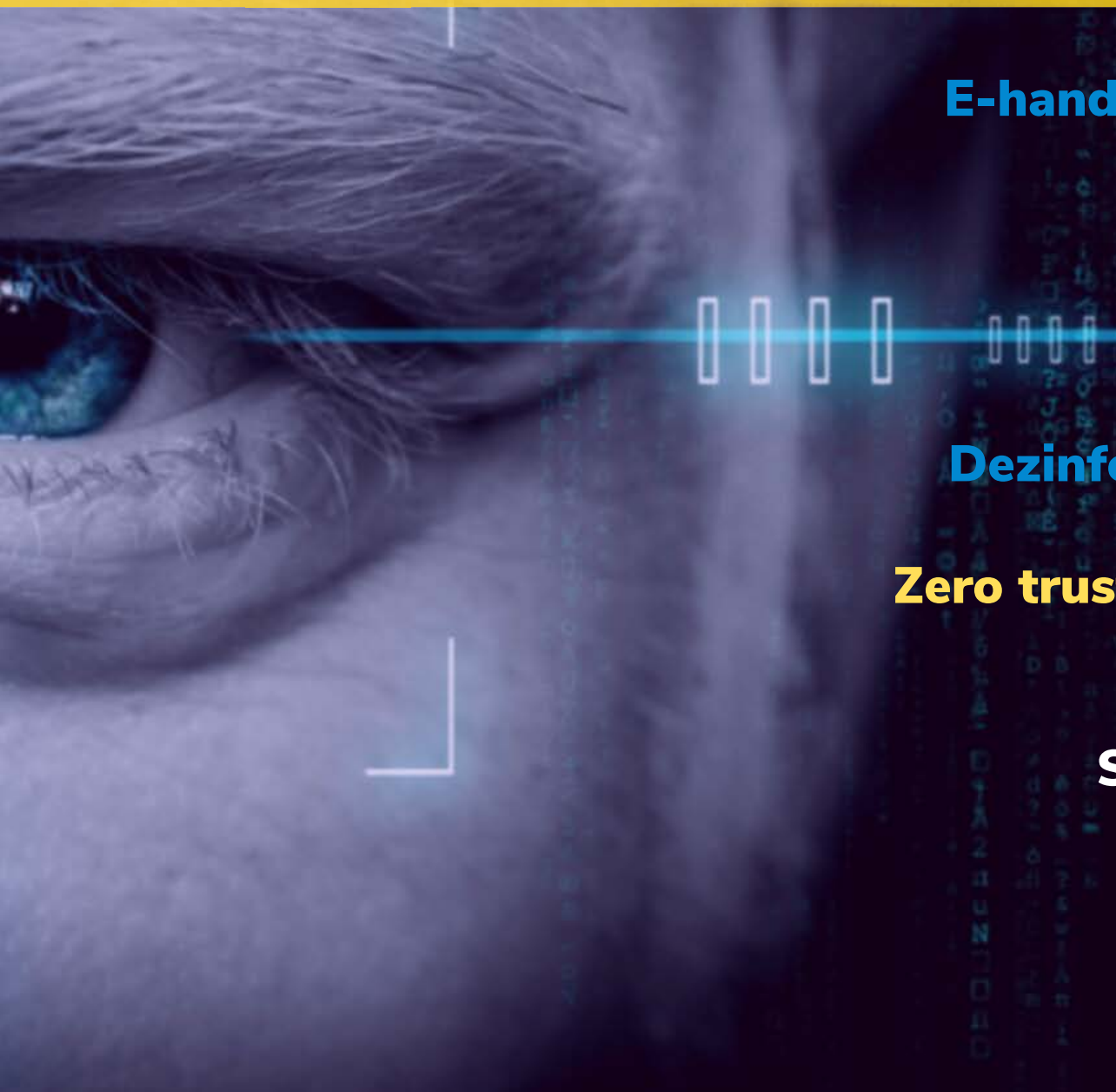
02/2022

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



E-handel na muszce cyberprzestępców Jak powinien bronić się rynek?

Passwordless, czyli przyszłość to logowanie bez haseł

Dezinformacja i fake newsy w biznesie

Zero trust i ochrona cyfrowej tożsamości

Twój e-sklep teraz sprzedaje? Skuteczny monitoring podstawą bezpieczeństwa w e-commerce

6 rad jak efektywnie budować bezpieczeństwo organizacji

SPIS TREŚCI

SZANOWNI PAŃSTWO,

Ostatnie dwa miesiące dobitnie pokazały, jak ważne jest cyberbezpieczeństwo. Ogromna fala dezinformacji, niezliczona ilość trolli oraz wzmożone działania phishingowe skutecznie zakłócały działania firm, zarówno w obszarze IT, jak i biznesowo.

Po raz kolejny widać, jak ważne jest budowanie świadomości w zakresie bezpieczeństwa - zarówno w sferze prywatnej, jak i zawodowej.

Ostatnie wydarzenia pokazały jak dużo informacji prywatnych udostępniamy publicznie. Posiadany majątek, miejsce zamieszkania, czy też upodobania i światopogląd - to tylko część danych, które dzięki skrupulatnie wykonanemu OSINT'owi mogą być wykorzystane w różnych celach, niekoniecznie leżących w interesie danej osoby.

"We are anonymous, we are legion, we do not forgive, we do not forget - expect us" - to specyficzne pożegnanie, w najbliższym czasie, zapewne niejednej osobie będzie spędzać sen z powiek.

Rafał Stępniewski

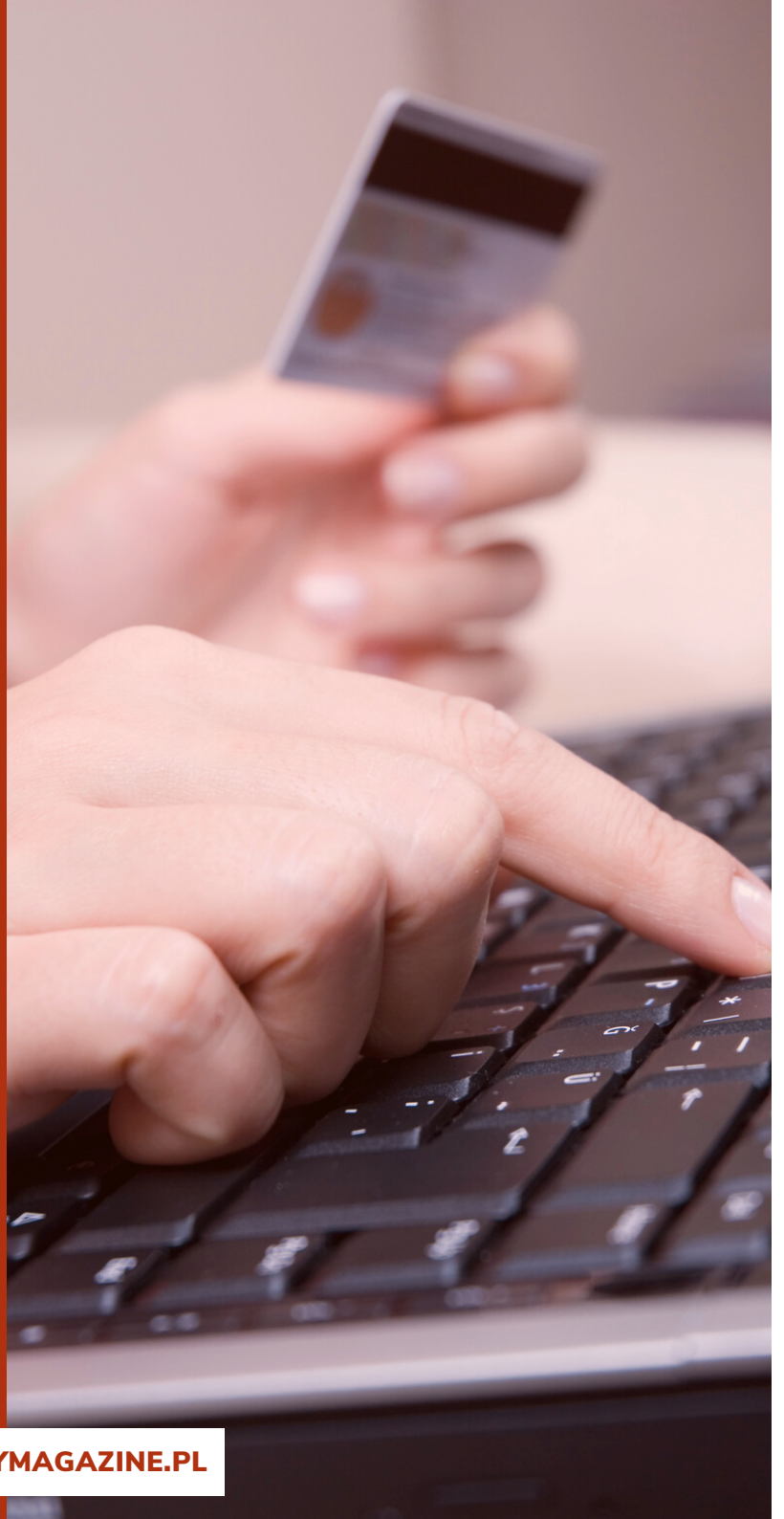
E-HANDEL NA MUSZCE CYBER-PRZESTĘPCÓW. JAK POWINIEN BRONIĆ SIĘ RYNEK?

Maciej Pawlak
Tpay

O tym, czy i jak Polacy dbają o bezpieczeństwo w trakcie aktywności w sieci, w jaki sposób bronić się przed cyberatakami i co w sprawie bezpiecznych zakupów robią właściciele sklepów internetowych we współpracy z operatorami płatności, rozmawiamy z Maciejem Pawlakiem odpowiedzialnym za zarządzanie ryzykiem i bezpieczeństwem informacji w Tpay.

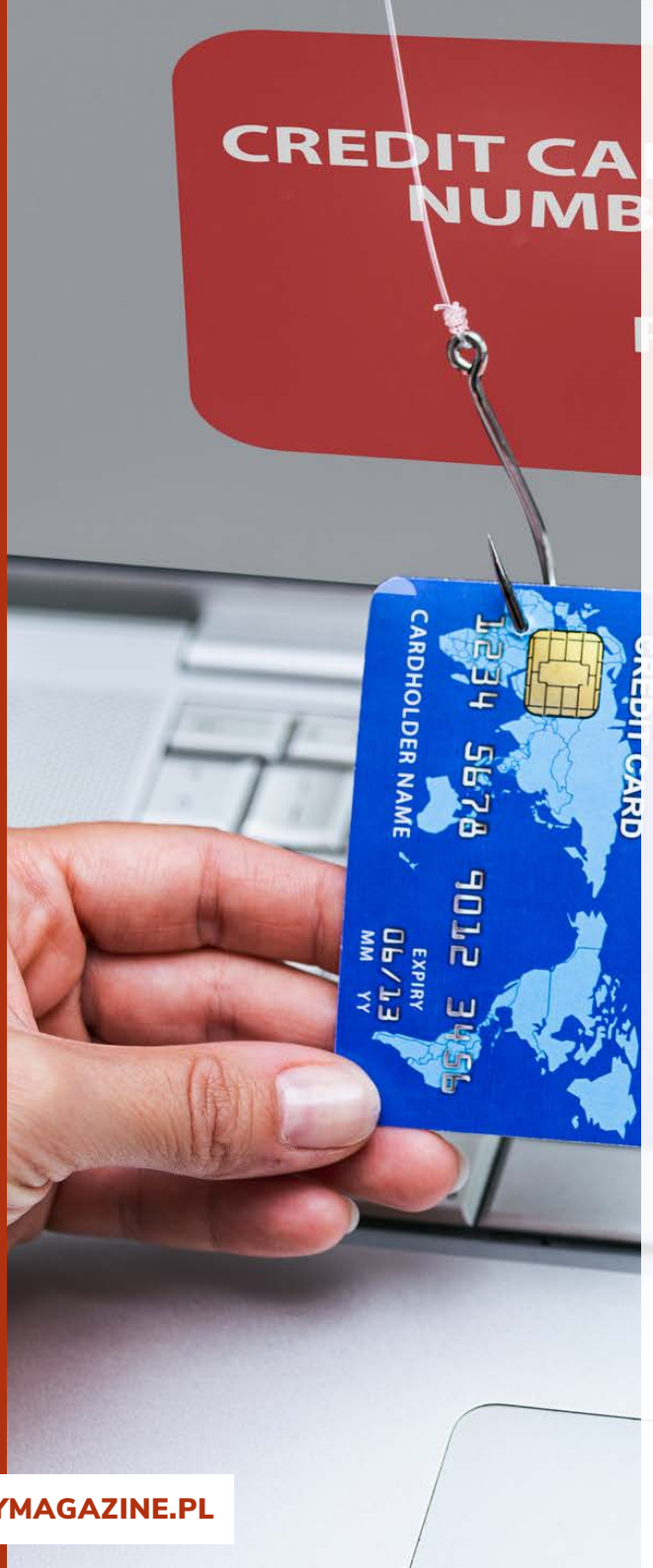
ŻYJEMY W CZASACH, KIEDY LICZNE SPRAWY MOŻNA ZAŁATWIĆ ONLINE: ZAKUPY, OPŁACENIE RACHUNKÓW ETC. NIE MA PAN WRAŻENIA, ŻE POLACY TROCHĘ ZBYT MOCNO PRZESZLI DO PORZĄDKU DZIENNEGO NAD SWOJĄ AKTYWNOŚCIĄ W SIECI I WCIĄŻ ZBYT RZADKO PAMIĘTAJĄ O BEZPIECZEŃSTWIE, KTÓRE PRZECIEŻ JEST TAK ISTOTNE?

Przejście kupujących do kanału online to zupełnie naturalny proces, który dynamicznie przyspieszył w trakcie pandemii. Temat dotyczący bezpieczeństwa nieco nam jednak spowszedniał, a nadmiar informacji spowodował, że wiele kwestii zaczęło po prostu umykać. Choć więc informacji samych w sobie jest bardzo dużo, to mam wrażenie, że Polacy nie wiedzą, z jakich korzystać narzędzi, aby w tym natłoku wiadomości czuć się bezpiecznie. Warto zwracać uwagę na to, co i u kogo kupujemy oraz jaką metodę płatności wybieramy. Jeśli wchodzimy na stronę sklepu, w którym nie robiliśmy wcześniej zakupów, musimy zachować czujność, sprawdzić opinie o nim oraz poznać model płatności, z jakim jest zintegrowany. Nie uciekniemy przed rozwojem i kierunkiem, w jakim podążają aktywności online. To, co możemy i powinniśmy zrobić, to zadbać o ochronę w sieci. Jak wynika z badania Tpay, mimo że aż dla 90 proc. Polaków bardzo ważne jest bezpieczeństwo transakcji podczas e-zakupów, to jednak wielu konsumentów wciąż pada ofiarą różnych, coraz bardziej wymyślnych metod cyberprzestępców.



WŁAŚNIE. JAK POKAZUJĄ ANALIZY RYNKOWE, ŚWIADOMOŚĆ POLAKÓW W TAKIM OBSZARZE WIEDZY FINANSOWEJ, JAKIM JEST CYBERBEZPIECZEŃSTWO, Z ROKU NA ROK ROŚNIE, JEDNAK NA TLE INNYCH OBSZARÓW, JAK NP. OSZCZĘDZANIE, PŁATNOŚCI BEZGOTÓWKOWE CZY KREDYTY I POŻYCZKI, W TYM ASPEKCIE WYPADAMY NAJSŁABIEJ. JAK PAN SĄDZI, DLACZEGO TAK JEST?

To być może wynika z tego, że zbyt szybko i w zasadzie nagle przeszliśmy do kanału e-commerce. Sam przeskok był dynamiczny, nie był procesem płynnym, tzn. wiele osób nie było ani przygotowanych na tego typu aktywności, ani nie miało wystarczającej wiedzy, jak to zrobić. Warto zauważyć, że nasze nawyki w sieci nie dotykają wyłącznie zakupów czy płatności, ale także sposobu, w jaki poruszamy się w internecie w ogóle. Cyberbezpieczeństwo dotyczy całej naszej działalności online, a to z kolei przekłada się na to, jak w takich wrażliwych procesach będziemy się zachowywać. Jeśli więc Polakom brakuje podstawowej wiedzy na temat bezpiecznego poruszania się w internecie, to później nawet z pozoru drobny błąd, jak na przykład za słabe hasło do poczty e-mail, może kosztować bardzo wiele.



Często wydaje nam się, że skoro jesteśmy we własnym domu, a komputer ląduje na naszych kolanach, to jesteśmy bezpieczni. Tymczasem świadomy użytkownik jest mniej narażony na ataki, a jeśli zdarzy się przykry incydent, to wie, gdzie w pierwszej kolejności szukać pomocy.

AŻ JEDNA TRZECIA INTERNAUTÓW DEKLARUJE, ŻE ZOSTAŁA OSZUKANA PODCZAS ZAKUPÓW W SIECI. NA CO POLACY POWINNI ZWRÓCIĆ WIĘC UWAGĘ, ABY NIE DAĆ SIĘ OSZUKAĆ? SKĄD MOGĄ CZERPAĆ WIEDZĘ NA TEMAT CYBERBEZPIECZEŃSTWA?

Badania rynkowe pokazują, że jednym z pierwszych celów cyberprzestępców jest m.in. przejęcie skrzynki mailowej, dlatego z pozoru błahą kwestią, o której powinniśmy pamiętać, jest zarządzanie hasłami. Istnieje wiele narzędzi, które nam w tym pomogą, np. dedykowane aplikacje typu KeePass, przechowujące wszystkie hasła czy też autoryzacja SMS. Niestety często można spotkać się z opinią, że posiadanie wielu różnych haseł do różnych portali, bankowości etc. jest sporym utrudnieniem. Bezpieczna aktywność w sieci zawsze będzie kwestią kompromisu pomiędzy wygodą a odpowiednią ochroną. Jeśli chodzi o czerpanie wiedzy, to większość instytucji finansowych opracowuje i udostępnia własne poradniki. Często obszerne informacje są także publikowane na stronach WWW banków i instytucji finansowych w zakładce dotyczącej bezpieczeństwa. Na rynku jest również kilka portali internetowych, które udostępniają wiedzę w tym temacie, informują o aktualnych, popularnych wśród cyberprzestępców akcjach phishingowych. Rzeczywistość pokazuje jednak, że cyberataki to problem nie tylko dla zwykłego Kowalskiego, ale mogą one dotknąć też każdy biznes.

WEŹMY NA TAPET WŁAŚCICIELI E-SKLEPÓW – ONI TAKŻE SĄ UCZESTNIKAMI RYNKU FINANSOWEGO. JAK POKAZUJĄ DANE, TYLKO W UBIEGŁYM ROKU W 47 PROCENTACH ZA STRATY ZWIĄZANE Z CYBER-OSZUSTWAMI DOTYCZĄCYMI PŁATNOŚCI CYFROWYCH ODPOWIEDZIALNE BYŁY ZAKUPY ONLINE. JAKIEGO RODZAJU CYBERPRZESTĘPSTWA NAJCZĘŚCIEJ DOTYKAJĄ SEKTOR E-COMMERCE?

Pierwszą grupą ryzyka są dane kartowe, które mogą zostać wykradzione od konsumenta. W tym przypadku merchant, tj. właściciel e-sklepu, nie wie o tym, że ten proces ma miejsce, a co za tym idzie – jest on z punktu widzenia sprzedawcy bardzo trudny do wykrycia. Inny, również popularny mechanizm oszustwa, to klasyczny phishing – konsument otrzymuje np. maila z oszukańczej strony internetowej z pozornie bardzo atrakcyjną ofertą produktową. Konsument – dając się nabrać i klikając w link zawarty w mailu – zostaje przekierowany na fałszywą stronę płatności i bankowości, a ktoś wyprowadza jego środki finansowe. Mimo że wektor ataku jest w tym przypadku inny, to tego typu oszustwo również jest bardzo trudne do wykrycia.

W ostatnim czasie bardzo popularne jest też oszustwo metodą „na BLIKA". Oszust, przejmując należący do kogoś profil w mediach społecznościowych, kontaktuje się ze znajomymi osoby, której profil przejął, prosząc ich o wsparcie finansowe (uzasadnione nagłą, wyjątkową sytuacją) i podanie kodu do płatności mobilnych (BLIK). Reasumując, wszystkie strony sektora e-commerce muszą zachować należytą czujność – konsumenci powinni zwiększać swoją świadomość na temat metod i działań cyberprzestępców i wiedzieć, jak się przed nimi chronić, a właściciele e-sklepów muszą zapewniać swoim klientom bezpieczeństwo.

CO ZATEM MOŻE ODPOWIADAĆ ZA SZEROKO ROZUMIANE CYBERBEZPIECZEŃSTWO W TEJ BRANŻY?

Pojawia się szereg rygorystycznych regulacji prawnych, które są gwarancją jakości i bezpieczeństwa obsługiwanych transakcji. Przykładowo my, tj. Tpay, jako operator płatności musimy mieć całkowitą pewność, że właściciel e-sklepu, który jest aktywnym uczestnikiem rynku finansowego, jest w stu procentach zaufany: jego sklep istnieje, sprzedaje produkty/usługi i będzie wywiązywał się ze wszystkich zobowiązań na rzecz swoich klientów. Taka skrupulatna weryfikacja to przede wszystkim wymóg prawny. W przypadku właścicieli e-sklepów, poza zwiększeniem wydatków na cyberbezpieczeństwo, bardzo istotna jest edukacja – zarówno wśród nich samych, jak i płatników. Tym, co musi zrobić e-sprzedawca, jest umieszczenie regulaminu sklepu w widocznym miejscu – zobowiązuje go do tego Ustawa o prawach konsumenta. Zwiększone zaufanie wzbudza także informacja o dostępnych metodach płatności oraz współpracy z operatorem płatności. Warto więc umieścić logo, link i nazwę operatora, z którego usług korzysta sklep. Przydatne są również wszelkie instrukcje i poradniki dotyczące procesu zakupowego, które ułatwią konsumentowi zakupy i zwiększą jego zaufanie do sklepu. Sporo na ten temat piszemy na naszym blogu Tpay.

POROZMAWIAJMY ZATEM O KONIECZNYCH REGULACJACH RYNKU FINANSOWEGO. JAKIE MAMY OBECNIE REGULACJE, MAJĄCE ISTOTNY WPŁYW NA BEZPIECZEŃSTWO UCZESTNIKÓW PROCESU PŁATNOŚCI?

Instytucje płatnicze, aby świadczyć swoje usługi, muszą posiadać stosowną licencję. W Polsce taką licencję wydaje Komisja Nadzoru Finansowego w ramach Ustawy o usługach płatniczych. Zadaniem tego typu regulacji jest sprawienie, by sposób działania w internecie był bezpieczny i zrozumiały dla wszystkich uczestników rynku finansowego. Operatorzy płatności odpowiedni poziom ochrony zapewniają poprzez certyfikaty, jak chociażby PCI DSS (Payment Card Industry Data Security Standard), który jest potwierdzeniem spełniania norm wymaganych przez instytucje płatnicze VISA i MasterCard do dostarczania płatności kartami. Na kształt rynku finansowego ma także wpływ Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML), która zobowiązuje do identyfikowania i weryfikowania tożsamości właścicieli e-commerce, ustawa o świadczeniu usług drogą elektroniczną czy też ustawa RODO, normalizująca zakres i sposób przetwarzania danych osobowych.

DLACZEGO MERCHANT MUSI PRZEJŚĆ PROCES WERYFIKACJI I JAK MUSI ON BYĆ ZORGANIZOWANY?

Pomijając wcześniej wspomniany przeze mnie aspekt, jakim jest odgórny wymóg ustawowy, to wszystkie regulacje mają za zadanie zapewnić szeroko rozumiane bezpieczeństwo, zarówno merchantowi, jak i klientowi. Dla właściciela e-sklepu jednym z celów jest chociażby zbudowanie zaufanie ze strony płatnika. Posiadanie licencji jest bowiem równoznaczne z pozytywnym przejściem procesu licencyjnego.

DLACZEGO I W JAKI SPOSÓB REGULACJE MAJĄ SŁUŻYĆ BEZPIECZEŃSTWU KLIENTA, TJ. PŁATNIKA, A W JAKIM MERCHANTA?

Ideą jest bezpieczeństwo całego sektora i zabezpieczenie wszystkich uczestników rynku, tym samym budując efektywną i elastyczną przestrzeń do prowadzenia działalności e-commerce. Z jednej strony, ma to być bezpieczeństwo płatnika, który kupując daną usługę, chce mieć pewność, że środki, jakie przekaże za usługę lub produkt trafią do merchanta. Z drugiej zaś, merchant również powinien być pewny, że taka transakcja zostanie zrealizowana w sposób niezakłócony. Regulacje mają więc na celu zbudowanie efektywnej i elastycznej przestrzeni, zarówno do prowadzenia działalności e-commerce, jak i aktywności zakupowych.

JAKIE ZAGROŻENIA I RYZYKA POWSTAJĄ W MOMENCIE BRAKU POPRAWNIE PRZEPROWADZONEGO PROCESU WERYFIKACJI?

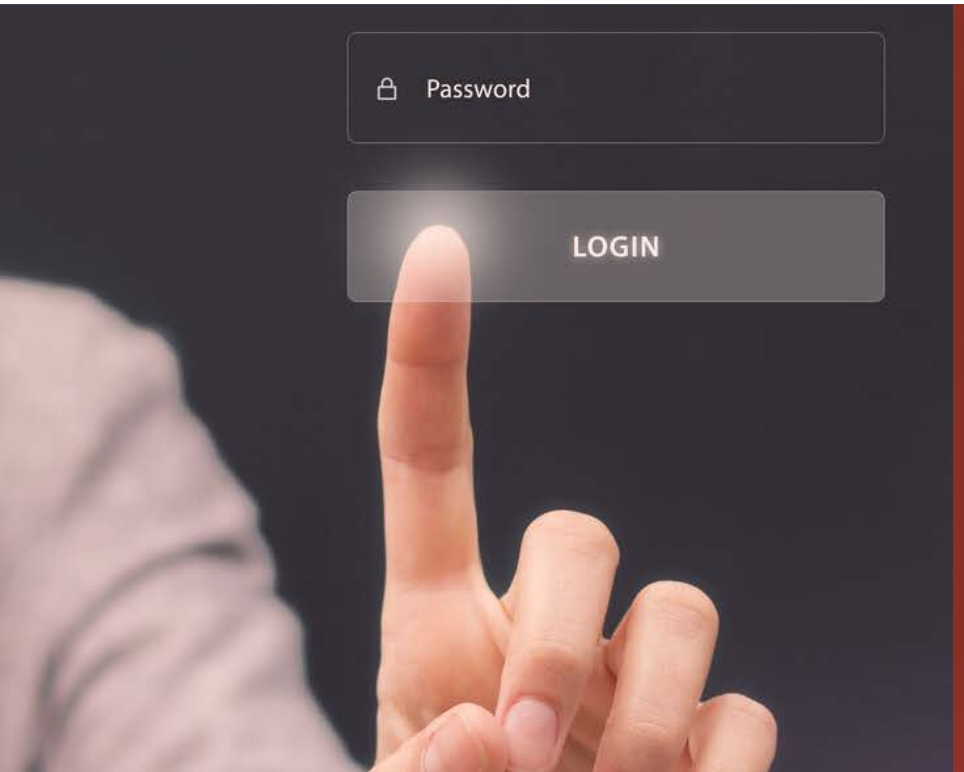
To pytanie trochę prowokacyjne (śmiech). Proces weryfikacji powinien być tak skonstruowany, żeby takich zagrożeń nie było. Proszę sobie wyobrazić sytuację, gdybyśmy jako operator płatności chociażby nie weryfikowali merchantów. Oczywiście, zdarza się, że fałszywe sklepy powstają i funkcjonują, sprzedając produkty w pozornie atrakcyjnych cenach. I faktycznie, dany sklep jakiś czas działa, buduje zaufanie u swoich klientów, po czym, gdy skala zamówień rośnie do poziomu dla niego intratnego, to zaczyna on przyjmować bardzo dużo zamówień, ale ich nie realizuje. To jest tylko jeden z wielu przykładów nadużyć, przestępstw, które w świecie e-commerce'owym mogą zaistnieć, dlatego też proces weryfikacji musi być dokładny i precyzyjny, aby takich sytuacji uniknąć.

Rozmawiała: Izabela Świątkowska


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

PASSWORDLESS, CZYLI PRZYSZŁOŚĆ TO LOGOWANIE BEZ HASEŁ

Patryk Bogdan
Grandmetric



Zdarza się, że, o ile system tego od nas nie zażąda, latami nie zmieniamy hasła do skrzynki mailowej. Beztrosko używamy tej samej kombinacji znaków, logując się do wielu różnych usług. Nie mogąc odnaleźć skomplikowanej sekwencji liter, cyfr i symboli w otchłani przepełnionej pamięci, po prostu resetujemy hasło.

LOGOWANIE WYMAGANE

Komunikatory, aplikacje firmowe w chmurze, urządzenia IoT, sieci WiFi i w zasadzie większość cyfrowych usług wymaga od nas zalogowania się na konto użytkownika. W efekcie, przeciętna osoba posługuje się hasłami, które można liczyć w dziesiątkach, a może nawet setkach. Choć na rynku istnieją rozwiązania pozwalające uwolnić nas od obowiązku zapamiętywania niezliczonej ilości haseł (choćby KeePass), których na co dzień używamy, wciąż powielamy stare błędy.

Jaki jest tego efekt? Zbyt słabe lub wykradzione przez cyberprzestępców hasła znajdują się na szczycie listy przyczyn wycieków danych i ataków hakerskich. Według zeszłorocznego raportu Data Breach Investigations przygotowanego przez firmę Verizon, aż 61% naruszeń danych powstaje z użyciem nieautoryzowanych dostępów.

Sam pomysł używania haseł, czyli poufnych ciągów znaków weryfikujących tożsamość jest prawdopodobnie tak stary, jak ludzki język. Jak wiemy z pism Swetoniusza i innych rzymskich autorów, hasłami posługiwano się zarówno na polach bitewnych, jak i w korespondencji do przyjaciół (vide Juliusz Cezar i jego szyfr cezariański).

Pierwsze hasło zabezpieczające dostęp do komputera ustawił prawdopodobnie Fernando J. Corbató z Massachusetts Institute of Technology w połowie lat 60. XX wieku. Użył go, by uniemożliwić niepowołanym dostęp do plików w systemie komputerowym CTSS (Compatible Time-Sharing System). Z powodu błędu bezpieczeństwa w oprogramowaniu, był to też prawdopodobnie pierwszy system, z którego wykradziono hasła użytkowników.
Choć współczesne rozwiązania stosowane do uwierzytelniania dostępu korzystają ze znacznie bardziej zaawansowanej kryptografii, trudno zignorować password fatigue. Stres i frustracja wywołane przez konieczność zapamiętywania coraz to nowych haseł to zjawisko zidentyfikowane i opisane w Macmillan Dictionary już przed kilkunastoma laty. Mniej więcej w tym samym czasie specjaliści cyberbezpieczeństwa zaczęli wieszczyć “śmierć hasła”.

Popularność urządzeń mobilnych, powszechność pracy zdalnej i rosnąca akceptacja dla identyfikacji biometrycznej to kolejne czynniki, otwierające nowe możliwości weryfikacji użytkowników.

JAKIE METODY DAJE NAM WSPÓŁCZESNA TECHNOLOGIA?

Zacznijmy od wspomnianej identyfikacji biometrycznej. To metoda bazująca na rozpoznawaniu użytkownika na podstawie cech fizycznych bądź behawioralnych, unikalnych dla każdej osoby. Najczęściej są to linie papilarne, a ich porównywanie stosowano w technikach śledczych już na przełomie XIX i XX wieku.

Pierwsze urządzenia mobilne, które wykorzystywały tę technikę identyfikacji właścicieli, pojawiły się na rynku w 2013 roku dzięki modułowi Touch ID firmy Apple. W 2017 roku ta sama marka uczyniła kolejny krok milowy w dziedzinie rozwiązań bezhasłowych, wprowadzając do swoich urządzeń technikę rozpoznawania twarzy Face ID.

Inne technologie używane do potwierdzania tożsamości użytkowników rozpoznają mowę, skanują siatkówkę oka, a nawet układ żył na dłoniach z wykorzystaniem światła zbliżonego do podczerwonego. Jak w przypadku pozostałych faktorów biometrycznych, żyły tworzą u każdej osoby unikalny wzór, który jest dodatkowo znacznie trudniejszy do sfalsyfikowania. Amerykańska firma Global ID w 2019 opatentowała technologię biometryczną, która umożliwia skanowanie żył w 3D.

TECHNOLOGIA BIOMETRYCZNA

Wśród zalet czytników naczyń krwionośnych wymienia się fakt, że umożliwiają potwierdzenie tożsamości użytkownika bez konieczności bezpośredniego kontaktu z urządzeniem w czasie poniżej dwóch sekund. Rozwiązania tego rodzaju mają także zastosowanie w szpitalach, umożliwiając identyfikację pacjentów, z którymi komunikacja z różnych względów jest utrudniona lub niemożliwa. Potencjalnie tego typu czytniki mogłyby badać również oznaki życia użytkowników - przewodnictwo elektryczne, mruganie czy puls.

Kolejnym przykładem rozwiązań biometrycznych jest uwierzytelnianie behawioralne. Po stylu wysyłania sygnałów rozpoznawali się już operatorzy i operatorki telegrafów pod koniec XIX wieku. Współcześnie wykorzystuje się sztuczną inteligencję do analizowania, jak użytkownik wchodzi w interakcję z urządzeniem. Dla każdej osoby unikalna jest bowiem dynamika pisania na klawiaturze, sposób poruszania myszką czy trzymania telefonu. Niewątpliwą zaletą czynników behawioralnych jest pasywna natura – nie wymagają dodatkowego zaangażowania użytkowników, dostarczając precyzyjnych informa-

cji do potwierdzania tożsamości. Wykorzystuje się je szczególnie w branżach wymagających szczególnego bezpieczeństwa, jak bankowość i finanse.

UWIERZYTELNIANIE WIELOSKŁADNIKOWE

W uwierzytelnianiu wieloskładnikowym do potwierdzania tożsamości potrzebne są minimum dwa składniki, **tzw. faktory**. Jednym z nich najczęściej jest **hasło**, a zwiększeniu bezpieczeństwa służy konieczność podania dodatkowego faktora. Może nim być coś, co znajduje się w posiadaniu użytkownika, np. **fizyczny token** czy dostęp przez wcześniej zarejestrowane urządzenie. Wykorzystuje się również **faktory** związane z fizyczną obecnością użytkownika, jak wspomniane wcześniej **czynniki biometryczne** lub schematy behawioralne i gesty. Inne możliwe faktory to **geolokalizacja, adres IP, potwierdzanie dostępu w dedykowanej aplikacji** (*push-up notification*). Także jeśli chodzi o uwierzytelnianie adaptacyjne, do potwierdzania tożsamości wykorzystuje się analizę zachowania użytkownika. Sztuczna inteligencja uczy się np. charakterystyki pisania na klawiaturze danej osoby i identyfikuje odstępstwa od ustalonej normy. W takiej sytuacji, w zależności od skali ryzyka, może zażądać dodatkowej weryfikacji lub całkowicie zablokować dostęp do logowania.

Oczywiście, możemy mieć do czynienia również z rozwiązaniem Passwordless MFA, kiedy użytkownik uzyskuje dostęp do danego zasobu (usługi) dzięki weryfikacji tożsamości przy pomocy kombinacji faktorów, z których żaden nie jest hasłem (np. rozpoznawanie twarzy potwierdzane logowaniem w aplikacji na smartfonie).

NIEPEWNA PRZYSZŁOŚĆ HASEŁ

Podstawowym powodem, dla którego zaczęto poszukiwać nowych rozwiązań mających całkowicie wyeliminować konieczność używania haseł, było zwiększenie bezpieczeństwa. Hasła są bowiem z wielu względów zabezpieczeniem najłatwiejszym do złamania przez hakerów i najczęstszym wektorem cyberataków.

Rozwiązania bezhasłowe, a szczególnie uwierzytelnianie biometryczne jest znacznie trudniejsze i droższe do złamania przez hakerów. Wymagałoby pokonania zabezpieczeń przez każdorazowe fizyczne sfałszowanie np. skanu odcisku palca na urządzeniu należącym do konkretnego użytkownika w realnym świecie. Absolutnie jest to jednak możliwe, jak udowodnił niemiecki haker znany jak Starbug, któremu "oszukanie" sensorów w iPhone 5S zajęło mniej niż 24h od premiery w 2013 roku.

Kolejną zaletą uwierzytelniania bezhasłowego jest łatwiejsza możliwość śledzenia użycia. Ponieważ uzyskanie dostępu jest powiązane z konkretnym urządzeniem lub obecnością użytkownika, nie jest możliwe ich masowe używanie, a zarządzanie dostępami jest szczelniejsze.

REDUKCJA KOSZTÓW

Nie bez znaczenia jest też redukcja kosztów dla działów IT. Wraz z rezygnacją z haseł, znika potrzeba tworzenia i aktualizacji dotyczących ich polityk, śledzenia wycieków, jak również resetowania zapomnianych haseł.

Zwiększa się też wyraźnie komfort użytkowników. Z ich ramion znika ciężar dziesiątek i setek haseł, które do tej pory musieli przechowywać w pamięci, zapi-

sywać w dedykowanych programach lub, co gorsza, na karteczkach przyklejanych do monitorów swoich komputerów. Rozwiązania uwierzytelniania bezhasłowego dają łatwą skalowalność i możliwość szybkiej weryfikacji.

KOSZTY IMPLEMENTACJI

Do wad zdecydowanie należą koszty implementacji, choć długodystansowo używanie takich rozwiązań jest mniej kosztowne.

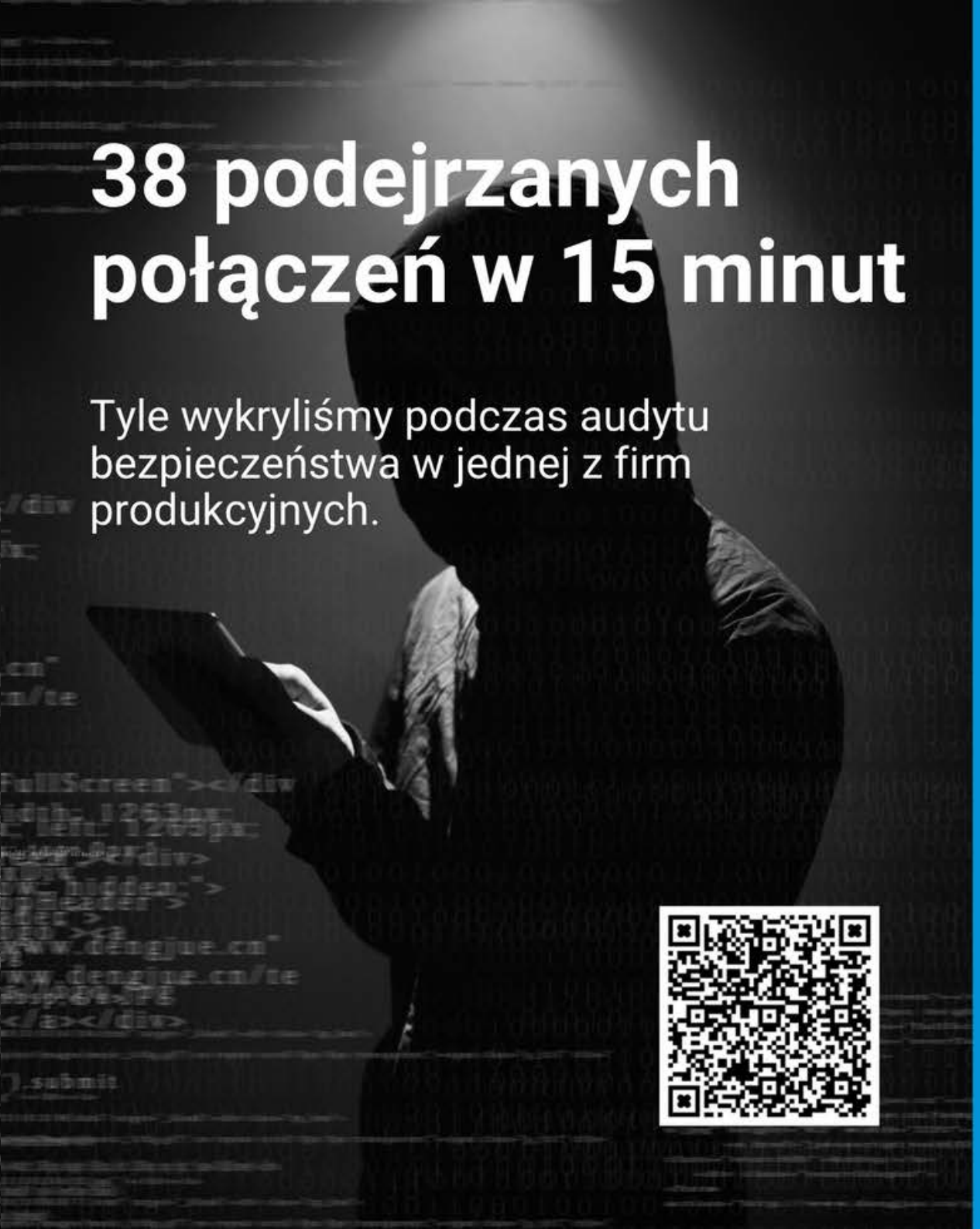
Wprowadzenie jest związane z wydatkami na implementację systemów uwierzytelniania oraz hardware'u potrzebnego do jego identyfikacji (np. skanera tęczówki oka).

Samo wdrożenie również może być problematyczne. Rodzi się konieczność adaptacji użytkowników i teamów IT do nowego rozwiązania i zmiana wieloletnich przyzwyczajeń. W grę wchodzi też konieczność przełamania bariery psychologicznej, która pojawia się szczególnie w przypadku bardziej "inwazyjnych" technologii, jak skanery unikalnych wzorów naczyń krwionośnych użytkowników.

Uciążliwy jest też pojedynczy punkt awarii, szczególnie w przypadku rozwiązań wykorzystujących powiadomienia push na smartfonie. Uzależnienie powodzenia weryfikacji tożsamości od dodatkowego urządzenia, które może się przecież zgubić, rozładować lub mieć nieaktualne oprogramowanie, stanowi ryzyko trudne do zignorowania.

JAKA CZEKA NAS PRZYSZŁOŚĆ UWIERZYTELNIANIA?

Wygląda na to, że w najbliższym czasie będzie spełniał się sen o całkowitym uniezależnieniu się od haseł. Z rozwiązaniami wykorzystującymi biometrię, takimi jak Apple Face ID, Touch ID, Windows Hello czy Samsung Iris Scan – z pewnością będziemy mieć coraz mniej haseł do zapamiętania. Będą im towarzyszyć dodatkowe warstwy bezpieczeństwa, miejmy nadzieję z gatunku tych niewymagających akcji od użytkowników, jak uwierzytelnianie behawioralne i adaptacyjne. A wraz z nimi odpowiednie regulacje prawne, gwarantujące bezpieczeństwo i kontrolę użytkownikom nad unikalnymi danymi, których przecież nie da się zresetować czy zmienić.



38 podejrzanych połączeń w 15 minut

Tyle wykryliśmy podczas audytu bezpieczeństwa w jednej z firm produkcyjnych.

Standardy, które wykorzystujemy podczas audytów bezpieczeństwa

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

GRANDMETRIC
STAY CONNECTED.

Diamenty Miesięcznika Forbes 2022

CISCO INNOVATION PARTNER OF THE YEAR 2021

JAK CHRONIĆ SIĘ PRZED CYBERATAKAMI NA ŚWIECIE I W POLSCE?

Redakcja
SECURITY MAGAZINE

Liczba incydentów cybernetycznych w 2021 jest wstrząsająca, choć jest już pewne, że rok 2022 przyniesie kolejne rekordy. Dlaczego wiedza o tym, z jakimi rodzajami cyberataków mierzymy się obecnie, jest ważna? Dlaczego warto przyglądać się, jak sytuacja rozwija się nie tylko w Polsce, ale na całym świecie?

WZROST CYBERRYZYKA FINANSOWEGO

Światowe Forum Ekonomiczne (The World Economic Forum) określiło cyberataki jako piąte największe ryzyko w 2020 roku. Ponieważ 77% ekspertów ds. bezpieczeństwa przewiduje naruszenia infrastruktury krytycznej, ważne jest, aby firmy, duże i małe, były gotowe na kolejne trendy hakerskie. Ponieważ szacuje się, że wartość branży IT do końca 2022 roku osiągnie 170,4 miliarda dolarów, oznacza to szybki wzrost cyberryzyka finansowego. Przy czym zaznaczyć trzeba że w obliczeniach nie wzięto pod uwagę toczącej się właśnie cyberwojny.

Cyberataki mogą się zdarzyć w naszej firmie w każdej chwili, zwłaszcza teraz. Musimy stawić im czoła i podejmować właściwe decyzje. Ataki mogą być aktywne lub pasywne, z wewnątrz lub z zewnątrz organizacji. Dzięki wczesnemu im rozpoznawaniu organizacje mogą zaoszczędzić pieniądze i uniemożliwić dalszy dostęp do poufnych informacji, wyłączając systemy i powiadamiając współpracowników.

Przygotowaliśmy listę najczęstszych rodzajów cyberataków w 2021 roku z całego świata. Możemy się domyślać, że są one wykorzystywane również teraz, kiedy toczy się cyberwojna.

Czym są cyberataki? To działania cyberprzestępców, których celem są systemy komputerowe, bazy danych, infrastruktura i osoby odwiedzające strony internetowe. I tak najpopularniejsze w ciągu ostatnich 6 miesięcy są:

1 WYŁUDZANIE INFORMACJI

Phishing to atak wykorzystujący pocztę e-mail do nakłaniania ludzi do pobierania złośliwego oprogramowania na swoje urządzenia. W 2020 roku około 75% organizacji doświadczyło phishingu.

Rodzaje phishingu na świecie:

- spear-phishing – ataki wymierzone w określone osoby, na przykład administratorów systemu,
- wielorybnictwo – ataki wymierzone w kadrę kierowniczą wyższego szczebla,

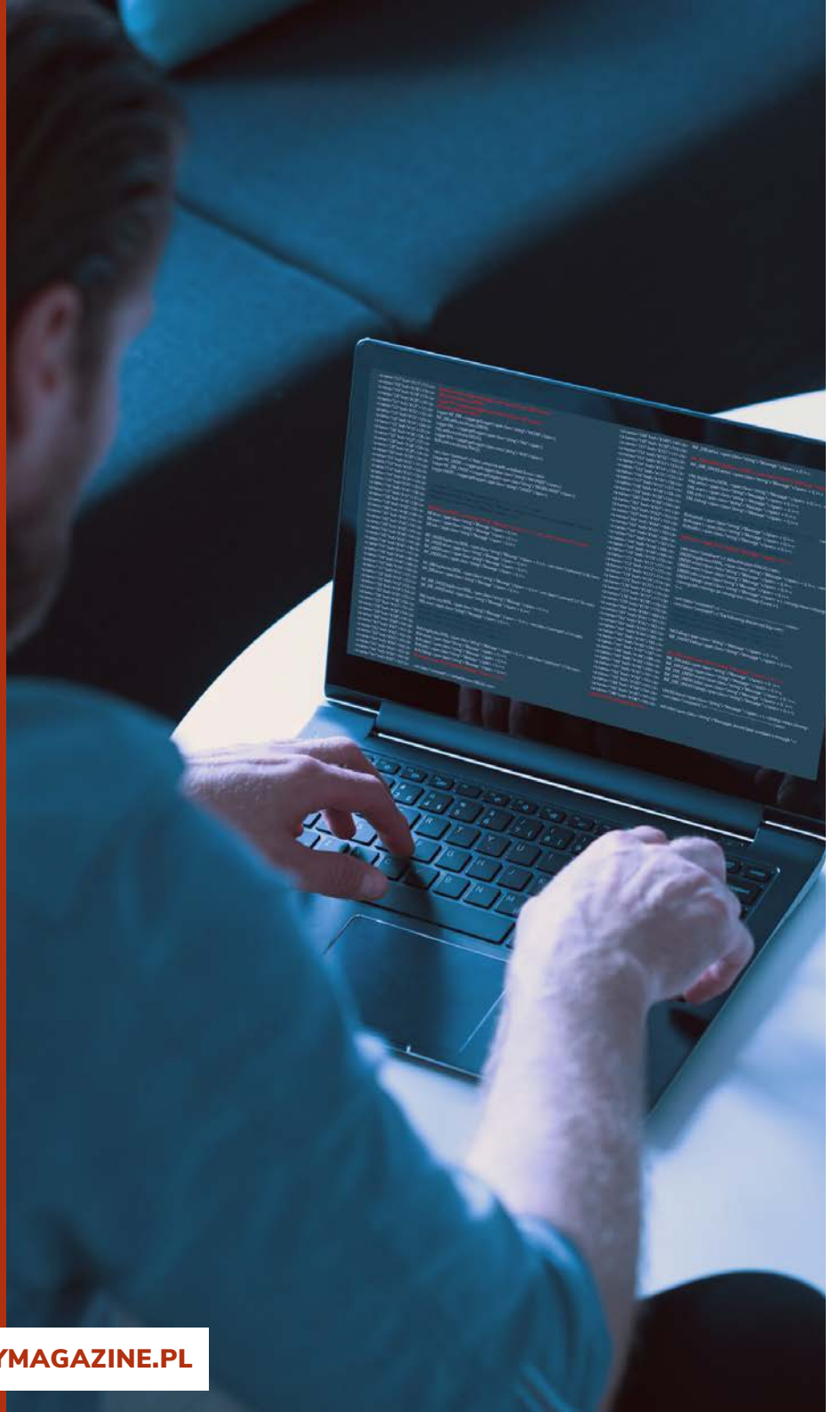
- smishing – ataki wykorzystujące wiadomości tekstowe lub SMS do przyciągnięcia uwagi ofiary,
- phishing w wyszukiwarkach – ataki wykorzystujące SEO do podbijania stron internetowych, którymi zainteresowany jest haker,
- phishing email – atak za pośrednictwem poczty elektronicznej,
- vishing – atak za pośrednictwem poczty głosowej.

Wiele ataków phishingowych wykorzystuje łącza i pliki, które na pierwszy rzut oka nie wydają się podejrzane. Hakerzy stosują również sztuczki psychologiczne. Wiedzą, kogo udawać, wiedzą kim jest ofiara, jaką może mieć osobowość, czy jest podatna na manipulacje.

W 2020 roku pojawiło się wiele e-maili phishingowych związanych z COVID-19. Atakujący wysłali informacje rzekomo w imieniu Światowej Organizacji Zdrowia, grając na naszych obawach. Inni cyberprzestępcy wykorzystywali nagłówki typu clickbait związane z biznesem, kredytami i polityką.

Jak się chronić przed phishingiem?

Zapobieganie to jedyny właściwy sposób! Stale podnoś świadomość pracowników. Pomocne byłoby również oprogramowanie antyphishingowe i silniejsze uwierzytelnianie poczty e-mail.



2 ATAKI RANSOMWARE

Ransomware to złośliwe oprogramowanie, które blokuje użytkownikom dostęp do ich oprogramowania i żąda zapłaty okupu. Zazwyczaj ransomware rozprzestrzenia się za pośrednictwem spamu lub socjotechniki.

W 2021 roku eksperci od cyberprzestępczości zauważyli więcej przykładów oprogramowania ransomware szyfrującego, które szyfruje pliki ofiary, a następnie żąda zapłaty, aby przywrócić jego działanie. Ale czy wiesz, że aż 42% organizacji, które zapłaciły przestępcom za okup, nigdy nie odzyskało dostępu do swoich plików? Osoby pracujące zdalnie stały się nowym celem dla oprogramowania ransomware.

Jak się chronić przed atakami ransomware?

Kiedy firma wykryje zagrożenie i zgłosi oprogramowanie ransomware władzom, może zapłacić okup, usunąć złośliwe oprogramowanie lub usunąć wszystkie dane i spróbować je odzyskać za pomocą kopii zapasowych.

3 ZŁOŚLIWE OPROGRAMOWANIE

Złośliwe oprogramowanie zatrzymuje lub znacznie spowalnia działanie urządzeń. Oprogramowanie szpiegujące, wirusy, robaki, oprogramowanie ransomware, trojany są wykorzystywane przez cyberprzestępców.

Na urządzenia trafiają np. za pośrednictwem załączników do wiadomości e-mail ze złośliwym kodem lub programów do udostępniania plików.

Jak się chronić przed złośliwym oprogramowaniem?

Dostępnych jest wiele narzędzi anty-malware, które potrafią je wychwycić, np. Bitdefender i wiele innych. Zapory sieciowe i systemy zapobiegania włamaniom mogą również pomóc w ochronie danych.

4 WYCIEKI DANYCH

Z wyciekiem danych mamy do czynienia wtedy, gdy fragment poufnych informacji staje się zagrożony. W 2020 roku wiele firm zgłosiło naruszenia danych i są przypuszczenia, że trend ten będzie się nadal utrzymywał.

Nie tak dawno hakerzy opublikowali bazę danych zawierającą 2,5 miliona rekordów firmy Drizly dostarczającej alkohol. Prestige Software, system rezerwacji obsługujący Expedia, Booking.com i Hotels.com, ujawnił dane kart kredyto-

86% NARUSZEŃ DANYCH JEST MOTYWOWANA FINANSAMI, ALE W GRĘ WCHODZI TEŻ SZPIEGOSTWO LUB CZYNNIKI LUDZKIE.

wych podróżnych i biur podróży, w tym wszystkie ważne kody CVV, szczegóły płatności, szczegóły rezerwacji oraz dane osobowe (PII), w tym nazwiska, adresy e-mail, krajowe numery identyfikacyjne i numery telefonów. Ofiarami padło ponad 10 milionów klientów od 2013 roku. Trzeba przy tym pamiętać o wyciekach danych z naj-większych serwisów społecznościowych: Facebook, LinkedIn, które miały miejsce w ostatnim czasie.

Jak się chronić przed wyciekiem danych?

86% naruszeń danych jest motywowana finansami, ale w grę wchodzi też szpiegostwo lub czynniki ludzkie. Gdy dojdzie do naruszenia, firmy muszą podjąć natychmiastowe działania, aby chronić swoją reputację i uniknąć astronomicznych kar, chociażby w związku z RODO. Naruszenia zwykle ujawniają się w wewnętrznych rejestrach, powiadomieniach bankowych, organach ścigania lub raportach klientów.

5 ATAKI DDOS

W tym przypadku atakujący kieruje duży ruch do systemu lub serwera, zmuszając go do zatrzymania lub zawieszenia operacji. Biorąc pod uwagę, że przestoje IT kosztują od 300 000 do 1 miliona dolarów na godzinę, takie sytuacje mogą kosztować firmę masę pieniędzy.

Przykładem niedawnego ataku jest ten, o którym poinformowała firma Google. Przeszła atak DDoS o szybkości 2,5 Tb/s - największy dotychczas atak, który dotknął 180 000 serwerów internetowych.

Jak się chronić przed tego typu atakiem?

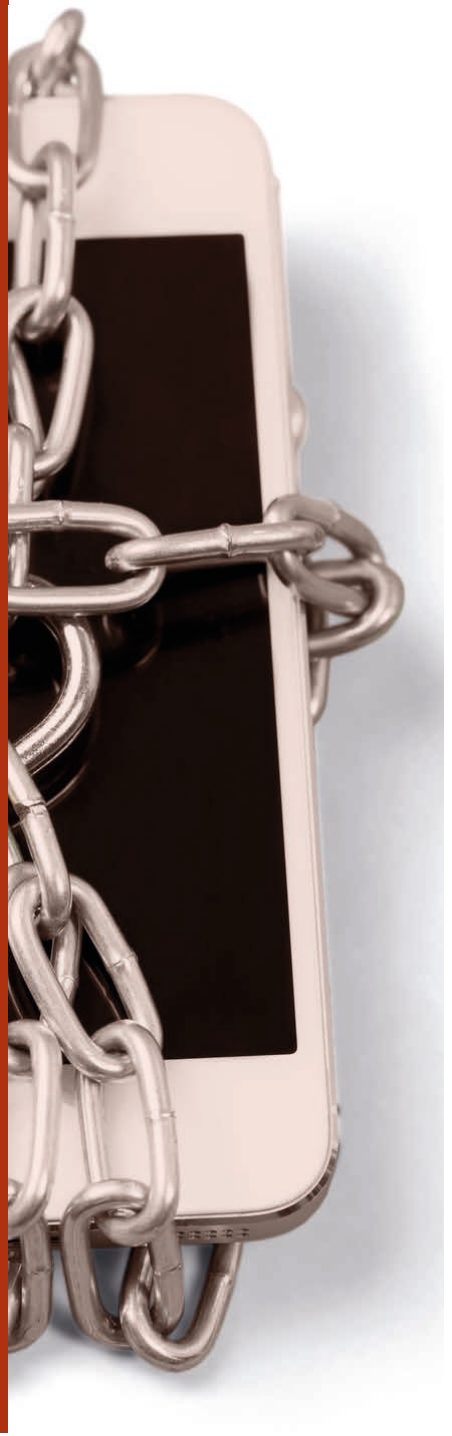
Najlepiej upewnić się, że firma korzysta z serwerów internetowych opartych na chmurze, które mogą pochłaniać ruch związany z przepełnieniem. Ponadto należy przeprowadzać regularne testy bezpieczeństwa, aktualizacje oprogramowania i przepustowości. Wskazana jest też współpraca z dostawcami usług internetowych lub bezpiecznych rozwiązań outsourcingowych. Wszystko po to, by złagodzić takie ataki.

6 ATAK MAN-IN-THE-MIDDLE (MITM)

Ataki „człowiek pośrodku" mają miejsce, gdy atakujący przechwytuje i zmienia komunikację elektroniczną. Przykładem może być fałszywy hotspot Wi-Fi, który wygląda i działa jak prawdziwy, ale przechwytuje nasze informacje. Wraz z rosnącym trendem pracy zdalnej i komunikacji cyfrowej coraz ważniejsze staje się dla firm stosowanie szyfrowania typu end-to-end do przesyłania wiadomości i wideokonferencji.

W odpowiedzi na krytykę na początku pandemii firma Zoom wprowadziła szyfrowanie typu end-to-end, aby chronić firmy podczas rozmów wideo. Echem odbił się atak podczas wideokonferencji firmy CCC. 250 osób, w tym założyciel, analitycy giełdowi, dziennikarze, zarządzający funduszami inwestycyjnymi i menedżerowie firmy obejrzeli dwa razy film pornograficzny, nim zdecydowano o zakończeniu spotkania online.

Należy przeprowadzać regularne testy bezpieczeństwa, aktualizacje oprogramowania i przepustowości. Wskazana jest też współpraca z dostawcami usług internetowych lub bezpiecznych rozwiązań outsourcingowych.



To nie wszystkie popularne obecnie roku rodzaje cyberataków. Hakerzy mogą aktywnie korzystać również z takich narzędzi jak:

- **wstrzyknięcie instrukcji SQL** – zdobywanie nieautoryzowane,
- **atak zero-day** – szybkie wykorzystywanie luk bezpieczeństwa,
- **ataki brute-force** – łamanie haseł przez przechodzenie przez wszystkie możliwe warianty klucza,
- **tunelowanie w protokole DNS** – fizyczne połączenie się z zasobami firmy za pomocą internetu.

JAKIE MOGĄ BYĆ KONSEKWENCJE CYBERATAKU?

Wyniki cyberataku zależą od typu cyberprzestępczości, której firma doświadczy. Dla uproszczenia wypunktowujemy kilka najważniejszych konsekwencji:

- Ataki DDoS mogą spowodować **zablokowanie strony internetowej, a tym samym utratę naturalnego ruchu, a nawet utratę reputacji.**
- Kradzież własności i wyłudzenie poufnych danych **wpływa na firmę finansowo, ale także szkodzi jej reputacji.** Może to również skutkować nawet **wielomilionowymi karami** z powodu naruszenia ogólnego rozporządzenia o ochronie danych (RODO). Przykładem wielkiego wycieku danych jest ten z kwietnia ubiegłego roku. Udostępniona online baza danych z Facebooka zawierała loginy ponad pół miliarda jego użytkowników, ich imiona i nazwiska, daty urodzenia i numery telefonów.
- Ataki firmowe i inne nadużycia poczty e-mail, takie jak Business Email Compromise (BEC), skutkują **dużymi stratami finansowymi.**
- Infiltracje lub uszkodzenia systemu komputerowego oraz inne naruszenia dostępu s**powalniają lub zatrzymują bieżące operacje.**

Wszystkie te ataki mogą mieć ogromne konsekwencje i przyczynić się m.in.do szybkiej utraty środków pieniężnych firmy. Co gorsze, firmy ubezpieczeniowe czasami wykorzystują atak, aby podnieść swoje stawki. Ze względu na ogromne ryzyko ataków, niezależnie od rodzaju działalności, warto mieć wiedzę, jakiego rodzaju ataki są obecnie wykorzystywane przez hakerów i jak minimalizować ich skutki.

sygnisoft

Bądź o krok przed innymi.

W Sygnisoft sprawnie projektujemy, tworzymy
i wdrażamy Twój pomysł.

sygnisoft.com

Software house – dedykowane aplikacje i systemy!

DEZINFORMACJA I FAKE NEWSY W BIZNESIE

Piotr Kantorowski
Kancelaria Prawna Kantorowski, Głąb i Wspólnicy

Dezinformacja to zamierzona i konsekwentna formuła przekazu informacji (w tym fałszywych lub zmanipulowanych) i fabrykowanie takiego przekazu poprzez tworzenie różnego rodzaju fałszywych dokumentów, organizacji itd., które wprowadzają w błąd (powodują powstanie obrazu świata niezgodnego z rzeczywistością).

DEZINFORMACJA A FAKE NEWSY

Wszystkie te przekazy wywołują określone efekty w postaci:

1) podejmowania przez odbiorcę błędnych decyzji,
2) wytworzenia poglądu,
3) działania lub jego braku, zgodnych z założeniem **podmiotu dezinformującego**.

Z kolei **fake newsy** to nieprawdziwa lub częściowo nieprawdziwa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorców w błąd, w celu **osiągnięcia korzyści finansowych, politycznych lub prestiżowych.**

To, że oba zjawiska potrafią być bardzo niebezpieczne można było zaobserwować już w czasie kampanii wyborczej w USA, kiedy prezydentem został Donald Trump, następnie w trakcie pandemii, choć w obliczu wojny w Ukrainie i przekazu jaki jest w jej kontekście kreowany w rosyjskich mediach widać je jeszcze bardziej. Aby dopełnić obrazu warto jeszcze podkreślić, kto zajmuje się przekazywaniem tego rodzaju „informacji". Są to tak zwane trolle.

> **Zgodnie z definicją trolling to antyspołeczne zachowanie, charakterystyczne dla internetowych forów dyskusyjnych i mediów społecznościowych, polegające na zamieszczaniu kontrowersyjnych, napastliwych, często nieprawdziwych treści w celu zwrócenia na siebie uwagi albo sprowokowania, ośmieszenia lub obrażenia innych użytkowników.**

WYMIAR EKONOMICZNY FAKE NEWSÓW I DEZINFORMACJI

Ofiarami dezinformacji i fake newsów mogą padać jednak tak pojedyncze jednostki, jak i całe państwa. Wskazuje się wręcz, że szeroko pojęta dezinformacja ma trzy wymiary: polityczny, społeczny i ekonomiczny. W ramach tego ostatniego podkreśla się, że ma ona na celu

wywieranie wpływu na kierownictwo firmy i jej decyzje, ograniczenie wyboru inwestorów, wartości giełdowe spółek, pracowników i związki zawodowe, współprace zagraniczne, marki i reputacje przedsiębiorców.

INNYMI SŁOWY, DEZINFORMACJA I FAKE NEWSY MAJĄ NA CELU REALNE WPŁYWANIE NA BIZNES.

Warto przytoczyć za badaniami NASK, że według opinii i obserwacji Polaków, jeśli chodzi o działania dezinformacyjne w sieci:

- zdaniem respondentów – nieprawdziwe lub zmanipulowane informacje występują **w sieci powszechnie,**
- codziennie styka się z nimi **8,3% ankietowanych, kilka razy w tygodniu - 15,6%,**
- raz w tygodniu - **11,1%,**
- **tylko 2,3% respondentów wybrało odpowiedź „nigdy”,**
- **fake news** – to najczęstszy rodzaj dezinformacji, z jakim spotykają się Polacy (29,9%),
- respondenci wymieniają też **trolling** (15,6%), działania przez fałszywe konta, np. na portalach społecznościowych (14,9%) i zmanipulowane zdjęcia (8,3%),
- portale informacyjne – **46,1% badanych wskazało je jako miejsce, w których manipulacja i dezinformacja występują najczęściej,**
- 19% badanych wprost twierdzi, że nie sprawdza wiarygodności internetowych informacji, ani ich źródeł,
- na pytanie, czy w ostatnich miesiącach spotkali się z fałszywymi lub zmanipulowanymi informacjami – 32,8% badanych odpowiedziało „trudno powiedzieć”.

19% BADANYCH WPROST TWIERDZI, ŻE NIE SPRAWDZA WIARYGODNOŚCI INTERNETOWYCH INFORMACJI, ANI ICH ŹRÓDEŁ.

W sposób co prawda arbitralny, jednak pokusiłbym się postawić tezę, że z dezinformacją i fake newsami spotykamy się nawet częściej niż wynika to z powyżej wspomnianego badania, tyle tylko, że z założenia części informacji, które do nas docierają, a które nie dotyczą istotnych dla nas kwestii, nie usiłujemy nawet weryfikować, a często na poziomie świadomym nie poddajemy nawet refleksji nad nimi.

CZY DEZINFORMACJA I FAKE NEWSY MAJĄ REALNY WPŁYW NA BIZNES, A JEŚLI TAK TO CZY SĄ SKUTECZNE METODY DO WALKI Z NIMI?

Odpowiedź na pierwsze z pytań wydaje się nasuwać sama przez się – nasze przekonania i poglądy, wierzenia i przesądy, wiedza i niewiedza, a nawet radości i lęki zawsze miały i mieć będą wpływ na biznes. Jeśli więc zostaną one zmanipulowane to z pewnością znajdzie to odzwierciedlenie w wynikach biznesowych przedsiębiorców. Nie budzi wątpliwości, że zdjęcie pustych półek sklepowych czy też pustych dystrybutorów na stacji benzynowych potrafiły odpowiednio pobudzić wyobraźnie i sprowokować niejedną osobę do określonego, nie zawsze uzasadnionego, działania, które finalnie miało określone przełożenie na biznes. Cóż z tego, że prapoczątkiem wszystkiego mogła być jednostkowa sytuacja, skoro została nam ona przekazana w ten sposób, że w naszych mózgach wzbudziła obawę o to, czy i dla nas nie zabraknie towaru. Działania takie nie zawsze muszą być w skali makro.

Na własnym przykładzie mogę podać, że znajoma współpracując z jednym ze znanych MLMów usiłowała mnie kiedyś nakłonić do zakupu oferowanych przez nią suplementów takimi stwierdzeniami jak: „W USA procedura certyfikacji nie jest taka jak w Polsce. Tak byle co nie przejdzie", czy też zachęcając mnie do zakupu sprzedawanej przez nią pasty do zębów, podkreślając, że w tych „zwykłych" często jest azot, a on przecież był też wykorzystywany w obozach koncentracyjnych. Czasem skala jest jednak makro, czego przykłady mieliśmy tak w kontekście technologii 5G czy też w kontekście szczepionek, które jakby nie było wywodzą się z biznesów farmaceutycznych. Analizując tego ty-

pu działania można powiedzieć, że z jednej strony nie mają one teoretycznie związku z żadną firmą, a z drugiej – w sposób ewidentny co najmniej mogą oddziaływać na zachowania konsumentów i z założenia mają na celu nakłonienie go do nabycia produktów od osoby, która przedstawia te (dez)informacje.

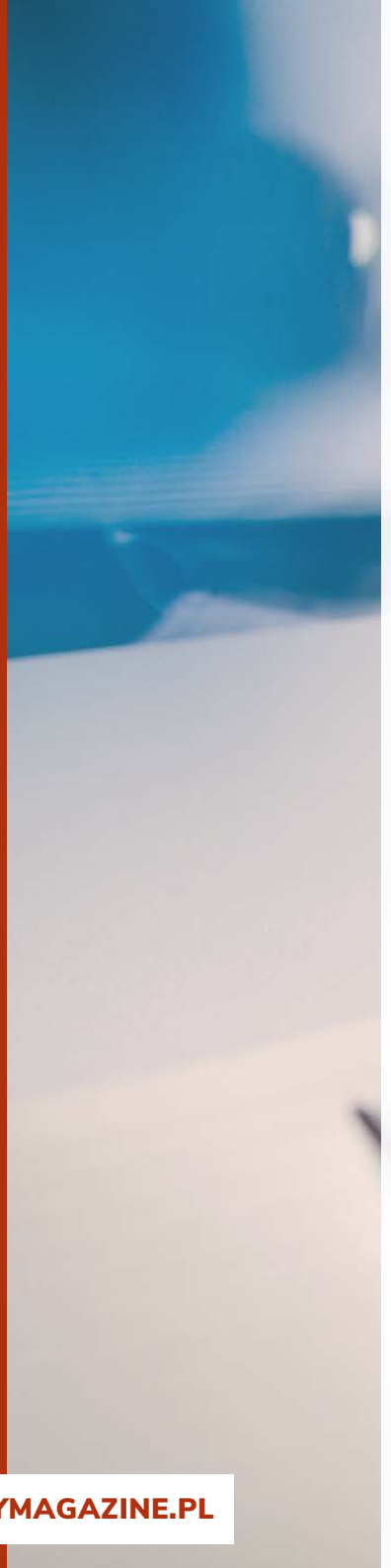
Warto podkreślić, że działania o podobnym charakterze mogą też przybierać „znamiona" czynu nieuczciwej konkurencji i zostać skierowane znacznie bardziej precyzyjnie. Otóż najczęściej spotykanym przykładem takich działań jest z jednej strony reklama ukryta, a z drugiej rozpowszechnianie nieprawdziwych informacji dotyczących danej firmy, jej kadry zarządzającej i tym podobnych, by podważyć renomę, wiarygodność czy też rzetelność przedsiębiorstwa.

Skoro już wiemy, w jakiej skali problemem są te zjawiska to warto też wiedzieć, czy są prawne sposoby, aby walczyć z nimi w biznesie. Oczywistym wydaje się, że jeśli tego rodzaju dezinformacja czy fake newsy pojawią się w przestrzeni cyfrowej, to co do zasady odpowiedzialność ponosi za tego typu treści o-

soba, która je rozpowszechnia. Jest tu jednak pewien problem, ponieważ dla przeciętnego użytkownika, nawet tego biznesowego, może niekiedy graniczyć z niemożliwością ustalenie autora wpisu na forum czy pod artykułem prasowym.

Warto więc wiedzieć, że co najmniej od momentu otrzymania zawiadomienia o bezprawności danego wpisu odpowiedzialność za jego dalsze pozostawanie na takiej stronie obciążać będzie także jej administratora.

Co istotne, w przypadku tak forów internetowych, jak i portali społecznościowych, najczęściej regulamin określa procedurę zgłaszania takich wpisów. Jeśli natomiast takie fake newsy pojawiają się w prasie, to warto wiedzieć, że zupełnie za darmo możliwe jest na jej łamach opublikowanie ich sprostowania. Polega to na tym, że na wniosek zainteresowanej osoby redaktor naczelny właściwego dziennika lub czasopisma jest obowiązany opublikować bezpłatnie rzeczowe i odnoszące się do faktów sprostowanie nieścisłej lub nieprawdziwej wiadomości zawartej w materiale prasowym.



SPROSTOWANIE powinno zostać nadane w placówce pocztowej operatora pocztowego lub złożone w siedzibie odpowiedniej redakcji na piśmie, w terminie nie dłuższym niż 21 dni od dnia opublikowania materiału prasowego. Bardzo istotne jest też, że sprostowanie powinno zawierać podpis wnioskodawcy, jego imię i nazwisko lub nazwę oraz adres korespondencyjny. Tym samym, nie możemy go po prostu wysłać mailem. Jeśli nasze sprostowanie nie zostanie opublikowane bez powodu, to o jego publikacje można wystąpić na drogę sądową. Do tego, jeśli taki materiał prasowy narusza dobra osobiste naszej firmy czy nas samych albo też godzi w nasz biznes jeszcze na inny sposób, możemy też dochodzić dalej idących roszczeń.

Zakładam, że niektórzy mogli pomyśleć, że ten sposób działania jest zupełnie nieprzydatny w Internecie, bo co do zasady brak w nim prasy. Otóż wręcz przeciwnie! Po pierwsze, niemal wszystkie portale informacyjne będą stanowić dziennik, a w najlepszym razie czasopismo. Co więcej, do tej kategorii zaliczyć trzeba też sporą część blogów, vlogów, czy podcastów i to nawet jeśli jako takowa nie zostanie zarejestrowane. W ich przypadku procedura sprostowania także może znaleźć zastosowanie. Idąc dalej, jeśli dane działanie w cyberprzestrzeni jest dezinformacją lub fake newsem uderzającym w konkretną firmą to trzeba wiedzieć, że prócz odpowiedzialności cywilnej takie zachowanie może stanowić także przestępstwo.

Jak wynika bowiem z ustawy o zwalczaniu nieuczciwej konkurencji, kto rozpowszechnia nieprawdziwe lub wprowadzające w błąd wiadomości o przedsiębiorstwie, w szczególności o osobach kierujących przedsiębiorst-

wem, wytwarzanych towarach, świadczonych usługach lub stosowanych cenach albo o sytuacji gospodarczej lub prawnej przedsiębiorstwa, w celu szkodzenia przedsiębiorcy, podlega karze aresztu albo grzywny. Analogicznie, za przestępstwo może zostać uznana także **ukryta reklama**, gdyż tej samej karze podlega też ten, kto w celu przysporzenia korzyści majątkowej lub osobistej sobie, swojemu przedsiębiorstwu lub osobom trzecim, rozpowszechnia nieprawdziwe lub wprowadzające w błąd wiadomości o swoim przedsiębiorstwie lub przedsiębiorcy, w szczególności o osobach kierujących przedsiębiorstwem, wytwarzanych towarach, świadczonych usługach lub stosowanych cenach albo o sytuacji gospodarczej lub prawnej przedsiębiorcy lub przedsiębiorstwa.

Powyżej przedstawiłem podstawowe sposoby radzenia sobie z dezinformacją i fake newsami w biznesie. Warto podkreślić, że obecnie coraz bardziej powszechne stają się regulacje prawne mające na celu wprowadzenie adekwatnych sposobów ochrony przed tymi zjawiskami, co dotyczy w szczególności deepfake'ów, czyli animacji komputerowych, których celem jest stworzenie filmów wideo przedstawiających realne osoby, w których one jednak nie występują. Nie zawsze mają one co prawda na celu szkodzenie - jednym z ciekawszych przykładów tego rodzaju „twórczości" był film przedstawiający Baracka Obamę przestrzegającego przed dezinformacją i fake newsami, który sam był deepfak'em – jednak z całą pewnością mają największy potencjał jeśli o to chodzi. Dla tego w niektórych krajach pojawia się obowiązek oznaczania takich filmów, jako deepfake właśnie, a brak tego oznaczenia ma stanowić przestępstwo.

PROWADZONE SĄ PRACE LEGISLACYJNE NAD USTAWĄ, KTÓRA MIAŁABY PRZECIWDZIAŁAĆ FAKE NEWSOM I DEZINFORMACJI. MOWA TU O PROJEKCIE USTAWY O OCHRONIE WOLNOŚCI SŁOWA W INTERNETOWYCH SERWISACH SPOŁECZNOŚCIOWYCH.

Wracając jeszcze na grunt naszego rodzimego prawa warto wiedzieć, że prowadzone są prace legislacyjne nad ustawą, która miałaby przeciwdziałać fake newsom i dezinformacji. Mowa tu o projekcie ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych, która ma tę kwestię regulować w zakresie działania serwisów społecznościowych. Co prawda ustawa jest jeszcze w trakcie prac legislacyjnych, ale z obecnego kształtu projektu wynika, że **wprowadzi ona kilka pojęć, do których należy dezinformacja, treści o charakterze przestępczym oraz treści o charakterze bezprawnym.** Ustawa wprowadzić ma wewnętrzną procedurę w ramach działalności portali społecznościowych, które zostaną zobligowane do stworzenia postępowania umożliwiającego kierowanie do nich zgłoszeń dotyczących treści wyróżnionych powyżej. Po rozstrzygnięciu zgłoszenia przysługiwać ma także reklamacja.

W przypadku pewnych rozstrzygnięć dotyczących usunięcia treści lub odmowy ich usunięcia ma zostać także wprowadzona skarga do Rady Wolności Słowa.

Co ciekawe, do walki z fake newsami mają zostać powołane zaufane podmioty działające w interesie publicznym w celu przeciwdziałania dezinformacji rozpowszechnianej za pośrednictwem internetowych serwisów społecznościowych.

Do pełnienia tej funkcji może zostać wyznaczony człowiek, posiadający specjalistyczną wiedzę, w szczególności z zakresu medycyny, prawa, praw człowieka, rynku finansowego lub bezpieczeństwa publicznego oraz organizacja społeczna, do której statutowych celów należy zwalczanie dezinformacji w przestrzeni publicznej. Na zakończenie warto dodać jedynie, że nieco niepokojącym może być w ocenie niektórych to, że Rada Wolności Słowa będzie organem administracyjnym i będzie wybierana przez Sejm Rzeczypospolitej Polskiej, który powoływać będzie jej członków większością 3/5 głosów.

Źródła:

Dezinformacja, dostęp dnia 14 marca 2022 r.

Fake news, dostęp dnia 14 marca 2022 r.

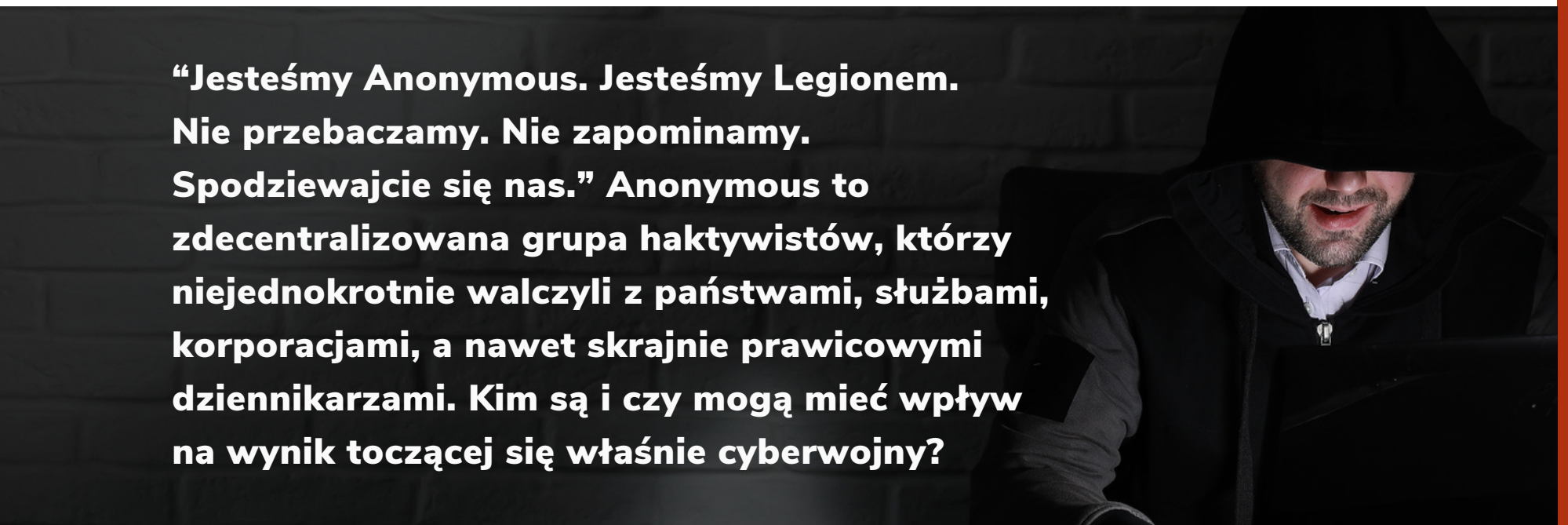
Trollowanie, dostęp dnia 14 marca 2022 r.

Dezinformacja i manipulacja w internecie. Wyniki badań NASK, dostęp 14 marca 2022 r.


Bitdefender
Bitdefender ANTIVIRUS PLUS
Bitdefender INTERNET SECURITY
20% RABATU
KOD RABATOWY:
BITDEFENDER20
Do końca kwietnia
Promocja dla czytelników Security Magazine!
Antivirus Plus i Internet Security taniej o 20%

ANONYMOUS - SOJUSZNICY CZY WROGOWIE? JAKI MAJĄ WPŁYW NA TOCZĄCĄ SIĘ CYBERWOJNĘ?

Redakcja
SECURITY MAGAZINE



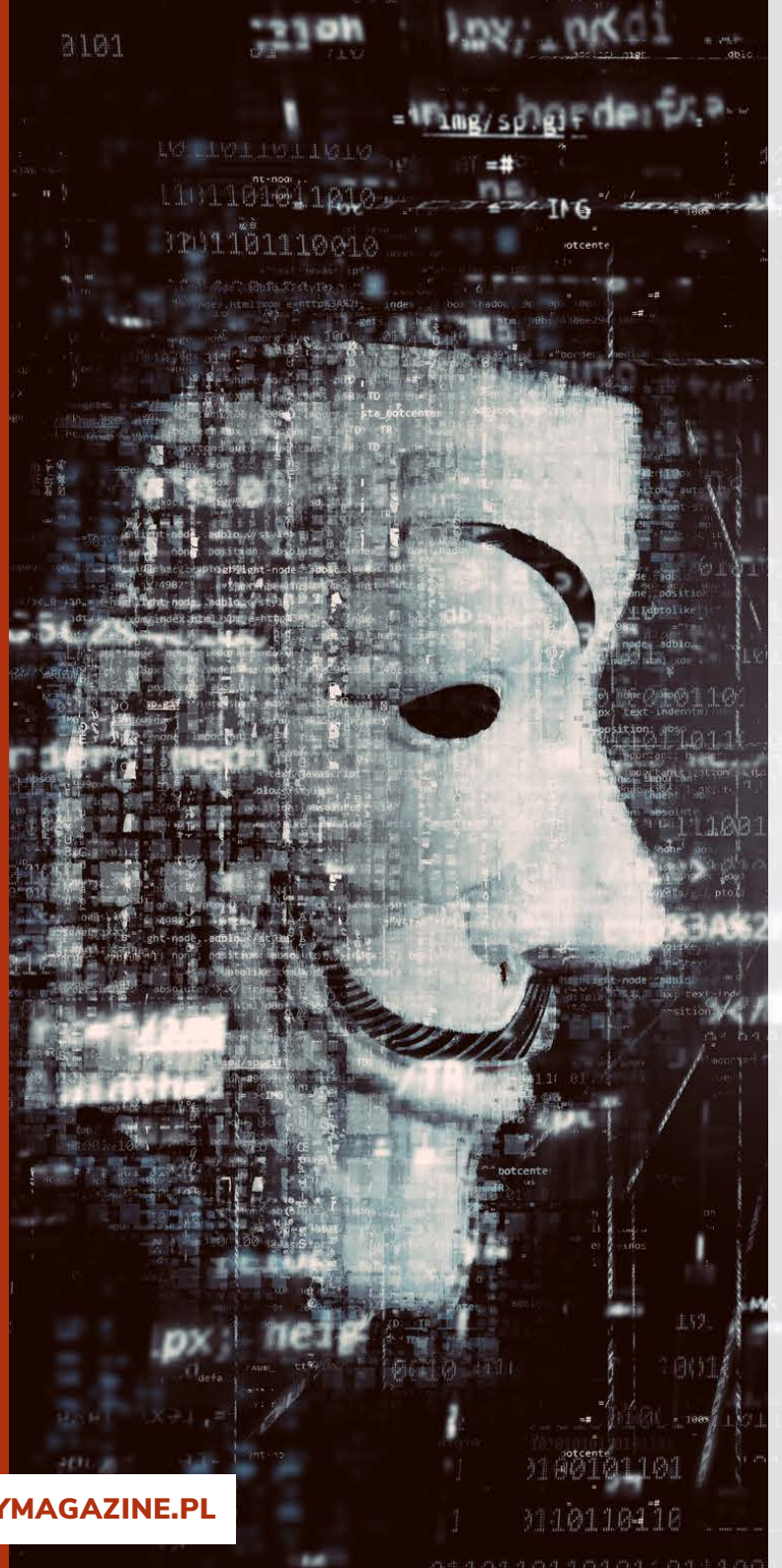
“Jesteśmy Anonymous. Jesteśmy Legionem. Nie przebaczamy. Nie zapominamy. Spodziewajcie się nas.” Anonymous to zdecentralizowana grupa haktywistów, którzy niejednokrotnie walczyli z państwami, służbami, korporacjami, a nawet skrajnie prawicowymi dziennikarzami. Kim są i czy mogą mieć wpływ na wynik toczącej się właśnie cyberwojny?

ANONYMOUS WYWODZĄ SIĘ OD 4CHANOWYCH TROLLI?

W internecie można znaleźć wiele różnych dat dotyczących powstania Anonymous. Wymieniane są 2003 rok, 2004, 2006, a nawet 2000. Choć kwestie dat są niespójne, to w przypadku miejsca powstania Anonymous nie ma takich problemów. Wymienia się tutaj fora internetowe 4chan i Something Awful – to zresztą temu pierwszemu grupa zawdzięcza swoją nazwę. Użytkownicy 4chana automatycznie podpisywani są na forum jako „Anonymous", czyli – anonimowy. Dale Beran – dziennikarz The Atlantic jako twórcę Anonymous wskazuje kanadyjskiego hakera Aubreya „Kirtanera" Cottle'a, który w okolicach 2000 roku miał należeć do grupy internetowych trolli.

To właśnie ta grupa miała określać siebie jako Anonymous i rozpoczynała pierwsze hakerskie ataki. Cottle miał wówczas około 13–14 lat. Początkowo grupa spamowała, rajdowała i DDoSowała różne strony internetowe, gry online, czaty, a czasem atakowała także skrajnie prawicowego dziennikarza Hala Turnera czy Kościół Scjentologiczny. To właśnie z tych dwóch ostatnich wydarzeń Anonymous zasłynęli przy początkach swojej działalności najbardziej. Z czasem 4chan przestał akceptować tego typu trolling, toteż w około 2005 roku grupa przeniosła się na stronę stworzoną przez Cottle'a – 420chan.

Forum to istnieje do dziś i już od początku swojego istnienia było poświęcone... **rekreacyjnemu zażywaniu narkotyków** (głównie marihuany, stąd 420 w nazwie serwisu), społeczności LGBT, ale też atakom hakerskim. W 2007 roku do drzwi domu Aubreya miało zapukać CSIS (Kanadyjska Tajna Służba Wywiadowcza), która zapytała hakera, czy chce wykorzystać swoje umiejętności w słusznym celu – w **walce z Al-Kaidą**, choć ten nie bardzo wiedział, jak miałby w tej kwestii pomóc. Rok później Cottle zaczął się jednak wycofywać z haktywizmu, gdyż miał zostać sfotografowany przez członków **Kościoła Scjentologicznego**. Cottle obawiał się o życie swoje i swoich bliskich. Jak sam przyznał – starał się w jakiś sposób zakończyć działalność Anonymous, a nawet zdyskredytować grupę, jednak bez skutku.



Haker wycofał się na kilka lat i powrócił dopiero w 2020 roku, kiedy to **odrodzone Anonymous** postanowiło walczyć z ruchem QAnon – prawicowymi teoretykami spiskowymi wspierającymi Donalda Trumpa. QAnon twierdzą m.in., że światowymi bankami centralnymi steruje rodzina Rothschildów, administracja Baracka Obamy była uwikłana w handel dziećmi, Angela Merkel to wnuczka Hitlera, a Kim Dzong Un to marionetka ustanowiona w Korei Płn. przez CIA. To także zwolennikom QAnon przypisuje się atak na Kapitol USA w 2021 roku.

POCZĄTKI DZIAŁALNOŚCI ANONYMOUS. WALKA ZE SCJENTOLOGIĄ

Anonymous początkowo nie było związane ściśle z haktywizmem. Wręcz przeciwnie – grupa ta wykazywała się sporą szkodliwością. W 2006 roku Anonymous zaatakowało fińską grę społecznościową Habbo Hotel, blokując użytkownikom dostęp do cyfrowej pływalni, twierdząc, że jest ona zablokowana z powodu „awarii i AIDS". Z kolei w 2008 roku hakerzy zaatakowali stronę Epilepsy Foundation, która pomaga osobom cierpiącym na padaczkę. Anonymous miało zamieścić na witrynie mnóstwo migających animacji, które mogły wywołać napady epileptyczne u użytkowników. Atak ten potwierdził w 2021 roku sam Aubrey Cottle w wywiadzie dla Vice News i przeprosił za niego po latach.

Pierwsi członkowie związani z grupą Anonymous dręczyli również rodziców Mitchella Hendersona – nastolatka, który za-

strzelił się z powodu zgubienia swojego iPoda. Na 4chanie pojawiały się parodie kondolencji składanych rodzinie samobójcy, jak i drastyczne filmiki i zdjęcia. Jeden z członków Anonymous zadzwonił nawet do rodziców Hendersona, podając się za jego ducha. Sporą część wybryków wczesnego Anonymous dokumentowała **Encyclopedia Dramatica.**

Z haktywizmem grupa związała się w zasadzie w 2008 roku właśnie przy okazji serii działań przeciwko Kościołowi Scjentologicznemu. Dlaczego? To ze względu na list, jaki wystosował Kościół wobec bloga plotkarskiego Gawker. Serwis ten opublikował wideo z Tomem Cruisem – jednym z członków Kościoła Scjentologicznego – w którym chwalił on swoją religię. Członkowie Kościoła uznali to za „naruszenie praw autorskich". Haktywiści zamieścili na YouTubie film, w którym przekazali wiadomość do przywódców Kościoła Scjentologicznego: **„Dla dobra twoich zwolenników, dla dobra ludzkości – dla śmiechu – usuniemy was z internetu."**

Anonymous blokowało linię telefoniczną organi-

zacji, wysyłało masowo czarne faksy, żeby marnować wkłady atramentowe w siedzibie kościoła i DDoSowała jego strony internetowe za pomocą aplikacji Gigaloader i JMeter (później także Low Orbit Ion Cannon). Scjentolodzy szybko obronili się przed atakiem Anonymous, a co więcej – doprowadzili do aresztowania kilku haktywistów, którzy nie ukryli swoich adresów IP. Te wydarzenia wyciągnęły 10 lutego 2008 roku na ulicę setki protestujących, którzy manifestowali przy budynkach scjentologów na całym świecie.

PROTESTUJĄCY, ŻEBY UKRYĆ SWOJĄ TOŻSAMOŚĆ, ZAKŁADALI MASKI GUYA FAWKESA – ANGIELSKIEGO SPISKOWCA Z XVII WIEKU, KTÓREMU POPKULTURA NADAŁA DRUGIE ŻYCIE DZIĘKI KOMIKSOWI ALANA MOORE'A – „V JAK VENDETTA" I JEGO ADAPTACJI

Główny bohater dzieła niejaki V walczył z totalitarnym systemem, toteż haktywiści i ich zwolennicy zaczęli się utożsamiać z tym symbolem. Maska Fawkesa zastąpiła dotychczasowy znak rozpoznawczy hakerów – czarnoskórego mężczyznę w szarym garniturze i afro.

Walka ze scjentologią, jak i same protesty trwały blisko rok, jednak nie przyniosły większych efektów. **Był to jednak pierwszy moment w historii Anonymous, kiedy haktywiści poczuli, że mają jakąś formę mocy sprawczej i wpływ na świat rzeczywisty – a nie tylko ten wirtualny.** Od tamtej pory Anonymous znacznie poprawiło swoje bezpieczeństwo w sieci, a sama grupa podzieliła się na haktywistów tzw. moralflags, jak i trolli. Haktywiści są jednak znacznie bardziej kojarzeni z Anonymous i niejako stanowią trzon tej toż-samości. Trolle z kolei funkcjonują nadal, ale utożsamia się ich obecnie bardziej z kulturą tzw. chanów, czyli serwisów podobnych do 4chana. Polskim ich odpowiednikiem są np. karachany – użytkownicy zamkniętego forum karachan.org

W tym miejscu warto jednak zaznaczyć, że Anonymous jako takie jest bardziej symbolem. To zdecentralizowana grupa pozbawiona przywódcy. W różnych momentach swojej historii miała odmienne cele i filozofię.

Anonymous są czymś w rodzaju pirackiej bandery Wesołego Rogera – flagą wywieszaną przez różne grupy, a nawet pojedyncze osoby, które niekoniecznie muszą ze sobą współpracować. **W różnych krajach występują też pewne lokalne oddziały, które mogą być bardziej scentralizowane i skoordynowane, przykładem jest chociażby AnonPoland czy AnonSlovenia.**

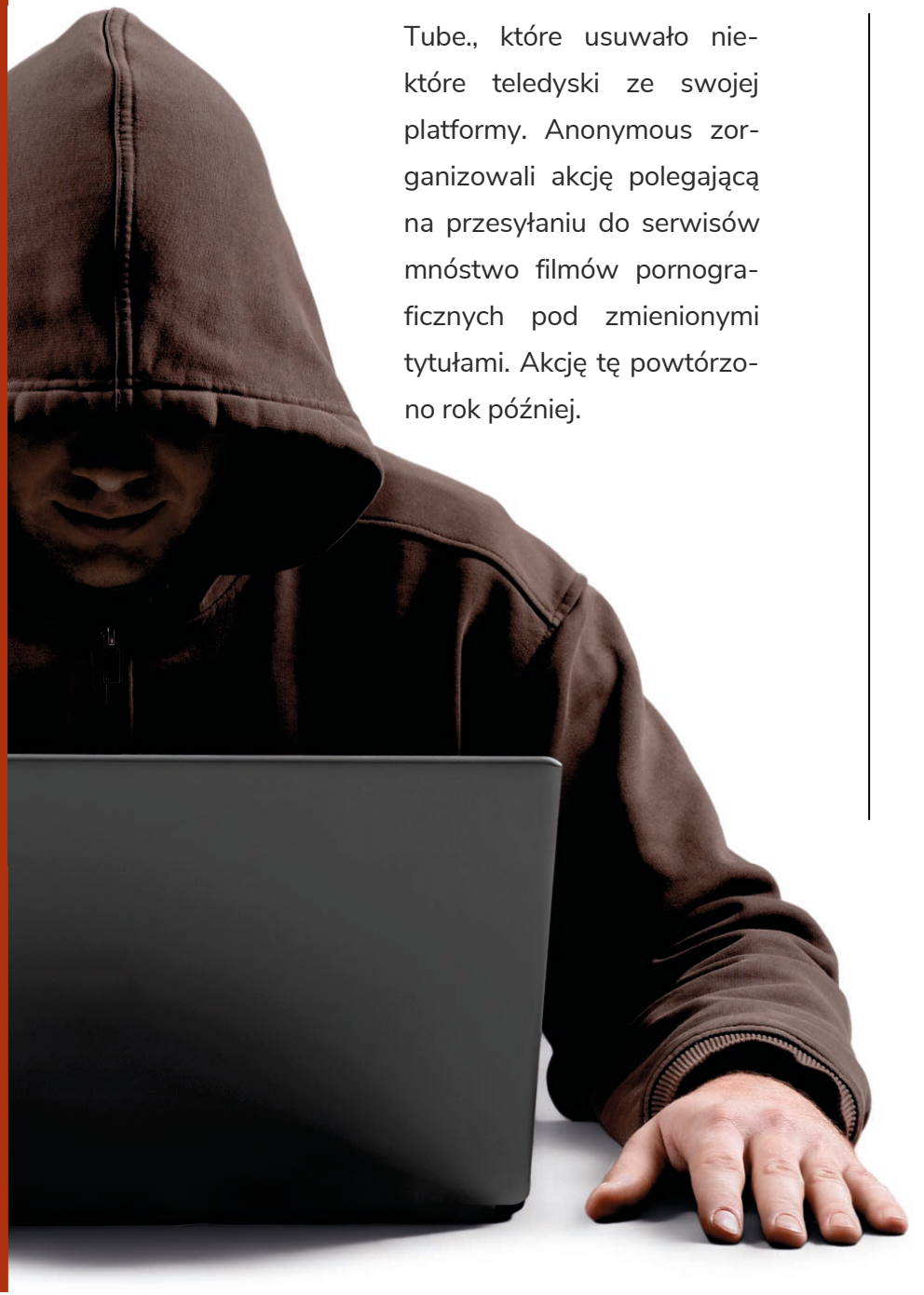
ANONYMOUS PRZECIWKO ACTA, RASIZMOWI W POLICJI I REŻIMOM

Po akcji przeciwko scjentologii haktywiści coraz częściej zaczęli występować przeciwko reżimom. W 2009 roku wsparli Irańczyków protestujących przeciwko fałszerstwom wyborczym i sytuacji politycznej w ich kraju. Anonymous wraz z pirackim serwisem The Pirate Bay założyli stronę z międzynarodowym poparciem dla protestujących, umożliwiając im także wymianę informacji.

W międzyczasie wykazywali także poparcie dla niecenzurowania treści w internecie i piractwa. Anonymous są bowiem mocno powiązani ze wspomnianym The Pirate Bay, które udostępnia mnóstwo kradzionych treści, plików, materiałów wideo i gier w internecie.

2 maja 2011 roku Anonymous wypowiedziało wojnę przeciwko faszystom i nacjonalistom. Na początku stycznia 2012 roku zaatakowali liczne strony i fora powiązane z organizacjami faszystowskimi, a także sklepy sprzedające gadżety kojarzone z tą ideologią. Anonymous upubliczniło dane adresowe tysięcy faszyzujących osób i wskazało na powiązania byłego kandydata na prezydenta USA Rona Paula z neonazizmem. Haktywiści walczyli też przeciwko Fideszowi, Watykanowi, rządowi Nigerii, ChRL, Ku Klux Klan, ISIS, talibom i Al-Kaidzie, jak i wspierali Arabską Wiosnę. Anonymous występowało także przeciwko policji w Missouri, której funkcjonariusz w 2014 roku zastrzelił 18-letniego Afroamerykanina Michaela Browna. Podobną akcję przeprowadzili w 2020 roku przy okazji śmierci George'a Floyda.

Haktywiści nigdy nie zapomnieli jednak o swoich korzeniach, tj. walce przeciwko korporacjom i dla wolności słowa oraz treści w internecie. W 2009 roku ich atakiem padło You-



Tube., które usuwało niektóre teledyski ze swojej platformy. Anonymous zorganizowali akcję polegającą na przesyłaniu do serwisów mnóstwo filmów pornograficznych pod zmienionymi tytułami. Akcję tę powtórzono rok później.

Stąd też nie dziwi sprzeciw grupy wobec projektów ustawy PIPA, SOPA i ACTA, wokół których wybuchły protesty w całej Europie i USA w 2012 roku. Hakerzy zablokowali wówczas m.in. oficjalną stronę premiera RP, CIA, kolumbijskiego ministerstwa obrony czy chilijskiej biblioteki narodowej, atakowali Lady Gagę, Kim Kardashian, Taylor Swift czy Justina Biebera, którzy poparli projekty, a nawet udostępnili kodowaną telekonferencję między FBI a Scotland Yardem. Haktywiści upublicznili także dane adresowe 28 tys. członków rządzącej w Czechach Obywatelskiej Partii Demokratycznej.

W okolicach 2016 roku działalność Anonymous znacząco osłabła. Sporo haktywistów zostało aresztowanych m.in. przez Interpol, a operacje przeprowadzane przez hakerów nie były aż tak głośne i wpływające na życie społeczne czy polityczne. Ruch „odrodził się” w zasadzie w 2020 roku. Haktywiści włamali się na oficjalny serwis ONZ, gdzie utworzyli podstronę dla nieuznawanego przez większość państw Tajwanu (Republiki Chińskiej). Kraj ten od 1971 roku nie ma siedziby ONZ, a to za sprawą Chińskiej Republiki Ludowej.

O Anonymous ponownie zaczęło być głośno jednak dopiero przy okazji wspomnianej śmierci George'a Floyda. Wówczas haktywiści zDDo-Sowali stronę policji w Minneapolis.

ANONYMOUS KONTRA ROSJA

Obecnie Anonymous przeżywa „drugą młodość" z powodu rosyjskiej inwazji na Ukrainę. Haktywiści oficjalnie wypowiedzieli wojnę przeciwko Rosji, a także markom, które postanowiły nadal prowadzić w niej działalność. Hakerzy atakowali strony rosyjskich mediów czy ministerstw. Zhakowali także tamtejszą telewizję, gdzie puszczali materiały przedstawiające obraz wojny na Ukrainie. Anonymous upubliczniło także 200 GB maili od białoruskiego producenta broni Tetraedr, który zapewnia wsparcie logistyczne Rosji. Udostępnili także 28 GB danych z Rosyjskiego Banku Centralnego, a także atakowali putinowskich oligarchów.

To nie pierwszy raz, kiedy grupa występuje przeciwko rosyjskiemu rządowi. Rosja była atakowana przez hakerów już w 2012 roku. Nigdy nie działo się to jednak na tak dużą i skoordynowaną skalę. Anonymous zaatakowało

także koncerny, które nie chciały wycofać swojej działalności z Rosji, chodzi m.in. o Nestle. Haktywiści ujawnili 10 GB danych, które zawierały informacje na temat 100 tys. klientów biznesowych koncernu.

Czy Anonymous to nasi sojusznicy, a może wrogowie? Trudno to jednoznacznie określić, bo – nie ma de facto jednej grupy Anonymous. Pod tym szyldem działało wielu hakerów, trolli i haktywistów, którzy mieli różne cele i odmienne poglądy polityczne. Grupie, która obecnie stoi za Anonymous przypisuje się idee lewicowo liberalne, a czasem wręcz libertariańskie. W końcu występują oni przeciwko reżimom, walczą z rasizmem, faszyzmem czy nacjonalizmem, wspierają społeczność LGBT i występują przeciwko wojnom. Jednak jednocześnie wspierają piractwo, a ich działalność niejednokrotnie stoi na granicy prawa, a niekiedy wręcz je przekracza. Ponadto nie wszystkie osoby stojące za Anonymous są w porządku wobec innych haktywistów czy wolontariuszy. Dość powiedzieć, że ofiarami aresztowań w 2008 r., kiedy grupa walczyła ze scjentologią, były przede wszystkim osoby, którym wręcz wmówiono, że atakowanie poprzez Low Orbit Ion Cannon jest całkowicie legalne.

Obecnie skupienie się grupy na Rosji jest bardzo ważne – nie tyle przez cyfrowe ataki, co nagłaśnianie wydarzeń na Ukrainie i zwracanie uwagi świata przeciwko reżimowi Putina. W ostatecznym rozrachunku Anonymous nie są czarno-biali i nie można powiedzieć, że zawsze postępują właściwie. Jeśli są naszymi sojusznikami, to sojusz ten może być wyjątkowo kruchy. A czy mają jakiś znaczący wpływ na wojnę w Ukrainie? Raczej symboliczny i PR-owy. Upubliczniane przez nich dane nie spowodują, że sytuacja Ukrainy jakoś znacząco się polepszy. Jednak dzięki swojej działalności zwracają uwagę świata na to, co dzieje się w Ukrainie i przypominają o firmach, które nie wycofały się ze swoimi działaniami biznesowymi z Rosji. Pod względem cyberbezpieczeństwa mogą im nieco nabruździć, ale nie spowodują bezpośrednio przegranej Rosji czy bankructwa firm.

ZERO TRUST I OCHRONA CYFROWEJ TOŻSAMOŚCI. JAK SPROSTAĆ AKTUALNYM WYZWANIOM CYBERBEZPIECZEŃSTWA?

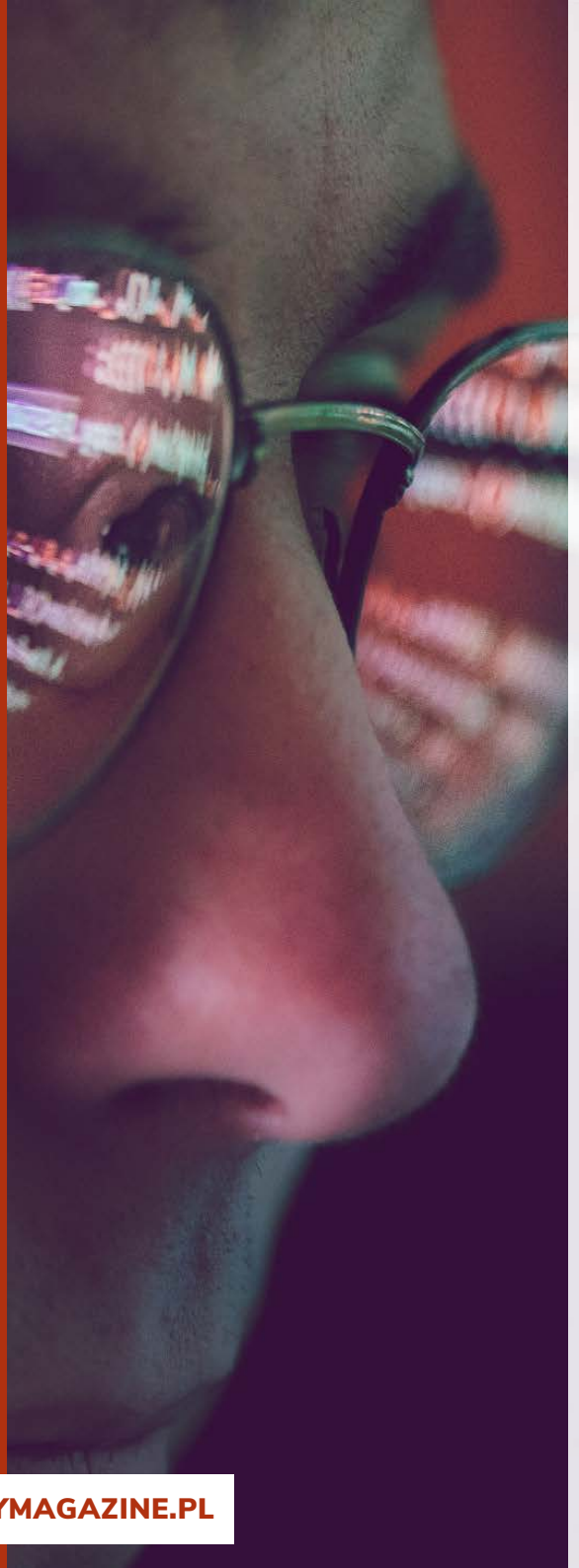
Krzysztof Andrian
Concept Data

Obecnie polskie przedsiębiorstwa mierzą się z dwoma głównymi wyzwaniami w obszarze cyberbezpieczeństwa. Oba związane są z globalnymi wydarzeniami z ostatnich lat i wymagają nowego podejścia do ochrony firm i ich danych.

Pierwszym wyzwaniem jest praca hybrydowa, którą w oparciu o doświadczenia czasu covidowego wprowadza dziś coraz więcej przedsiębiorstw. Taki model pracy sprawia, że poszerza się infrastruktura firmy i zakres zarządzania nią. Pracownicy są mobilni, korzystają z wielu różnych urządzeń, łączą się z firmowymi sieciami z domowych lub niezabezpieczonych sieci. To wymusza na firmach nowe podejście do ochrony zasobów, w tym do ochrony urządzeń używanych przez pracowników w codziennych działaniach.

Drugie wyzwanie powiązane jest z aktualną sytuacją za wschodnią granicą Polski. Niepokoje w Ukrainie, podwyższone zagrożenie cyberatakami oraz obowiązujący na terenie całego kraju trzeci stopień alarmowy CRP (CHARLIE–CRP) sprawiają, że firmy analizują swoją gotowość do walki z zagrożeniami. Instytucje – zwłaszcza z sektora bankowości i ubezpieczeń oraz obszaru infrastruktury krytycznej – przeprowadzają audyty wewnętrzne. Sprawdzają, gdzie są luki i podatności, oraz analizują, jak lepiej wykorzystać wdrożone narzędzia zabezpieczające, by stawić czoło tym ryzykom.

W obu przypadkach rozwiązaniem, które proponujemy naszym klientom, jest wprowadzenie polityki zero trust,



zakładającej ścisłą kontrolę dostępu i domyślny brak zaufania do wszystkich, którzy są lub próbują dostać się do firmowej sieci.

WIELOSKŁADNIKOWE UWIERZYTELNIANIE I KONTROLA APLIKACJI

Ważnym elementem tej polityki jest odpowiednie zarządzanie tożsamością cyfrową (Identity Management) i zabezpieczenie jej (Identity Security), między innymi przez wdrożenie wieloskładnikowego uwierzytelniania, czyli MFA. MFA wprowadza do procesu uwierzytelniania drugi lub kolejny składnik. Firmy przestają więc polegać na zawodnych i łatwych do przejęcia hasłach. Coraz częściej sięgają za to po biometrię (odcisk palca czy skan twarzy) lub inny dodatkowy element, taki jak SMS czy powiadomienie push na telefonie. Dzięki nim można mieć pewność, że osoba, która loguje się do firmowych systemów, rzeczywiście jest tą, za którą się podaje.

Coraz większą popularnością cieszą się elastyczne **systemy MFA** (takie jak choćby CyberArk Identity Adaptive MFA), oparte na sztucznej inteligencji oraz uczeniu maszynowym, które rozpoznają kontekst (biorąc pod uwagę między innymi lokalizację użytkownika, porę dnia, adres IP, typ urządzenia oraz zdefiniowane przez administratora reguły) i pozwalają na indywidualny wybór składników uwierzytelniania.

Jak to działa? Narzędzie to wykorzystuje analizę behawioralną opartą na uczeniu maszynowym, rejestrującym standardowe zachowania użytkownika i alarmującym, gdy jego zachowanie odbiega od normy. Jeśli logowanie przebiega w standardowych okolicznościach, nie jest konieczne zastosowanie dodatkowych elementów uwierzytelniających. Jeśli jednak coś jest nie tak, system może wymusić podanie dodatkowych danych lub zablokować dostęp.

Drugim aspektem zarządzania tożsamością jest definiowanie i monitorowanie tego, co użytkownik robi, gdy już dostanie się do firmowej sieci. Nowoczesne rozwiązania klasy Identity Management pozwalają na stworzenie na urządzeniach końcowych użytkowników listy aplikacji i serwisów, z jakich dany pracownik czy kontraktor ma prawo korzystać. Jeśli będzie chciał uruchomić aplikację, która nie znajduje się na tzw. białej liście, system zablokuje taką możliwość. Co więcej, zrobi to automatycznie. Dodatkowo w razie jakiegokolwiek podejrzenia, że do sieci dostała się niepowołana osoba, system może zastosować tzw. red button, czyli wstrzyma wszystkie dostępy do czasu wyjaśnienia sytuacji. Lepiej jest bowiem odebrać i przywrócić dostęp nawet ważnej osobie na wysokim stanowisku, niż pozwolić oszustowi dostać się do infrastruktury i wyrządzić szkodę, która spowoduje ogromne starty.

BEZPIECZEŃSTWO KOŃCOWYCH URZĄDZEŃ UŻYTKOWNIKÓW

Bezpieczeństwo punktów końcowych to praktyka ochrony sieci przedsiębiorstwa przed zagrożeniami pochodzącymi z urządzeń lokalnych lub zdalnych.

Punktem końcowym jest każdy sprzęt używany przez pracowników, kontrahentów czy klientów zewnętrznych do tego, by dostać się do zasobów i aplikacji firmowych. Każdy z nich – a mówię o komputerach stacjonarnych, laptopach, serwerach, stacjach roboczych, smartfonach i tabletach – jest potencjalnym punktem cyberataku. Dlatego tak ważne jest zabezpieczenie wszystkich tego typu urządzeń. Jak to zrobić skutecznie?

W PRZESZŁOŚCI WIĘKSZOŚĆ ORGANIZACJI KORZYSTAŁA Z KONWENCJONALNYCH ŚRODKÓW BEZPIECZEŃSTWA, TAKICH JAK ZAPORY SIECIOWE, SIECI VPN, ROZWIĄZANIA DO ZARZĄDZANIA PUNKTAMI KOŃCOWYMI I PROGRAMY ANTYWIRUSOWE, ABY CHRONIĆ POUFNE INFORMACJE, ZAPOBIEGAĆ NIEAUTORYZOWANEMU DOSTĘPOWI DO KRYTYCZNYCH APLIKACJI I SYSTEMÓW IT ORAZ CHRONIĆ PRZED ZŁOŚLIWYM OPROGRAMOWANIEM I INNYMI PODATNOŚCIAMI.

Te środki są dziś jednak niewystarczające, bo przedsiębiorstwa coraz częściej stosują w swojej codziennej pracy aplikacje mobilne czy usługi w chmurze. Cyberprzestępcy stają się natomiast coraz bardziej wyrafinowani i każdego dnia lepiej radzą sobie z omijaniem tradycyjnych zabezpieczeń. Dlatego wiele przedsiębiorstw wprowadza obecnie nowe podejście do ochrony punktów końcowych, obejmujące szerszy zakres kontroli bezpieczeństwa. Jego podstawą są systemy EDR oraz EPM.

SYSTEMY ENDPOINT DETECTION AND RESPONSE (EDR)

To narzędzia służące do proaktywnego identyfikowania i badania podejrzanej aktywności na urządzeniach końcowych.

Większość rozwiązań EDR stale monitoruje, rejestruje i analizuje takie zdarzenia, pomagając w skutecznym wykrywaniu i ograniczaniu zaawansowanych zagrożeń.

SYSTEMY ENDPOINT PRIVILEGE MANAGEMENT (EPM)

Pozwalają zarządzać uprawnieniami w taki sposób, by przyznawać użytkownikom i procesom minimalny zestaw uprawnień, tylko taki, który jest im potrzebny do wykonywania wymaganych zadań. Taka zasada najmniejszych przywilejów usuwa lokalne prawa administratora na serwerach i komputerach osobistych, ograniczając uprawnienia dostępu do autoryzowanych użytkowników i aplikacji.

Rozwiązania tej klasy wprowadzają także tzw. Application Control, czyli możliwość tworzenia bezpiecznych (tzw. white list) lub zabronionych (tzw. black list) list aplikacji. Dodatkową elastyczność daje możliwość zdefiniowania niezaakceptowanych aplikacji i polityk obsługi wyjątków (tzw. grey list).

Wprowadzając zmiany w zakresie cyberbezpieczeństwa w swojej firmie, warto pamiętać, że jeśli zero trust ma zadziałać w pełni, musi być wdrożone w całej organizacji.

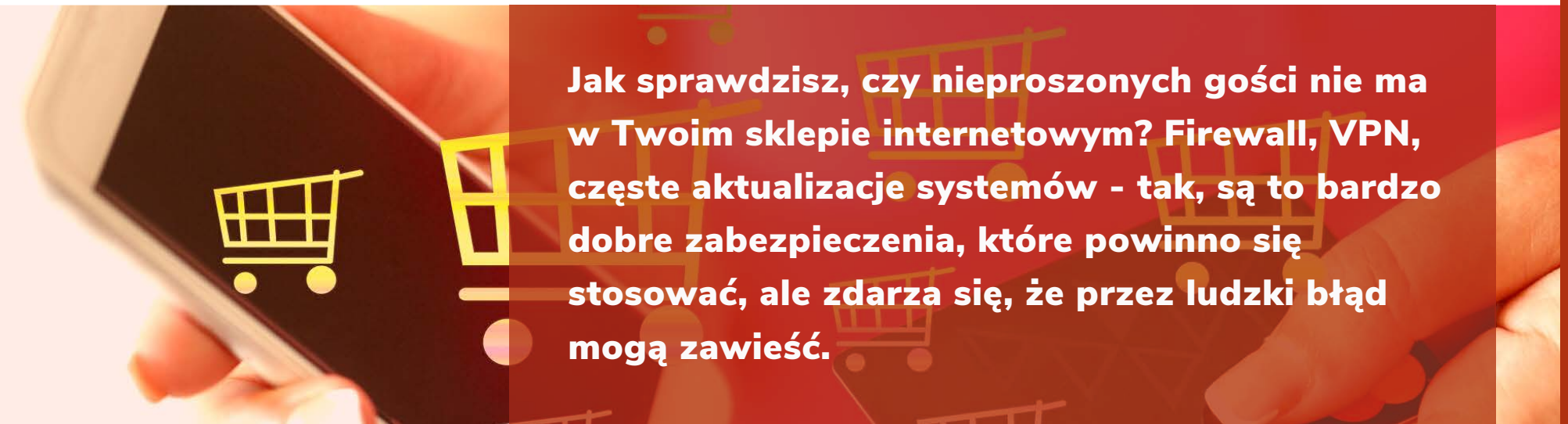
Do tej pory przedsiębiorstwa chroniły głównie systemy krytyczne, a przecież atakujący często wybierają środowiska testowe lub deweloperskie, by stamtąd dostać się do sieci firmowej. Ochrona musi więc objąć całą infrastrukturę. Tylko wtedy instytucja będzie w pełni przygotowana na stawianie czoła wyzwaniom w cyberprzestrzeni.

OBSŁUGA PRAWNA E-COMMERCE

WWW.RZETELNYREGULAMIN.PL

TWÓJ E-SKLEP TERAZ SPRZEDAJE? SKUTECZNY MONITORING PODSTAWĄ BEZPIECZEŃSTWA W E-COMMERCE

Krzysztof Witkowski
Advox Studio



Jak sprawdzisz, czy nieproszonych gości nie ma w Twoim sklepie internetowym? Firewall, VPN, częste aktualizacje systemów - tak, są to bardzo dobre zabezpieczenia, które powinno się stosować, ale zdarza się, że przez ludzki błąd mogą zawieść.

O KROK ZA ZŁODZIEJAMI

Osoby zajmujące się bezpieczeństwem systemów prawie zawsze są o krok za złodziejami. W tym artykule chcę poruszyć kwestię, która często jest pomijana w kontekście zabezpieczeń wielu systemów e-commerce - monitoringu dedykowanego dla właścicieli sklepów.

MONITORING SKLEPU INTERNETOWEGO - SKAZANY NA CIEBIE

Gdy pojawia się temat monitoringu sklepu internetowego, wielu właścicieli firm otwiera szeroko oczy i mówi, że hostingodawca monitoruje serwery, a to powinno wystarczyć, więc czemu ja się mam tym zajmować?

Prowadzenie biznesu w takim przeświadczeniu może doprowadzić do negatywnych konsekwencji. Tak się składa, że firmy hostingowe nie zajmują się dbaniem o to, by Twój e-commerce był bezpieczny. Ich zadania sprowadzają się do sprawdzania, czy procesory nie są przeciążone, czy na dysku jest wystarczająco dużo miejsca i jak wygląda sytuacja innych tego typu parametrów. Musisz mieć na uwadze, że Twoje środowisko jest całkowicie odizolowane, a każda, nawet najmniejsza luka w zabezpieczeniach, jest wyłącznie Twoim problemem.

MONITOROWAĆ - ALE CO?

Dla każdego właściciela sklepu internetowego najważniejszym parametrem jest to, czy sklep sprzedaje. Składanie nowych zamówień to nie jedyny proces, który powinien być przez nas monitorowany. Znaczenie ma również to, czy sklep dostaje powiadomienia o płatnościach. Należy także pamiętać o tym, by w przypadku posiadania kilku systemów płatności sprawdzać każdy z nich z osobna.

Kwestie drugorzędne związane są z rejestracją użytkowników, dodawaniem produktów do koszyka i każdym innym procesem, o którym jest w stanie pomyśleć właściciel sklepu internetowego.

MONITOROWAĆ - ALE GDZIE?

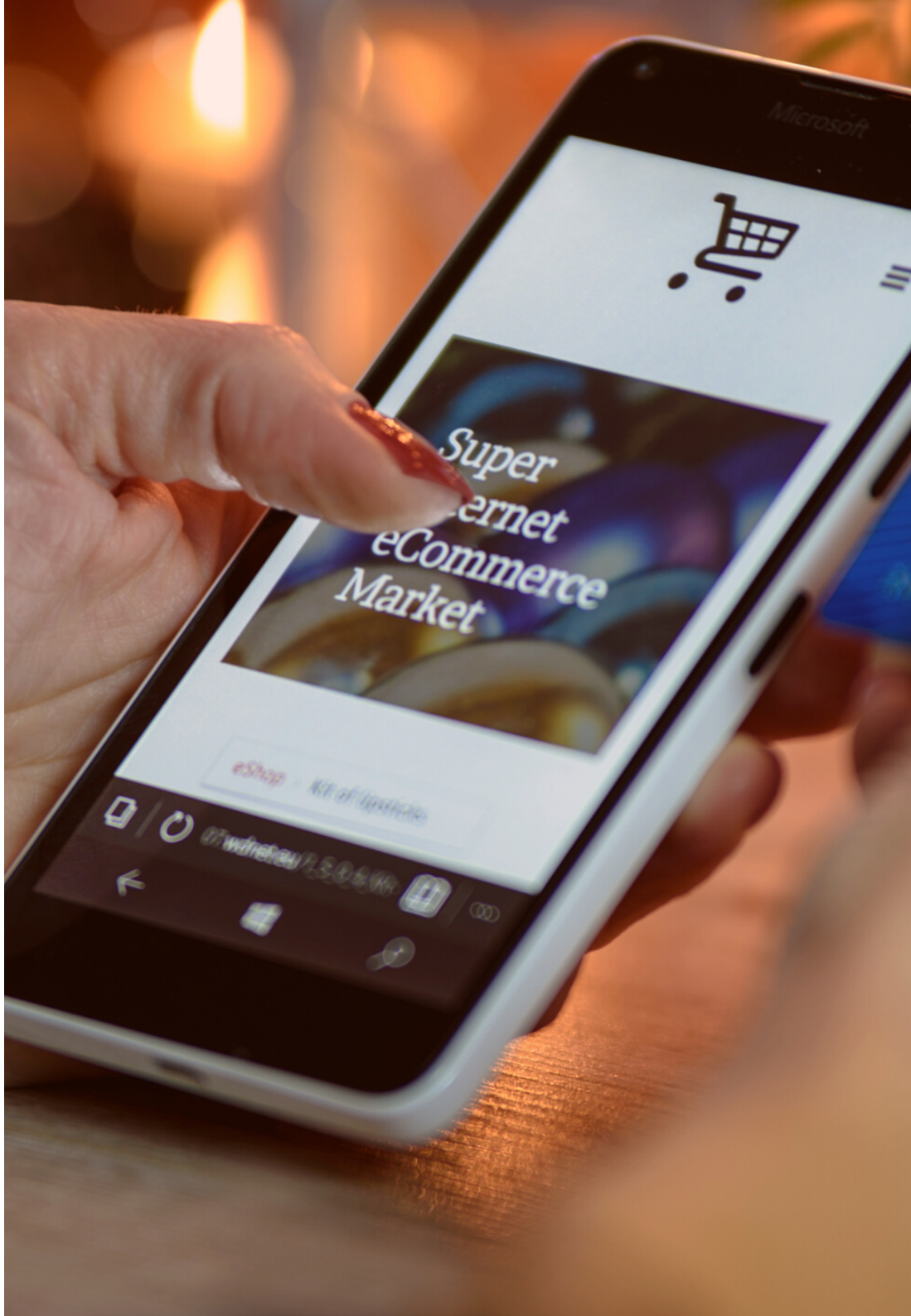
Wiele sklepów prowadzących sprzedaż przez Internet ma wbudowane statystyki. Dlaczego nie powinno się rozszerzać tej przydatnej funkcjonalności o monitoring?

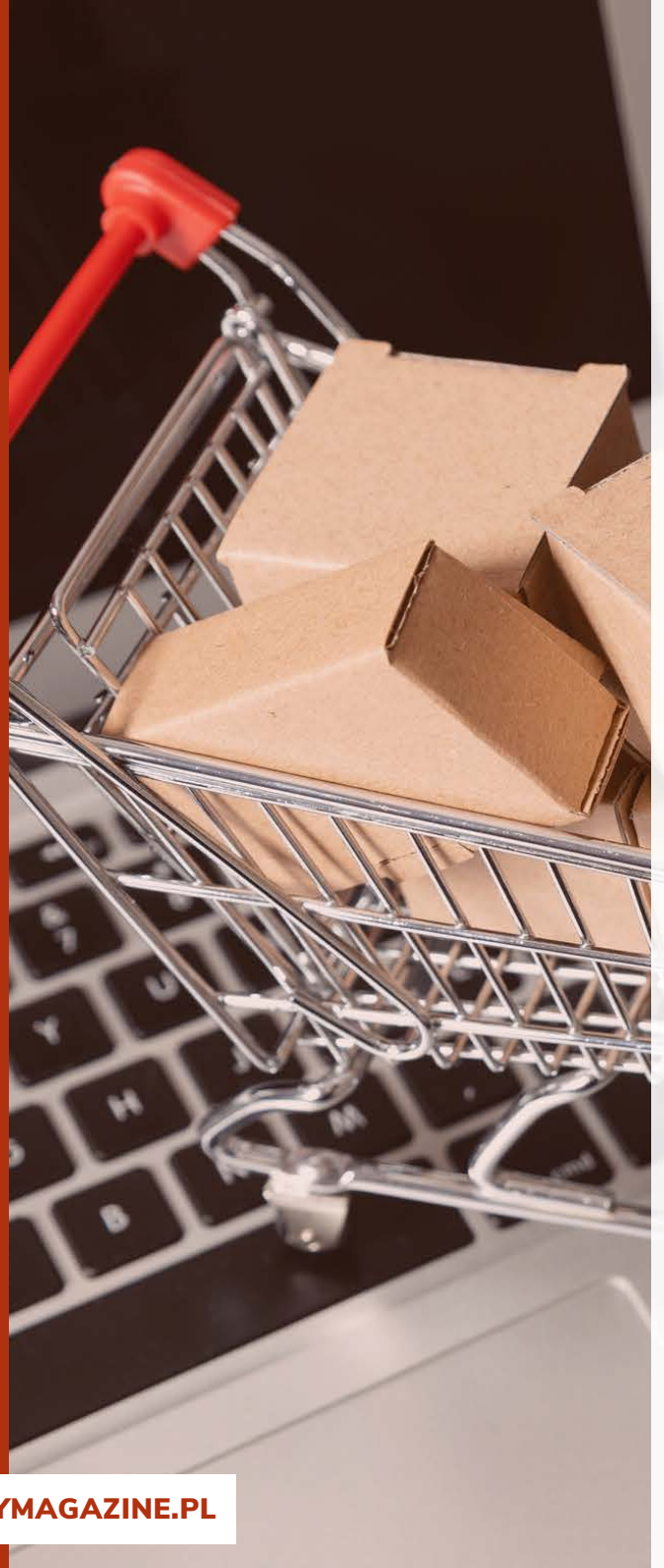
Powodów można wymienić kilka:

- monitoring powinien być niezależny od monitorowanej aplikacji - możemy to porównać do sytuacji, gdy podłączasz monitoring zasilania instalacji elektrycznej i zasilasz go z tej instalacji, bez żadnego zapasowego źródła zasilania. W takich okolicznościach, gdy Twój sklep przestanie działać, po prostu się o tym nie dowiesz,
- podobnie jak zbieranie statystyk, monitoring potrafi być obciążającym procesem - sklepów lepiej jest dodatkowo nie obciążać,
- system monitoringu może obsługiwać wiele sklepów czy systemów - nie tylko jeden. Co więcej, może zajmować się także monitoringiem wydarzeń w sklepach stacjonarnych (IoT)!
- monitoring może być skonfigurowany przez niezależnych dostawców, dzięki czemu nie wpłynie na proces rozwoju sklepu.

MONITOROWAĆ - ALE JAK?

Prawie wszystkie aplikacje, które dotychczas zostały stworzone, przechowują informacje w różnego rodzaju bazach danych - nie ma znaczenia czy w formie pliku, czy wieloserwerowego klastra.





Nam zależy na tym, by monitorować dane, które pojawiają się w bazach danych.

W momencie, gdy w sklepie internetowym pojawia się zamówienie, w bazie danych, w tabeli odpowiedzialnej za przechowywanie danych o zamówieniach, tworzony jest nowy wpis. Analogicznie - gdy przychodzi powiadomienie o dokonaniu płatności, tworzony jest kolejny wpis powiązany z zamówieniem. Właśnie takie informacje możemy monitorować.

Kluczem do skutecznego monitoringu są przede wszystkim powiadomienia o anomaliach.

- Jest wtorek, godzina 12:00, a od godziny nie pojawiło się żadne zamówienie? Wysyłamy powiadomienie na czacie.
- Przez ostatnie dwa dni nie zostało złożone żadne zamówienie z jednego z popularniejszych systemów płatności? Wysyłamy maila do właściciela sklepu.
- W ciągu całego tygodnia nie było żadnej rejestracji klienta? Wysyłamy automatyczne zgłoszenie do firmy, która stworzyła sklep.

Monitorować można właściwie każdy aspekt działania sklepu internetowego. Najlepsze jest to, że system sam może porównywać aktualne dane z danymi historycznymi. Nie będzie błędem stwierdzenie, że wielu właścicieli sklepów nieraz odkryło, że budżet na ich kampanię reklamową magicznie się skończył. Wystarczyłoby, aby monitoring wysłał powiadomienie, że ilość odwiedzin zmniejszyła się o 20% w stosunku do poprzedniego tygodnia.

W sobotę o godzinie 22:00 jeden z pracowników zalogował się do panelu administracyjnego? W tej sytuacji SMS z systemu monitoringu mógłby uratować dane klientów z niejednego systemu.

MONITOROWAĆ - ALE CZYM?

Cały temat sprowadza się do narzędzi, które możemy wykorzystać w monitoringu. Ich lista jest naprawdę długa, a omówienie każdego z nich mogłoby zająć cały artykuł. Z tego powodu przedstawiam dwa narzędzia, które, moim zdaniem, są najpopularniejsze w e-commerce i sprawdzą się idealnie w monitorowaniu praktycznie każdego sklepu internetowego.

ZABBIX

Jest to bardzo elastyczne narzędzie stworzone w PHP. Doświadczony administrator jest w stanie zaprojektować reguły do monitorowania niemalże wszystkich elementów, które uznane zostaną za istotne. Narzędzie umożliwia monitorowanie niezliczonej liczby systemów, co sprawia, że docenia je wiele firm parających się administracją serwerów.

GRAFANA

Zbieranie danych to nie jedyny istotny proces. Chcąc mieć jak najlepszy pogląd na aktualną sytuację swojego sklepu, należy zaprezentować dane w sposób czytelny i ułatwiając ich analizę. Właśnie takim narzędziem jest Grafana. Dzięki niej można przedstawić zbiór dowolnych informacji w przystępny do analizy sposób. Idealne narzędzie do wyświetlania danych na ekranie umieszczonym w biurze - wszystkie istotne parametry sklepu dostępne są dzięki jednemu krótkiemu spojrzeniu.

BEZPIECZEŃSTWO E-COMMERCE PODSUMOWANIE

Dbałość o bezpieczeństwo sklepu to temat wielowymiarowy i nie opiera się wyłącznie na bezpiecznej infrastrukturze, częstych aktualizacjach oprogramowania, tworzeniu kopii zapasowych, korzystania z programów antywirusowych czy szkoleniach pracowników z zakresu bezpieczeństwa. To także monitoring - możliwość upewnienia się w dowolnej chwili, że nasz sklep jest gotowy na przyjmowanie zamówień oraz zminimalizowanie czasu reakcji na nieprawidłowości.

ARCHIWIZACJA DANYCH W FIRMIE A BACKUP. CO MUSISZ WIEDZIEĆ?

Redakcja
SECURITY MAGAZINE

Jednym z najważniejszych aspektów działalności firmy jest archiwizowanie i odpowiednie przechowywanie danych, które każdego dnia przetwarzane są dziesiątki, setki razy. Pliki, dokumenty, faktury, przeróżne dane - o wszystkie trzeba właściwie zadbać, zabezpieczyć przed osobami postronnymi, a także pamiętać o kopiach zapasowych.

CZYM JEST ARCHIWIZACJA DANYCH?

Najprościej mówiąc, jest jednym ze sposobów ochrony ważnych plików przed nieupoważnionym dostępem. Każdy przedsiębiorca i jego pracownicy powinni wiedzieć, w jaki sposób dane archiwizować, pamiętając przy tym, że archiwizacja danych na komputerze to nie to samo, co tworzenie kopii bezpieczeństwa. Archiwizacja sama w sobie to kopiowanie danych, w tym plików, dokumentów, faktur, danych zapisanych na partycji lub na dysku twardym użytkowników komputerów, na osobny nośnik i usuwanie ich z pierwotnej lokalizacji. Natomiast kopia zapasowa danych choć też wiąże się z kopiowaniem plików na inny nośnik, to dane nadal znajdują się w głównej lokalizacji, nie są usuwane. Bazy danych mogą być różnej wielkości i od tego zależy też zakres archiwizacji i jaki wyko-rzystamy jej rodzaj.

Pliki kopiowane są do wskazanego archiwum w taki sposób, że czyszczeniu podlegają atrybuty archiwizacji i przy każdej zmianie danego pliku zmieni się też jego archiwizowana kopia.

W przypadku, gdy archiwizację danych tworzymy pierwszy raz, mamy do czynienia właśnie z jej wersją standardową. Możemy pokusić się tutaj o utworzenie kopii pełnej, która obejmowałaby wszystkie zgromadzone przez nas dane.

Trzeba jednak brać pod uwagę, że proces ten zabierze nam sporo czasu. Jest jednak najlepszą formą zabezpieczenia danych i w pewnym stopniu fundamentem do następnych archiwizacji.

ARCHIWIZACJA PRZYROSTOWA

Obejmuje ona tylko te pliki, które powstały lub zmienione zostały po już wcześniej dokonanej archiwizacji danych. Od kopii standardowej jest zdecydowanie mniej czasochłonna i zajmuje zdecydowanie mniej miejsca w archiwum. Ponadto możemy ją wykonywać często. Natomiast trzeba brać pod uwagę, że ma dłuższy czas odtwarzania zarchiwizowanych danych.
Po już wykonanej kopii standardowej ten rodzaj archiwizacji przynosi najkorzystniejsze efekty i z ekonomicznego punktu widzenia jest najlep-

szym rozwiązaniem.

ARCHIWIZACJA RÓŻNICOWA

W przypadku tego rodzaju archiwizacji kopiujemy pliki zmodyfikowane od momentu wykonywania pierwszej pełnej kopii danych. W tym przypadku nie zmieniane są atrybuty archiwizacyjne plików.

Należy pamiętać o tym, że kopie różnicowe zajmują więcej miejsca na dysku niż kopie przyrostowe. Jednak można sobie z tym poradzić, zachowując jedynie najnowszą wersję kopii.

ARCHIWIZACJA DANYCH A BACK-UP

Bardzo często zdarza się, że oba terminy używane są na zmianę. Jest to jednak duży błąd, bo to dwie różne metody pracy na danych. Jak wspominaliśmy, archiwizacja to czynność, która polega na przeniesieniu danych w inne miejsce pamięci masowej.

Backup to tworzenie kopii bezpieczeństwa zawierającej najważniejsze pliki. Warto pamiętać, że backup zabezpiecza pliki przed złośliwymi zmianami, a przede wszystkim chro-

ni przed błędami np. człowieka przez usunięcie lub przypadkową utratę danych. Ryzyko utraty danych może nastąpić choćby przez awarię sprzętu w naszej firmie czy ataki na komputery lub sieć.

TRZY REGUŁY BACKUPU

Istnieją trzy zasady, których trzymając się przy wykonywaniu backupu, będziemy pewni, że właściwie zabezpieczyliśmy ważne dane firmowe.

Po pierwsze. Dane powinniśmy przechowywać w trzech kopiach, to znaczy mając jeden oryginał i dwie kopie zapasowe, ale na różnych nośnikach.
Dlaczego to takie ważne? Bo prawdopodobieństwo awarii trzech nośników jest mniejsze niż prawdopodobieństwo awarii dwóch nośników w tym samym czasie. Trzecia kopia daje czas i spokój, że bez problemu możemy zrobić dodatkowe kopie.

Po drugie. Kopie przechowujemy na dwóch różnych nośnikach. Wyobraź sobie, że masz dwie kopie i obie trzymasz na jednym dysku twardym. Gdy dojdzie do jego awarii, dane mogą być już nie do odzyskania. Mówiąc o różnych nośnikach, mamy na myśli np. przechowywanie jednej kopii na pendrive, a drugiej na dysku twardym. Inne opcje to, np. płyta DVD, chmura czy dysk lokalny.

Po trzecie. Kopie przechowujemy w innych lokalizacjach, np. dane firmowe - również poza biurem. A to na wypadek kradzieży nośników bądź komputera, czy pożaru, zalania lub podtopień.

Jeśli któryś z naszych firmowych dokumentów, plików wymaga archiwizacji, to prawdopodobnie ma dla nas duże znaczenie. Dlatego tak istotne jest, by był przechowywany właściwie. Takie działanie usprawnia funkcjonowanie firmy, nie naraża na ogromne straty i pomaga uniknąć wielu kłopotów.

JAK SIĘ „CYBER-ZABEZPIECZYĆ”?

Artur Bicki
EMCA Software Sp. z o.o.

**Aktualna sytuacja polityczna spowodowała w każdym z nas i w każdej organizacji konieczność odpowiedzi na pytanie:
czy jesteśmy bezpieczni?
Cyberprzestrzeń budzi szczególne emocje z uwagi na nasze ogromne uzależnienie od technologii informatycznych podczas dnia codziennego.**

CZUJNOŚĆ. DLACZEGO JEJ BRAKUJE?

Gwałtowny rozkwit komputerowych technologii spowodował, że z dziecinnym zauroczeniem korzystamy z nowinek tej branży, odsuwając na później troskę o bezpieczeństwo. To ten powszechnie nazywany **„boom” technologiczny** uśpił naszą czujność, której przecież nie brakuje nam w codziennym podejmowaniu decyzji przy kontaktach z nowymi osobami, ruchu ulicznym itp.

Szukając odpowiedzi na pytanie : **jak się „cyber-zabezpieczać”**, należy szukać analogii właśnie z życia codziennego. Te zasady dobrze znamy. Parkując samochód w centrum miasta, nie zostawiamy na desce rozdzielczej cennych przedmiotów. Słysząc dzwonek do drzwi, nie otwieramy ich na oścież wprowadzając nieznajomego do środka.

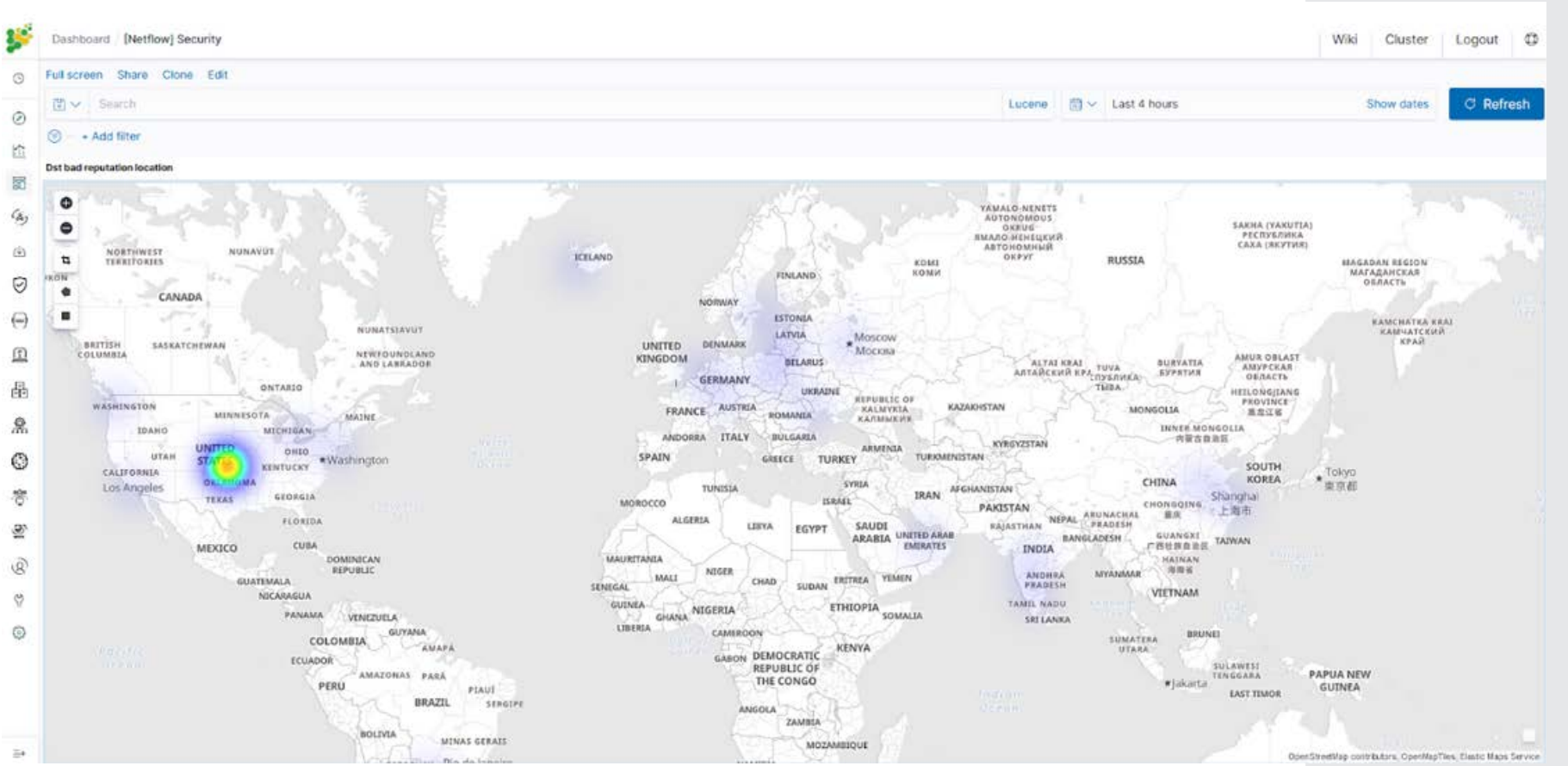
Rozmawiając o sekretach, nie podnosimy głosu. Gdy widzimy osobę o wyglądzie który jest dla nas podejrzany, zmienimy stronę ulicy po której spacerujemy. Uczymy nasze dzieci: „Nie rozmawiaj z nieznajomym”.

Z niejasnych powodów, te zdrowe odruchy w świecie IT są dopiero dziś wprowadzane w życie. Od pierwszych dni internet stosuje zasadę otwartej komunikacji i dopiero od pewnego czasu nieśmiało rozmawiamy o nowych zasadach i ograniczeniach w komunikacji. Tylko dlaczego nasze podejście w IT ma być inne niż w życiu codziennym?

Słysząc pukanie do drzwi, naturalnie pytamy „Kto tam?”. Uzyskując odpowiedź w niezrozumiałym języku, na pewno drzwi się nie otworzą. Nie wiadomo dlaczego ruch ze wszystkich krajów świata swobodnie dociera do naszych serwerów.
Zespoły administratorów poczty codziennie toczą walkę z niechcianą korespondencją, gdzie 80% nadawców pochodzi z krajów, o których nigdy nie słyszeliśmy.

Tłumacząc zasady bezpieczeństwa codziennego na politykę dobrych praktyk cyber świata, należy schować to, co cenne. Systemy informatyczne powinny działać w takich strefach, które bezwzględnie potrzebują mieć do nich dostęp. Poza tymi strefami usługi nie powinny być dostępne. W praktyce może to również oznaczać zamknięcie komunikacji dla terytoriów o podwyższynym ryzyku ataku, gdzie jednocześnie nie utrzymujemy relacji biznesowej.

Spójrzmy na prawdziwą mapę ataków informatycznych,
uzyskanych od działu bezpieczeństwa EMCA S.A.



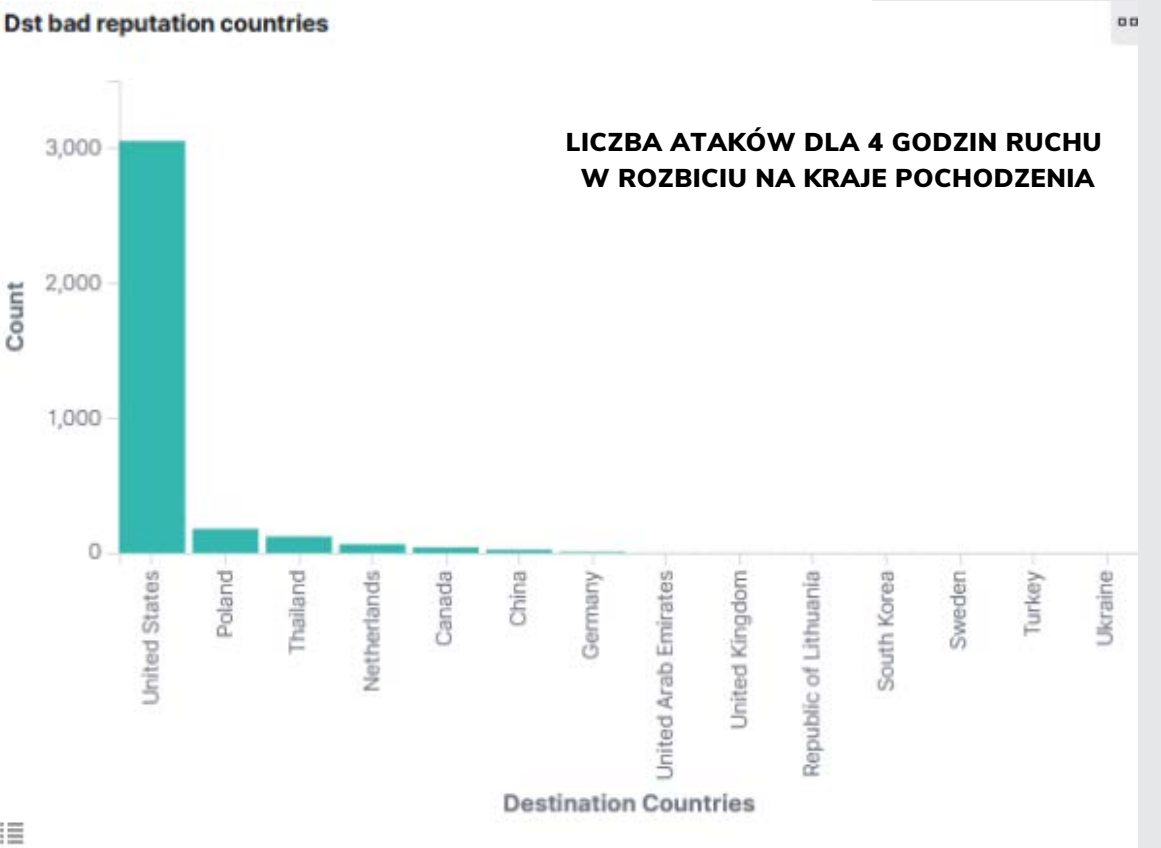
Kolory pochodzą z analizy 4 godzin ruchu sieciowego pod kątem bezpieczeństwa. Mówiąc wprost, czy działalność polskiej spółki ucierpi, gdy zablokuje komunikację ze Zjednoczonymi Emiratami lub prowincją Bengaluru w Indiach?

Przeprowadźmy audyt usług, który powinien jasno wykazać, które z nich posiadają charakter wewnętrzny i nie ma potrzeby ich ekspozycji dla gości z zewnątrz. Usługi publiczne, również ograniczajmy terytorialnie blokując odpowiednie klasy adresowe.

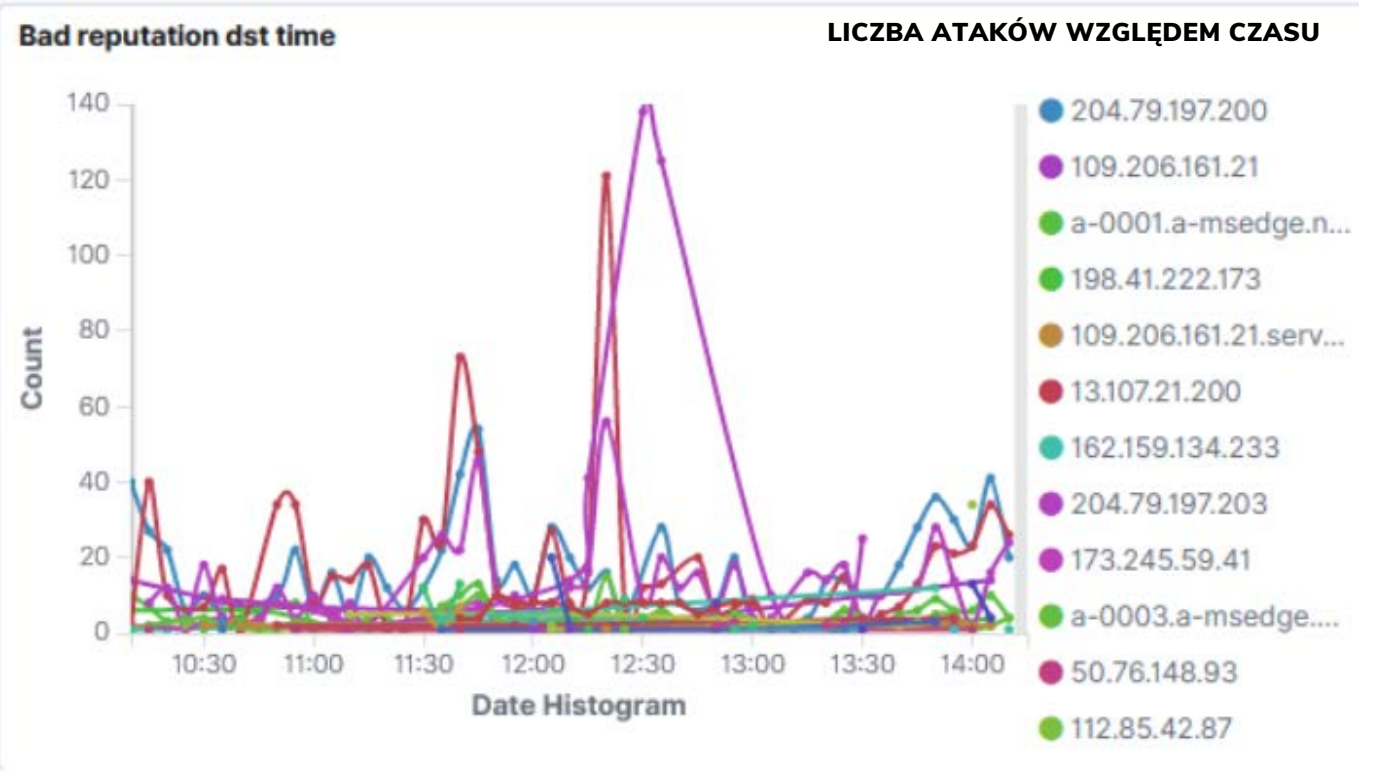
Kolejne zagadnienie, to czy nasze zamki do drzwi działają jak należy? W domu szybko zaplanujemy wymianę zepsutego, zaniedbanego zamka.
W systemach informatycznych również dbajmy o korzystanie z najnowszych wersji oprogramowania. Każdy produkt posiada błędy. Poprawki bezpieczeństwa są jednak szybko dostępne, a aktualizacje często darmowe. Uruchommy proces kontroli i aktualizacji wersji użytkowanego oprogramowania.

Wchodząc do własnego domu zauważymy na pewno fakt, że złodziej próbował sforsować nasze drzwi. Ślady włamania do infrastruktury informatycznej również muszą być szybko zabezpieczane i analizowane. Zdarzenia pochodzące z krytycznych punktów przetwarzania, urządzeń sieciowych i aplikacji muszą być w pierwszym kroku gromadzone w bezpiecznym miejscu oraz cyklicznie poddawane analizie. Odbywa się to w dedykowanych systemach typu SIEM, jakim jest nasz Energy Logserver.

To, co niewątpliwie odróżnia problemy dnia codziennego od działań w cyberprzestrzeni to skala problemu. Ataków IT odbieramy tysiące dziennie. Można wprost powiedzieć, że procent ruchu informatycznego związanego z nadużyciami informatycznymi to około 70% całości. Spójrzmy jeszcze raz na wynik analizy 4 godzin ruchu sieciowego wykonanego przez biuro bezpieczeństwa EMCA SA.



LICZBA ATAKÓW DLA 4 GODZIN RUCHU W ROZBICIU NA KRAJE POCHODZENIA



Już małych organizacji ataki liczone są w tysiącach, dla dużych przedsiębiorstw to zdecydowanie większe liczby i w konsekwencji ogrom pracy do wykonania w zakresie analizy problemów. Nie jest tajemnicą, że wiele technik ataku oraz stosowanych mechanizmów obronnych powtarza się. Jest to doskonałe miejsce na automatyzację obsługi incydentów, która realizowana jest przez systemy klasy Energy SOAR. To w takich narzędziach należy zaszywać automatyczna logikę obsługi, która pozwoli na szybką klasyfikację problemów i określenie jego priorytetu.

Rozszerzając swoją świadomość w obszarze bezpieczeństwa, dojdziemy szybko do wniosku, że nasza wiedza jest niewystarczająca. Walczymy ze zorganizowanymi grupami przestępczymi, dlatego też w obronie nie działajmy w pojedynkę. Konieczne jest stałe i konsekwentne poszerzanie wiedzy z nowych technik ataków. Szkolenie pod-

noszące świadomość problemów powinno obejmować wszystkich pracowników. Dodatkowo szkolenia powinny objąć pracowników biur bezpieczeństwa, aby ułatwić im realizację obrony systemów informatycznych. Połączenie sił posiada jeszcze jeden wymiar. Funkcjonują w Polsce **globalne Centra Bezpieczeństwa (CERT - Computer Emergency Response Team)** które stanowią centra wiedzy o aktualnych atakach. Cert to jednostki funkcjonujące zazwyczaj z ramienia globalnych firm telekomunikacyjnych, odpowiedzialnych za dostarczaną infrastrukturę sieciową. Na stronach CERT warto śledzić najnowsze doniesienia o zagrożeniach obszaru **cybersecurity**. Do jednostek CERT należy zgłaszać zauważone incydenty pochodzące z utrzymywanej infrastruktury. Duże organizację posiadają wypracowane automaty (w systemach SOAR), które incydenty o odpowiednich cechach raportują do jednostki CERT.

Czy po wdrożeniu tych i innych zabezpieczeń możemy czuć się bezpieczni? Nie. Znacząco jednak obniżamy ryzyko awarii systemu w wyniku ataku, czy też kradzieży informacji. Wojna w sieci trwa od dawna i codziennie stawia nam nowe wyzwania.


ZDARZYŁ SIĘ W TWOJEJ FIRMIE
WYCIEK DANYCH OSOBOWYCH?
MOŻEMY CI POMÓC
SPRAWDŹ JAK

SECURITYMAGAZINE.PL

6 RAD, JAK EFEKTYWNIE BUDOWAĆ BEZPIECZEŃ-STWO ORGANIZACJI

Marcin Święty
Relativity

Każda organizacja buduje i rozwija swoje bezpieczeństwo w oparciu o swoich pracowników - świadomie lub nie. Jedne korzystają z branżowych schematów i procesów, inne liczą na kontekstową pomoc konsultantów, a jeszcze inne odsuwają ten temat na lepsze czasy. Niezależnie od profilu firmy, są rzeczy, które będą uniwersalne - i pomogą budować efektywnie bezpieczeństwo organizacji.

1 POSTAW NA LUDZI

Ile razy słyszeliśmy, że człowiek jest najsłabszym ogniwem? Ba, ile razy sami powtórzyliśmy te słowa chcąc sprzedać usługi bezpieczeństwa, uzyskać dodatkowy budżet, wdrożyć nowe rozwiązanie, czy po prostu postraszyć incydentami? Powtarzamy te słowa od lat, często już bezwiednie. Czasy natomiast się zmieniły.

Dzisiaj to pracownicy budują nasze bezpieczeństwo i to od ich skuteczności zależy to czy nasza organizacja będzie bezpieczna. To pracownicy budują świadomość, oni implementują i zarządzają naszymi systemami, i to pracownicy podejmują kluczowe decyzje dotyczące rozwoju bezpieczeństwa.

Stawiając na ludzi - zarówno na role bezpośrednio związane z bezpieczeństwem, jak i resztę populacji pracowników - mamy możliwość przekuć utarte najsłabsze ogniwo w aktywną tarczę, która im lepiej wyszkolona i uzbrojona w narzędzia, da nam najlepszy zwrot z inwestycji w zakresie budowy i rozwoju bezpieczeństwa.

ZABAWKI SĄ FAJNE, ALE TE TEŻ TRZEBA OBSŁUŻYĆ 2

Podążając za raportem DBIR Verizona, blisko 85% incydentów jest teraz związana z ludźmi. Skala ataków socjotechnicznych, najczęściej przeprowadzanych w formie phishingu, jest tak duża (1 na 4200 maili), że w dużych organizacjach zaczynamy mieć ogromne prawdopodobieństwo, że któryś z pracowników się kiedyś złapie.

Brzmi to jak potwierdzenie tezy pracownika będącego najsłabszym ogniwem, ale jest to też argument do pytania - czemu jednak duże korporacje opierają się tym atakom?

Oczywiście, pierwsza myśl jaka się pojawia to narzędzia. Mamy systemy na poziomie sieci, infrastruktury, na poziomie naszych urządzeń końcowych. Te rzeczywiście są dzisiaj bardzo zaawansowane, szczególnie jeśli mówimy o uczeniu maszynowym i marketingowej sztucznej inteligencji. Każde z tych narzędzi trzeba jednak wybrać, wdrożyć, skonfigurować, obsługiwać i utrzymać.

To nawiązuje mocno do punktu poprzedniego - potrzebujemy kompetencji, które katalizują możliwości dane nam przez narzędzia i także zapewnią, że wartość wnoszona przez nasze systemy będzie taka sama lub nawet większa im dłużej nimi operujemy.

Powinniśmy wybierać najlepsze dostępne na rynku systemy, ale też takie, które będziemy mogli efektywnie wykorzystać w naszej organizacji.

ODPOWIEDNIA STRATEGIA 3

To dopasowanie powinno być wielopoziomowe. To jak dobieramy narzędzia, musi być spójne z tym jak dobieramy kompetencje i z tym jak zarządzamy kapitałem ludzkim. Na tym jednak nie koniec. Nasz program bezpieczeństwa musi być przede wszystkim dopasowany do naszego biznesu i strategii. Nawet największe chęci i najmocniej wsparte finansowo inwestycje w bezpieczeństwo zawiodą, jeśli biznes nie będzie na te zmiany gotowy, a działania nie będą układały się w spójną strategiczną całość. I nie chodzi tutaj o techniczne i wewnętrzne roadmapy, które wszyscy tak lubimy. Chodzi o wyznaczenie misji i wizji dla programu bezpieczeństwa, o wyrażenie intencji i planu w formie, która będzie zrozumiała zarówno dla szeregowych pracowników, jak i osób decyzyjnych w naszej organizacji. Wizja powinna energetyzować, a misja wskazywać to jak powinniśmy działać by tę wizję osiągnąć. Nasza strategia będzie tym, czym będziemy przekonywać zarząd do kolejnych inwestycji, tym czym będziemy wyznaczać ramy priorytetów i tym przez co będziemy określać efektywność naszych działań.

Raport IBM Data Breach wskazuje, że znacząca większość zarządów organizacji (88%) zaczęła uznawać bezpieczeństwo komputerowe jako ryzyko biznesowe. Skala zmagań z incydentami i atakami stawia coraz to nowsze wymagania dla budujących program bezpieczeństwa, ale też buduje mocniejszą świadomość osób decyzyjnych. Aby odpowiednio z tej świadomości skorzystać musimy mieć mechanizm, który przedstawi co tak dokładnie za budżet organizacja dostanie. Strategia jest w tym przypadku lepszym produktem wewnętrznego marketingu dla inwestycji w bezpieczeństwo niż potrzeba zakupu kolejnego narzędzia czy zapotrzebowanie na zwiększone zatrudnienie.

Budowa strategii wraz z jasną misją i wizją będzie wyznaczać kierunek dla wszelkich działań i wymusi też priorytetyzację.

4 MIERZ SIŁY NA ZAMIARY

W początkowych fazach rozwoju programu bezpieczeństwa chcielibyśmy pokryć wszystko i wziąć pod uwagę każdą domenę zarządzania nim. Niejednokrotnie kończy się to klęską zbyt wielu równoległych projektów, które będąc rozsynchronizowane lub zbyt mnogie nie dostarczają oczekiwanej wartości na poprawie bezpieczeństwa organizacji.

Z drugiej strony mamy przed sobą też projekty czy wdrożenia, które po rozpisaniu mogą ciągnąć się nawet latami. Obawa, że efekt końcowy rozminie się z potrzebami z uwagi na zmiany w świecie technologii czy naszego biznesu okazuje się być boleśnie rzeczywista.

Odpowiednio przygotowana strategia powinna łączyć długoplanowy zysk/wartość z bardziej taktycznymi i łatwiej zarządzalnymi projektami. Różne raporty wskazują, że zaledwie około 10% organizacji realizuje przynamniej dwie trzecie swojej strategii, a ponad 50% organizacji nie osiąga nawet połowy zamierzonych celi.

Implementacja i odpowiednie zabezpieczenie zasobów do wdrożenia jest równie istotne co dobrze sformułowana strategia, a co za tym idzie - powinniśmy mierzyć siły na zamiary. Coś, co wydaje się być tylko prostym procesem PoC (Proof of Concept), potem etapem testów i wdrożenia, może rozciągnąć się na żmudną implementację przypadków brzegowych, integracji z naszym środowiskiem, czy chociażby adopcją wśród pracowników. Każda godzina spędzona przez eksperta na kompensowaniu błędnych planów czy założeń, mogłaby być spożytkowana w kolejnym projekcie lub wdrożeniu.

5 INWESTUJ W AUTOMATYZACJĘ

Innym obszarem, gdzie organizacje tracą cenny czas eksperta jest praca manualna.

Eksperci, których potrzebujemy by skutecznie przeprowadzić wdrożenie i stabilizację nowego rozwiązania, często zostają już z narzędziami by je utrzymać i obsługiwać. Taki model nie tylko marnuje czas wysoce wyspecjalizowanego pracownika, ale nie pozwala się też odpowiednio skalować, pomijając też kwestie wypalenia czy zmniejszonej innowacyjności pracowników na stałe przypisanych do manualnych procesów.

Imperatywem powinno być wczesne i szybkie automatyzowanie. Raporty Gartnera mówią nawet o hiperautomatyzacji - tj. automatyzowaniu wszystkiego co jest możliwe. Oczywiście, są zadania, które zawsze będą wymagały ludzkiego czynnika. Powinniśmy te zadania bardzo skrupulatnie zidentyfikować, tak by skoncentrować na nich uwagę naszych zespołów, a resztę zautomatyzować.

Dobrym przykładem jest adopcja systemów klasy **SOAR** (Security Orchestration, Automation, and Response). Już sama obsługa np. podejrzeń incydentów, ma ogromną przestrzeń do automatyzacji - przez lepsze wzbogacenie danych, pozyskanie dodatkowych informacji z systemów dających nam Threat Intelligence, czy podjęcie reakcji w wielu wewnętrznych systemach, by ograniczyć wpływ ataku.

To, co kiedyś wymagało kilku inżynierów i analityków, może sprowadzić się do bardzo efektywnego runbooka, który będzie wymagał interakcji z ekspertem w momentach decyzji, czy chociażby potwierdzenia proponowanej reakcji.

Co ważniejsze, taki schemat jest mniej podatny na błąd ludzki - bo interakcja z pracownikiem jest ograniczona do meritum wymaganej wiedzy eksperckiej.

PO PROSTU SŁUCHAJ

6

Wielu liderów nie docenia woli i możliwości pracowników do rozwiązywania dużych problemów korporacyjnych. Częstym modelem jest budowa strategii odgórnie i narzucenie roadmapy na zespół, chcąc jak najszybciej osiągnąć cele, które komunikowane są nam ze strony zarządu. Niemniej jednak, stawiając na ludzi, budując spójną kulturę bezpieczeństwa firmy, która wraz ze strategią, misją i wizją będzie delegować bezpieczeństwo firmy do naszych pracowników, mamy szanse na uzyskanie lepszych, efektywniejszych inicjatyw oddolnie.

Budowa bezpieczeństwa na wiedzy eksperckiej pracowników bezpośrednio odpowiedzialnych za bezpieczeństwo, ale też naszych Guardianów, Championów, czy Ambasadorów pozwoli szybciej automatyzować, lepiej mierzyć siły na zamiary, budować strategię dopasowaną

do biznesu i kultury, a końcowo uzyskać największy zwrot z inwestycji naszego najcenniejszego zasobu - zasobu ludzkiego.

SZUKASZ

EKSPERTA W ZAKRESIE PEŁNIENIA FUNKCJI

INSPEKTORA OCHRONY DANYCH

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

SPRAWDŹ NASZĄ OFERTĘ

BEZPIECZEŃSTWO W SOCIAL MEDIA. JAK BRONIĆ SIĘ PRZED DEZINFORMACJĄ I CHRONIĆ SWOJE DANE?

Bartosz Baziński
SentiOne

Od początku inwazji Rosji na Ukrainę obserwujemy w sieci niepokojące wzmożenie działań dezinformacyjnych. Sytuacja jest napięta, rząd, firmy i zwykli obywatele pomagają poszkodowanym jak tylko mogą. Wysyp fałszywych informacji ma na celu zakłócenie i destabilizację tego typu działań.

NA CO UWAŻAĆ?

Ostatnie kilkanaście lat pokazało wyraźnie, jak media społecznościowe mogą zostać wykorzystane przeciwko nam. Firma Cambridge Analytica pomagała w manipulacji wyborcami w Stanach Zjednoczonych, kampanie rozpowszechniające fałszywe informacje wpłynęły na wyniki referendum w sprawie Brexitu, a algorytmy Facebooka zostały wykorzystane do nasilenia napięć społecznych w Birmie, co bezpośrednio przyczyniło się do ludobójstwa. Nikogo zatem nie powinno dziwić, że wojna, jaką wypowiedziała Ukrainie Rosja, prowadzona jest także na tym froncie. W SentiOne monitorujemy Internet już od 10 lat i doskonale wiemy, jakie treści padają na podatny grunt.

W przypadku informacji na temat wojny w Ukrainie warto zwrócić szczególną uwagę na następujące aspekty:

CLICKBAJTOWY TYTUŁ

niektóre portale chcą zarobić na wojnie i zwiększyć ruch na swojej stronie, więc będą przyciągać uwagę chwytliwymi tytułami na pograniczu kłamstwa,

INFORMACJE WZBUDZAJĄCE SKRAJNE EMOCJE

szok, strach, gniew, ale też śmiech i radość, mają wysoki potencjał viralowy. Dlatego news o zablokowaniu dostępu do serwisu Pornhub w Rosji, który ostatecznie okazał się być fałszywy, tak szybko się rozprzestrzenił. A w przypadku wojny spreparowanie treści szokujących i strasznych nie jest problemem,

FILMY, ROLKI I RELACJE

również mają duży potencjał viralowy, nie tylko dlatego, że algorytmy tych platform są nastawione na promowanie treści video. Również my jako ludzie dużo intensywniej odbieramy treści video, niż sam tekst,

ZDJĘCIA Z INNYCH MIEJSC LUB CZASÓW

łatwo jest dokonywać manipulacji z pomocą archiwalnych materiałów, np. zdjęć z wojny w Jemenie prezentowanych jako zdjęcia z Kijowa. Media społecznościowe pozwalają szybko podawać informacje, ale niestety często brakuje czasu na weryfikację danych,

DEEPFAKE

sfabrykowany materiał video - bardzo łatwo teraz spreparować lub zmontować film tak, by ukazywał dowolne treści czy osoby w nieprawdziwych sytuacjach.

JAK DZIAŁA ROZPOWSZECHNIANIE FAŁSZYWYCH INFORMACJI W PRAKTYCE?

Dezinformacja może przybrać wiele form. Czasami są to zwyczajne plotki, które powielamy bez sprawdzania ich wiarygodności. Nic w tym dziwnego - łatwiej jest kliknąć „udostępnij" niż szukać wiarygodnych źródeł. Tak właśnie było w przypadku newsa o Pornhubie. Na Twitterze pojawiła się plotka, że w ramach protestu przeciwko działaniom wojennym serwis zablokował dostęp użytkownikom z Rosji. Plotka, oczywiście, została zdementowana natychmiast, ale nie przeszkodziło to serwisowi odnotować 500% wzrostu liczby wzmianek na jego temat.

Powstała specjalnie do walki z fałszywymi informacjami organizacja EUvsDisinfo szczegółowo przeanalizowała strategie i taktyki kampanii dezinformacyjnych Kremla. Odnajdywanie i wykorzystywanie różnic w społeczeństwach pluralistycznych, staranne opracowywanie komunikatów dezinformacyjnych pod kątem docelowych odbiorców, budowanie fałszywych stwierdzeń wokół jądra prawdy, wzmacnianie narracji z wykorzystaniem niczego niepodejrzewających ludzi – to podstawowe cechy kampanii dezinformacyjnych Kremla. I są bardzo skuteczne.

JAK BRONIĆ SIĘ PRZED DEZINFORMACJĄ?

Przede wszystkim nie należy bezmyślnie powielać niezweryfikowanych informacji. Sensacyjne treści i tytuły w social media są zaprojektowane tak, by grać na emocjach - a jeśli damy się im ponieść, dużo trudniej będzie trzeźwo ocenić sytuację, zweryfikować dane czy poszukać innych źródeł informacji. Warto także przyglądać się profilom zamieszczającym tego typu treści. Czy to prawdziwe osoby? A może fałszywe profile, które powstały tydzień temu? Jeśli podejrzewamy, że dana osoba nie jest tym, za kogo się podaje, warto to zgłosić. Operatorzy danej platformy mają dużo większe możliwości weryfikacji.

Ostatnio pojawiło się też wiele inicjatyw, mających na celu wykrywanie i nagłaśnianie przypadków dezinformacji. Jedną z nich jest zor-

ganizowana przez NASK akcja **#WłączWeryfikację**. Z kolei Fundacja Panoptykon przygotowała szczegółowy poradnik „Stop dezinformacji".

Skąd zatem czerpać informacje? Przede wszystkim ze sprawdzonych redakcji i agencji prasowych, jak np. Agencja Reuters czy Associated Press, które mają odpowiednie doświadczenie, zasoby i zespół odpowiedzialny za weryfikację wiadomości.

Skąd nie czerpać? Z przepełnionych emocjami i niezweryfikowanych kont w social media. Jeśli jakiś news pojawi się na Telegramie, to Reuters i Associated Press z pewnością go zweryfikują i, jeśli okaże się prawdą, podadzą dalej.

JAK DBAĆ O BEZPIECZEŃSTWO SWOICH DANYCH?

Nawet niosąc pomoc trzeba zachować czujność. Od początku wojny w Internecie pojawiło się wiele stron, które zbierają informacje o osobach mogących udzielić schronienia uchodźcom i proszą o podanie ich danych oraz numeru telefonu. Kolejne grupy na Faceboku ochoczo podają linki do **arkuszy Google**, w których zbierane są informacje o możliwościach lokalowych, adresach i numerach telefonów - tych samych, z których korzysta się do weryfikacji konta w banku. Powstaje więc dokładna baza danych na temat osób niosących pomoc i samych uchodźców dostępna dosłownie dla każdego. Być może te informacje posłużą do organizacji pomocy dla rodzin ukraińskich, ale mogą też zostać sprzedane albo wykorzystane w inny sposób.

Oprócz tego wiele osób bez żadnych podejrzeń otwiera linki do zbiórek na rzecz Ukrainy, które znajduje w Internecie lub otrzymuje od nieznanych nadawców. Bardzo łatwo w ten sposób pobrać zainfekowane oprogramowanie na swój komputer lub telefon.

PODZIWIAMY DZIAŁALNOŚĆ HAKTYWISTÓW ANONYMOUS I ŚMIEJEMY SIĘ, GDY WYKRADAJĄ DANE Z ROSYJSKICH MINISTERSTW, ALE NIE ROBIMY NIC, BY ZABEZPIECZYĆ WŁASNE DANE.

POPULARNOŚĆ HASZTAGU #FAKENEWS

Z naszych wyliczeń wynika, że od 2 tygodni treści które zawierają #fakenews lub #dezinformacja zyskują nawet o 1000% więcej zasięgów teraz niż miesiąc temu.
Wniosek? Wiele marek, twórców internetowych, dziennikarzy i mediów próbuje się podpiąć pod te hashtagi, ponieważ przynoszą one ruch na stronę, klikalność i zasięgi.

Czasem udostępniane treści są w dobrej wierze (np. realna demistyfikacja rosyjskich trolli), a czasem wychodzi niestety na odwrót, bo np. powoduje wśród ludzi strach i nieracjonalne zachowania (np. kupowanie papieru toaletowego lub masowe napełnianie kanistrów benzyną).

DLACZEGO TREŚCI #FAKENEWS I #DEZINFORMACJA TAK DOBRZE SIĘ TERAZ KLIKAJĄ?

Z tych samych powodów opisanych wyżej:

- wywołują emocje (strach, gniew),
- zazwyczaj przedstawiane są w formie video relacji (TikTok święci triumfy teraz), a więc treści które ostatnio najłatwiej się konsumują oraz algorytmy social media im najbardziej sprzyjają,
- stara prawda marketingowa mówi, że największą szansę na treści wiralowe mają te, które wywołują silne emocje,
- z naturalnych przyczyn wszyscy są teraz zainteresowani wojną.

Nasilona dyskusja o fake news, może dodatkowo nakręcić fakenewsa. Czasem w internecie pada apel “stop making stupid people famous”. Tutaj mam podobny apel “stop making fake news famous”

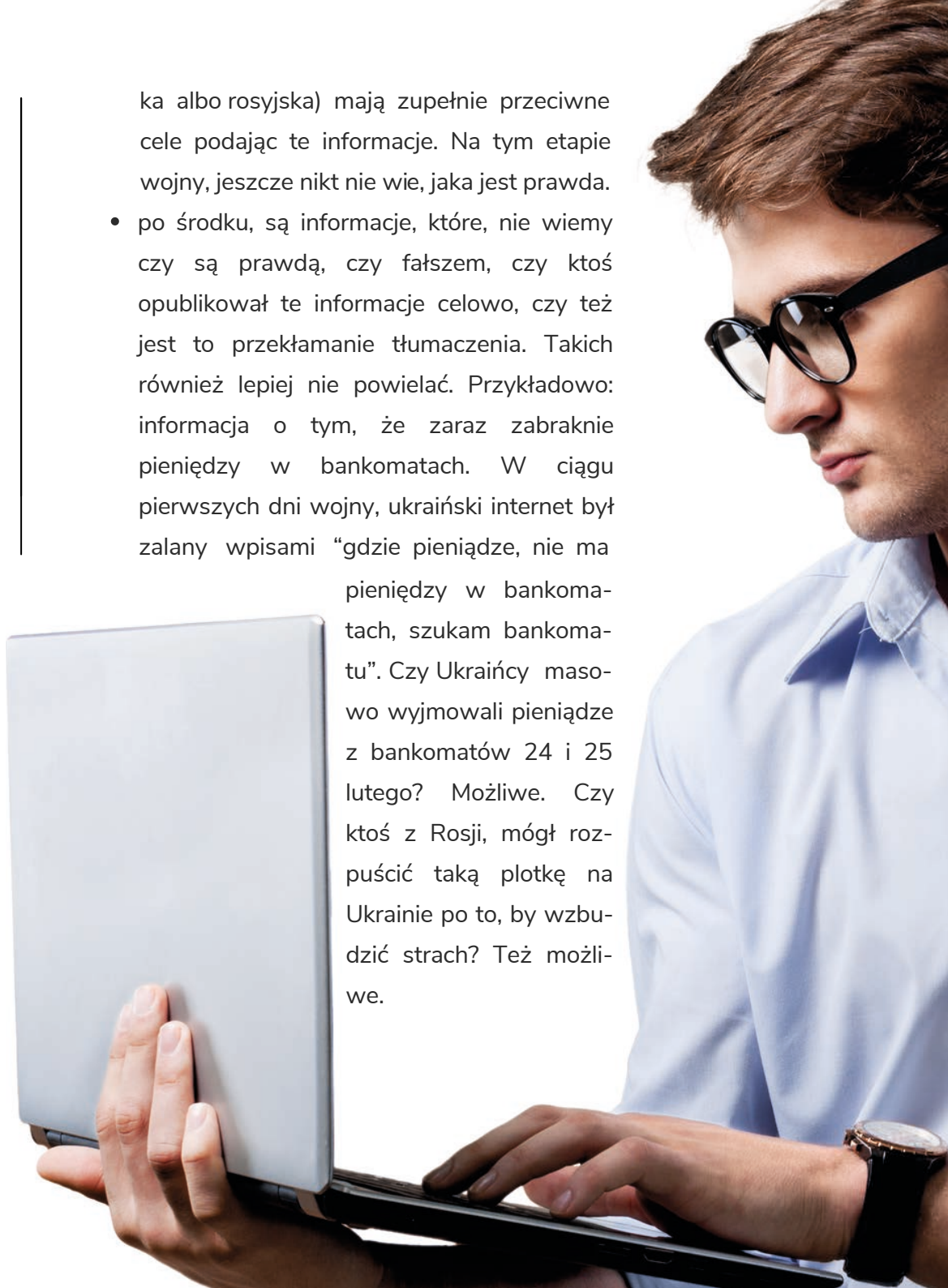
CO ZROBIĆ BY NIE NAKRĘCAĆ FAKENEWSÓW JESZCZE BARDZIEJ?

- Jeśli masz zasięgi (jako dziennikarz, media, twórca internetowy, influencer, celebryta), jesteś odpowiedzialny za szerzenie treści. Musisz być w stanie je zweryfikować dwukrotnie lub trzykrotnie u sprawdzonych źródeł (agencje Reuters, Associated Press, dziennikarze, którzy są bezpośrednio w Ukrainie przy konwojach wojennych). Powielanie krzykliwych clickbaitowych tytułów, zdjęcia zapłakanego dziecka z manipulacyjnym podpisem tylko doda więcej zasięgów osobie, która wymyśliła danego fakenewsa.
- Nie wiesz, co sharować? Sharuj treści agencji fact-checkingowych - w Polsce to Demgagog lub europejskie Euvsdesinfo.
- Jeśli nie możesz zweryfikować - nie sharuj.
- Pomyśl, jak reakcję wśród ludzi wywoła twój news. Przykładowo: jeśli ktoś teraz opublikuje newsa “w aptekach brakuje leków przeciwbólowych”, to co zrobią ludzie? Ruszą do sklepów, na stacje benzynowe lub do aptek internetowych, by wykupić resztki leków przeciw-bólowych.
  Panic-buying jest zjawiskiem, które stało się popularne podczas pierwszych fali covid-19.

NIE KAŻDY FAKE NEWS JEST FAKE

Od 3 tygodni bacznie w SentiOne przyglądamy się, jakie treści są najczęściej sharowane, klikalne lub wręcz powielane w tej samej treści. Pamiętajmy, że w morzu informacji mamy też takie przypadki, jak oczywiste pomyłki w relacji (np. złe tłumaczenie), celową dezinformację, propagandę (zarówno ze strony ukraińskiej, rosyjskiej, amerykańskiej czy polskiej), oraz zwykłe kłamstwa. Wszystkie te informacje można podzielić na trzy filary i na podstawie tego zdecydować, czy są warte dalszego powielania:

- oczywisty fake news, łatwy do weryfikacji. np, Pornhub zablokował wejścia dla użytkowników z Rosji. Można przeczytać oficjalne oświadczenie firmy Pornhub, zainstalować VPN, ustalić lokalizację jako Rosja i sprawdzić stronę Pornhub.
- na drugim końcu spektrum, są informacje, których nie potrafimy zweryfikować. “W ciągu ostatni trzech tygodni Rosja straciła 13 tysięcy żołnierzy. Lub 5 tysięcy. Lub tysiąc. Lub 20 tysięcy.” Fizycznie nikt z nas nie jest w stanie tego zweryfikować, a źródła, które to podają (albo strona ukraińska albo rosyjska) mają zupełnie przeciwne cele podając te informacje. Na tym etapie wojny, jeszcze nikt nie wie, jaka jest prawda.
- po środku, są informacje, które, nie wiemy czy są prawdą, czy fałszem, czy ktoś opublikował te informacje celowo, czy też jest to przekłamanie tłumaczenia. Takich również lepiej nie powielać. Przykładowo: informacja o tym, że zaraz zabraknie pieniędzy w bankomatach. W ciągu pierwszych dni wojny, ukraiński internet był zalany wpisami “gdzie pieniądze, nie ma pieniędzy w bankomatach, szukam bankomatu”. Czy Ukraińcy masowo wyjmowali pieniądze z bankomatów 24 i 25 lutego? Możliwe. Czy ktoś z Rosji, mógł rozpuścić taką plotkę na Ukrainie po to, by wzbudzić strach? Też możliwe.



SECURITY MAGAZINE

Redakcja zaprasza

PRAKTYKÓW I SPECJALISTÓW

do grona

EKSPERTÓW WYDANIA

redakcja@securitymagazine.pl

EKSPERCI WYDANIA

PIOTR KANTOROWSKI
Radca prawny
Kantorowski, Głąb i Wspólnicy

Założyciel Kancelarii Prawnej Kantorowski, Głąb i Wspólnicy, wspierającej przedsiębiorców na rynkach e-commerce, digital marketingu i IT. Autor i współautor wielu publikacji, w tym książek "Prawo dla Biznesu. E-commerce", „Zabezpieczanie umów i biznesu. Praktyczny poradnik z wzorami dokumentów (z suplementem elektronicznym)". Prowadzi swój podcast Prawo dla Biznesu.

ARTUR BICKI
CEO
EMCA Software Sp. z o.o.

Założyciel i prezes firmy EMCA Software Sp. z o.o. - producenta rozwiązania Energy Logserver. Odpowiada za całość strategii rozwoju produktu oraz koordynację prac deweloperskich. Posiada szerokie kompetencje w obszarze monitorowania i bezpieczeństwa sieci oraz metod zapobiegania cyberzagrożeniom i atakom.

MACIEJ PAWLAK
Head of Risk & Security
Tpay

W Tpay odpowiedzialny za zarządzanie ryzykiem i bezpieczeństwem informacji. Od ponad 10 lat związany z branżą fintech. Ekspert w dziedzinie compliance oraz zarządzania ryzykiem niezgodności w instytucjach regulowanych. Współodpowiedzialny za proces uzyskiwania licencji instytucji płatniczej dla pierwszego kantoru internetowego w Polsce.

PATRYK BOGDAN
Security Officer & Team Leader
Grandmetric

Od ponad 10 lat wykonuje testy penetracyjne i szuka podatności w systemach i aplikacjach IT. Rozpoczynał jako uczestnik programów bug bounty, dziś realizuje projekty pentesterskie i związane z audytami bezpieczeństwa jako Security Officer w Grandmetric.

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.

MARCIN ŚWIĘTY
Dyrektor Global Security i IT
Relativity

Globalny ekspert ds. bezpieczeństwa, koncentrujący się na korzyściach technicznych i technologicznych wynikających z przejścia do chmury oraz na tym, jak firmy mogą bezpiecznie działać w skali globalnej. Posiada wiele profesjonalnych certyfikatów uznanych organizacji InfoSec - CGEIT, CISSP, CRISC, CISM, CISA, CEH i inne.

BARTOSZ BAZIŃSKI
współzałożyciel i COO
SentiOne

Programista, przedsiębiorca, pasjonat wdrażania innowacyjnych technologii do świata biznesu. Od 2011 roku kieruje rozwojem narzędzia do monitoringu internetu i automatyzacji obsługi klienta - SentiOne.

KRZYSZTOF WITKOWSKI
Head of DevOps, Programista
Advox Studio

Jeden z pierwszych programistów w Advox. Aktualnie przewodzi zespołowi DevOps, a wcześniej pracował jako programista Magento2, Symfony, Zend Framework, AngularJS oraz wielu innych technologii. Odpowiada za utrzymanie infrastruktury serwerowej, a także wspiera zespoły w zakresie optymalizacji działania serwisów internetowych oraz ich bezpieczeństwa.

PARTNERZY WYDANIA

PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW
Z DZIENNIKARZAMI

ROCKET SCIENCE COMMUNICATIONS

AGENCJA PUBLIC RELATIONS

POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE

SECURITYMAGAZINE.PL

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
Projekt i skład: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL