarach. Zdarza się, że cyberprzestępca nie musi się nawet za specjalnie starać, bo wykrywa luki w nieaktualnej wersji wspomnianych już wtyczek czy motywów.

Aby zapobiec takim sytuacjom twórcy tych dodatków publikują regularne aktualizacje.

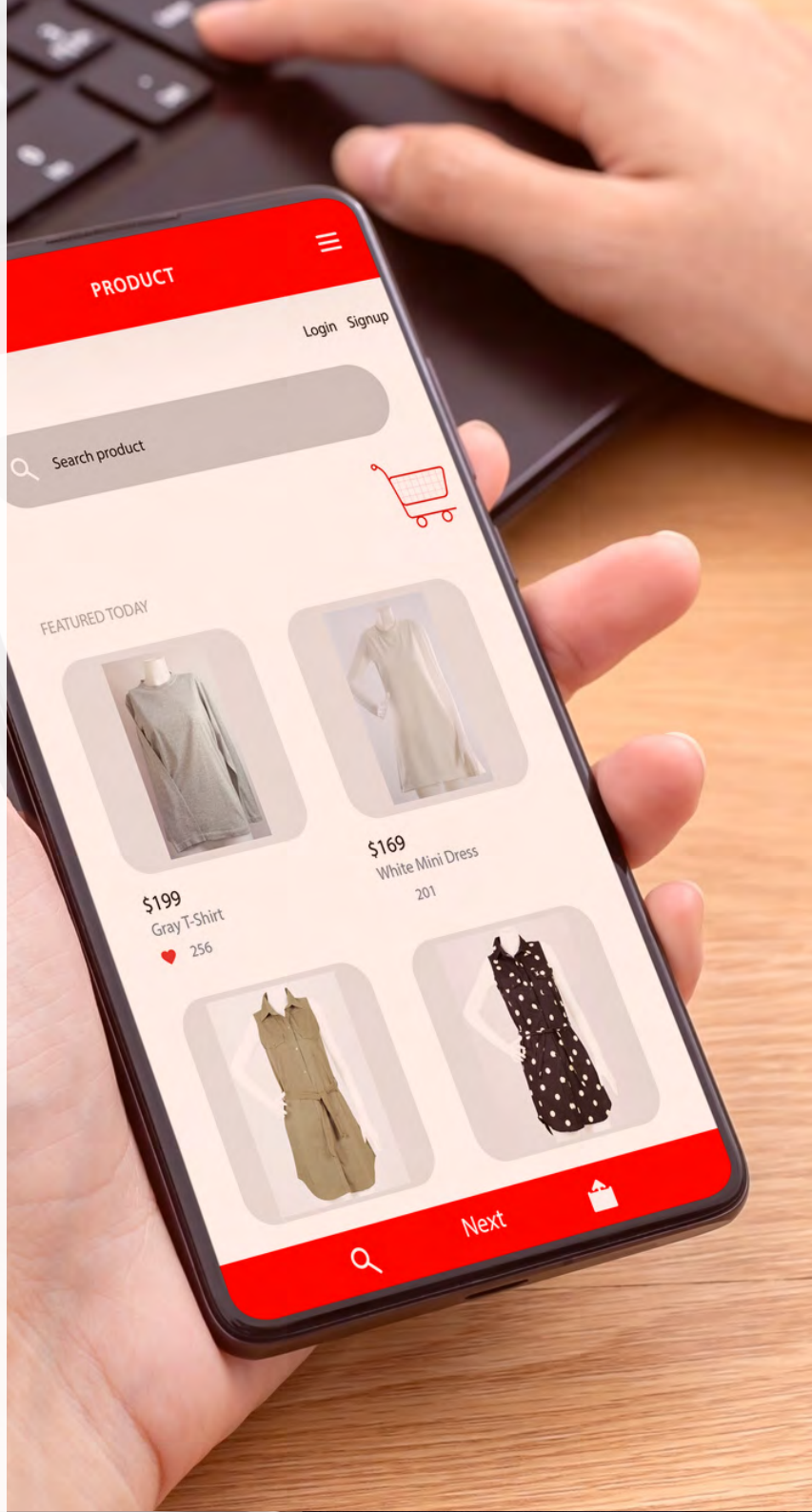
To dlatego co jakiś czas na łamach serwisów technologicznych pojawiają się alerty z prośbą o przeprowadzenie aktualizacji wtyczki. Wniosek jest taki, że jeśli współpracujemy z osobą oddelegowaną do opieki nad witryną, powinniśmy upewnić się, czy takie aktualizacje są przez nią dokonywane. Jeśli sami sprawujemy pieczę nad swoim e-biznesem, starajmy się, aby nie zapominać o kokpicie administracyjnym w dniu premier aktualizacji wtyczek. Zaglądajmy na zaplecze swojego e-commercu lub bloga regularnie oraz obserwujmy, czy pojawiają się nowe aktualizacje.

CZY AUTOMATYCZNE AKTUALIZACJE SĄ BEZPIECZNE?

Trend niestety jest, jaki jest – duża część użytkowników nie zagląda do kokpitu administracyjnego witryny, gdy ta jest już opublikowana. Dlatego twórcy i społeczność starają się zachęcać do regularnych odwiedzin panelu poprzez różne kanały komunikacji, od artykułów po maile. Jednak, ponieważ nie jest to zbyt skuteczne, wprowadzono dość kontrowersyjną funkcjonalność, jaką jest automatyczna aktualizacja. Oznacza to, że open source i elementy, z których w ramach niego korzystamy, mogą aktualizować się automatycznie, gdy tylko wykryją nowszą wersję oprogramowania. Czy to rozwiązało problem bezpieczeństwa? I tak, i nie.

Faktycznie twórcom zależy na tym, aby użytkownicy korzystali z najnowszych wersji ich narzędzi. Ale wciąż pojawia się ryzyko, że jakaś aktualizacja zostanie wypuszczona z błędami. Nie są to tak częste sytuacje, jak włamania poprzez stare wersje wtyczek, ale ryzyko istnieje. Z reguły, w przypadku wypuszczenia aktualizacji z błędami, pojawia się pilny komunikat na stronie twórców dodatku. Czym prędzej wdrażana jest również przez nich kolejna iteracja aktualizacji, tak zwany „hotfix". Ma ona na celu pilną poprawę krytycznych błędów ostatniej wersji oprogramowania.

Co zatem robić? Najlepiej jednak zaglądać do kokpitu CMS-a, przeprowadzać ręczną aktualizację wtyczki i sprawdzać, czy po aktualizacji wszystko w serwisie działa jak należy.



OPEN SOURCE? TAK, ALE DBAJMY O AKTUALNOŚĆ DODATKÓW

Ogólnodostępne dodatki do CMS-ów open source są przydatne, ale miewają luki bezpieczeństwa. Ich ręczne aktualizacje pomogą zapobiegać awariom i atakom, ale pamiętajmy też, że w systemie możemy mieć zainstalowane nieaktualne i nieużywane wtyczki. Warto profilaktycznie co jakiś czas najzwyczajniej usuwać je z aplikacji.

Unikajmy też pluginów wysyłanych przez email czy hostowanych w darmowych serwisach z plikami – nie przechodzą one żadnej weryfikacji i nie podlegają kontroli. Aktualizujmy dodatki – najlepiej ręcznie, aby nasze strony i e-biznes nie były narażone na niepotrzebne niebezpieczeństwo.

Rzetelny® Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

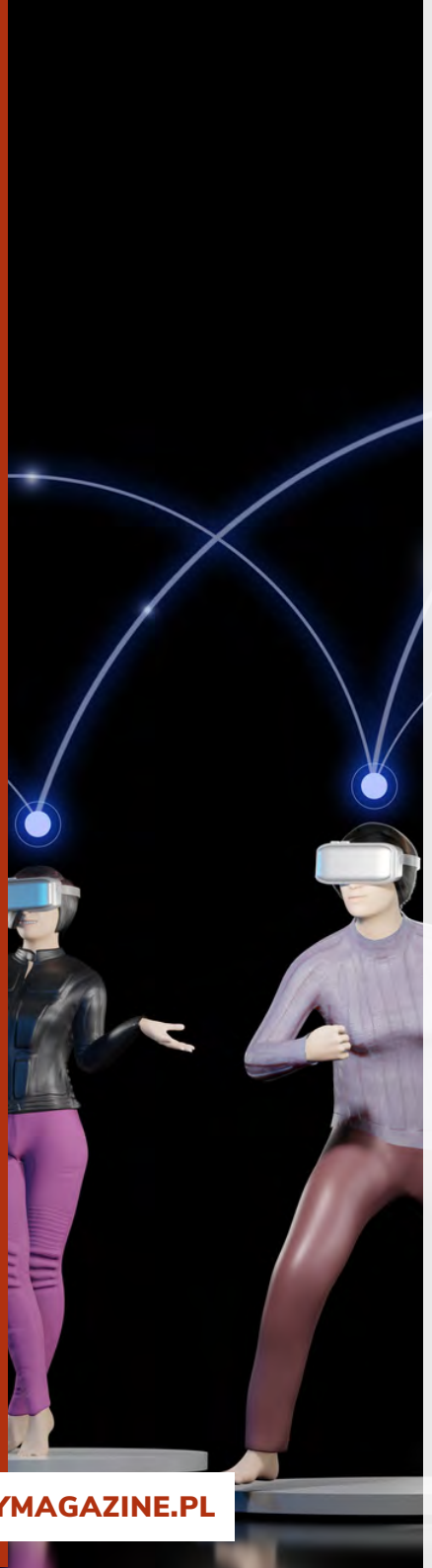
SECURITYMAGAZINE.PL

METAVERSE A BEZPIECZEŃSTWO

Redakcja
SECURITY MAGAZINE

we współpracy z
EPIC VR

Z szacunków wynika, że przestrzeń „Metaverse” do 2030 roku może być warta nawet 13 bilionów dolarów. Zdaniem wielu - ten wirtualny świat stanie się przyszłością i nieodłącznym elementem biznesu. Należy jednak pamiętać, że jak zawsze kluczowe dla nich powinny być względy bezpieczeństwa. Czy można uniknąć pułapek związanych z nową, wirtualną rzeczywistością?



POTENCJAŁ METAVERSE

Jak twierdzi Marty Resnick, wiceprezes ds. badań w Gartnerze, do 2026 roku 30 procent światowych organizacji będzie dysponować produktami i usługami gotowymi na meta-przestrzeń. Jako przykłady wymienia m.in. kupowanie cyfrowej ziemi oraz budowanie wirtualnych domów.

Nie trudno domyślić się, że jeśli w metaverse, do którego będziemy wchodzić przy pomocy gogli VR-owych, pojawią się użytkownicy, to w ślad za nimi pójdą duże marki, które będą chciały im coś sprzedać. Już teraz w świecie tym swoje produkty i usługi oferują choćby firmy takie jak Gucci, Coca Cola czy Nike. Potencjałem metaverse interesują się też bardziej tradycyjne branże jak np. przemysł samochodowy i budowlany.

Sama Meta nie ukrywa, że ma zamiar, zarabiać na swoim pomyśle tworząc, na przykład wirtualne sklepy służące sprzedaży produktów sponsorowanych. W osiągnięciu jak najlepszych rezultatów ma pomóc m.in. śledzenie pozycji ciała i wyrazu twarzy użytkowników po to, by przesyłać do nich jak najtrafniej dostosowane reklamy i treści marketingowe. Wniosek jest jeden: metaverse wydaje się zbyt dużym potencjałem i rynkiem, żeby firmy mogły go zignorować.

W metaprzestrzeni ludzi reprezentują ich awatary, które w zamyśle mają spędzać czas tak jak my: pracować, spotykać się z rodziną i przyjaciółmi oraz korzystać z różnego rodzaju atrakcji, a także kupować i sprzedawać.

Mark Zuckerberg zgodnie ze swoją wizją chce przenieść internet i sposób, w jaki się komunikujemy na znacznie wyższy poziom. Nie będzie to klikanie przy użyciu palców na ekranie telefonu czy komputera, a fizyczne uczestniczenie w wirtualnych rozrywkach, spotkaniach, pokazach i w zasadzie w wielu różnych aktywnościach znanych nam ze świata realnego. Za pośrednictwem wirtualnej rzeczywistości będziemy wykonywać codzienne czynności (powoli już wykonujemy), w tym kupować, co zresztą już ma miejsce.

I jeśli w świecie realnym oraz w sieci musimy niemal na każdym kroku dbać o bezpieczeństwo, dlaczego nie rozpocząć publicznej debaty o ochronie w przestrzeni wirtualnej już teraz?

Choć metaverse nie jest jeszcze naszą codziennością, to, jak wyjaśnia **Lewis Duke, Senior Security Engineer w Trend Micro**, dużo czasu zajęło ludziom zrozumienie plików cookie.

"Dopiero teraz, w ciągu ostatnich lat naprawdę pojawiły się przepisy dotyczące zarządzania tym, w jaki sposób użytkownicy są informowani o wykorzystywaniu ich danych" - zaznaczył Duke w rozmowie z redakcją ZDNET.

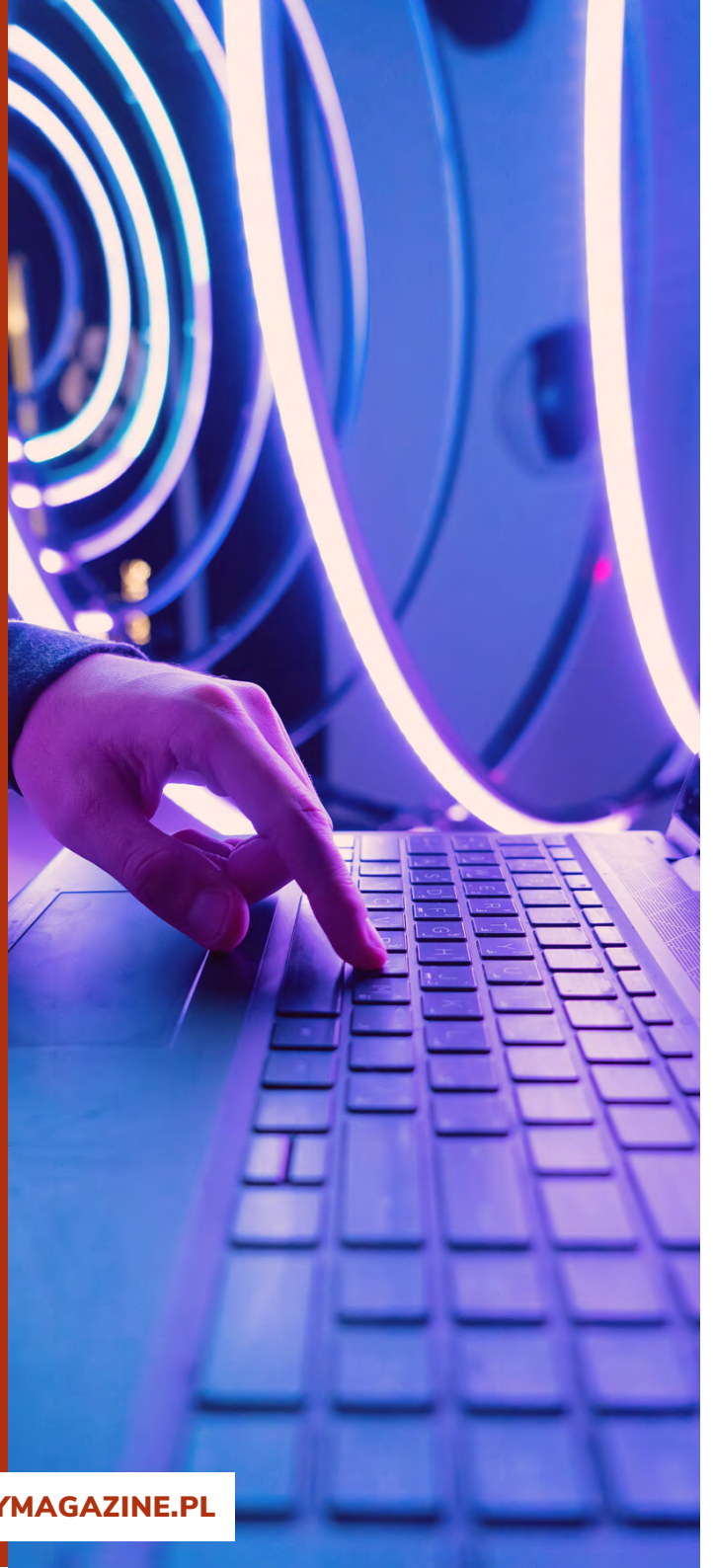
PRAWO A BEZPIECZEŃSTWO W METAVERSE

Problem również w tym, że prawodawstwo ma tendencję do powolnego reagowania na postęp technologiczny. A to oznacza, że zanim zasady i przepisy dotyczące metaverse zostaną wprowadzone, może być już za późno – wystarczy spojrzeć, w jakim tempie wprowadzane czy aktualizowane są przepisy dotyczące cyberbezpieczeństwa czy prywatności w Internecie rzeczy. Metaverse może mieć ten sam problem.

A przecież metawersum daje cyberprzestępcom nieograniczone możliwości. Niestety, do tej pory niewiele instytucji skupia się na tym, jakie zagrożenia cybernetyczne oraz kłopoty z prywatnością może zawierać ten nowy wirtualny wszechświat. Powinny być one analizowane już na etapie tworzenia się tej zupełnie nowej przestrzeni.

Tymczasem eksperci biją na alarm: metaverse może być obszarem praktycznie nieuregulowanym. Co to znaczy? Brak nadzoru ze strony instytucji oznacza również brak mechanizmów ochronnych dla potencjalnych ofiar przestępstw. Nowość tej przestrzeni wiąże się też z tym, iż ludzie nie wiedzą jeszcze dokładnie, jak się w niej poruszać i funkcjonować.

W styczniu tego roku firma Gartner chciała sprawdzić, jaką wiedzę na temat metaverse mają konsumenci. W tym celu skontaktowała się z ponad 300 osobami. 70 procent bada-



nych nie potrafiło wówczas powiedzieć, czym jest metaprzestrzeń. Zaledwie niecałe 30 procent pytanych rozumiała to pojęcie, a tylko 6 procent osób uważało, że zna je na tyle dobrze, aby być w stanie wytłumaczyć innym.

Znany na całym świecie wydawca serwisów związanych z technologiami - **TechTarget** - spróbował uporządkować to, na czym należy się skupić, wdrażając cyberbezpieczeństwo w metaverse.

Mamy zatem trzy elementy cyberbezpieczeństwa w metaverse:

- cyberbezpieczeństwo platformy hostingowej,
- cyberbezpieczeństwo cyfrowej przestrzeni,
- cyberbezpieczeństwo użytkowników wchodzących w interakcje wewnątrz przestrzeni cyfrowej.

1. Właściciele platform

Najwięksi giganci technologiczni inwestują w budowę platform metaverse, ale przez brak regulacji - praktyki w zakresie bezpieczeństwa i prywatności są niespójne. Prowadzi to m.in. do niespójnego UX.

2. Właściciele/najemcy VR

Użytkownicy wirtualnych nieruchomości to klienci, partnerzy i goście. W wielu przypadkach właściciele/najemcy nieruchomości są również nowicjuszami, tworząc atmosferę, w której brakuje najlepszych praktyk w zakresie cyberbezpieczeństwa

i prywatności, są one błędnie interpretowane, błędnie przedstawiane lub po prostu ignorowane.

Tymczasem właściciele VR powinni poświęcić czas na zrozumienie bezpieczeństwa i prywatności platformy, na której są hostowani, zbadać usługi, które budują czy używają na platformie, oraz podjąć kroki w celu zapewnienia bezpieczeństwa i prywatności tych usług.

Ważne jest, aby właściciele nieruchomości rozumieli, jakie dane użytkowników są gromadzone przez dostawcę platformy, a następnie nakładali na to dane użytkowników, które zbierają. Następnie muszą podać – w formie zrozumiałej dla użytkownika – czym są te dane, dlaczego są gromadzone oraz jakie prawa do danych mają ich klienci.

3. Konsumenci/użytkownicy

Korzystanie z zestawów słuchawkowych wyposażonych w czujniki i moduły śledzące w celu zapewnienia wciągających wrażeń może spowodować, że konsumenci nie będą zdawać sobie sprawy ani zwracać uwagi na to, w jaki sposób i ile ich danych osobowych jest gromadzonych. Konsumenci są zagrożeni, ponieważ w przeciwieństwie do prawdziwego świata, który ma akty o ochronie prywatności danych wzmacniające konsumentów, takie jak RODO i CCPA, nie ma takiego odpowiednika w metaverse.

Brak procesów weryfikacji poświadczeń, szczególnie w przypadku manifestacji awatarów, naraża konsumentów na ryzyko. Deepfake'i stają się coraz bardziej powszechne w filmach, podobnie jak podszywanie się pod osoby podczas połączeń konferencyjnych. Metaverse stanowi jeszcze większe wyzwanie.

Ponadto prawa komunikacyjne różnią się w zależności od platformy metaverse. W światach AR prawa do komunikacji obejmują interakcje fizyczne-wirtualne, a także interakcje między wirtualnymi.

W świecie VR wszystkie interakcje są wirtualne. W związku z tym, użytkownicy muszą zrozumieć zabezpieczenia i prywatności stosowane przez dostawcę platformy i właściciela metaprzestrzeni. Konsument musi zadawać pytania dostawcy platformy i właścicielowi VR: Jakie dane są gromadzone? Jak długo będą przechowywane? Jak je usunąć?

Mark Zuckerberg w ubiegłym roku poinformował, że budowa platformy, jaką stanie się metaverse,

może zająć nawet kilka lat i będzie wymagać wdrożenia w życie wielu nowoczesnych i przełomowych technologii. Samo stworzenie metaprzestrzeni to niesamowicie trudne i ambitne zadanie, przed którym stoi wiele wyzwań o charakterze nie tylko technologicznym, ale też prawnym, etycznym i filozoficznym. Nie ulega wątpliwości, że sam projekt budzi sporo kontrowersji.

BEZPIECZEŃSTWO NA PIERWSZYM MIEJSCU

Tymczasem przedsiębiorstwa w metaverse widzą szansę na rozwój swoich biznesów, a tym samym na zwiększenie zysków. Należy pamiętać jednak, że jak zawsze kluczowe dla nich powinny być względy bezpieczeństwa. W przeszłości, kiedy ludzie po raz pierwszy zetknęli się z internetem i nie wiedzieli, co kryje się za tą technologią - wykorzystywali to cyberprzestępcy, tworząc np. fałszywe witryny udające banki w celu wyłudzenia danych finansowych i personalnych. Tego typu oszustwa nadal są powszechne.

Z danych firmy Check Point, która zajmuje się cyberbezpieczeństwem, wynika, że tylko w 2021 roku odnotowano 50-procentowy wzrost ogólnej liczby tygodniowych ataków na sieci korporacyjne w porównaniu z rokiem poprzednim.

Jak sytuacja będzie wyglądać w przypadku metaverse? Jeśli przyjmiemy, że jest to nowa przestrzeń - zapewne jej nieznajomość również będzie starano się wykorzystać.

Już dziś firmy wykorzystują różnego rodzaju zabezpieczenia - chociażby po stronie sieci czy serwera po to, aby uchronić się przed wyciekiem wrażliwych informacji i danych. Wiele zależy też od tego, w jakiej gałęzi gospodarki prowadzi się działalność, a co za tym idzie, jakie przepisy nas obowiązują.

- Jeśli tworzymy rozwiązanie wirtualnej rzeczywistości dla medycyny, to obowiązują nas wszystkie zalecenia dotyczące przechowywania danych medycznych, a jeśli np. dla przemysłu - powiedzmy, że tam są mniej restrykcyjne te ograniczenia, więc to zależy dla kogo oraz dla jakiej branży pracujemy - mówi **Adrian Łapczyński, prezes EpicVR.**

Wiele pojawiających się pytań i wątpliwości związanych z bezpieczeństwem w metaprzestrzeni wynika też z niedoboru pracowników specjalizujących się w tematyce cyberbezpieczeństwa. Według badania Cybersecurity Workforce Study z 2021 roku brakuje nam około 3 milionów specjalistów w tym obszarze.

CZY MOŻNA UNIKNĄĆ PUŁAPEK?

Jednym z najważniejszych aspektów w kwestii bezpieczeństwa w świecie metaverse stanie się to, aby zadbać o ochronę kluczowych danych, które jednak użytkownicy będą musieli podać, by móc korzystać z tego, co zaoferuje nam ta wirtualna przestrzeń. Zdaniem Adriana Łapczyńskiego z EpicVR, dbać o swoje bezpieczeństwo w metaprzestrzeni będzie można w taki sam sposób, w jaki robimy to teraz.

- Z mojej perspektywy ważne jest rozważne oraz rozsądne posługiwanie się własnymi danymi i poufnymi informacjami na nasz temat. Czy metaverse tutaj wprowadza coś nowego? Wydaje mi się, że nie. To są te same zagrożenia, które znany z tradycyjnego intenetu - aczkolwiek przy metaverse ważne jest to, że jeśli korzystamy z niego w goglach wirtualnej rzeczy-

wistości, no to te gogle w jakiś sposób przetwarzają naszą pozycję, nasze otoczenie. Natomiast producenci gogli VR twierdzą, że to wszystko się dzieje lokalnie i nie jest wysyłane do nich, ale nigdy nic nie wiadomo, lepiej być czujnym - twierdzi Adrian Łapczyński, dodając: - *Mówiąc wprost: jeśli ktoś już idzie w tę wirtualną rzeczywistość, musi się zgadzać na to, czego od niego wymagają wszyscy producenci gogli VR-owych.*

JAKIE JESZCZE ZAGROŻENIA NIESIE METAVERSE?

Metaverse jest wyzwaniem dla branży cybersecurity, bo niemal na każdym kroku może dojść do cyberprzestępstw czy błędów wynikających z braku wiedzy, jak funkcjonować w takiej rzeczywistości.

1. W większości metawersów nie ma w ogóle dostępu do pomocy czy wsparcia. Brakuje moderacji.

2. Tożsamość użytkowników Metaverse może zostać sfałszowana, ich konta mogą zostać zhakowane a ich awatary mogą zostać przejęte. Tożsamość osoby, z którą mają do czynienia użytkownicy metaverse, może być wątpliwa.

3. Słabe zabezpieczenia urządzeń. VR i AR to ciężkie maszyny z dużą ilością oprogramowania i pamięci. Są też celami złośliwych i nieumyślnych włamań. Ponadto fałszowanie lokalizacji i manipulowanie urządzeniami umożliwiają sprawcom przejęcie tożsamości użytkowników.

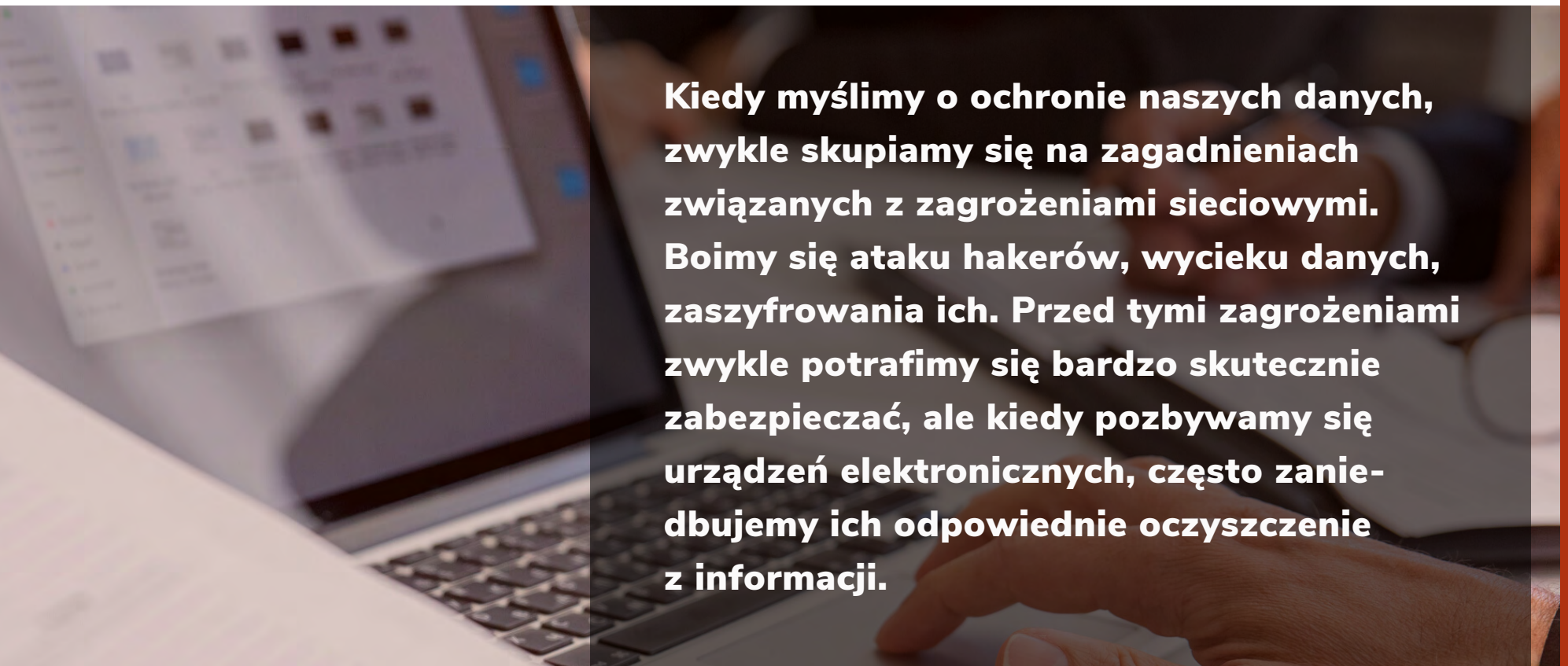
4. Komunikacja użytkowników. Z definicji, metaverse ma jednoczyć różnych sfery działania Internetu w jedną rzeczywistość, z silnym naciskiem na wirtualną społeczność. Zatem podstawą metaversu jest ułatwianie komunikacji między użytkownikami. Relacje te są zazwyczaj budowane na bazie dokładności danych (lokalizacja, informacje o użytkownikach).

5. Prywatność. Jak już wiemy, nie istnieją żadne przepisy metaverse, a potrzeba gromadzenia danych w celu uzyskania spersonalizowanego wciągającego doświadczenia wymaga ingerencji w prywatność. Użytkownicy zazwyczaj nie mają jednak wiedzy na temat poziomu dostarczanych danych. W przeciwieństwie do RODO i innych przepisów, które mają wymogi suwerenności regionalnej, wirtualne doświadczenia nie mają granic, a zatem zapewnienie prywatności jest na łasce właściciela platformy i właścicieli VR.


/GDPSYSTEM.EU
ZGODA NA COOKIES
Czy Twoja strona WWW spełnia wymogi prawne i daje możliwość elastycznego zarządzania cookies osobom, które ją odwiedzają?
SPRAWDŹ
SPEŁNIJ WYMOGI PRAWNE

JAK SKUTECZNIE USUNĄĆ ZBĘDNE DANE?

Paweł Kaczmarzyk
Serwis komputerowy Kaleron



Kiedy myślimy o ochronie naszych danych, zwykle skupiamy się na zagadnieniach związanych z zagrożeniami sieciowymi. Boimy się ataku hakerów, wycieku danych, zaszyfrowania ich. Przed tymi zagrożeniami zwykle potrafimy się bardzo skutecznie zabezpieczać, ale kiedy pozbywamy się urządzeń elektronicznych, często zaniedbujemy ich odpowiednie oczyszczenie z informacji.

SKUTECZNE I NIESKUTECZNE METODY NISZCZENIA DANYCH

Jeśli już pamiętamy o tym, by usunąć zbędne dane, stajemy przed wyborem odpowiedniej metody. Metody niszczenia danych można klasyfikować na wiele sposobów, np. na programowe, pozwalające na dalsze wykorzystanie nośnika oraz fizyczne – skutkujące zniszczeniem urządzenia.

Jednak z punktu widzenia bezpieczeństwa informacji najważniejszy jest podział na metody skuteczne i nieskuteczne.

Za metodę skuteczną będziemy uważali taką metodę, która uniemożliwia odzyskanie danych jakimikolwiek sposobami, także nieznanymi obecnie, ale możliwymi do opracowania w przyszłości.

Wszystkie pozostałe, to metody nieskuteczne, nawet, jeśli obecnie nie są znane środki pozwalające na odzyskanie danych w konkretnej sytuacji. Dane w różnych nośnikach przechowywane są w postaci pewnych stanów fizycznych, które interpretowane są jako stany logiczne – zera i jedynki składające się na interpretowalną informację.

Metody skuteczne prowadzą do zmiany tych stanów w taki sposób, żeby ustalenie poprzedniego stanu nie było możliwe. Z kolei metody nieskuteczne jedynie utrudniają dostęp do tych stanów poprzez uszkodzenie struktur logicznych (metody programowe) lub nośnika (metody fizyczne).

Nieskutecznymi są też metody polegające na uszkodzeniu urządzenia, w którym znajduje nośnik danych, jeśli odpowiedniemu uszkodzeniu nie ulegnie sam nośnik. W części urządzeń nośniki danych są łatwo demontowalne (np. dyski, które można łatwo wyjąć z komputerów i laptopów), w innych są one przylutowane do płytek elektronicznych urządzenia (na przykład, pamięci wewnętrzne w smartfonach, tabletach i dyktafonach cyfrowych). Dlatego zalania urządzenia, rozbicia ekranu, czy spowodowania niekontrolowanych uszkodzeń elektronicznych lub mechanicznych bez pewności zniszczenia wewnętrznego nośnika nie można uważać za skuteczny sposób zniszczenia danych.

METODY MECHANICZNE

Mechaniczne metody niszczenia danych sprowadzają się do powodowania różnych uszkodzeń nośników.

Jak skutecznie usunąć zbędne dane?

Często dane z nośników uszkodzonych mechanicznie są możliwe do odzyskania i często udaje się to w praktyce. W przypadku dysków twardych dane są przechowywane na talerzach i dopóki jest możliwość wprowadzenia talerza w ruch obrotowy, można podjąć próbę odzyskania zawartości powszechnie stosowanymi metodami.

Podobnie w przypadku nośników półprzewodnikowych pozostawienie nieuszkodzonych układów Flash-NAND otwiera drogę do odzyskiwania danych. Z tego względu popularne metody sprowadzające się do uderzenia nośnika młotkiem są nie tylko nieskuteczne, ale też obarczone dużym ryzykiem realnej możliwości odzyskania tych danych.

W przypadku złamania lub wygięcia talerza, a także przewiercenia talerzy lub układów NAND nie istnieją techniczne możliwości odzyskania danych, jednak odpowiednie metody mogą powstać w przyszłości.

Uszkodzone w ten sposób nośniki są materiałem nadającym się do analizy mikroskopami sił atomowych popularnie zwanych mikroskopami elektronowymi. Użycie profesjonalnych rozdrabniarek również nie usuwa danych, a jedynie utrudnia do nich dostęp w stopniu czyniącym sukces odzyskiwania danych skrajnie nieprawdopodobnym.

Tym niemniej badania przeprowadzone przez **United States Center for Magnetic Recording Research** wykazały możliwość odzyskania dzięki analizie namagnesowania powierzchni z typowych ścinków zmielonego dysku spójnych kilkunastokilobajtowych fragmentów danych. W zależności od formatu pliku, to może być np. dokument tekstowy obejmujący treść tego artykułu.

Także w przypadku uszkodzonych układów pamięci typu Flash-NAND jest możliwość obrazowania potencjałów elektrycznych bramek pływających odpowiedzialnych za przechowywanie danych.

DEMAGNETYZACJA

Demagnetyzacja polega na zniszczeniu uporządkowania namagnesowania dysku twardego lub innego nośnika magnetycznego. Zazwyczaj przeprowadzana jest przy pomocy specjalnego urządzenia – demagnetyzera zwanego również degausserem.

Musimy przy tym pamiętać, że demagnetyzacja niszczy dane wyłącznie na nośnikach magnetycznych – dane na płytach optycznych, czy nośnikach półprzewodnikowych są odporne na tę metodę niszczenia. W przypadku dysków hybrydowych SSHD część danych może przetrwać w buforze Flash-NAND.

Skuteczność demagnetyzacji jest warunkowana zaindukowaniem pola magnetycznego o wartości przekraczającej koercję (siłę odpowiedzialną za utrzymanie namagnesowania) nośnika. Dla współczesnych dysków twardych wystarczające są demagnetyzery indukujące ok. 1 T, jednak powoli na rynku pojawiają się dyski z zapisem wspomaganym energetycznie. W przypadku tych nowych technologii koercja warstwy magnetycznej może przekraczać 6 T, co spowoduje konieczność wykorzystania silniejszych demagnetyzerów.

TERMICZNE NISZCZENIE DANYCH

Dane na nośnikach cyfrowych mogą być niszczone przez oddziały-

wanie wysokiej temperatury.

W przypadku płyt CD i DVD, taśm magnetycznych i dyskietek wykorzystujących jako podłoże dla nośnika danych tworzywa sztuczne, do degradacji danych dochodzi w momencie stopienia tego tworzywa. W dyskach twardych wykorzystujących jako podłoże aluminium lub szkło, konieczne jest osiągnięcie punktu Curie – temperatury, w której substancje magnetyczne tracą swoje namagnesowanie.

Wprawdzie dokładny skład stopów używanych jako warstwa magnetyczna dysków twardych jest objęty tajemnicą producentów, ale wiadomo o nich wystarczająco dużo, by spodziewać się, że w ich przypadku punkt Curie leży ok. 700 °C. To znacznie więcej, niż temperatury uzyskiwane w ogniskach i piekarnikach, a także więcej od typowych temperatur występujących podczas pożarów. Dlatego nawet rozległe uszkodzenia termiczne nie zawsze gwarantują zniszczenie danych.

Podobnie w przypadku nośników wykorzystujących układy Flash-NAND, takich, jak dyski SSD, pendrivy i karty pamięci włożenie ich do piekarnika nie spowoduje zniszczenia danych.

Wprawdzie wewnętrzna struktura pamięci typu Flash zaczyna się degradować już w temperaturach powyżej 150 °C, jednak dzieje się to podczas pracy, a zwłaszcza w czasie wykonywania operacji kasowania i zapisu. Procedurę lutowania układów scalonych w temperaturze ok. 300 °C powszechnie uważa się za bezpieczną dla zawartości, a przegrzewanie układów podczas lutowania skutkuje zwiększeniem ilości błędów bitowych, jednak nie niszczy danych całkowicie.

METODY CHEMICZNE

Metody chemiczne opierają się na wykorzystaniu odpowiednich roztworów, w których rozpuszczane są nośniki. Ich zaletą jest zniszczenie nośników w sposób niepozostawiający żadnego materiału, który mógłby zostać poddany analizie. Wadą – konieczność rygorystycznego przestrzegania zasad BHP oraz odpowiedniej utylizacji roztworu.

PROGRAMOWE METODY NISZCZENIA DANYCH

Najważniejszą zaletą programowych metod niszczenia danych jest to, że nie uszkadzają nośnika, który może być nadal wykorzystany. Jednak decydując się na programowe usunięcie informacji trzeba mieć świadomość, w jaki sposób dane są

przechowywane i co trzeba zrobić, by naprawdę je zniszczyć.

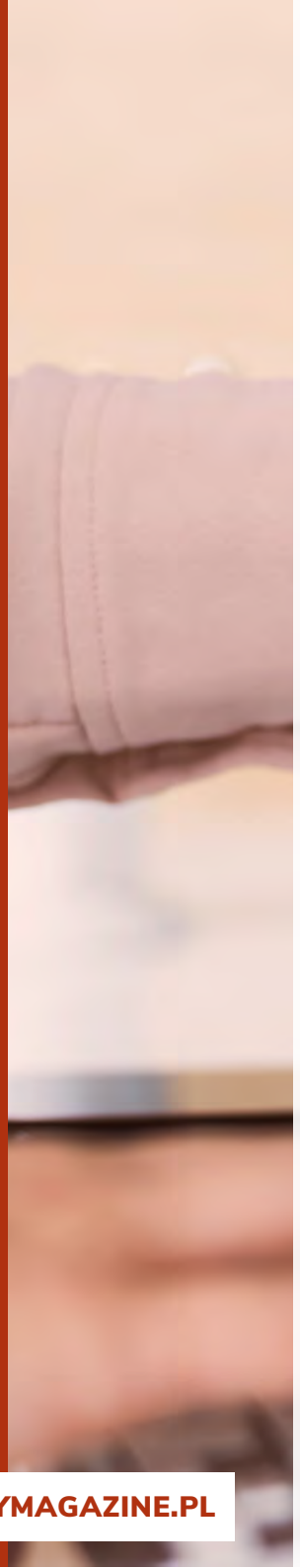
Za dostęp do naszych danych odpowiadają struktury logiczne systemów plików. To one przechowują nazwy plików, informację pozwalającą te pliki odpowiednio zaadresować, a także inne atrybuty plików. Szczegóły różnią się w zależności od użytego systemu plików, jednak cechą wspólną wszystkich systemów jest to, że usuwanie plików jest operacją na strukturach logicznych, a nie na samych plikach.

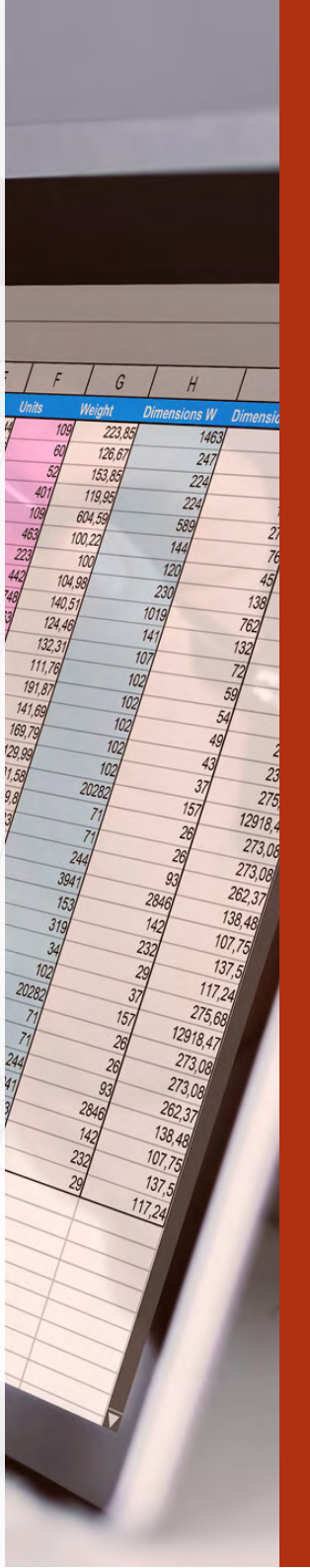
Odpowiednie zmodyfikowanie tych struktur sprawia, że plik przestaje być widoczny, ale dopóki jego zawartość nie zostanie fizycznie zastąpiona innymi danymi, wciąż jest możliwy do odzyskania. Podobnie sformatowanie partycji oznacza utworzenie nowych struktur logicznych, a poprzednie dane w dużym stopniu są możliwe do odzyskania, dopóki nie zostaną nadpisane.

I to właśnie nadpisanie jest kluczowe dla skuteczności zniszczenia danych. Nadpisanie jest równoznaczne ze zmianą stanu fizycznego odpowiedzialnego za przechowywanie informacji. Jeśli ten stan zmienimy, nie ma powrotu do poprzedniej zawartości.

O ile, oczywiście, nie przywrócimy jej np. z kopii zapasowej. Przy tym dla zniszczenia danych nie jest konieczne wielokrotne nadpisywanie. Wystarczający jest już pierwszy przebieg, a każdy kolejny jest jedynie stratą czasu i energii. Nie ma także znaczenia użyty wzorzec nadpisujący – istota procedury polega na zastąpieniu tej zawartości, którą chcemy zniszczyć jakąkolwiek inną.

Wprawdzie algorytmy wieloprzebiegowe są promowane jako bezpieczniejsze zarówno w wielu publikacjach, jak i przez firmy oferujące komercyjne usługi niszczenia danych, jednak nie przemawiają za tym żadne argumenty techniczne. Szczegółowe wyjaśnienie tego zagadnienia wykracza poza ramy artykułu, gdyż wymagałoby szer-





szego omówienia budowy i zasad funkcjonowania nośników danych. Jeśli zależy nam na zwiększeniu bezpieczeństwa procesu nadpisywania, zamiast użycia algorytmów wieloprzebiegowych powinniśmy się zainteresować technicznymi możliwościami ukrycia części obszarów nośnika poza widoczną dla użytkownika adresacją LBA, rozwiązaniami buforowania danych oraz istnieniem ewentualnych kopii niszczonych danych na innych nośnikach.

Zaletą metod programowych jest możliwość selektywnego niszczenia wybranych danych bez konieczności zniszczenia pozostałej zawartości. Fizyczne metody niszczenia danych z racji równoczesnego zniszczenia nośnika, na takie operacje nie pozwalają.

Aby selektywnie zniszczyć wybrane dane, należy je zlokalizować, posługując się strukturami logicznymi systemu plików. W podobny sposób można również oczyścić, na przykład, cały obszar partycji niezaalokowany w strukturach logicznych, aby w ten sposób fizycznie zapobiec możliwości odzyskania danych niezaadresowanych na poziomie logicznym.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

WYKRYWANIE OSZUSTÓW, POŻARÓW I KRADZIEŻY TOŻSAMOŚCI

Redakcja
SECURITY MAGAZINE

#SECURITY
#STARTUP

Czy wiedziałeś, że kogoś, kto podszywa się pod Twojego pracownika, można wykryć po sposobie pisania na klawiaturze? Albo, że dzięki dronom i oprogramowaniu możesz łatwo ustrzec się przed pożarem? A czy wiesz, co zrobić w przypadku kradzieży tożsamości? Polskie startupy mają dla Ciebie rozwiązania.

DIGITAL FINGERPRINTS – WYKRYJ OSZUSTA PO JEGO NACISKU NA KLAWIATURZE

Każda firma jest zagrożona atakiem cyberprzestępców. A zagrożenie to będzie tylko rosło. Startupy i firmy chcą ustrzec się przed hakerami na najróżniejsze sposoby. Dwuetapowe uwierzytelnianie logowania, to już standard, który, niestety, coraz łatwiej złamać. Pojawia się zatem coraz więcej organizacji oferujących np. zewnętrzne klucze wpinane do urządzeń po USB w celu uwierzytelniania oraz firm stosujących biometrykę.

I do tej drugiej grupy zalicza się **Digital Fingerprints**. Nie ma tu jednak mowy o skanowaniu odcisków palców czy twarzy, do czego już przywykliśmy. Digital Fingerprints sięga po wykrywanie sposobu, w jakim piszemy i sile, z jaką naciskamy klawisze. Startup przekonuje, że nie ma dwóch osób, które pisałyby na klawiaturze tak samo. Tak jak nie ma dwóch identycznych charakterów pisma. Podobnie jest w przypadku ruchów myszką czy z korzystaniem z urządzenia mobilnego.

Metodę, którą stosuje startup, określa się jako biometrię behawioralną. Za pomocą uczenia maszynowego mechanizm rozpoznaje, czy użytkownik jest faktycznie tym, za kogo się podaje. System startupu ma zbierać dane, a następnie przekształcać je w ponad 80 cech, które pozwalają wykryć model zachowań. Dzięki temu od razu wiesz, kto tak naprawdę korzysta z urządzeń w Twojej firmie.

Startup chwali się, że chroni przed cyberprzestępcami stosującymi techniki **man-in-the-middle, ataki na IoT, DDoS czy za pomocą botów.** A także wykorzystujących **exploity, wycieki danych, brute force czy phishing.** Jednocześnie dane zbierane na temat pracowników mają być w zgodzie z RODO, ponieważ są od razu anonimizowane. To zdecydowanie jedno z najciekawszych rozwiązań uwierzytelniających, które da się wdrożyć w praktycznie każdej organizacji.

CYBERRESCUE, CZYLI POGOTOWIE CYBERBEZPIECZEŃSTWA

„*Twoja straż pożarna w sieci*" – tak określa się startup **CyberRescue**. I to w zasadzie najlepsze określenie pola działań tej organizacji. Startup oferuje swoje usługi zarówno w formie B2C, jak również B2B. I skupia się przede wszystkim na fakcie dokonanym (ale nie tylko, o czym później).

Ktoś przejął Twoje konto w mediach społeczno-

ciowych? Otrzymałeś maila o wycieku danych? A może skradziono Ci smartfon, na którym miałeś wrażliwe informacje czy prywatne zdjęcia? CyberRescue rusza wówczas na pomoc.

Startup zweryfikuje, czy faktycznie doszło do wycieku Twoich danych, zdalnie skasuje zagrożone pliki, pomoże odzyskać pieniądze czy zhakowany profil, przeprowadzi Cię przez kontrolę szkód. Organizacja pomaga także w przypadku kradzieży tożsamości, zakupach w fałszywym sklepie internetowym itd.

A zatem porównanie CyberRescue do pogotowia czy straży pożarnej jest niezwykle trafne, bo startup faktycznie „gasi pożary" i pomaga, kiedy już coś poważnego się wydarzyło. Profilaktyka jest niezwykle ważna, ale nie ma co ukrywać, że nigdy nie zetkniemy się z udanym cyberatakiem na naszą firmę czy osobę. Tak jak każdy z nas może ulec wypadkowi na ulicy, tak każdy analogicznie może mieć „wypadek" w sieci.

To jednak nie wszystko, co oferuje startup. Działa też w systemie abonamentowym, który ma być kompleksową ochroną. Czyli właśnie zapobieganiem. Oferta CyberOchrona+ blokuje zagrożone strony czy określone treści, a także weryfikuje witryny z płatnościami online, wyznacza limit dostępu do sieci, lokalizuje urządzenia czy zdalnie kasuje z nich dane oraz pliki. I co ważne – działa 24 godziny na dobę przez cały rok.

SMOKED – WYKRYJ POŻAR, ZANIM BĘDZIE ZA PÓŹNO

Jak twierdzi sam startup – celem organizacji jest pomoc w ochronie ludzkiego życia i obiektów potencjalnie narażonych na zajęcie ogniem. SmokeD stworzyło oprogramowanie do wczesnego wykrywania pożarów i natychmiastowego powiadamiania użytkowników o ich wystąpieniu.

Startup wykorzystuje do tego drony i sztuczną inteligencję, które pozwalają na wykrycie dymu i płomieni z odległości do 16 km. Dzięki temu masz szansę zareagować, zanim pożar stanie się na tyle duży, że będzie trudny do okiełznania.

SmokeD wysyła powiadomienia z dokładną lokalizacją na stronę internetową lub do aplikacji mobilnej. Startup chwali się, że pożary wykrywa w ciągu 10 minut od zaprószenia ognia.

Organizacja kieruje swoje usługi przede wszystkim do firm telekomunikacyjnych, spółek energetycznych, lasów państwowych i parków narodowych, samorządów, plantatorów czy rolników, branży nieruchomości, ubezpieczycieli i spółdzielni mieszkaniowych.

Dzięki SmokeD Twoi pracownicy mogą ocalić swoje życia na wypadek wybuchu pożaru.

Masz też czas i możliwość zareagować, aby zabezpieczyć swoją infrastrukturę i błyskawicznie powiadomić straż pożarną. Co więcej – startup oferuje swoje usługi także osobom prywatnym.

IV KONFERENCJA

POLSKA IZBA PRODUCENTÓW URZĄDZEŃ I USŁUG NA RZECZ KOLEI

BEZPIECZEŃSTWO NA KOLEI

8-9 grudnia 2022 r.

Hotel NADMORSKI
Gdynia

PATRONAT
SECURITY MAGAZINE

IV KONFERENCJA
BEZPIECZEŃSTWO NA KOLEI
8-9 GRUDNIA

WŚRÓD GOŚCI MIĘDZY INNYMI:

- Państwowa Komisja Badania Wypadków Kolejowych – Tadeusz Ryś
- Akademia Marynarki Wojennej – dr hab. Grzegorz Krasnodębski prof. AMW
- Polskie Koleje Państwowe S.A. – Rafał Zgorzelski
- Instytut Kolejnictwa – Andrzej Massel
- PKP Informatyka Sp. z o.o. – Tadeusz Turzyński
- PKP S.A. – Centrum Bezpieczeństwa Dworców Kolejowych – Michał Zagalski
- NASK-PIB – CERT Polska – Krystian Szefler
- PKP Szybka Kolej Miejska w Trójmieście sp. z o.o. – Grzegorz Przysiężny – Komendant SOK
- Komenda Główna Straży Ochrony Kolei – Adam Morawski

Zapraszamy do udziału w IV Konferencji „BEZPIECZEŃSTWO NA KOLEI" która odbędzie się w Gdyni 8-9 grudnia 2022 roku w Hotelu Nadmorskim. Zachęcamy do uczestnictwa w konferencji w formie słuchacza, prezentacji multimedialnej promującej rozwiązanie oraz uczestnictwa w wystawie rozwiązań i usług.

Panele, debaty i prezentacje z udziałem polskich i zagranicznych gości będą skupiały się na tematyce cyberobrony w aspekcie wojskowym i cywilnym, prywatności danych, roli dyplomacji w branży cyberbezpieczeństwa, sztucznej inteligencji czy suwerenności w kontekście gospodarki cyfrowej.

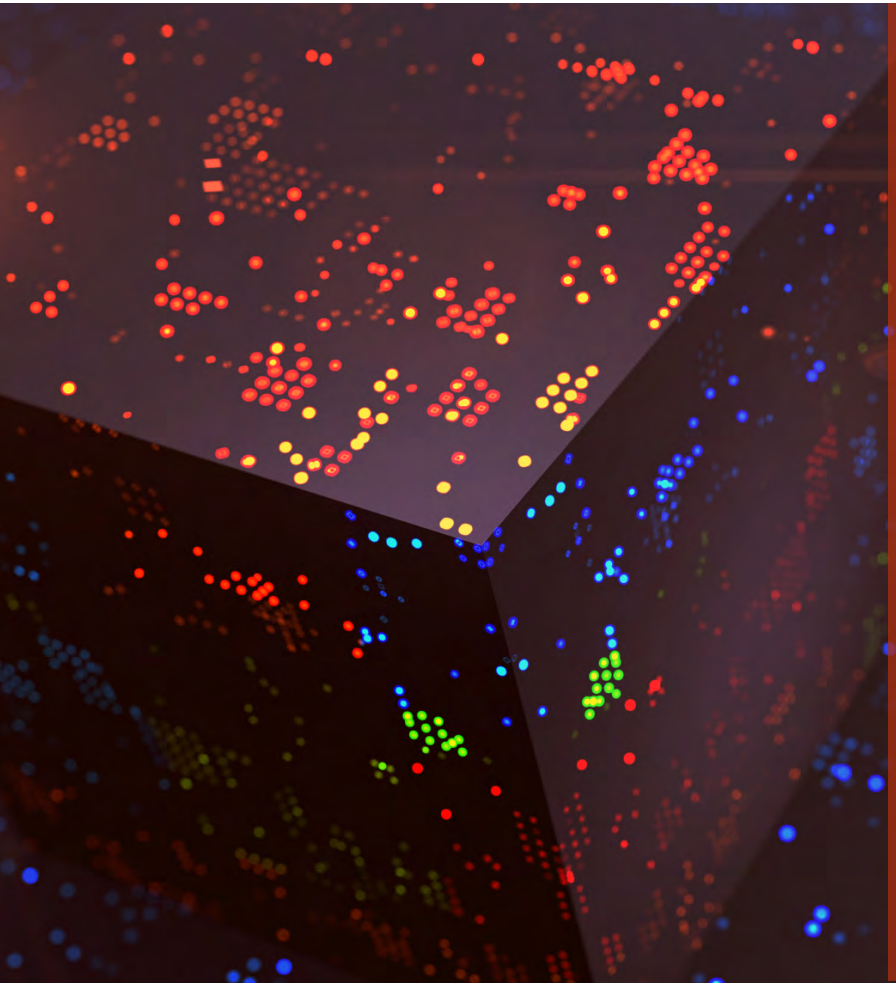
Zakres tematyczny konferencji:

- Prawo – procedury, przepisy, instrukcje, certyfikacja i akredytacja
- Zarządzanie bezpieczeństwem – SMS, oraz ryzykiem
- Bezpieczeństwo ruchu pociągów (ERTMS, przejazdy, urządzenia srk, automatyka, systemy wspomagające, łączność)
- Mobilny i stacjonarny monitoring wizyjny, drony, urządzenia dostępowe
- Bezpieczeństwo kolejowej infrastruktury energetycznej i transportowej
- Cyberbezpieczeństwo i ochrona danych (podatności, luki, środki naprawcze, monitoring procesów, nadzór)
- Inteligentne systemy informacji pasażerskiej
- Pojazdy szynowe – monitorowanie poziomów utrzymania, systemy bezpieczeństwa w taborze
- Współpraca służb (SOK, POLICJA, STRAŻ POŻARNA, Służby Ratownicze, Kolejowe Ratownictwo Techniczne)
- Infrastruktura dworcowa i przestrzeń publiczna – bezpieczny pasażer i pierwsza pomoc.

POBIERZ KARTĘ ZGŁOSZENIA

PODSTAWY KRYPTOGRAFII

Kris Durski
Vault Security

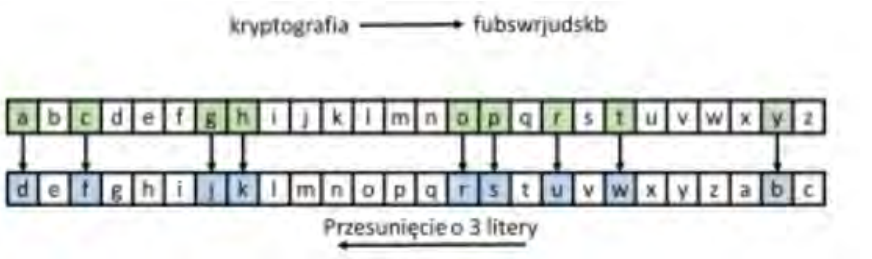


Podczas codziennych czynności w internecie lub przeglądania wiadomości często widzimy lub słyszymy o kryptografii, cyberbezpieczeństwie, kryptowalutach lub blockchainie. Dla większości z nas są to określenia owiane częściowo magią i często nie do końca rozumiemy, co naprawdę się za nimi kryje. Czy są w jakiś sposób powiązane ze sobą, czy też nie mają ze sobą nic wspólnego?

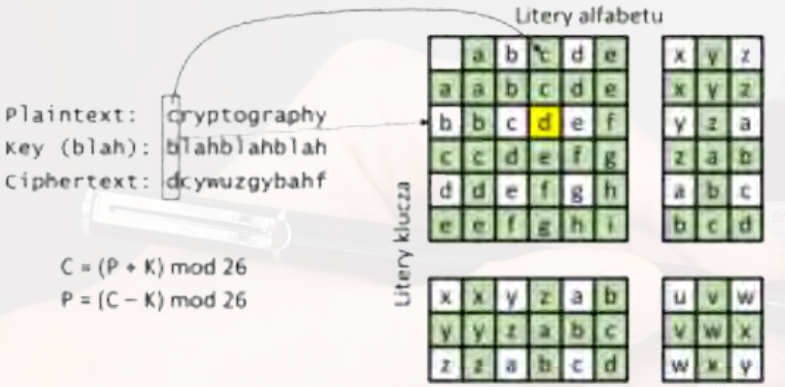
DEFINICJA

Kryptografia jest definiowana nieco inaczej w różnych miejscach, ale generalnie odnosi się do praktyki i nauki technik kodowania danych, dzięki czemu można je ukryć przed oczami osób niepowołanych.

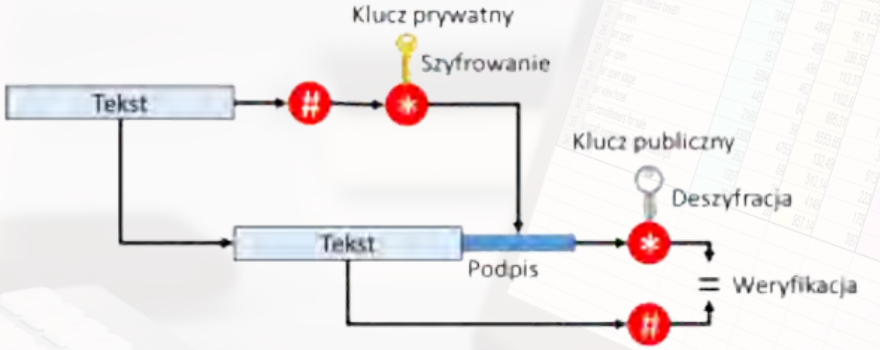
Słowo "kryptografia" pochodzi od greckiego słowa „kryptos”, co oznacza ukryte lub tajne. Pierwsze dowody kryptografii znaleziono w grobowcu w Egipcie, który powstał około 1900 p.n.e. Odnaleziona wiadomość składała się z niezwykłych symboli hieroglificznych. Kolejny dowód kryptografii został znaleziony w wiadomościach, które Juliusz Cezar wysyłał do swoich generałów armii na froncie wojennym około 100 p.n.e. Posługiwał się szyfrem, zwanym dziś również szyfrem Cezara lub szyfrem systemowym, w którym znaki alfabetu są przesunięte o daną liczbę pozycji, w tym przypadku o 3. Szyfry systemowe są bardzo mało tajne i można je łatwo złamać.
(Na zdjęciu zaszyfrowano słowo „cryptography”).



Kryptografię można odnaleźć także, w pierwszym szyfrze, który wprowadził ideę klucza szyfrującego i został zaprojektowany przez Vigenere’a w XVI wieku. Jednak pomimo wprowadzenia elementu klucza szyfrującego, szyfr ten był również bardzo łatwy do złamania.



Nie szukając dalej innych przykładów w historii, przejdźmy do czasów współczesnych, w których algorytmów nie można już stosować bez komputerów elektronicznych. Nietrudno jest odgadnąć, że głównym celem kryptografii jest kodowanie wiadomości za pomocą algorytmów, które mogą być w pełni opublikowane, co nie zmienia faktu, że odgadnięcie kluczy jest nadal niezwykle trudne.



Ta technika, która uniemożliwia odczytanie wiadomości bez wstępnego przetwarzania nazywa się szyfrowaniem. Szyfrowanie ze względu na swoją prawdziwą naturę jest odwracalne, co oznacza, że wiadomości można zaszyfrować do postaci tekstu zaszyfrowanego, aby uczynić je nieczytelnymi, a następnie odszyfrować, aby przywrócić je do pierwotnej treści.

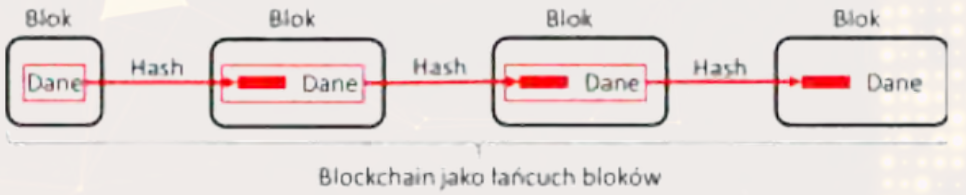
Jeśli algorytm używa tego samego klucza do szyfrowania i odszyfrowywania, nazywa się go **symetrycznym**, w przeciwieństwie do algorytmów, które wymagają klucza publicznego do szyfrowania i prywatnego do odszyfrowania. Te nazywane są **asymetrycznymi.**

Oprócz szyfrowania i deszyfrowania, algorytmy asymetryczne są również wykorzystywane do podpisywania wiadomości, gdzie klucz prywatny jest używany do generowania podpisu cyfrowego, a odpowiedni klucz publiczny służy do weryfikacji podpisu. Podpis to wartość skrótu wiadomości zaszyfrowanej kluczem prywatnym, a ponieważ klucz prywatny musi być dobrze chroniony przez podpisującego, gwarantuje to niezaprzeczalność podpisu, a tym samym wiadomości.

W tym miejscu wprowadziliśmy kolejną ważną koncepcję, bardzo często używaną w kryptografii, a mianowicie funkcję skrótu i jej zaszyfrowaną wersję, zwaną podpisem cyfrowym. Podczas gdy szyfrowanie ukrywa treść wiadomo-

ści, podpis cyfrowy służy do udowodnienia pochodzenia wiadomości, który najczęściej przedstawiany jest w postaci zwykłego tekstu z dołączonym podpisem w celu udowodnienia autorstwa.

Teraz, gdy wiemy, że potrzebujemy funkcji mieszającej, pytanie brzmi, co to jest? Mówiąc prościej, funkcja skrótu (mieszająca) konwertuje wiadomość czy dane o dowolnym rozmiarze na wartość o stałym rozmiarze, zwykle w postaci tablicy bajtów. W przeciwieństwie do szyfrowania, wartości skrótów nie są odwracalne, czyli innymi słowy, nie można ich przekonwertować z powrotem na wiadomość z powodu niewykonalności obliczeniowej.



Blockchain jako łańcuch bloków

Ta cecha skrótów (haszy) jest znana jako preimage resistance. Jak łatwo się domyślić, jeśli bardzo długą wiadomość można przekonwertować na bardzo krótką tablicę bajtów, może istnieć wiele wiadomości, które mogą generować ten sam skrót. W kryptografii to zdarzenie nazywa się kolizją skrótów lub po prostu kolizją.

Jednak im dłuższa wartość skrótu i im wyższa jakość algorytmu, tym mniejsze prawdopodobieństwo kolizji, ponieważ dłuższe skróty mają znacznie więcej unikalnych wartości. Najnowsze znane algorytmy, takie jak szeroko stosowany standard SHA-2 (Secure Hash Algorithm), bardzo dobrze wykorzystują te unikalne wartości,

a tym samym unikają kolizji.

Bardzo ważne jest również, aby wspomnieć tutaj, że małe zmiany w oryginalnych danych powodują duże zmiany wartości skrótu, więc kierunek zmiany danych nie przewiduje kierunku zmiany wartości skrótu. Ta nieprzewidywalność jest wykorzystywana w kopaniu kryptowalut, które wymagają docelowego hasza.

Skoro słyszeliśmy o szyfrowaniu, deszyfrowaniu i hashowaniu (mieszaniu), jak ma się do tego termin blockchain? Niefortunne jest to, że zbyt wiele osób uważa magię blockchaina za panaceum na prawie wszystko, na czym skupia się cyberbezpieczeństwo. To ten sam problem, co w przypadku biometrii; kiedy potrzebna jest zmiana, nie jest to możliwe.

Istnieje szeroko rozpowszechnione błędne przekonanie, że łańcuch bloków (blockchain) może zwiększyć zaufanie do danych, ponieważ danych nie można zmienić bez zerwania łańcucha bloków.

Co by było, gdyby dane, które zostały wprowadzone do łańcucha bloków, były fałszywe? Przede wszystkim zaufanie musi być w źródle danych, a potem zaufanie, że dane nie zostały zmienione. Blockchain może chronić tylko łańcuch nagrań i faktów, zarówno wiarygodnych, jak i fałszywych.

Przyjrzyjmy się, na czym polega blockchain i jak może chronić dane przed zmianami. Podstawą łańcucha bloków jest powiązanie jednego fragmentu danych z hashem poprzedniego fragmentu danych zwanych blokami. Koncepcja pochodzi z drzewa haszującego opatentowanego przez Ralpha Merkle w 1979 r., który jest współtwórcą kryptografii z kluczem publicznym i wynalazcą haszowania kryptograficznego.

Chociaż w wielu publikacjach blockchain jest przedstawiany jako rodzaj rozproszonej księgi, która składa się z rosnącej listy rekordów, zwanych blokami, w uproszczeniu, tak naprawdę sprowadza się do łańcucha bloków połączonych hashami.

Wiemy już, że hash to skrót danych w postaci krótkiej tablicy bajtów, a dobre algorytmy haszujące tworzą unikalne skróty dla różnych wiadomości lub zestawów danych. Jeśli dane zostaną zmodyfikowane w dowolnym bloku, ich hash nie będzie już odpowiadał hashowi, który jest przechowywany w następnym bloku. Pomimo tego, że blockchain jest przez wielu kojarzony z kryptowalutą, w rzeczywistości jest to samodzielna koncepcja, która ma wiele zastosowań, nie mających powiązań z żadną walutą czy nawet rozproszoną księgą.

BLOCKCHAIN

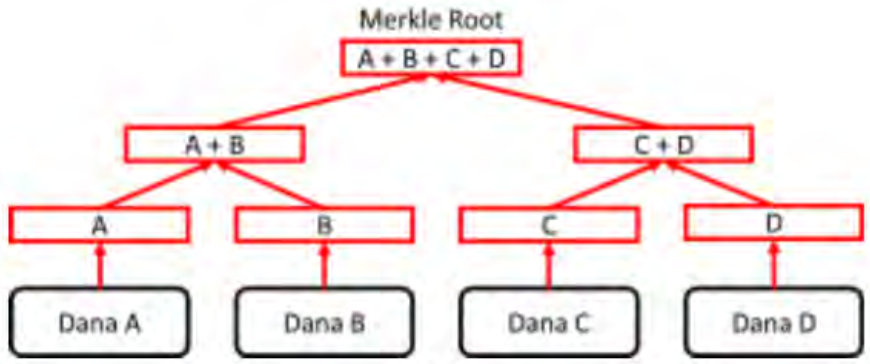
Blockchain to rozwiązanie z wyboru do zamrażania transakcji, które nie powinny być zmieniane w żadnym momencie w przyszłości. Należy jednak pamiętać, że blockchain nie zapewnia żadnej prywatności, czyli innymi słowy, wszystkie dane w każdym bloku są dostępne publicznie. Aby dodać prywatność do danych, należy zastosować inne techniki, takie jak na przyk-

ład szyfrowanie. Kolejną zaletą blockchaina jest to, że nie musi być przechowywany w jednym miejscu i mocno chroniony przed manipulacją, ponieważ ze swej natury jest odporny na manipulacje.

Nawet jeśli różne fragmenty blockchaina są przechowywane w różnych lokalizacjach, zastosowanie skrótów kryptograficznych pozwala na pełną weryfikację każdego elementu blockchaina.

Inną ważną koncepcją efektywnego wykorzystania skrótów jest korzeń Merkle, który pozwala na walidację big data podzielonych na mniejsze części. Ponieważ skrót jest skrótem porcji danych, jego skrót ma również taką samą zdolność do sprawdzania poprawności tych danych.

Załóżmy, że mamy cztery dane A, B, C i D i dla każdego z nich generujemy skróty. Następnie łączymy pary tych skrótów i ponownie je mieszamy. Na górze otrzymujemy hash dwóch hashów najwyższego poziomu, który nazywa się Merkle root.



Zaletą tego katalogu głównego jest to, że reprezentuje on wszystkie fragmenty danych i jako taki może je wszystkie jednocześnie sprawdzać. Ktoś może zapytać, po co zawracać sobie głowę, jeśli możemy hashować wszystkie dane razem i mieć tylko jeden hash. Cóż, czasami dane są tak duże, że mogą nawet nie zmieścić się na jednym komputerze lub dane mogą nie być tworzone w jednym miejscu. To drzewo haszujące pozwala na walidację danych, na przykład w pobranych plikach.

Jeśli odtworzony root Merkle nie pasuje do oryginału, musi istnieć fragment danych, który jest uszkodzony lub złośliwie zmieniony i musi zostać pobrany ponownie. Drzewo pozwala zlokalizować, który element danych jest zły, ponieważ można go łatwo przeszukać do problematycznego fragmentu danych.

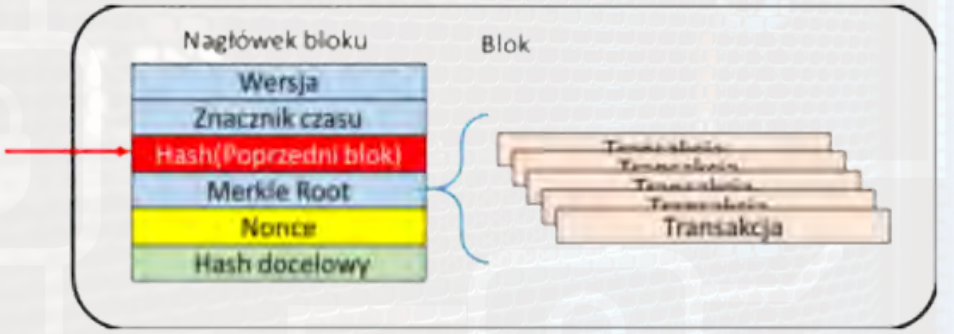
NONCE

Zanim przejdziemy do kryptowalut, jest jeszcze jedna koncepcja, którą trzeba wyjaśnić, a mianowicie nonce. Ogólnie rzecz biorąc, nonce jest wartością jednorazową, co oznacza, że jest używana tylko raz, a następnie odrzucana i zwykle reprezentowana przez tablicę losowych bajtów wylosowanych kryptograficznie. Kryptografia wy-

maga, aby generator liczb losowych nie produkował tego samego numeru przez bardzo, bardzo długi czas, więc atakujący nie może odgadnąć jego następnej wartości w przewidywalnej przyszłości.

BITCOIN

Jedna z dobrze znanych kryptowalut jest Bitcoin, choć nie był on pierwszą, ale jako pierwszy zwrócił uwagę opinii publicznej. Składa się z rozproszonej księgi, która tworzy blockchain, w którym bloki są tworzone podczas procesu zwanego wydobywaniem lub tworzeniem dowodu pracy. Wydobywanie nowego bloku polega na generowaniu skrótów nad nagłówkiem najnowszego bloku.



Sieć Bitcoin wymaga, aby wygenerowany hash był równy lub mniejszy niż docelowy hash. Aby manipulować uzyskanym haszem, górnicy modyfikują nonce, dopóki kryterium nie zostanie spełnione. Po znalezieniu nowego skrótu, konkretny górnik publikuje blok w sieci, aby można go było dodać do zainteresowanych części księgi. Ten nowy blok zawiera również nagrodę dla odnoszącego sukcesy górnika. Inni, którym się nie udaje, odrzucają swoją pracę i przechodzą do wydobycia nowego bloku.

Jak trudny jest ten proces, musimy przyjrzeć się cechom hasha. Wiemy, że inżynieria wsteczna hasza w celu uzyskania zaszyfrowanych danych jest prawie niemożliwa. Górnicy muszą odgadnąć wartość jednorazówki, a następnie wygenerować nowy hash, aby sprawdzić, czy warunek jest spełniony, a wygenerowanie właściwego może zająć astronomiczną liczbę prób. Należy również pamiętać, że niewielka zmiana danych może skutkować dużą zmianą wartości skrótu. Przyrostowy wzrost wartości jednorazowej nie powoduje przyrostowego wzrostu wartości skrótu.

Wszystkich zainteresowanych poznaniem szczegółów na temat konkretnych pojęć zachęcam do eksploracji zasobów szeroko dostępnych w internecie, ale bądźcie czujni na wiarygodność informacji.

Nie chcę też komentować, czy kryptowaluty mają uzasadnione istnienie jako legalny sposób „dodrukowania własnych pieniędzy", zwłaszcza w świetle marnotrawstwa energii i potencjalnego tworzenia większego zanieczyszczenia, skoro ich tworzenie spala około 0,4% do 0,9% rocznego globalnego zużycia energii elektrycznej, a to więcej, niż może sobie pozwolić wiele mniejszych gospodarek. Historycznie waluty miały reprezentować wartość wyprodukowanych dóbr, które były wynikiem pracy; ale ta idea zniknęła we wszystkich paradoksach dzisiejszego świata. Rozwiązania częściowe nigdy nie będą adekwatne i satysfakcjonujące, zwłaszcza, jeśli istnieją lepsze.

-20%

SECURITY MAGAZINE
WWW.SECURITYMAGAZINE.PL

NOWOROCZNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

WAŻNY DO
28.02.2023

KONTAKT I SZCZEGÓŁY: REDAKCJA@SECURITYMAGAZINE.PL

SECURITYMAGAZINE.PL

WŁAMANIE NA FACEBOOKA I LINKEDIN. CO ROBIĆ?

Redakcja
SECURITY MAGAZINE

Włamania na Facebooka, LinkedIn i inne media społecznościowe to codzienność. Każdego dnia ktoś pada ofiarą oszustów, którzy włamują się na nasze konta. I choć takie działanie wciąż wielu osobom wydaje się niewinnym żartem, niesie ze sobą w wielu przypadkach poważne konsekwencje.

FACEBOOK. WŁAMANIE NA KONTO

Facebookowe konta przedsiębiorców bardzo często powiązane są z Meta Business Managerem. To wiąże się z tym, że często w ten sposób oszust może dostać się do danych kart płatniczych, ukraść zbudowane strony/profile na Facebooku/Instagramie. Kolejna kwestia, może spróbować oszukać naszych znajomych z listy: wyłudzić przelewy na BLIK, rozsyłać im podejrzane linki, publikować nielegalne treści (pornografia, szerzenie nienawiści, itp.).

KONTO PRYWATNE ZOSTAŁO ZHAKOWANE?

Czasami haker, który włamał się na nasze konto przez jakiś czas zostanie niezauważony. Warto stale obserwować, co dzieje się z naszym profilem, sprawdzać, czy na tablicy nie pojawiają się materiały, których wcześniej nie opublikowaliśmy. Ponadto śledźmy, czy nasze dane osobowe nie są zmienione, a w liście znajomych nie ma osób, których po prostu nie znamy.

KONTO FIRMOWE PRZEJĘTE PRZEZ HAKERA

W wypadku Konta Firmowego na Facebooku w pierwszej kolejności należy obserwować, czy nie pojawiają się na nim płatności, które są dla nas podejrzane. To szczególnie istotne, jeśli mamy podpiętą pod konto kartę debetową lub kredytową. Jeśli mamy uruchomione kampanie, warto skontrolować, czy nie zmienił się ich budżet dzienny lub całkowity. Sprawdźmy także, czy do konta nie dołączono stron Facebook, których nie znamy i nie uruchomiono nowych kampanii reklamowych.

Te ostatnie są o tyle niebezpieczne, że ryzykujemy nie tylko utratą pieniędzy. Mogą one bowiem reklamować produkty, których promowanie jest zakazane regulaminem tego portalu społecznościowego. Wtedy ryzykujemy całkowitą blokadę naszego konta reklamowego. Obserwujemy także, czy do konta nie dodano innych użytkowników.

MAMY DOSTĘP DO KONTA, ALE PODEJRZEWAMY WŁAMANIE

Pierwszym krokiem po zauważeniu podejrzanego logowania lub aktywności na profilu powinno być zmienianie haseł dostępu oraz użycie funkcji wyloguj mnie na wszystkich urządzeniach. W tym celu należy wejść w Ustawienia i Ustawienia prywatności. Wybrać “Bezpieczeństwo i logowanie” i spojrzeć na rubrykę “Miejsce logowania”.

Procedurę sprawdzania logowań warto wprowadzić na stałe do naszego kalendarza i sprawdzać je min. raz w tygodniu. Ideałem byłoby codzienne ich sprawdzanie. Pozwoli nam to na uniknięcie niemiłych niespodzianek.

Ponadto znajdziesz tutaj:

1. **"Facebook Protect"**, czyli dodatkowe, mocno zaawansowane opcje ochrony konta na Facebooku. Warto z nich korzystać!
2. **"Polecane".** W tym miejscu możesz sprawdzić, czy Twoje hasło jest w porządku. Ponadto włączysz lub skontrolujesz, czy masz włączone uwierzytelnianie dwuskładnikowe. Znajdziesz tutaj informację, czy Twoje alarmy logowania na Facebooku i na poczcie są włączone. Gdy jakiś z obszarów wymaga naprawy, Facebook poprzez Twoje kliknięcie "Kontynuuj" poprowadzi Cię krok po kroku.
3. **"Miejsce logowania"**. Tu przejrzysz listę wszystkich logowań: miast, czasu i urządzeń, z których nastąpiło logowanie. Tu jednak polecamy ostrożność, bo Facebook jest w tym przypadku mocno nieprecyzyjny. Dla przykładu, logowania z Rzeszowa wskazują lokalizację: Bielsko-Biała lub Wrocław, choć czas i rodzaj urządzenia są właściwe. Jeśli z którychś urządzeń już nie korzystasz i chcesz z nich wylogować aplikacje ze swoim kontem, bo np. miałeś ją aktywną w telefonie służbowym, który oddałeś, skorzystaj z przycisku "Wyloguj się ze wszystkich sesji" lub kliknij w trzy kropki przy konkretnej sesji i tam "Wyloguj się". Klikając w "To nie Ty", będziesz dalej kierowany przez Facebooka, po kliknięciu dalej w "Zabezpiecz konto".

4. "Logowanie". Właśnie tu masz opcję "Zmień hasło". Klikasz w "Edytuj", dalej wpisujesz w okno hasło bieżące, nowe i ponownie nowe, a następnie "Zapisz zmiany".

NIE MAMY DOSTĘPU DO KONTA FACEBOOK. CO WTEDY?

Znacznie gorzej sytuacja wygląda, jeśli już nie mamy możliwości logowania się na konto Facebooka. W takim przypadku warto działać szybko i wejść na stronę i postępować krok po kroku według instrukcji.
W ten sposób Facebook zabezpieczy Twoje konto, a Ty będziesz mógł zmienić nazwę użytkownika.

Możesz to zrobić także, wykonując kilka prostych ruchów.

Co ważne, zgłosić włamanie na Twoje konto może także osoba z rodziny, współpracownik, czy inny znajomy. W tym celu:

- Wejdź na stronę **Centrum pomocy** – Facebook.
- Znajdź, na liście z lewej strony i rozwiń kategorię **Zasady i zgłaszanie**.
- Kliknij w **Fałszywe konta i konta, na które ktoś się włamał.**
- Wybierz z listy problem, który dotyczy konta Twojego lub Twojego znajomego.

KONTAKT Z ADMINISTRACJĄ FACEBOOKA

Kolejną możliwością, która ma pomóc w odzyskaniu konta Facebook jest kontakt z supportem serwisu. Warto uzbroić się w cierpliwość i odzywać się do supportu do skutku. Nie zawsze bowiem już pierwszy kontakt z pracownikiem da zadowalające efekty. Czasami trzeba uzbroić się w cierpliwość. Proces odzyskiwania konta może potrwać kilka dni, a może nawet miesiąc lub dwa. Wpływa na to wiele zmiennych, m.in. jego wielkość, podpięte konta Manager Firmy i inne.

WŁAMANIE NA LINKEDIN. I CO DALEJ?

LinkedIn to drugi serwis społecznościowy, który

często wybierają hakerzy. Jest on dla nich cenny ze względu na informacje gospodarcze. Ten portal jest bowiem miejscem w którym buduje się głównie wizerunek biznesowy. Może być zatem potężnym narzędziem do zdobywania informacji gospodarczych o konkurencji w nie do końca legalny sposób.

LinkedIn pozwala na korzystanie z tzw. konta premium, co może stanowić dodatkową zachętę dla potencjalnego hakera. Takie konto daje większe możliwości nawiązywania kontaktów.

JAK POZNAĆ, CZY KONTO PRYWATNE LUB BIZNESOWE JEST ZHAKOWANE?

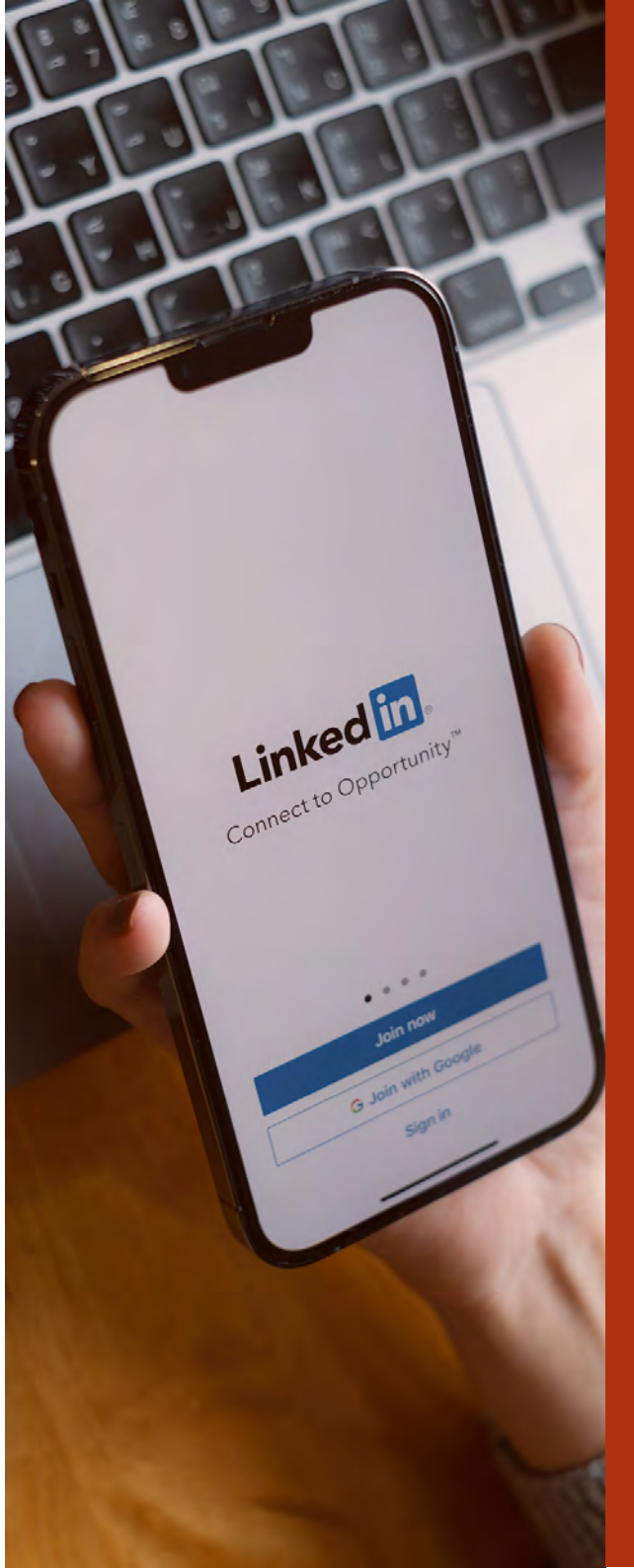
Pierwszym dostrzegalnym problemem są trudności z zalogowaniem się na sam profil. Czasami jednak haker działa w ukryciu. W takim wypadku Twój niepokój powinna wzbudzić podejrzana aktywność na LinkedIn, na przykład osoby z listy znajomych, których nie znasz, wiadomości prywatne, publikacja treści, których nie znasz, czy obserwowanie nieznanych profili.

MAMY DOSTĘP DO KONTA. PROCEDURY

Jeśli nadal masz dostęp do swojego kota na LinkedIn i zauważyłeś nieprawidłowe logowanie się, masz dużo możliwości. Bardzo ważne jest, by odpowiednio zabezpieczyć konto przed kolejnym takim zdarzeniem.

Pierwszym krokiem powinno być zgłoszenie włamania na konto i opis sytuacji przy pomocy formularza. Później, jeśli możemy zalogować się na konto, wykonujemy to działanie oraz podejmujemy następujące kroki:

- Zmieniamy hasło do LinkedIn. Warto stworzyć kombinację cyfr i liter, któ-



ra będzie uznawana za silne hasło, którego nie można łatwo zmienić. Unikaj używania takiego samego hasła jakie masz w innych usługach online.

- Uruchom dwuskładnikowy proces weryfikacji logowania. Dzięki temu każde logowanie będziesz autoryzować z pomocą smartfona.
- Sprawdź ostatnie logowania i aktywne sesje pod linkiem. Pozwoli Ci to zweryfikować, kto, gdzie oraz przy pomocy jakiego połączenia sieciowego korzystał z Twojego konta.
- Zweryfikuj, czy dodano nowe adresy e-mail oraz numer telefonu powiązane z Twoim kontem.
- Oceń i sprawdź, czy email powiązany z kontem na LinkedIn jest bezpieczny. Zmień na jego koncie hasło i pamiętaj o tym, by robić to regularnie.

PROCEDURY, GDY NIE MAMY DOSTĘPU DO KONTA LINKEDIN

W takim wypadku oficjalna pomoc LinkedIn sugeruje natychmiastowy kontakt z ich administracją. W tym celu należy zgłosić zdarzenie przez specjalny formularz dostępny pod linkiem. Wystarczy podać adres URL profilu LinkedIn, na który dokonano włamania. W tym celu wystarczy wpisać LinkedIn + Imię i nazwisko. W drugim kroku możemy także opisać zaistniałą sytuację i podać jak najwięcej informacji na temat zaistniałego zdarzenia.

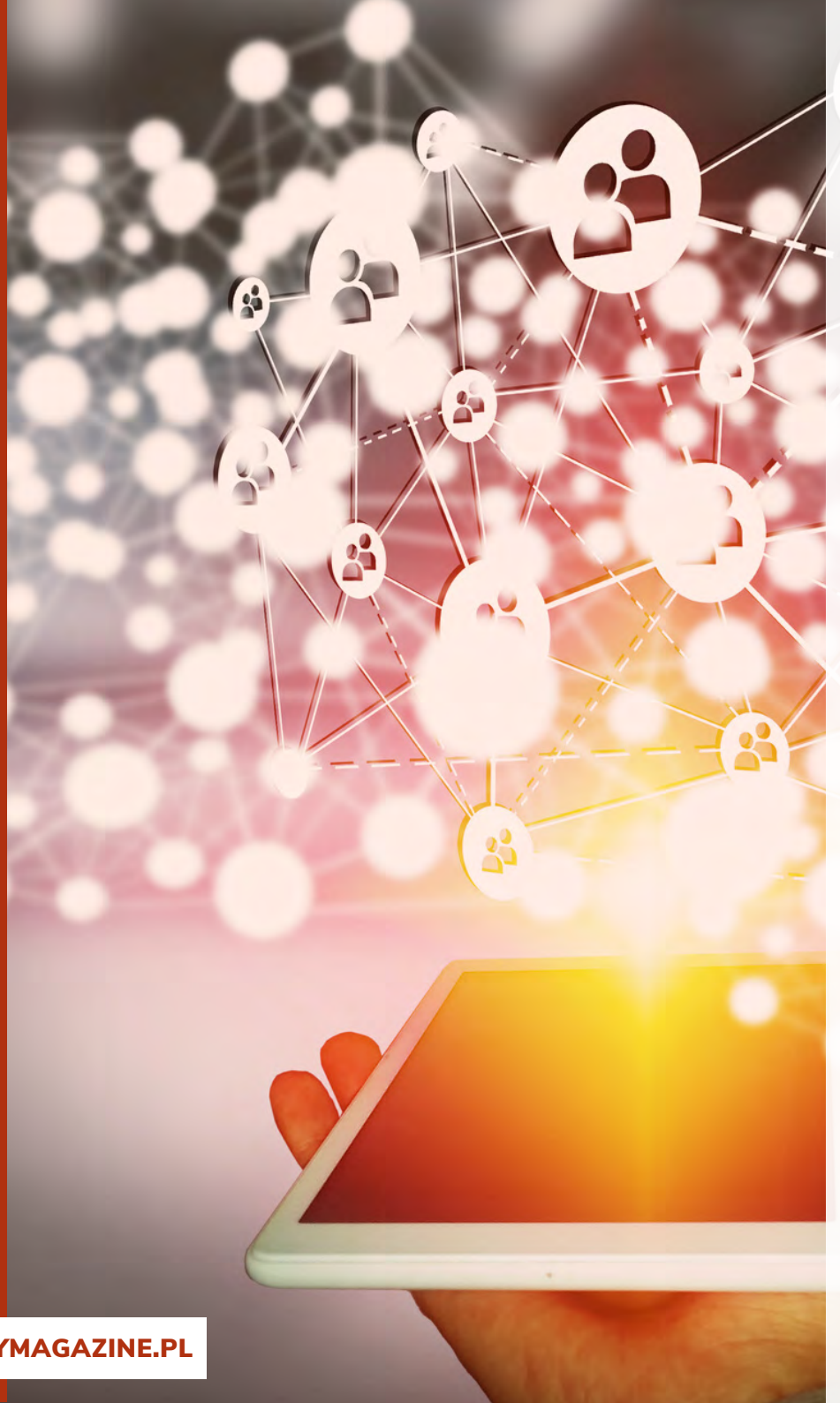
CZY MOŻNA SKORZYSTAĆ Z KONTAKTU Z ADMINISTRACJĄ LINKEDIN?

Czasami sprawy zajdą za daleko: ktoś podepnie swoją kartę kredytową pod inne konto, zostaną ściągnięte z niej pieniądze, czy zostanie skradziona strona firmowa. Albo zwyczajnie chcemy usprawnić proces odzyskiwania dostępu do konta. Wtedy warto skorzystać z możliwości kontaktu z supportem - działem **LinkedIn Help.** W tym celu, po zalogowaniu się na LinkedIn warto wejść **na stronę**.

Ponadto na stronie głównej “LinkedIn Wsparcie” możemy rozpocząć rozmowę tekstową na żywo.
W tym celu należy kliknąć na niej **Czat z Asystentem Pomoc**. Co jest istotne, w tym wypadku istnieje możliwość rozmowy z supportem tylko w języku angielskim.

SKAN DOWODU OSOBISTEGO NA POTWIERDZENIE TOŻSAMOŚCI. ZGODNY Z PRAWEM?

Supporty LinkedIn, jak i Facebooka czasami życzą sobie przesłania dokumentu ze zdjęciem. potwier-



dzającego tożsamość. Istnieje kilka powodów, dla których mogą to zrobić. Tak tłumaczy to Facebook:

- *“Potwierdzenie, że konto, do którego chcesz uzyskać dostęp, należy do Ciebie. Dbamy o Twoje bezpieczeństwo. Prosimy o dokument tożsamości, aby nikt inny oprócz Ciebie nie uzyskał dostępu do Twojego konta."*

- *"Potwierdzenie Twojego imienia i nazwiska: Prosimy wszystkie osoby na Facebooku o posługiwanie się imieniem i nazwiskiem, którego używają na co dzień. W ten sposób chronimy naszą społeczność przed skutkami podszywania się pod inne osoby."*

- *"Innym powodem, dla którego możemy prosić o potwierdzenie tożsamości, jest zapobieganie nadużyciom, takim jak oszustwa, phishing oraz wpływanie na politykę z zewnątrz.”*

Budzi to niemałe kontrowersje wśród użytkowników tych social mediow.

- Przesyłanie kopii dowodu osobistego do Facebooka celem weryfikacji osoby i odblokowania konta budzi kontrowersje pod względem ochrony danych osobowych. Z jednej strony są przepisy, które wskazują, że tylko niektóre podmioty mogą

przetwarzać dane osobowe zawarte w dokumentach tożsamości. Z drugiej natomiast mamy zasadę swobody umów, która pozwala nam na dowolne kształtowanie umowy między stronami, jak i nie-posiadanie konta na portalu społecznościowym w ogóle. Obydwa rozwiązania niosą za sobą też pewne ograniczenia, stąd dyskusje w tym temacie. Natomiast Facebook poza dowodem osobistym wymienia również możliwość przesłania kopii innego dokumentu - wyjaśnia **Aneta Grala, specjalistka ds. ochrony danych osobowych w Rzetelnej Grupie.**

POWIADOM POLICJĘ O WŁAMANIU NA KONTO FACEBOOK I LINKEDIN

Warto iść na najbliższy komisariat policji w celu zgłoszenia włamania na konto i jego kradzieży. Dzięki temu możemy uniknąć wielu nieprzyjemnych sytuacji. Jeśli osoba, która włamała się na nasze media społecznościowe zacznie wyłudzać pieniądze lub oszukiwać w inny sposób, podszywając się pod nas, unikniemy odpowiedzialności za jej czyny. Haker może w ten sposób nawet wyczyścić z pieniędzy nasze konto bankowe! Ponadto oszust może wykorzystać przeciwko nam nasze wrażliwe dane z rozmów prywatnych na Messengerze czy osobiste, intymne zdjęcia.

Osobie, która włamała się na nasze konto w mediach społecznościowych oraz uniemożliwia korzystania z niego właścicielowi, grozi kara pozbawienia wolności do 3 lat. Policja dysponuje wieloma narzędziami, które pozwolą na zlokalizowanie oszusta.


Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?
Sprawdź ofertę
PATRONATU
MEDIALNEGO
SECURITY MAGAZINE
Napisz do nas:
redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL

CZARNE ŁABĘDZIE ISTNIEJĄ. ADVANCED THREAT SUMMIT 2022

PATRONAT
SECURITY MAGAZINE

Czarny łabędź - nieoczekiwane zdarzenie, którego prawie nikt nie jest w stanie przewidzieć. Ma często ogromny (i negatywny) wpływ na świat i społeczeństwo. Często dopiero po czasie da się logicznie wyjaśnić przyczyny i początek czarnego łabędzia. Na takie czarne łabędzie musimy być przygotowani. ”W przypadku cyberbezpieczeństwa wymaga to jeszcze większej pracy i pełniejszej perspektywy niż dotychczas” - uważają organizatozy ATS2022 - święta cyberbezpieczeństwa w Polsce.

Fot. Evention oraz redakcyjne

ZNAK ROZPOZNAWCZY? PROFESJONALIZM

9. edycja konferencji Advanced Threat Summit trwała aż trzy dni i wypełniona była po brzegi wiedzą z zakresu cyberbezpieczeństwa. Odbyła się formule hybrydowej - pierwszego dnia uczestnicy mogli spotkać się stacjonarnie w warszawskim hotelu Marriott albo online. Dwa kolejne dni to już aktywności online (konferencja, warsztaty technologiczne oraz Fora Dobrych Praktyk).

Nie bez powodu organizatorzy - firma Evention oraz ISSA Polska - określili wydarzenie jednym z największych i najważniejszych w naszym kraju z zakresu cyberbezpieczeństwa. Nad wysokim poziomem merytorycznym programu konferencji czuwała Rada Programowa złożona z doświadczonych praktyków, a w roli prelegentów znaleźli się wytrawni eksperci cybersecurity. Podczas wykładów oraz dyskusji w formie videorozmowy można było uzyskać wiedzę z pierwszej ręki oraz wymienić się doświadczeniami.

Konferencja była tak zorganizowana, by odpowiadała na potrzeby i zainteresowania profesjonalistów, którzy odpowiadają za bezpieczeństwo cyfrowe swoich organizacji.

Patronat Security Magazine.
Advanced Threat Summit

PROGRAM

Program był niezwykle rozbudowany i znalazły się w nim tematy m.n. z zarządzania powierzchnią ataku, bezpieczeństwo otoczenia, chmura, automatyzacja i AI w cyberbezpieczeństwie, Zero Trust czy zarządzanie ryzykiem.

Całe wydarzenie poprzedził dzień wprowadzający. Odbyły się wówczas warsztaty i spotkania specjalne oraz kolacja dla prelegentów i panelistów. Uczestnicy brali udział w warsztacie, który poprowadził Paul Simmonds, Cloud Security Alliance, The Global Identity Foundation. Spotkanie dla branży finansowej poprowadziła Teresa Walsh, Global Head of Intelligence, Financial Service Information Sharing and Analysis Centre z FS-ISAC.

Pierwszy dzień, 22 listopada, zgromadził 400 uczestników. Odbyły się dwie sesje: onsite i online. Pierwszą z nich poprowadził Grzegorz Turniak, drugą - Agnieszka Wielądek, Community Manager Evention. Uczestnicy internetowi byli losowo podzieleni na kilkuosobowe grupy po to, by w bezpośredniej rozmowie mogli porozmawiać i dowiedzieć się skąd są, co ich zachęciło do udziału w ATS oraz czym sami mogliby podzielić się z innymi.

Konferencję otworzyli oficjalnie: Mariusz Belka, Prezes Zarządu ISSA Polska, dr Shawn Murray, Chief Operating Officer ISSA International i Przemysław Gamdzyk, CEO, Meeting Designer Evention. Po tym rozpoczęły się sesje, panele dyskusyjne, a także spotkania towarzyszące.

Patronat Security Magazine.
Advanced Threat Summit

Obszar tematyczny był niezwykle szeroki i wyczerpujący. Każdy z uczestników znalazł coś dla siebie.

Wśród prezentacji znalazła się ta poświęcona zaufaniu do naszych partnerów biznesowych i temu, jak często oszuści wykorzystują ten słaby punkt, by zaatakować nas przez pośrednictwo czy zaatakować nas, choć jego celem jest zupełnie ktoś inny, z kręgu naszych współpracowników czy właśnie partnerów biznesowych.

- Im większe zaufanie, im silniejszy związek, tym gorzej dla bezpieczeństwa. Bo właśnie tą relację zaufania podczas ataku na łańcuch dostaw się wykorzystuje. Jak porozmawiacie sobie z tymi, którzy mieli okazje takie bardziej kompleksowe testy przeprowadzać, to się pewnie dowiecie, że pierwszą rzecz, jaką usiłują zrozumieć, to nie jest, jakie podatności ma cel, tylko jakie relacje zaufania są budowane ze światem zewnętrznym i w jaki sposób są one budowane pomiędzy ludźmi i innymi systemami. A podatności to już jest później technikalium, które się wykorzystuje. (...) Już co piąty atak jest motywowany tym, żeby wykorzystać uzyskany dostęp w celu zaatakowania kogoś innego, kto jest powiązany z naszym pierwszym celem - powiedział **Rafał Jaczyński, Regional Cyber Security Officer CEE & Nordics z Huawei Technologies,** dodając: - *Bezpieczeństwo, zaufanie w bezpieczeństwie z definicji jest podatnością. Dlatego ataki są tak groźne. A tymczasem większość firm traktuje to zagrożenie, bardzo poważne zagrożenie, takim procesem, który działa na takiej zasadzie odwróconej zasady pareto. To znaczy ładujemy w ten proces 80% zasobów, uzyskujemy zysk na poziomie redukcji ryzyka o 20%.*

Patronat Security Magazine.
Advanced Threat Summit

O tym jak firmy radzą sobie z cyberbezpieczeństwem zagranicą opowiedziała dr Magda Chelly z Responsible Cyber. Sebastijan Čutura z European Cybersecurity Organisation próbował znaleźć odpowiedź na pytanie: dlaczego brakuje współpracy pomiędzy społecznościami cybersecurity na poziomie europejskim? Przeszłość i teraźniejszość cyberwojny na Ukrainie przedstawił Robert Lipovsky z ESET. Na pytanie: z czym się mierzymy i jak “robimy” cyberbezpieczeństwo w czasach wielkiej zmiany? odpowiedział John Salomon z FS ISAC. Vandana Verma, wiceprezes OWASP wprowadził uczestników w tematykę mitygacji ryzyk w łańcuchu tworzenia oprogramowania.

O tym jak firmy radzą sobie z cyberbezpieczeństwem zagranicą opowiedziała dr Magda Chelly z Responsible Cyber. Sebastijan Čutura z European Cybersecurity Organisation próbował znaleźć odpowiedź na pytanie: dlaczego brakuje współpracy pomiędzy społecznościami cybersecurity na poziomie europejskim? Przeszłość i teraźniejszość cyberwojny na Ukrainie przedstawił Robert Lipovsky z ESET. Na pytanie: z czym się mierzymy i jak “robimy” cyberbezpieczeństwo w czasach wielkiej zmiany? odpowiedział John Salomon z FS ISAC. Vandana Verma, wiceprezes OWASP wprowadził uczestników w tematykę mitygacji ryzyk w łańcuchu tworzenia oprogramowania.

ZERO TRUST

Jeden z paneli dotyczył tematu “Zero Trust”. Michał Ceklarz, Eks-

Patronat Security Magazine.
Advanced Threat Summit

pert cyberbezpieczeństwa z Microsoft, Damian Kuźma, Ekspert ds. Cyberbezpieczeństwa z Advatech, Eryk Trybulski, Dyrektor Bezpieczeństwa Informacji z home.pl i Robert Wysocki, International Chief Information Security Officer z Aviva próbowali znaleźć odpowiedź na pytanie, czy faktycznie Zero Trust to bardziej definicja problemu niż jego rozwiązanie? Dlaczego tak brakuje wspólnego rozumienia, uznanych definicji, standardów. Czy to może się zmienić?

- Nie ufamy nikomu, ludziom, technologiom, procesom.Ten tradycyjny model nie do końca się sprawdza i mamy tego bardzo dobre przykłady. (...) W pewien sposób ufamy pracownikowi, którego zatrudniliśmy i w jakiś sposób sprawdziliśmy. Ale nie do końca. Zero Trust tak naprawdę w każdym elemencie sieci, infrastruktury, aplikacji, danych. W procesie identyfikacji powinniśmy mieć element weryfikujący. To jest trochę sprzeczne z takim ludzkim podejściem, bo my lubimy ufać. A nie powinniśmy ufać w ogóle - powiedział **Robert Wysocki, International Chief Information Security Officer z Aviva.**

- Zero Trust to podejście przez myślenie, że to nie tylko technologia, ale również zachowania behawioralne. Dlaczego Zero Trust zyskało taką popularność. Bo to jest ewolucja w cyberbezpieczeństwie - dodał **Eryk Trybulski, Dyrektor Bezpieczeństwa Informacji z home.pl. Z kolei Michał Ceklarz, Ekspert cyberbezpieczeństwa z Microsoft** podkreślił, że Zero Trust to swego rodzaju azymut, który określa nam kierunek, w jakim powinniśmy myśleć o bezpieczeństwie. - *Dlaczego Zero Trust zyskał na popularności? Dlatego, że jest w miarę prosty i łatwy do wytłumaczenia. (...) Zero Trust jest pewną drogą, którą podążamy po to, aby zapewnić to bezpieczeństwo w firmie z ograniczonym zaufaniem* - zaznaczył.

SESJE I CYBERWOMEN COMMUNITY

21 listopada odbyły się dwie sesje podzielone na trzy ścieżki. Każda z innych obszarów


ZERO DAY
ON EVERY DAY


High Value Assets
CISA
White House
ADVANCED THREAT
FORTINET
HUAWEI
ISSA

tematycznych cyberbezpieczeństwa: zero day, zaufanie i tożsamość, informacje i autonomia w cyberbezpieczeństwie i przeciwdziałanie zagrożeniom, a także trendy, studia przypadków oraz “na wojnie”. Pierwszego dnia odbyło się również spotkanie specjalne Cyberwomen Community traktujące o tym, jak wygląda praca i sytuacja kobiet w cyber w Wielkiej Brytanii, Irlandii i w Azji. Dzień zakończył wieczór integracyjny z gościem specjalnym, Piotrem Czuryłło, prezesem Fundacji Polish Preppers Network.

DNI WARSZTATÓW, KONFERENCJI ONLINE. FORA DOBRYCH PRAKTYK

Dwa kolejne dni to seria profesjonalnych warsztatów, sesji plenarnych i paneli dyskusyjnych. Jeden z warsztatów pod tytułem "Jak przekuć ryzyka w szanse czyli łatwe oraz efektywne zarządzanie ryzykiem IT" poprowadził Paweł Ładna, ekspert ds. rozwiązań IAM/PAM oraz GRC dla zarządzania ryzykiem w organizacji z SimplySec, który publikował już na łamach "Security Magazine" (*"Cyberbezpieczeństwo instytucji finansowych w świetle regulacji DORA, wydanie 5/2022).*

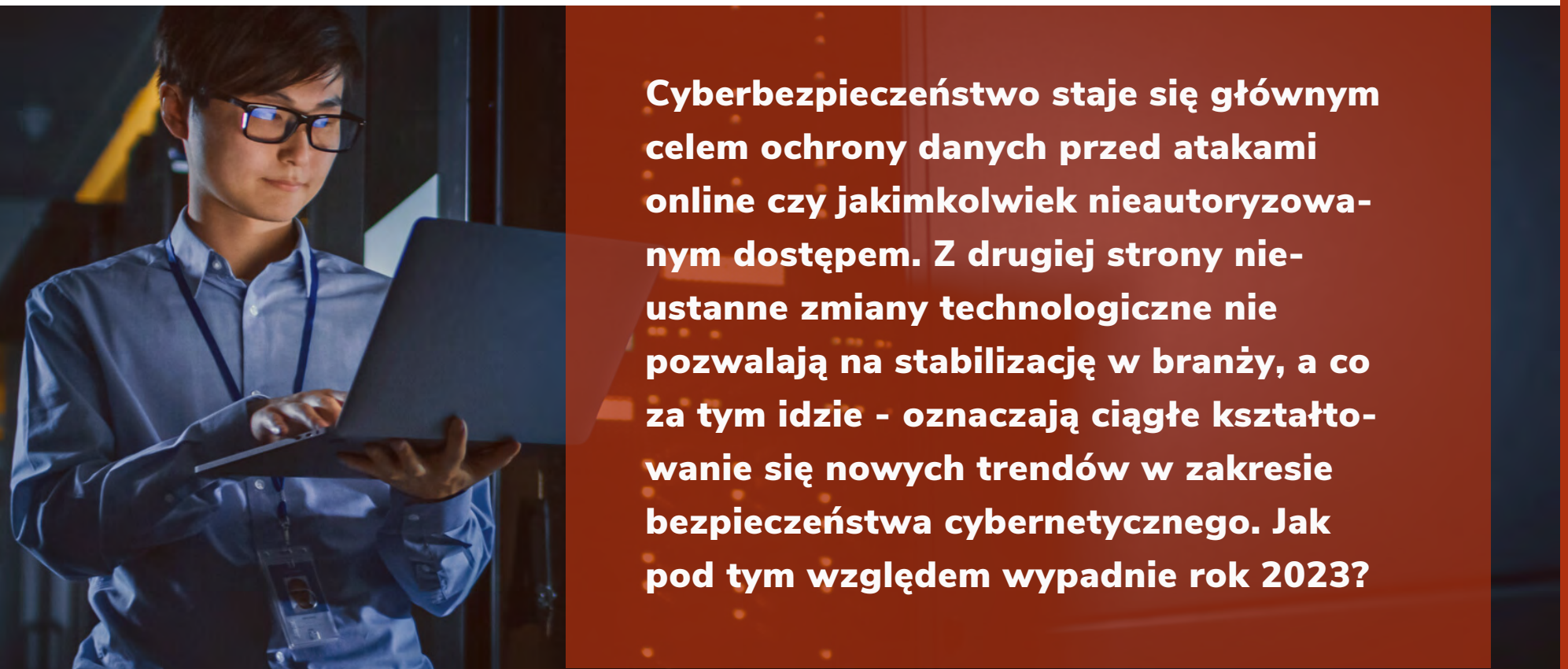
Podczas debaty strategicznej "Cyberbezpiecznik na straży metawersum" na pytania co metaświat oznacza dla osób zajmujących się cyberbezpieczeństwem, jak zmieni branżę i jakie otworzy możliwości i wyzwania, odpowiadali Lech Lachowicz, Senior Manager Global Cybersecurity Engineering z PepsiCo i ISSA Polska, prof. Jerzy Surma z Instytutu Informatyki i Gospodarki Cyfrowej SGH, Piotr Ciepiela, Partner, Global & EMEIA Architecture, Engineering & Emerging Technologies Security Leader z EY, Alicja Skraburska, Cybersecurity Technical Lead / CISO advisor z HSBC oraz Błażej Szymczak, Chief Security Officer z MODIVO.

ATS 2022 zamknął dzień pod hasłem "Forum Dobrych Praktyk". Odbyły się kameralne dyskusje w małych grupach, które miały na celu zapoznanie uczestników z najlepszymi praktykami wybranych przez nich obszarów.

SECURITYMAGAZINE.PL

2023 ROK W BRANŻY CYBERSECURITY

Redakcja
SECURITY MAGAZINE



Cyberbezpieczeństwo staje się głównym celem ochrony danych przed atakami online czy jakimkolwiek nieautoryzowanym dostępem. Z drugiej strony nieustanne zmiany technologiczne nie pozwalają na stabilizację w branży, a co za tym idzie - oznaczają ciągłe kształtowanie się nowych trendów w zakresie bezpieczeństwa cybernetycznego. Jak pod tym względem wypadnie rok 2023?

MARTA FYDRYCH-GĄSOWSKA
Akamai Technologies

Żyjemy w świecie niezwykłych połączeń. Walka USA i Chin o dominację nad globem wywołuje lawinę nowych cyberzagrożeń. Dzieje się tak, ponieważ wszystkie strony konfliktu traktują cyberprzestrzeń jako kolejną domenę rywalizacji.

Wyzwania

Po inwazji Rosji na Ukrainę cyberprzestępcy wzięli na celownik m. in. europejski sektor finansowy. Znacząco wzrosła liczba ataków DDoS, zaś w zakresie ataków na aplikacje webowe i API sektor ten doznał 3,5-krotnego wzrostu ataków rok do roku. Rośnie też ich złożoność (wzrost o 81 proc. aktywności z udziałem botów).

W 2023 roku możemy spodziewać się kontynuacji trendu odwrócenia celownika cyberprzestępców z Ameryki Północnej na region EMEA.

Do końca listopada 2022 roku liczba ataków DDoS spadła w Ameryce do 22,14 proc, natomiast w Europie wzrosła do 73,30 proc.

Szczególnie zagrożone mogą czuć się organizacje tzw. infrastruktury krytycznej, choć biorąc pod uwagę szeroki wachlarz motywacji przestępców (czy to ideologicznych, czy finansowych) ani sektor publiczny ani prywatny nie mogą się czuć bezpieczne.

Cierniem w tkance sektora finansowego jest phishing. Dzieje się tak, ponieważ pozwala on atakować masowo zwykłych ludzi, którzy zawsze są bardziej podatni niż instytucje. Automatyzacja oraz sztuczna inteligencja jeszcze bardziej poszerzą zakresy tego typu ataków.

Priorytety

Napięcia na linii USA-Chiny zagrażają zerwaniem łańcuchów dostaw – według Boston Consulting Group tylko 10 proc. firm jest przygotowanych na taką ewentualność. Nie możemy już bezgranicznie polegać na swoich dostawcach – gdy padną ofiarą cyberataku, mogą stać się źródłem realnego zagrożenia dla naszej organizacji.

Niepokoją także dane z raportu KPMG, wedle których prawie połowa firm (48 proc.) wcale nie planuje inwestować w bezpieczeństwo podczas wytwarzania oprogramowania, a 42 proc. nie zamierza ponosić nakładów na klasyfikację i kontrolę aktywów. Jest to mocno ryzykowne podejście, biorąc pod uwagę złożoność dzisiejszych powiązań i systemów.

Cyberprzestępstwa

Nie obronimy się przed wszystkim, ale możemy przygotować się na najbardziej prawdopodobne wektory ataku.

1. Monitorujmy styk organizacji z Internetem poprzez Web Application Firewall,
2. Zadbajmy o solidny system wykrywania i łatania podatności,
3. Zadbajmy o solidny i bezpieczny system autentykacji w systemach; cyberprzestępcy dużo częściej koncentrują się na kradzieży haseł niż na łamaniu wymyślnych systemów kryptograficznych. Może czas rozważyć podejście passwordless?
4. Przejrzyjmy i zaktualizujmy procedury reagowania na incydenty
5. Zweryfikujmy role i odpowiedzialności w organizacji
6. Wdróżmy w organizacji podejście Zero-Trust
7. Monitorujmy dostawców i kontrahentów
8. Zadbajmy o nieustającą edukację pracowników w zakresie bezpieczeństwa. Najsłabszym ogniwem łańcucha bezpieczeństwa bowiem nadal jest człowiek i najwymyślniejsze systemy zabezpieczeń przegrają, jeśli pracownicy nie będą świadomi czyhających na nich zagrożeń.

PRZEMYSŁAW KANIA
Cisco w Polsce

W ostatnim czasie obserwujemy zmianę podejścia do realizacji bezpiecznego dostępu zdalnego. Bardziej nowoczesne organizacje dążą w kierunku modelu VPN-less - mechanizmu, który umożliwia zdalny dostęp do aplikacji w oparciu o Zero Trust, bez konieczności korzystania z VPN lub bezpośredniego udostępniania tych programów w internecie. Daje to każdemu użytkownikowi końcowemu możliwość elastycznego korzystania z wybranych aplikacji z dowolnego urządzenia i z dowolnego miejsca, nakładając kontekstowe polityki dostępowe. Oczywiście, tego typu pracownik posiada dodatkowe mechanizmy bezpieczeństwa chroniące jego tożsamość, stację końcową czy aktywności w internecie.

Wyzwania

Coraz większe rozdrobnienie rynku cyberbezpieczeństwa oraz stale zmieniający się krajobraz cyberzagrożeń wywierają ogromną presję na działy IT. Jednocześnie na rynku brakuje specjalistów od cyberbezpieczeństwa. Dlatego organizacje coraz częściej zwracają się do zewnętrznych dostawców usług, którzy zdejmą z nich część obowiązków związanych z zapewnieniem ochrony infrastruktury IT i cyfrowych zasobów firmy, przy jednoczesnym stałym i przewidywalnym w dłuższej perspektywie czasu poziomie kosztów.

Priorytety

Gdy w wyniku pandemii i masowego przejścia na pracę zdalną i hybrydową granica między pracą a domem trwale się zatarła, nawyki wykorzystywane do aktywności osobistej są coraz częściej stosowane w pracy, co stanowi ogromne zagrożenie dla organizacji. Chociaż nie mogą one nigdy do końca wyeliminować ludzkiego błędu, z pewnością mogą złagodzić jego konsekwencje.

Firmy powinny bezpiecznie przechowywać dane w chmurze i umożliwiać dostęp w oparciu o zasady zerowego zaufania (zero trust), dostosowując dostęp do indywidualnych potrzeb i kontekstu.

Z kolei kontrolowanie dostępu do systemów w chmurze za pośrednictwem architektury Secure Access Service Edge (SASE) zapewnia zespołom bezpieczeństwa wgląd i kontrolę dostępu zdalnego.

Cyberprzestępstwa

Cyberprzestępcy coraz częściej wykorzystują różne ogólnodostępne narzędzia i skrypty. Warto zauważyć, że większość publicznie dostępnych narzędzi wykorzystanych w tym kwartale wydaje się skupiać na uzyskiwaniu dostępu i zbieraniu danych uwierzytelniających, co podkreśla rolę, jaką narzędzia te odgrywają w potencjalnym wspieraniu celów cyberprzestępców. Wg Cisco Talos, na stronach internetowych i w repozytoriach coraz częściej pojawiają się narzędzia i skrypty, które wspierają operacje cyberprzestępców na różnych etapach ataku.

W związku z tym, obniża się też próg wejścia (merytoryczny i finansowy), od którego można zostać cyberprzestępcą.

MICHAŁ ROSIAK
CERT Orange Polska

Od 24 lutego znacząco zmieniła się nasza rzeczywistość geopolityczna. Trwający przez cały ten czas stan alarmowy CRP-Charlie to nie przypadek, a ataki mające na celu zaburzenie działania czy to administracji, czy firm, mający wpływ na nasze codzienne życie, to nie scenariusz z Hollywood. Jeszcze przed wojną istotna część złośliwej aktywności w Polsce pochodziła ze wschodu. Ukierunkowanie jej na konkretne cele, a do tego „crowdsourcing" ataków DDoS wśród nienawidzących zachodu, czy też zbuntowanych młodych Rosjan, mogą przełożyć się na poważne zagrożenia nie tylko dla strategicznie ważnych firm.

Wyzwania

Wyzwaniem na następny rok wydaje się być zmiana podejścia. Z „nas nie zaatakują" na „kiedy nas zaatakują", na świadomość, że każdy może być celem. Przetestowanie swojej infrastruktury pod kątem podatności na zagrożenia – jeśli nie mamy takich kompetencji to na rynku jest sporo firm, które mają w tym doświadczenie.

Edukacja pracowników, przekonanie, by każde podejrzenie zgłaszali. Stworzenie miejsca, gdzie mogą się zgłaszać, obsługa tych zgłoszeń na bieżąco i absolutnie nie bagatelizowanie ich. Lepiej dostać 100 fałszywych alarmów, niż przegapić jeden prawdziwy.

Priorytety

Czynnik ludzki wciąż odpowiada za przeszło 95% udanych ataków, stawiałbym więc przede wszystkim na edukację. A w tej materii konsekwentnie i uparcie od lat promuję nierozróżnianie pomiędzy bezpieczeństwem „domowym" i „korporacyjnym".

Nie edukujmy pracowników, edukujmy ludzi! Przecież, jeśli nauczymy ich, czym jest phishing, co im grozi w sieci, w co nie klikać, to logując się do sieci w pracy o tym nie zapomną. A edukowani jako ludzie, właśnie ludźmi się poczują. A nie „zasobem przedsiębiorstwa".

Cyberprzestępstwa

Z punktu widzenia CERT Orange Polska drugie półrocze 2022 to w znaczącej części socjotechniczne ataki pod szyldem „inwestycji w krajowy przemysł".

Pojawiają się w potężnej liczbie jako reklamy na Facebooku, a docelowo do ofiary dzwoni „konsultant", przekonujący ją do instalacji aplikacji „inwestycyjnej", tak naprawdę dającej napastnikowi pełny dostęp do zainfekowanego komputera.

Efekt to strata wszystkich pieniędzy z kont bankowych i nierzadko zaciągnięcie kredytów na ofiarę. Biorąc pod uwagę liczbę tego typu ataków, ten schemat dobrze działa. A skoro tak, to nie ma podstaw, by w przyszłym roku cokolwiek miało się zmienić. Firmy ostatecznie sobie poradzą: czy to inwestując w rozwiązania, w ekspertów, czy w outsource usług bezpieczeństwa. Ale każdy oszukany zwykły internauta to wielka ludzka tragedia.

TOMASZ KOWALSKI
Secfense

W ostatnich czasach temat cyberbezpieczeństwa przenosił się coraz częściej z działów IT do sal zarządów. Poważne ataki grożące utratą zaufania klientów oraz wysokie kary regulacyjne stały się priorytetem na każdym szczeblu organizacyjnym. Niezależnie jednak od funkcjonujących aktualnie przepisów czy aktów, które dopiero wejdą w życie, silne i wieloskładnikowe uwierzytelnianie (MFA) nadal pozostanie podstawową rekomendacją dla firm w zakresie cyberbezpieczeństwa.

Wyzwania

Często myślimy o cyberbezpieczeństwie jako o bitwie toczącej się między cyberprzestępcami a ekspertami ds. bezpieczeństwa, która stale się nasila ze względu na ciągły postęp technologiczny. I faktycznie, czasami zagrożenia pochodzą od wrogich państw lub przebiegłych. obeznanych z technologią intruzów.

W rzeczywistości jednak problemy wynikają ze źle zabezpieczonych sieci i aplikacji. Na ataki narażają też firmy ich niedyskretni lub nieostrożni pracownicy, którzy korzystają z niezabezpieczonych urządzeń podczas pracy w domu.

Priorytety

W nachodzącym roku temat ochrony i zabezpieczenia użytkowników i aplikacji silnym, wieloskładnikowym uwierzytelnianiem będzie nie tylko trendem, a koniecznością. Wszystkie organizacje bowiem, którym zależy na najwyższym poziomie bezpieczeństwa, muszą nie tylko mieć włączone MFA na każdej aplikacji, ale powinny też zrezygnować z półśrodków i zastąpić je metodami dużo doskonalszymi i dającymi prawdziwą ochronę przed phishingiem. Mowa tu o uwierzytelnianiu opartym na standardzie FIDO2, czyli metodzie uwierzytelniania z wykorzystaniem nowoczesnej odmiany biometrii twarzy lub kciuka, lub fizycznych kluczy kryptograficznych FIDO2/U2F.

Tylko takie metody bowiem są w stanie dać 100% pewności co do osoby znajdującej się po drugiej stronie monitora.

Czy jest to właściwy pracownik, czy może intruz, któremu udało się wykraść lub kupić na czarnym rynku cudze loginy i hasła. W Secfense opracowaliśmy technologię, która w pełni automatyzuje proces wdrożenia silnego uwierzytelniania, umożliwiając szybkie i łatwe uruchomienie MFA na dowolnej liczbie aplikacji bez żadnej ingerencji w kod.

Cyberprzestępstwa

Miejmy nadzieję, że dzięki łatwości, szybkości i dużo mniejszej potrzebie zaangażowania specjalistów IT, których – jak wiemy – na rynku brakuje, implementacja dobrych i skutecznych metod uwierzytelniania na szeroką skalę utrudni „pracę" intruzom, którzy czerpią dziś ogromne zyski z kradzieży tożsamości w sieci.

RAFAŁ STĘPNIEWSKI
Rzetelna Grupa Sp. z o.o.

Mając na uwadze dzisiejszą wyjątkową aktywność cyberprzestępców w roku 2023 będzie królowało hasło zero trust. Dziś przy rozbudowanej sieci dostawców wielu usług lub komponentów, to właśnie firmy współpracujące stanowią główne wektory ataków. Edukacja w tym zakresie, zmiany organizacyjne i ciągłe zabezpieczanie łańcuchów dostaw, to tylko kilka z wielu wyzwań jakie będą stały przed firmami.

Wyzwania

W ostatnim czasie w mediach zaczęły pojawiać się spoty rządowe uświadamiające, czym są cyberprzestępstwa (w tym przede wszystkim phishing) i jakie niosą za sobą konsekwencje dla ofiar. Moim zdaniem, to o cały rok za późno, zważywszy na fakt, że cyberwojna trwa dużo dłużej.

Cyberprzestępcy chętnie wykorzystują ten fakt, stąd wręcz wysyp ataków phishingowych w tym roku.

Być może w 223 będzie większy nacisk na edukację i uświadamianie i to, uważam, będzie największym wyzwaniem dla branży cybersecurity. Branża bowiem powinna skupić się nie tylka na ochronie i obronie, ale również na edukowaniu innych.

Priorytety

W 2023 kluczową rolę odegra rozwój sztucznej inteligencji. Będzie ona nabierała na znaczeniu i będzie wykorzystywana przez obie strony tj. firmy do obrony przed zagrożeniami oraz przez cyberprzestępców do prowadzenia ataków.

Cyberprzestępcy używają jej do opracowywania inteligentnego złośliwego oprogramowania oraz ataków w celu obejścia naj-nowszych rozwiązań bezpieczeństwa. Z drugiej strony systemy wykrywania zagrożeń wykorzystujące sztuczną inteligencję mogą przewidywać nowe ataki i natychmiast powiadamiać o zagrożeniach.

Cyberprzestępstwa

Z naszego doświadczenia w prowadzeniu kanałów w mediach społecznościowych wynika, że na platformach wciąż istnieją luki, które albo już są albo mogą być wykorzystywane przez cyberprzestępców i mają oni tego pełną świadomość. Wiedzą doskonale, że administracja portali jest niemal niedostępna (co może wręcz dziwić, kiedy mamy do czynienia z rzeczywistym atakiem na konto - tu powinno się działać jak najszybciej, tymczasem sprawy ciągną się miesiącami, a nawe latami) pomoc dla użytkowników moderowana jest przez boty, co nie pozwala spojrzeć na sprawę w sposób indywidualny. Przykładem jest tu sytuacja jednej z polskich klinik, pod którą już od dwóch lat(!!!) podszywają się oszuści przy pomocy reklam i ani klinika, ani administracja portalu nie są w stanie namierzyć, kto stoi za tego typu phishingiem.

Powszechnie wiadomo, że najsłabszym ogniwem w temacie cyberbezpieczeństwa są ludzie, dlatego tak skuteczne są wszelkiego rodzaju manipulacje, w tym dezinformacje. Niemniej akcji uświadamiających jest coraz więcej, coraz częściej przyglądamy się dwa razy wysłanym do nas mailom, SMS-om, ofiary też częściej opowiadają o swoich przypadkach. Stąd, moim zdaniem, socjotechniki nadal będą wykorzystywane, jednak cyberprzestępcy mogą szukać zupełnie nowych rozwiązań.

KRZYSZTOF ANDRIAN
Concept Data

Liczba urządzeń podpiętych do Internetu i komunikujących się ze sobą rośnie z roku na rok. I nie chodzi tylko o inteligentne telewizory czy drukarki. Coraz częściej są to też elementy infrastruktury OT. Firmy muszą zarządzać stale rozrastającą się siecią xIoT (extended IoT, czyli urządzeniami IoT, OT oraz sieciowymi), także w kontekście bezpieczeństwa. A ataków na nią wciąż przybywa i nie zmieni się to w 2023 roku.

Wyzwania

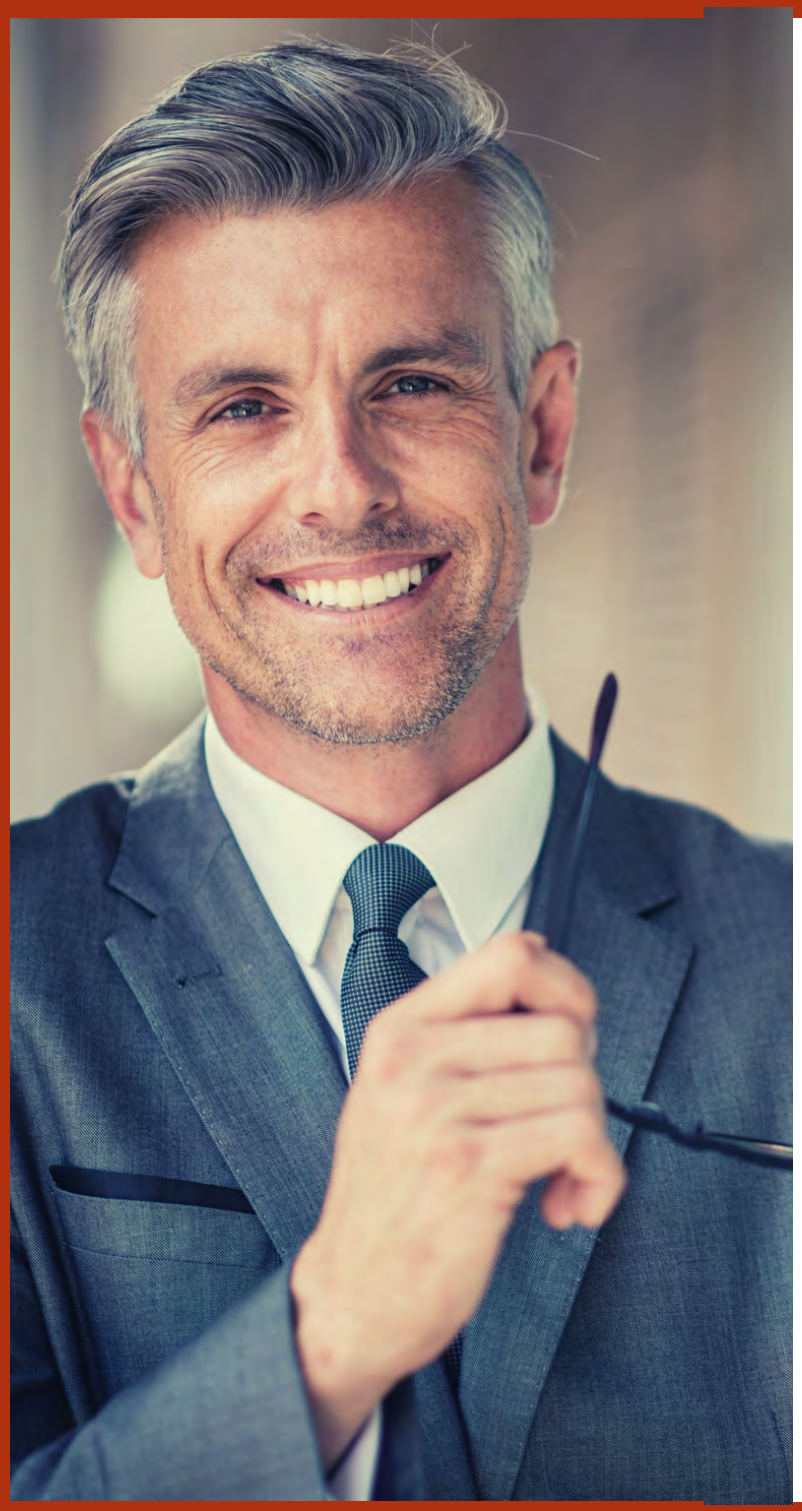
Kamery bezpieczeństwa, głośniki, switche, drukarki, kontrolery pracy maszyn, telefony VoIP, termostaty czy inteligentne telewizory – to wyposażenie wielu firm i zakładów przemysłowych. Według badań naszego partnera technologicznego, amerykańskiej firmy Phosphorus, na jednego pracownika w każdej firmie przypada od 3 do 5 takich urządzeń.

Oczywiście ułatwiają pracę, ale są też furtką dla cyberprzestępców. Dlaczego? Te same badania Phosphorusa pokazują, że 50% urządzeń xIoT ma domyślne i nigdy niezmieniane hasła, a 26% oprogramowania sterującego ich pracą nie ma już wsparcia producentów. Atak na sieci xIoT jest zatem prosty i może pozwolić cyberprzestępcom na infiltrację sieci IT, wykradanie tajemnic przedsiębiorstwa czy sabotowanie działań firmy.

Priorytety

O tym, że jest to poważny problem, świadczą statystyki przedstawione przez Barracuda Networks w lipcu 2022 roku. Aż 94% ankietowanych firm potwierdza, że w ciągu ostatnich 12 miesięcy doświadczyło incydentu związanego z bezpieczeństwem IoT. To nie zmieni się w najbliższym czasie, dlatego tak ważne jest dziś dbanie o bezpieczeństwo sieci xIoT w przedsiębiorstwach. Podstawą jest pełny wgląd w to, co znajduje się w sieci, identyfikacja wszystkich urządzeń, automatyczne wykrywanie, usuwanie i monitorowanie podatności i bieżące zapobieganie wykorzystaniu elementów xIoT do przeprowadzania ataków sieciowych.

Z tym na pewno firmy, zwłaszcza produkcyjne i przemysłowe, będą musiały się zmierzyć w 2023 roku.



DOŁĄCZ DO GRONA EKSPERTÓW

BUDUJ SWOJĄ MARKĘ
I ROZPOZNAWALNOŚĆ
SWOJEJ FIRMY

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PL

EKSPERCI WYDANIA

PRZEMYSŁAW KANIA
Dyrektor Generalny
Cisco w Polsce

Kieruje organizacją sprzedażową i techniczną oraz współpracą z niemal 800 partnerami Cisco w Polsce. Jest członkiem kadry kierowniczej Cisco w Europie Środkowej. Dołączył do Cisco w 1998 roku. Od tego czasu pełnił w firmie wiele funkcji związanych ze sprzedażą rozwiązań i usług Cisco. Absolwent informatyki na Akademii Górniczo-Hutniczej w Krakowie.

TOMASZ WOJAK
Prezes Zarządu
Seris Konsalnet

W Grupie Seris Konsalnet od 1995 r. Od 2000 r. w zarządach spółek Grupy. Od 2018 r. Prezes Zarządu Seris Konsalnet Holding S.A. Wykształcenie wyższe, absolwent studiów MBA, wykładowca w Wyższej Szkole Bankowej. Prezes Polskiego Związku Pracodawców Firm Ochrony oraz Wiceprezes Federacji Przedsiębiorców Polskich.

MARTA FYDRYCH-GĄSOWSKA
InfoSec & Compliance Advisor
Akamai Technologies

Audytor wiodący ISO 27001. Ekspertka bezpieczeństwa danych osobowych przy Radzie Europy i ENISA. Od 2014 roku związana z obszarem bezpieczeństwa informacji, prywatności i bezpieczeństwa danych osobowych. Ma doświadczenie we wdrażaniu zasad bezpieczeństwa w projektach IT). Ukończyła prawo na Uniwersytecie Warszawskim.

MICHAŁ ROSIAK
Cybersecurity Expert
CERT Orange Polska

Na co dzień bezpieczniak, hobbystycznie – gadżeciarz. Psycholog z wykształcenia, dziennikarz z doświadczenia, ojciec z wyboru, edukator z powołania. Dumny członek zespołu CERT Orange Polska, współautor m.in. CyberTarczy i Bezpiecznego Startera. Konsekwentnie edukuje internautów w zakresie bezpieczeństwa w internecie – słowem, obrazem i technologiami.

EKSPERCI WYDANIA

KATARZYNA KOLETYŃSKA
specjalistka
PIB - NASK

Autorka materiałów informacyjno-popularyzatorskich z zakresu bezpiecznego korzystania z internetu i nowych technologii oraz towarzyszących im zagrożeń. Odpowiedzialna za działania w zakresie budowania świadomości w obszarze cyberbezpieczeństwa, w tym m.in. kampanie edukacyjno-informacyjne, takie jak ECSM oraz współpracę z różnymi podmiotami w tym zakresie.

RAFAŁ JAKACKI
Head of E-commerce
home.pl

Od 2019 r. związany z firmą home.pl. Początkowo, jako kierownik produktu i specjalista od rozwiązań opensourcowych. Aktualnie, jako Head of e-commerce odpowiada za zarządzanie zespołem, wdrażanie nowych rozwiązań dla sklepów internetowych i optymalizację procesów.

KRIS DURSKI
Founder i dyrektor ds. technologii
Vault Security

Starszy analityk oprogramowania, programista, menedżer z ponad 20-letnim doświadczeniem w developingu i marketingu oprogramowania. Opracował koncepcję spersonalizowanego bezpieczeństwa w celu ochrony zasobów cyfrowych i materialnych. Współtworzył kilka start-upów z branży medycznej, technologii informacyjnej i cyberbezpieczeństwa.

ADRIAN ŁAPCZYŃSKI
Prezes Zarządu
EpicVR

Silnie zmotywowany CEO z 7-letnim doświadczeniem w dziedzinie zarządzania projektami informatycznymi, wdrażania innowacyjnych projektów z zakresu wirtualnej i rozszerzonej rzeczywistości, autor koncepcji wielu gier szkoleniowych i edukacyjnych VR.

EKSPERCI WYDANIA

KRZYSZTOF ANDRIAN
Prezes Zarządu
Concept Data

Na rynku ICT od ponad 20 lat. Wcześniej zarządzał zespołami i projektami oraz realizował strategie sprzedaży dla m.in.: Softbank, IBM Polska, Tieto Poland. W latach 2011-2014 zbudował i kierował nowym działem usług IT Contracting w Hays Polska.

INSP. DR MARIUSZ CIARKA
Rzecznik Prasowy
Komenda Główna Policji

Oficer Policji w stopniu inspektora, doktor nauk prawnych, od 2016 roku rzecznik prasowy Komendanta Głównego Policji. Członek Prezydium Rady Polityki Penitencjarnej III kadencji na lata 2020–2024. Dyrektor Biura Komunikacji Społecznej Komendy Głównej Policji. Redaktor naczelny Gazety Policyjnej i miesięcznika POLICJA997.

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

TOMASZ KOWALSKI
CEO i współzałożyciel
Secfense

CEO i współzałożyciel firmy z branży cybersecurity Secfense. Posiada ponad 20-letnie doświadczenie w sprzedaży technologii IT, brał udział w setkach wdrożeń sprzętu i oprogramowania w dużych i średnich firmach z sektora finansowego, telekomunikacyjnego, przemysłowego i wojskowego.

RAFAŁ STĘPNIEWSKI
Prezes Zarządu
Rzetelna Grupa Sp. z o.o.

Redaktor naczelny serwisów politykabezpieczenstwa.pl oraz dziennikprawny.pl, a także e-pisma "Security Magazine". Manager z 20-letnim doświadczeniem w branżach IT&T i zarządzaniu. Związany również z branżą e-commerce. Autor wielu publikacji z zakresu prawa e-commerce oraz bezpieczeństwa.

KATALOG FIRM

Walutomat®

CURRENCY ONE SA
WALUTOMAT.PL

ul. Szyperska 14
61-754 Poznań, Polska

Dane kontaktowe
+48 (61) 646 05 00
kontakt@walutomat.pl

Specjalizacje

- wymiana walut
- kursy walut
- przelewy zagraniczne
- e-kantor
- portfel wielowalutowy
- fintech
- waluty

Walutomat.pl to pierwsza i największa w Polsce społecznościowa platforma wymiany walut, na której Użytkownicy mogą indywidualnie ustalać kursy walut i bezpośrednio wymieniać je z innymi klientami. Serwis, który powstał w 2009 roku, jest jednym z najpopularniejszych e-kantorów w Polsce – korzysta z nie-go już ponad **530 tysięcy klientów biznesowych i prywatnych**. Co miesiąc wykonują ponad oni ponad 140 tysięcy operacji. Od początku istnienia, za pośrednictwem Walutomatu, wymieniono **115 miliardów złotych!**

Dlaczego warto korzystać z Walutomat.pl?

- Możliwość wymiany walut 24/7
- Wymiana jest bardzo szybka – walutę można wymienić nawet w 15 minut
- Konkurencyjne cenowo i szybkie przelewy zagraniczne do ponad 50 krajów
- Wymiana może być do 8% tańsza niż w bankach i tradycyjnych kantorach
- Walutomat.pl jest idealny dla każdego klienta – serwis odpowiada na potrzeby zarówno firm, jak i osób indywidualnych.
- Walutomat.pl obsługuje wszystkie banki w Polsce i oferuje darmowe przelewy do 9 z nich
- Szybki i wygodny przelew – wpłata poprzez Przelewy24
- Wygodny dostęp do środków - wypłaty 7 dni w tygodniu w godzinach 8.00-23.00
- Natychmiastowe przelewy w euro – SEPA Instant
- Intuicyjna aplikacja mobilna

Jak zabezpieczamy transakcje?

- Currency One, operator Walutomat.pl posiada licencję KNF na świadczenie usług płatniczych
- Dane klientów są przechowywane w bezpieczny sposób, zgodnie z wymogami obowiązujących regulacji
- Procedury AML
- Certyfikat SSL, umożliwiający zaawansowane szyfrowanie połączeń internetowych
- Transakcje tylko z pełnym pokryciem środków
- Autoryzacja SMS.

PARTNERZY WYDANIA

KOMENDA GŁÓWNA POLICJI

SYMETRIA PR

PR DLA BRANŻY IT I NOWYCH TECHNOLOGII

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY POLSKIEMU E-COMMERCE

POLICJA

symetriapr

Polityka® Bezpieczeństwa

Rzetelny® Regulamin

SECURITYMAGAZINE.PL

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

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

al. Jana Pawła II 61 lok. 212
01-031 Warszawa

KRS 284065
NIP: 524-261-19-51
REGON: 141022624
Kapitał zakładowy: 50.000 zł
Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

Redakcja: Monika Świetlińska, Damian Jemioło, Anna Petynia-Kawa
Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL