9(18)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Oprócz zdrowia zaczniemy sobie życzyć bezpieczeństwa?

Prawo a AI
Odpowiedzialność i ochrona

Cyberzagrożenia II kw. 2023.
Zmieniające się trendy

Wycieki danych w firmach.
Człowiek jest największym zagrożeniem?

Europejski Miesiąc Cyberbezpieczeństwa
Dołącz do inicjatywy

SPIS TREŚCI

UWAGA! PISMO "SECURITY MAGAZINE" JEST CHRONIONE PRAWEM AUTORSKIM I PRASOWYM. **ZABRANIA SIĘ** WYCINANIA, PRZETWARZANIA I PUBLIKOWANIA FRAGMENTÓW TEKSTOWYCH ORAZ GRAFICZNYCH MAGAZYNU DYSTRYBUOWANYCH W INTERNECIE JAKO ODRĘBNE MATERIAŁY.

SZCZEGÓŁY STR. 89

SZANOWNI PAŃSTWO,

zbliża się październik. Od 11 lat jest to Europejski Miesiąc Cyberbezpieczeństwa. Wszystkie kraje Unii Europejskiej aktywnie uczestniczą w tej inicjatywie, a głównym jej celem jest nie tylko edukacja, ale również podnoszenie świadomości społecznej oraz promowanie najlepszych praktyk w zakresie bezpieczeństwa cyfrowego.

W tym roku, tematyka skupia się wokół inżynierii społecznej. Kluczowym zagadnieniem będą techniki manipulacji stosowane przez cyberprzestępców. Mówimy tu o szerokim spektrum działań, począwszy od kampanii phishingowych, przez socjotechniki, aż po bardziej wyrafinowane metody, takie jak spear-phishing czy whaling. Wszystkie te techniki mają jeden wspólny cel - wykorzystanie ludzkiego błędu, naiwności lub nieuwagi, aby uzyskać dostęp do cennych informacji.

“Security Magazine” ponownie włącza się w tę inicjatywę. W tym roku zachęcamy ekspertów, specjalistów w dziedzinie cyberbezpieczeństwa oraz firmy technologiczne do aktywnego włączenia się do naszej inicjatywy: tworzenia materiałów edukacyjnych, które pomogą podnieść poziom wiedzy wśród przedsiębiorców i ich pracowników.

Wspólnie możemy przyczynić się do tego, by firmy były lepiej przygotowane na ewentualne ataki. Zapraszam do zapoznania się ze szczegółami na stronie 6.

Dobrej lektury!

Rafał Stępniewski


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

PROJEKT USTAWY WYCOFANY

W naszym poprzednim numerze opisywaliśmy projekt ustawy dotyczącej cyberbezpieczeństwa oraz ochrony dzieci przed treściami w internecie. Okazuje się jednak, że rząd zdecydował o wycofaniu go z prac parlamentarnych.
Decyzja ta wpłynie na planowane wysłuchania publiczne w tych sprawach. Projekty miały na celu wzmocnienie cyberbezpieczeństwa i ochronę małoletnich przed nieodpowiednimi treściami online. Powód decyzji nie został jeszcze wyjaśniony, ale wybory parlamentarne zaplanowane na 15 października mogą mieć wpływ na tę sytuację.

KWANTOWY GENERATOR W NASK

Kwantowy generator liczb losowych, stworzony przez naukowców z Instytutu Optoelektroniki WAT, TELDAT i NASK, trafi do testów w NASK. Jest częścią projektu "Technologie optyczne kryptologii kwantowej do ochrony danych w sieciach teleinformatycznych" (OptoKrypt), mającego na celu rozwój technologii ochrony danych. Generator będzie mógł być używany w sektorze wojskowym i finansowym. Jego prezentacja miała miejsce podczas Międzynarodowego Salonu Przemysłu Obronnego 2023 w Kielcach. NASK ocenia możliwość wykorzystania tej technologii w sieci telekomunikacyjnej. Po targach w Kielcach, prototyp trafi do laboratorium NASK. Projekt współfinansowany przez NCBiR.

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

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

Redakcja "Security Magazine"

ECSM W PAŹDZIERNIKU

Europejski Miesiąc Cyberbezpieczeństwa (European Cyber Security Month – ECSM) obchodzony jest w październiku już od 11 lat! To ogólnoeuropejska kampania organizowana przez ENISA (European Union Agency for Cybersecurity) z inicjatywy Komisji Europejskiej. Jej celem jest popularyzacja wiedzy, zwiększanie świadomości i wymiana dobrych praktyk w obszarze cyberbezpieczeństwa wśród szerokiej grupy użytkowników Internetu, profesjonalistów czy osób zajmujących się edukacją oraz profilaktyką dzieci i młodzieży. W Polsce kampanię od samego początku koordynuje NASK - PIB.

Europejski Miesiąc Cyberbezpieczeństwa jest inicjatywą bezpłatną, otwartą dla wszystkich, dlatego każdy może zgłosić swoje wydarzenie, (przykładowo: warsztat, konferencję, kampanię, seminarium, webinar, konkurs), jak również inne działanie promujące cyberbezpieczeństwo i cyberhigienę. Wydarzenia mogą być zorganizowane stacjonarnie lub online.

Tegoroczna edycja Europejskiego Miesiąca Cyberbezpieczeństwa skupia się na zagadnieniach związanych z **inżynierią społeczną**, czyli szerokorozumianym wykorzystaniem przez przestępców techniki manipulacji. Socjotechniki te są stosowane w kampaniach phishingowych skierowanych do użytkowników internetu, którzy każdego dnia narażeni są na różnego typu ataki.

W tegorocznej edycji ENISA zwraca **szczególną uwagę na zachowanie ostrożności i czujności podczas każdej aktywności w sieci**. Hasłem przewodnim kampanii jest **„bądź mądrzejszy niż oszust", które ma zachęcić użytkowników do mądrego i rozważnego korzystania z internetu**.

Wszystkie materiały dotyczące kampanii, a także informacje na temat zgłoszonych inicjatyw można znaleźć na: **Facebooku** oraz **X (dawny Twitter)**.

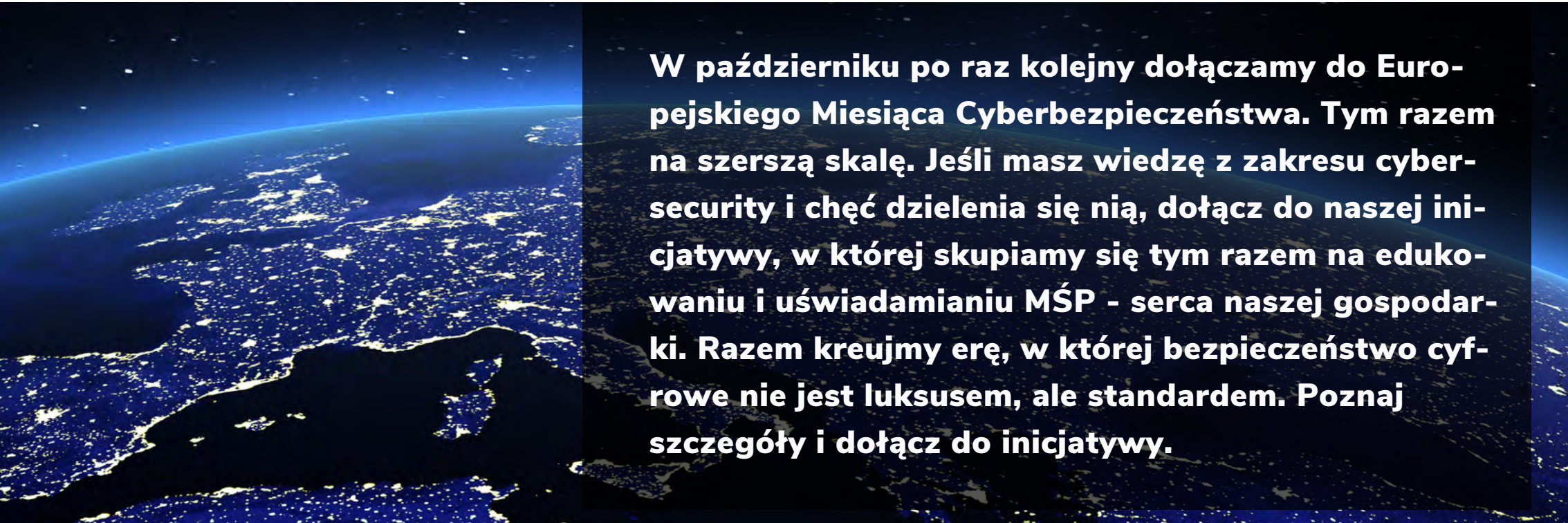
Zapraszamy do dzielenia się z nami newsami (do 500 zzs) z Twojej firmy, organizacji, które mają znaczenie ogólnopolskie i globalne.

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

Redakcja "Security Magazine"

PAŹDZIERNIK: EUROPEJSKI MIESIĄC CYBERBEZPIECZEŃSTWA

Rafał Stępniewski
Rzetelna Grupa



W październiku po raz kolejny dołączamy do Europejskiego Miesiąca Cyberbezpieczeństwa. Tym razem na szerszą skalę. Jeśli masz wiedzę z zakresu cybersecurity i chęć dzielenia się nią, dołącz do naszej inicjatywy, w której skupiamy się tym razem na edukowaniu i uświadamianiu MŚP - serca naszej gospodarki. Razem kreujmy erę, w której bezpieczeństwo cyfrowe nie jest luksusem, ale standardem. Poznaj szczegóły i dołącz do inicjatywy.

Październik jest wyjątkowy dla branży cybersecurity. Od 11 lat cała Europa właśnie w tym miesiącu skupia się na kwestiach związanych z cyberbezpieczeństwem - to Europejski Miesiąc Cyberbezpieczeństwa. Jego najważniejszym celem jest niezmiennie edukacja, podnoszenie świadomości oraz promowanie najlepszych praktyk w zakresie bezpieczeństwa cyfrowego.

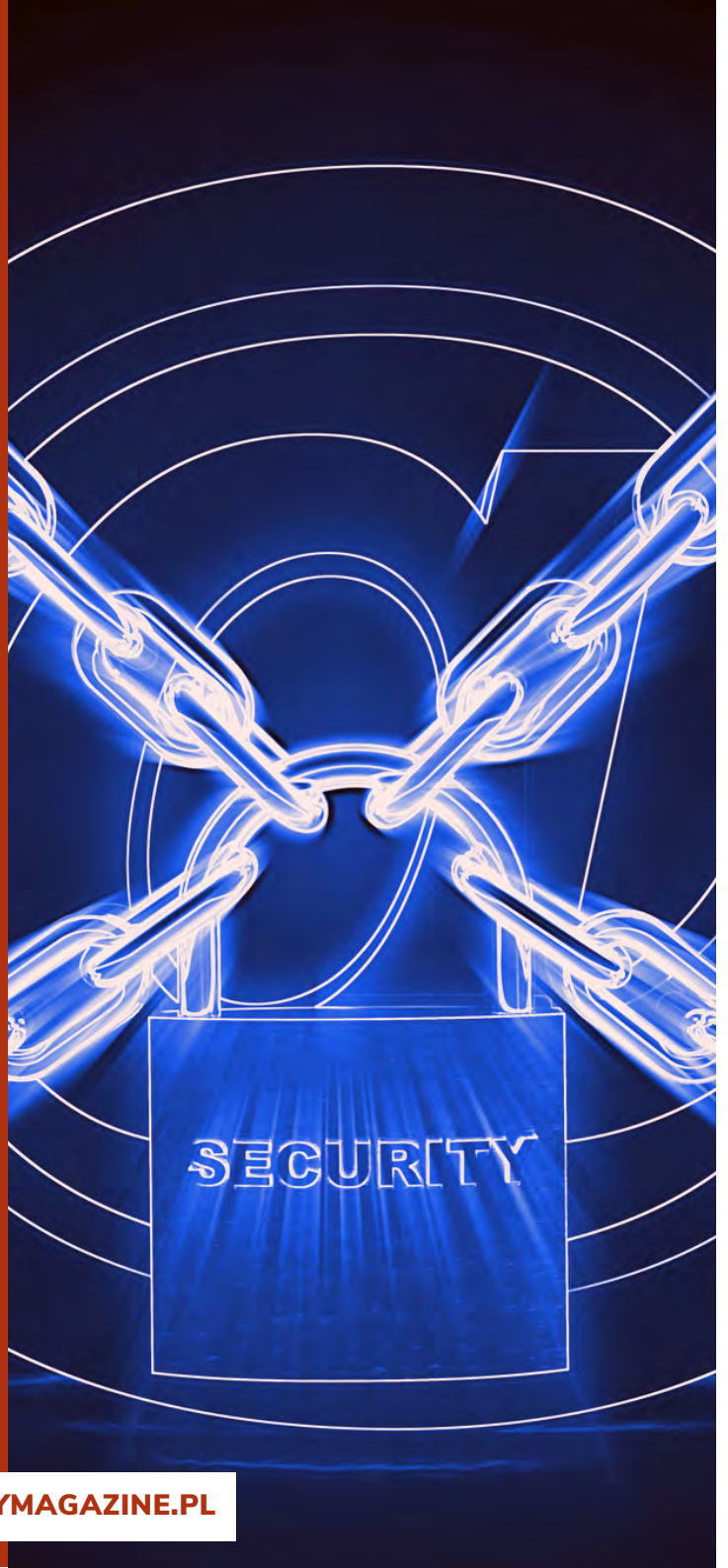
PHISHING, MANIPULACJE, SOCJOTECHNIKI

Anna Kwaśnik z NASK, który z ramienia ENISA jest koordynatorem inicjatywy w Polsce przekazała nam, że obecna edycja Europejskiego Miesiąca Cyberbezpieczeństwa skupiać się będzie na zagadnieniach związanych z inżynierią społeczną, czyli szeroko rozumianym wykorzystaniem przez przestępców techniki manipulacji. Socjotechniki te są stosowane w kampaniach phishingowych skierowanych do użytkowników internetu, którzy każdego dnia narażeni są na różnego typu ataki.

Europejska Agencja ds. Cyberbezpieczeństwa we wrześniu 2022 roku opublikowała kolejny, dziesiąty raport dotyczący zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych, zatytułowany ENISA Threat Landscape 2022.

Wymienia ona wszystkie działania mające na celu wykorzystanie ludzkiego błędu lub ludzkich zachowań, aby uzyskać dostęp do informacji lub usług. To tzw. socjotechnika (inżynieria społeczna), która stosuje różne formy manipulacji w celu nakłonienia ofiar do popełnienia błędów bądź przekazania wrażliwych lub tajnych informacji. Ten rodzaj zagrożeń składa się głównie z następujących wektorów ataku:

- **phishing** – kradzież ważnych informacji (numery kart kredytowych i hasła, za pośrednictwem e-maili, socjotechniki lub oszustwa);
- **spear-phishing** – bardziej wyrafinowana wersja phishingu, której celem są określone organizacje lub osoby, np. podszywanie się pod ministerstwa i wysyłanie do innych agend rządowych informacji nakazujących otwarcie pliku zawierającego złośliwe oprogramowanie;
- **whaling** – atak typu spear-phishing skierowany do użytkowników na wysokich stanowiskach (dyrektorów, polityków itp.);
- **smishing** – termin wywodzący się z połączenia słów „SMS” i „phishing”, który pojawia się, gdy informacje finansowe lub dane osobowe ofiar są zbierane za pomocą wiadomości SMS;
- **vishing** – połączenie phishingu i głosu – występuje, gdy informacje są przekazywane przez



telefon, z którego korzystają złośliwi aktorzy technik socjotechnicznych w celu wydobycia poufnych informacji od użytkowników;

- **kompromitacja poczty biznesowej (BEC)** – wyrafinowane oszustwo wymierzone w firmy i organizacje, w ramach którego przestępcy wykorzystują socjotechnikę, aby uzyskać dostęp do konta e-mail pracownika lub kierownika oraz inicjować przelewy bankowe lub inne czynności na nieuczciwych warunkach;
- **oszustwo** – celowe wprowadzenie w błąd lub zatajenie ważnego faktu, na podstawie którego ofiara podejmuje jakieś ważne decyzje;
- **podszywanie się** – działanie polegające na bezprawnym przyjęciu tożsamości innego podmiotu;
- podróbka – oszukańcza imitacja czegoś, np. podrobiona strona internetowa banku.

KILKA ISTOTNYCH FAKTÓW

Aby chronić się przez socjotechnikami nie wystarczy wiedzieć, że one istnieją. Dlaczego edukacja i uświadamianie są dziś kluczowe? Być może przekona Cię kilka faktów:

- **CyberDefence24** podał, że w 2022 roku najpopularniejszym rodzajem incydentu bezpieczeństwa był phishing.
- **CERT Polska:** w całym 2022 roku otrzymali ponad 322 tysiące zgłoszeń, które przełożyły się na ponad 39 tysięcy obsłużonych incydentów. Z tych zgłoszeń, 65% zaklasyfi-

kowano jako phishing, co oznacza, że było to około 209,3 tys. zgłoszeń dotyczących phishingu. Przypomnijmy, rok wcześniej było ich 22 tys. O ilu atakach nie wiemy?

- W 2022 roku na świecie odnotowano łącznie setki milionów prób ataków phishingowych. Rzeczywista liczba ataków może być jeszcze większa, biorąc pod uwagę te, które nie zostały wykryte lub zgłoszone. Dane podają m.in. **Trend Micro, AAG IT Support czy Statista.**
- Z raportu firmy **Egress** wynika, że globalnie 92% organizacji padło ofiarą ataków phishingowych w 2022 roku. To stanowi 29% wzrost w stosunku do 2021 roku, gdzie wykryto i zablokowano łącznie ponad 21 milionów ataków.
- **Egress** podał również, że ataki phishingowe przeciwko serwisom społecznościowym wzrosły z 8,5% wszystkich ataków w IV kwartale 2021 roku do 12,5% w I kwartale 2022 roku.
- Zaobserwowano 45% wzrost w wykrytych atakach phishingowych za pośrednictwem spamu w 2022 roku w stosunku do roku ubiegłego.
- Ataki phishingowe mające na celu kradzież informacji i danych, znane też jako ataki typu "credential phishing", odnotowały 4% wzrost w 2022 roku, z niemal 7 milionami wykryć.
- **Statista**: podczas czwartego kwartału 2022 roku, prawie 28% ataków phishingowych na świecie miało na celu instytucje finansowe.

MOŻESZ Z NAMI KREOWAĆ ERĘ SECURITY

W tym roku, nasze wydawnictwo "Security Magazine" po raz drugi stanie się częścią inicjatywy, jaką jest Europejski Miesiąc Cyberbezpieczeństwa. Szczególną uwagę chcemy skierować do MŚP, choć cała inicjatywa ENISA obejmuje każdego. Dlaczego zależy nam w szczególności na edukowaniu i uświadamianiu małych i średnich firm?

Ponieważ MŚP stanowią istotny element gospodarki, a ich bezpieczeństwo cyfrowe ma bezpośredni wpływ na stabilność i rozwój rynku. Ponadto to właśnie przedsiębiorcy tego sektora są w głównej mierze naszymi Czytelnikami. Do nich chcemy się zwrócić, publikując specjalne wydanie październikowe, wydanie poświęcone właśnie Europejskiemu Miesiącowi Cyberbezpieczeństwa.

Jeśli chcesz stać się częścią naszego projektu, możesz się do nas zgłosić, tak jak zrobiło to już 10 firm, które są w trakcie przygotowań eksperckich materiałów (artykułów, grafik, infografik i video) na wydanie październikowe. Liczba miejsc jest mocno ograniczona, dlatego **na zgłoszenia czekamy jedynie do 20 września.**

Podkreślmy, że głównym naszym celem, jak i celem ENISA jest realizacja misji edukacyjnej. Dodatkowo dla firm komercyjnych jest to wspaniała możliwość rozgłosu, budowy wizerunku oraz promocji oferowanych produktów, rozwiązań i usług. Oczywiście, uczestnicząc w tej inicjatywie, co podkreślamy na każdym kroku, należy pamiętać o tym, że **edukacja i budowanie świadomości są najważniejsze.**

Bez wątpienia cała akcja ma szczytny cel. Obecnie życie bez technologii jest niemożliwe, więc świadomość zagrożeń, jakie mogą nas spotkać w cyfrowym świecie, jest bardzo ważna. Nie każdy ma wiedzę techniczną i doświadczenie, a cyberprzestępcy wykorzystują naiwność, nieuwagę, a czasem i naturalną chęć skorzystania z okazji, żeby nie powiedzieć chciwość.

DLACZEGO WARTO NAWIĄZAĆ Z NAMI WSPÓŁPRACĘ PRZY EMC?

Publikując artykuły w "Security Magazine", mają Państwo możliwość podkreślenia swojego autorytetu, dzielenia się specjalistyczną wiedzą i wpływania na kształtowanie standardów w dziedzinie cyberbezpieczeństwa.

Nasza kampania będzie miała szeroki zasięg, dzięki temu, że z naszym magazynem docieramy do 30 tys. Czytelników miesięcznie, ponadto będziemy inicjatywę promować w mediach społecznościowych, serwisach Rzetelnej Grupy (politykabezpieczenstwa.pl, dziennikprawny.pl), będą ją promować również nasi partnerzy, w tym NASK jako koordynator Bezpiecznego Miesiąca.

Rozumiemy, że każdy ekspert ma swoją unikalną specjalizację, dlatego dajemy możliwość dostosowania tematu artykułu do Państwa specjalizacji, z zachowaniem spójności w zakresie tematu przewodniego kampanii.

W JAKICH OBSZARACH MOŻEMY WSPÓŁPRACOWAĆ W RAMACH EMC?

Może to być artykuł na łamach specjalnego wydania "Security Magazine", mogą to być grafiki, infografiki, video, które będziemy promować na naszych kanałach social media. Szczegóły oraz wymagania pod adresem: **redakcja@securitymagazine.pl**

Czasu jest bardzo niewiele. Na gotowe materiały czekamy jedynie **do 25 września.** Następnie przesyłamy je do NASK do akceptacji. Po uzyskaniu pozytywnej oceny, będziemy mogli je opatrzyć oficjalnym logo Europejskiego Miesiąca Cyberbezpieczeństwa.

Zachęcamy do podjęcia współpracy z nami w tym ważnym przedsięwzięciu. Razem możemy przyczynić się do podniesienia standardów cyberbezpieczeństwa wśród MŚP oraz podzielić się cenną wiedzą z szerokim gronem odbiorców.

24. KONFERENCJA BRANŻY OCHRONY

POLSKA IZBA OCHRONY
rok założenia 1994

POTENCJAŁ I ROLA SEKTORA PRYWATNEGO W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO

28 - 29 września 2023 |
Hotel Windsor
w Jachrance

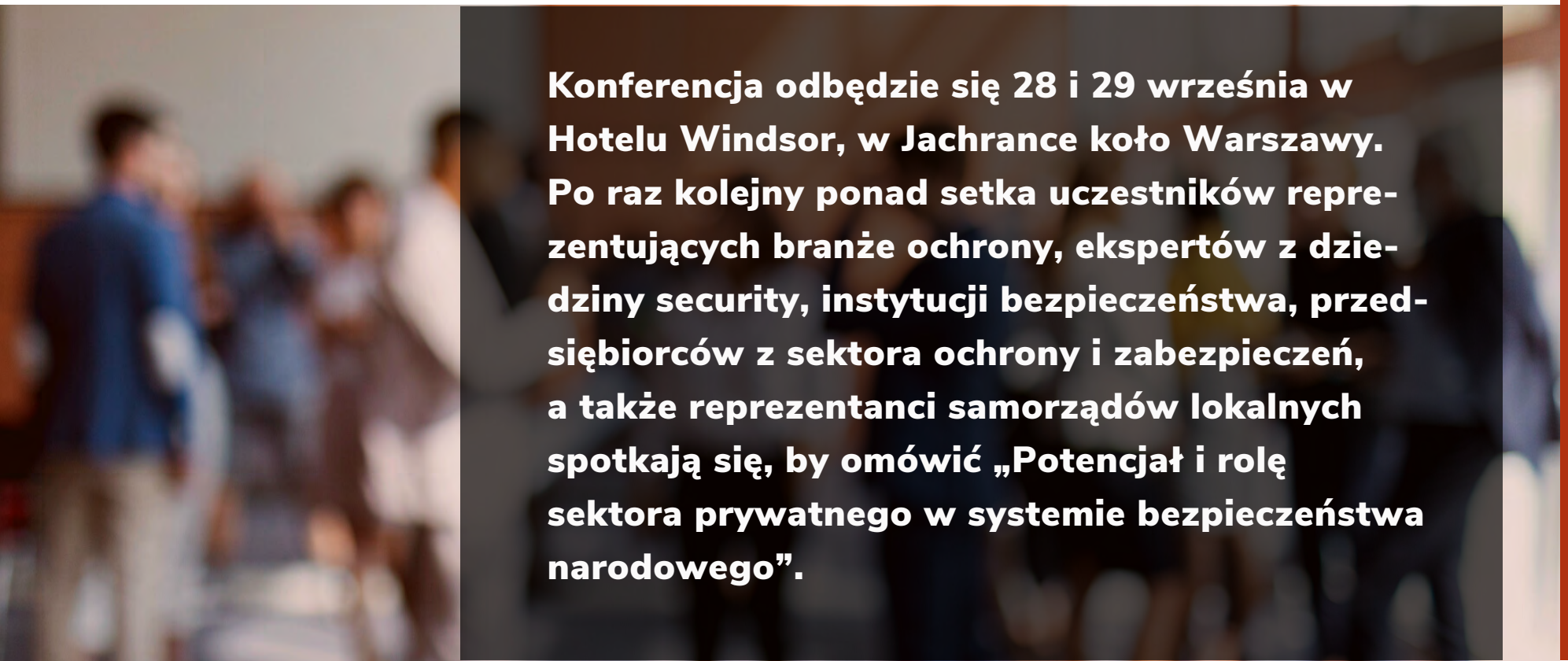
więcej informacji
WWW.KONFERENCJAPIO.PL

ZAREJESTRUJ SIĘ

SECURITYMAGAZINE.PL

24. KONFERENCJA BRANŻY OCHRONY. ZAREJESTRUJ SIĘ

PATRONAT
SECURITY MAGAZINE



Konferencja odbędzie się 28 i 29 września w Hotelu Windsor, w Jachrance koło Warszawy. Po raz kolejny ponad setka uczestników reprezentujących branże ochrony, ekspertów z dziedziny security, instytucji bezpieczeństwa, przedsiębiorców z sektora ochrony i zabezpieczeń, a także reprezentanci samorządów lokalnych spotkają się, by omówić „Potencjał i rolę sektora prywatnego w systemie bezpieczeństwa narodowego”.

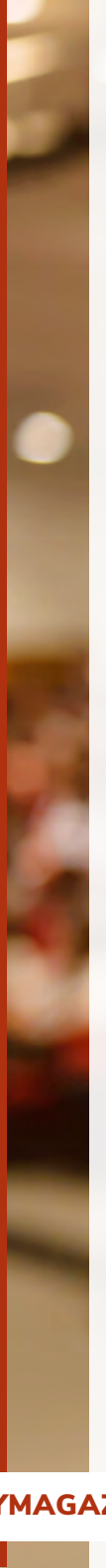
Podczas tego spotkania odbędą się prezentacje, panele eksperckie, prezentacje produktowe oraz networking. Dzięki współpracy z Partnerami Polskiej Izby Ochrony będą Państwo mogli poszerzyć swoją wiedzę dotyczącą najnowszych rozwiązań bezpieczeństwa samorządów lokalnych.

Polska Izba Ochrony (PIO) jako wiodąca organizacja przedsiębiorców w sektorze bezpieczeństwa, zrzesza około 180 firm współpracujących z podmiotami prywatnymi i publicznymi, w tym samorządem terytorialnym, w realizacji zadań ochronnych w Rzeczypospolitej Polskiej.

- Mamy przekonanie, że lokalny poziom bezpieczeństwa – gmina, miasto, powiat i metropolie to kluczowe obszary aktywności administracji, przede wszystkim samorządowej oraz Policji, służb i straży podejmujących codzienny wysiłek zmierzający do ograniczania zagrożeń dla mieszkańców, zapobiegania kryzysom i właściwego reagowania w przypadku identyfikacji niebezpieczeństw - mówią organizatorzy.

Konferencja jest adresowana, przede wszystkim, do władz miast, gmin, powiatów i urzędów oraz przedstawicieli komórek/jednostek odpowiedzialnych za bezpieczeństwo oraz zarządzanie kryzysowe w tych podmiotach.

Podczas tego spotkania organizatorzy pokażą potencjał branży ochrony i zaprezentują jej znaczący wpływ dla bezpieczeństwa narodowego.



Podstawowymi obszarami zagadnieniowymi omawianymi podczas 24. Konferencji PIO będą, m.in.:

- Technologie dla narodowego bezpieczeństwa — dostępność usług ochronnych (monitorowanie obiektów, ochrona fizyczna, systemy bezpieczeństwa, bezzałogowe statki powietrzne);
- Szanse i zagrożenia w realizacji obowiązkowej i szczególnej ochrony przez prywatny sektor bezpieczeństwa
- Bezpieczeństwo infrastruktury krytycznej w dobie zagrożeń hybrydowych;
- Praca zdalna w branży ochrony;
- Potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego w obecnej sytuacji geopolitycznej.

Szczegółowa agenda 24. KBO.

Partnerzy Honorowi, Merytoryczni/Wsparcie Merytoryczne, Medialni, Biznesowi: Securex, Akademia WSB w Dąbrowie Górniczej, Apeiron, Safety Project, Stowarzyszenie Polskich Specjalistów Bombowych, Centrum Prewencji Antyterrorystycznej ABW, Grupa WB, Linc Polska, Ganz, Reakto, Optex, Safestar, ASBIS, Security Magazine, A&S Polska, Security OPS.

Jak zarejestrować się na 23. Konferencję Branży Ochrony?
Wypełniając: **Formularz rejestracyjny dla partnera lub uczestnika**
Odsyłając wypełnione i zeskanowany formularz zgłoszeniowy na adres e-mail: biuropio@piooim.pl
Formularz rejestracyjny dla partnera lub uczestnika

Kontakt z Biurem Organizacyjnym 23. Konferencji Branży Ochrony: od poniedziałku do piątku, godz. 8 - 16 - tel. (22) 635-28-29, tel. kom: 696 719 615, lub mailowo: biuropio@piooim.pl

Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?

Sprawdź ofertę
PATRONATU
MEDIALNEGO

SECURITY MAGAZINE

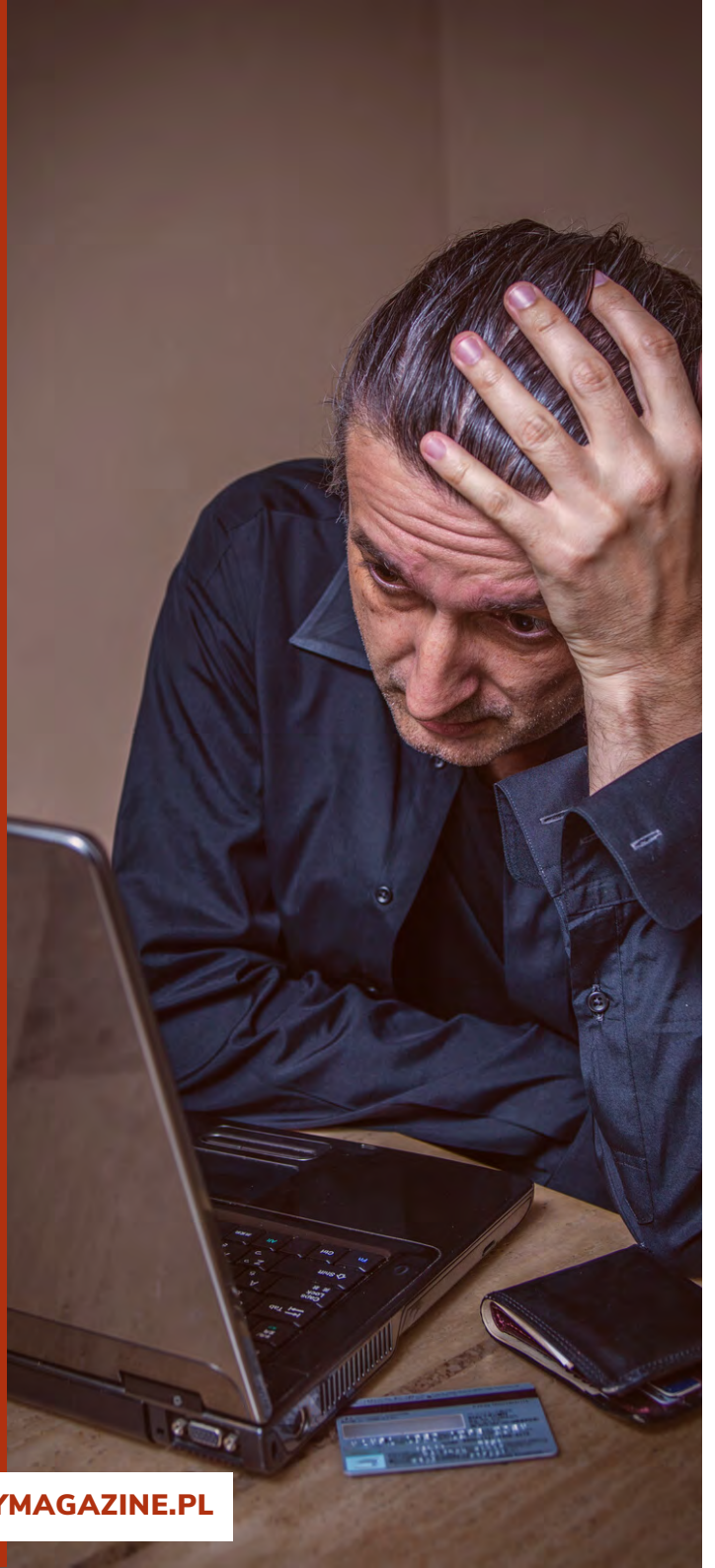
Napisz do nas:
redakcja@securitymagazine.pl

JAK POD WPŁYWEM UCZUĆ I EMOCJI MOŻEMY PAŚĆ OFIARĄ CYBER-PRZESTĘPSTWA?

Anna Kwaśnik
NASK - PIB

Większość z naszych aktywności przenieśliśmy do sieci. Wykorzystujemy ją w celach zawodowych, jak i prywatnych. Zakupy online, sprawy urzędowe, komunikacja z naszymi bliskimi, ze współpracownikami to tylko niektóre usługi, z jakich korzystamy na co dzień. Rozwój narzędzi, technologii oraz stale rosnąca popularność różnych aplikacji sprawia, że zdecydowanie częściej wybieramy rozwiązania internetowe niż te tradycyjnie.

Jak pod wpływem uczuć i emocji możemy paść ofiarą cyberprzestępstwa?



Popularność różnych serwisów społecznościowych, w tym również tych randkowych, a także brak czasu, ciągłe życie w biegu sprawia, sprawiają że coraz częściej decydujemy się na poznawanie nowych osób właśnie za pośrednictwem internetu. Niestety, również cyberprzestępcy coraz częściej wykorzystują naszą otwartość na znajomości online i w podstępny sposób próbują nas wykorzystać.

Na oszustwa romantyczne narażony jest każdy użytkownik Internetu, bez względu na wiek, płeć czy wykształcenie.* Przestępcy, którzy bazują na ich uczuciach, zaangażowaniu emocjonalnym i potrzebie bycia z kimś w związku za pomocą różnych narzędzi np. wiadomości email, komunikatorów, aplikacji, serwisów randkowych kontaktują się z nimi, i za pomocą różnych metod socjotechniki próbują wyłudzić dane, czy pieniądze.

Jednym z najpopularniejszych oszustw, na jakie narażeni są użytkownicy internetu w kontekście oszustw romantycznych to tzw. „oszustwo na amerykańskiego żołnierza". Przestępcy, którzy działają w ten sposób kontaktują się ze swoja ofiarą za pomocą różnych środków komunikacyjnych i przedstawiają siebie jako kogoś wyjątkowego, z bardzo dużym doświadczeniem życiowym i niebywale trudną sytuacją bytową.

Czasami jest to żołnierz, lekarka na misji lub więzień polityczny, który nie może wrócić do swojego kraju. Aby uwiarygodnić historię, przesyła swoje zdjęcia, które przedstawiają jego historię.

Coluccia A., Pozza A., Ferretti F., Carabellese F., Masti A., Gualtieri G., (2020), „Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review." Clinical Practice Epidemiology in Mental Health, v. 16 s. 24-35 [online], dostęp 7.09.2023r.

W swoich wiadomościach przekonuje swoją ofiarę do siebie i buduje z nią silną więź emocjonalną. W kolejnych wiadomościach zaczyna prosić o przesłanie pieniędzy, dzięki którym będzie mógł rozwiązać swoje problemy, wrócić do kraju lub przyjechać do swojej wybranki lub wybranka. Czasami nie chodzi o pieniądze.

Oszustwa typu romance scam są szczególnie niebezpieczne, ponieważ intensywnie zaangażowane w nową znajomość ofiary paść ofiarą nie tylko wyłudzenia finansowego, ale pod wpływem manipulacji, mogą przekazać przestępcom różne poufne dane, również te związane z firmą czy instytucją w której pracują. Zdarza się, że oszustwo tego typu jest elementem większej strategii szpiegostwa przemysłowego, w celu uzyskania dostępu do danych firmy lub szczegółów innowacyjnych rozwiązań.

Niestety, po przesłaniu pieniędzy lub danych czy dokumentów kontakt najczęściej się urywa, a ofiara pozostaje nie tylko bez oszczędności życia, ale również z poczuciem winy, krzywdy, oszukania a nawet wykorzystania.

W niektórych przypadkach oszuści mogą namawiać swoje ofiary do kliknięcia w przesłany im link czy załącznik, który w rzeczywistości może prowadzić do zainfekowanej strony internetowej lub pobrania szkodliwego oprogramowania szpiegującego, które umożliwi im przejęcie kontroli nad urządzeniem ofiary, co może być szczególnie niebezpieczne w przypadku sprzętu służbowego.

W JAKI SPOSÓB PRZESTĘPCY WYBIERAJĄ SWOJE OFIARY?

Podobnie jak w innych oszustwach opartych na socjotechnice, oszuści najczęściej stosują masową wysyłkę wiadomości na przypadkowe skrzynki użytkowników internetu lub konta w mediach społecznościowych. Zdarza się jednak, że oszuści wybierają swoją ofiarę celowo, i zanim się z nią skontaktują, przygotowują się do tego, zbierają informacje. Na celowniku mogą znaleźć się osoby zajmujące wysokie stanowiska, inżynierowie odpowiedzialni za rozwój produktów czy też handlowcy, posiadający dostęp do baz klientów.

Popularność serwisów społecznościowych, tych randkowych i zawodowych również spra-wia, że ich użytkownicy publikują w sieci bardzo

dużo prywatnych informacji o sobie, które z pozoru może wydawać się bezpieczne. Niestety, udostępnianie informacji na temat swojego miejsca zamieszkania, pracy, posiadanych umiejętności, kwalifikacji czy zainteresowań może być wykorzystane przez przestępców, którzy będą chcieli przeprowadzić spersonalizowany atak socjotechniczny (w tym również związany z oszustwami romance scam).

SKALA ZJAWISKA OSZUSTW NA TLE ROMANTYCZNYM

Według danych przekazanych przez Centralne Biuro Zwalczania Cyberprzestępczości, w latach 2020-2022 polska policja otrzymała co najmniej 400 zgłoszeń w sprawie oszustw na „amerykańskiego żołnierza". Ich skala jest prawdopodobnie dużo większa, jednak ofiary, z różnych względów, nie zawsze zgłaszają sprawę na policję lub do innych instytucji. Warto podkreślić, że osoby, które dały się oszukać, mogą czuć się wykorzystane, a wstyd i lęk przed oceną społeczną, może powodować, że stają się bezradni.

Choć wielu osobom mogłoby się wydawać, że oszustwa romantyczne nie stawią dużego zagrożenia, warto zwrócić uwagę na kwoty, jakie w ten sposób wyłudzają przestępcy. Według najnowszego raportu amerykańskiej Federalnej Komisji ds. Handlu (FTC) aż 40% ofiar, które straciły pieniądze w wyniku oszustwa internetowego, to ofiary „oszustw romantycznych". FTC podaje, że w 2022 roku cyberprzestępcy wyłudzili od swoich ofiar ponad 1,3 miliarda dolarów!**

JAK SIĘ CHRONIĆ PRZED TAKIMI OSZUSTWAMI?

Jedną z najważniejszych zasad o których należy pamiętać podczas korzystania

**Fletcher E., Romance scammers' favorite lies exposed, oficjalny serwis Amerykańskiej Komisji ds. Handlu (FTC), publikacja 9.02.2023r., dostęp 7.09.2023 r.

z Internetu, w tym również przy nawiązywaniu relacji, jest zasada ograniczonego zaufania. Nigdy nie należy ufać osobie, która się z nami kontaktuje, zwłaszcza gdy pojawiają się zapytania o nasze prywatne dane, informacje o miejscu pracy, prośby o jakiekolwiek transakcje finansowe.

W celu uniknięcia otrzymywania podejrzanych wiadomości warto włączyć filtry antyspamowe, natomiast niechciane wiadomości oznaczać jako spam.

Ze szczególną ostrożnością należy traktować wszystkie wiadomości, które zawierają linki i załączniki, co do których nie mamy pewności co zawierają i na jakie strony mogą nas przekierować. Nigdy nie należy instalować aplikacji lub oprogramowania, do którego zachęca rozmówca. Na komputerach służbowych warto ograniczyć uprawnienia pracownika do instalowania oprogramowania.

Oszustwa typu romance scam podobnie jak inne oszustwa phishingowe opierają się na ludzkich uczuciach i emocjach, dlatego niezwykle ważne jest, aby stale przypominać sobie podstawowe za-sady cyberihigeny i zwiększać świadomość na temat różnych zagrożeń internetowych.

Szkolenia pracowników dotyczące bezpiecznego zachowania w sieci wzmacniają odporność biznesu na różne zagrożenia związane z socjotechniką, w tym oszustwa romantyczne. Warto także uczulić kluczowych pracowników na możliwość wykorzystania oszustw o tym charakterze jako narzędzia nieuczciwej konkurencji.

W firmie należy ustanowić chociaż podstawowe procedury bezpieczeństwa informacji, zgłaszania nietypowych maili czy kontaktów.

GDZIE ZGŁASZAĆ OSZUSTWA ROMANCE SCAM?

Oszustwa typu romance scam podobnie jak inne oszustwa komputerowe należy zgłaszać do zespołu **CERT Polska poprzez formularz na stronie internetowej, email: incydent@cert.pl.**

Jeśli potrzebujesz wsparcia psychologicznego, wejdź na bezpłatną platformę pomocową 116sos.pl

- OH MY -

H @ C K

700 SPECJALISTÓW CYBERBEZPIECZEŃSTWA

Reprezentanci liderów branży fintech / IT,
m.in.: ACCENTURE, ALLEGRO, AVIVA, CERT Polska,
CSIRT KNF, EY, GSK, HSBC, IBM, ING, MICROSOFT,
NORDEA, ORANGE, Standard Chartered, T-MOBILE.

POKAŻ SIĘ!

NIECH POLSKA BRANŻA CYBERSECURITY CIĘ USŁYSZY

WYSTĄP NA SCENIE OMH 2023

KONFERENCJA POD PATRONATEM ZAUFANA TRZECIA STRONA.PL

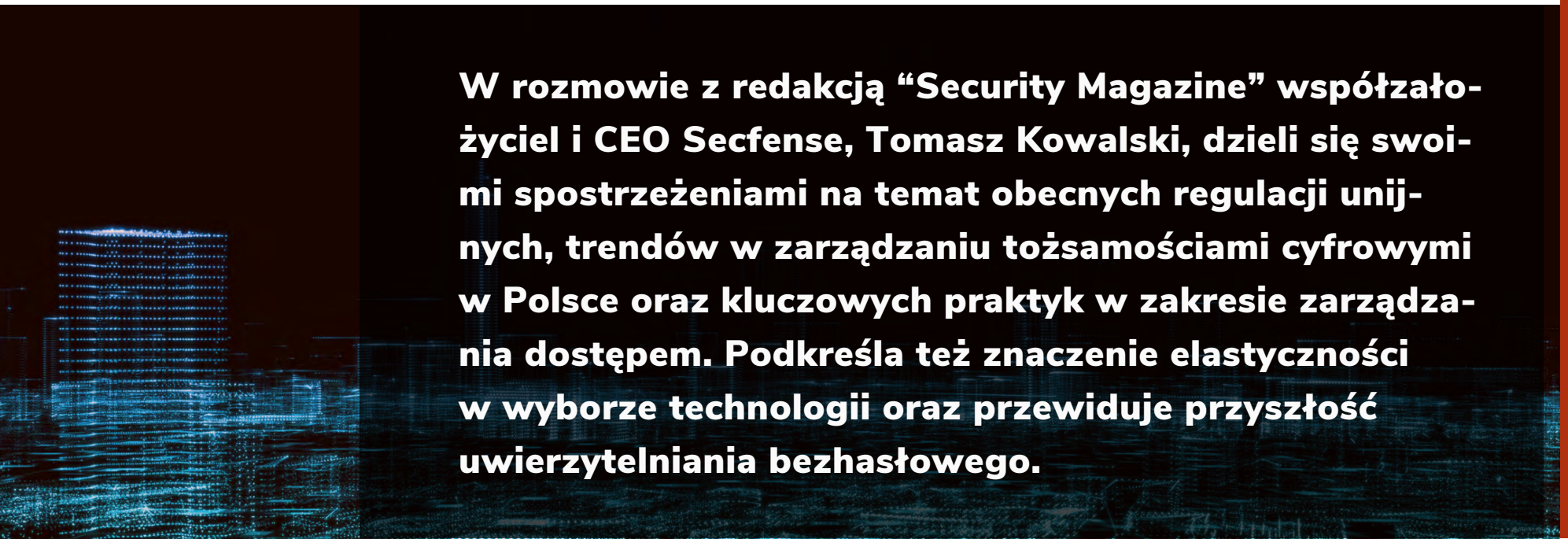
5.12.2023 / PGE Narodowy, Warszawa

CALL FOR PAPERS do 5 WRZEŚNIA 2023

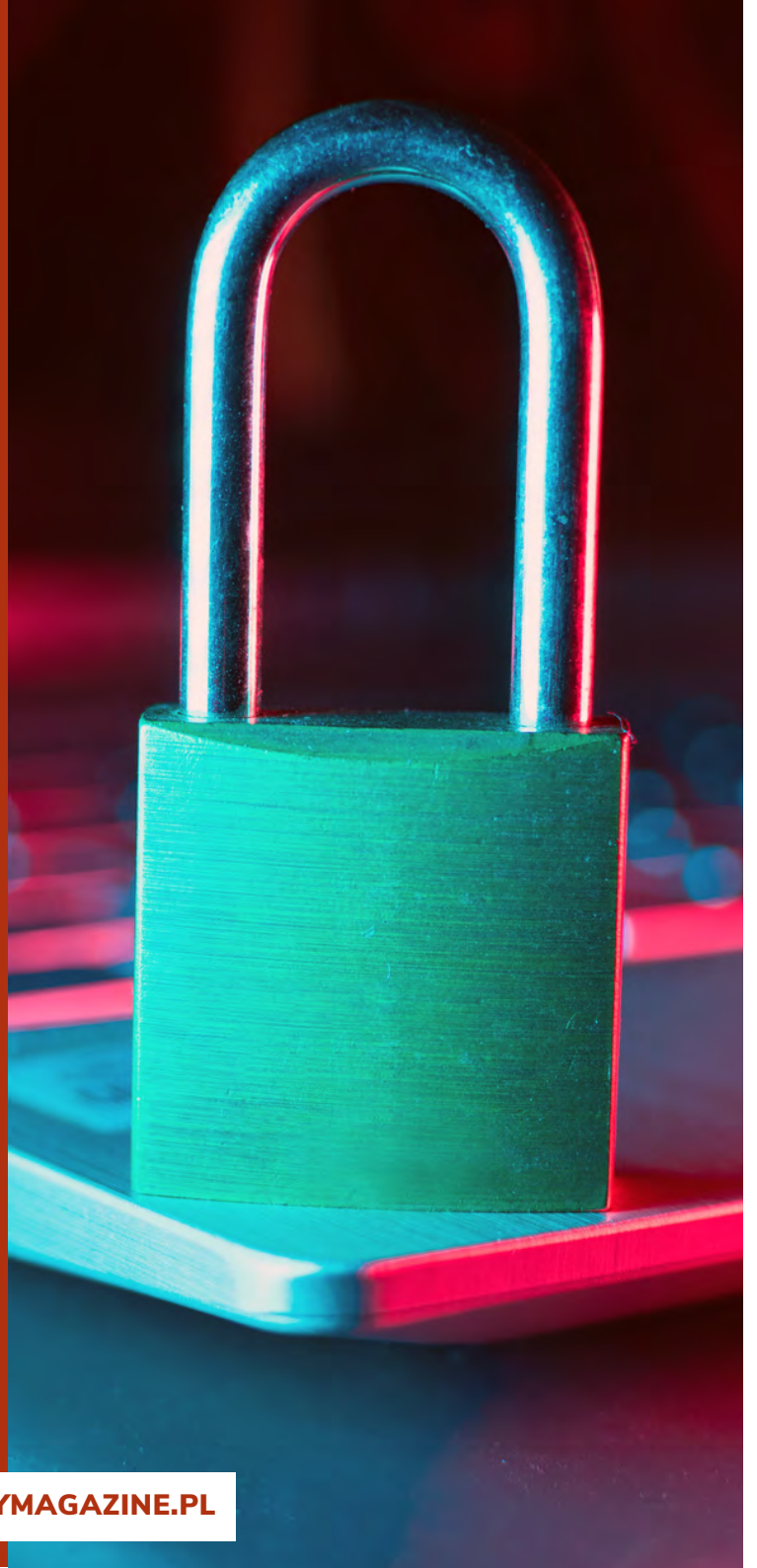
BILETY DOSTĘPNE: www.omhconf.pl

PRZYSZŁOŚĆ UWIERZYTELNIANIA I WYBORY TECHNOLOGICZNE

Tomasz Kowalski
Secfense



W rozmowie z redakcją “Security Magazine” współzałożyciel i CEO Secfense, Tomasz Kowalski, dzieli się swoimi spostrzeżeniami na temat obecnych regulacji unijnych, trendów w zarządzaniu tożsamościami cyfrowymi w Polsce oraz kluczowych praktyk w zakresie zarządzania dostępem. Podkreśla też znaczenie elastyczności w wyborze technologii oraz przewiduje przyszłość uwierzytelniania bezhasłowego.



Jakie są obecnie największe wyzwania w zakresie cyberbezpieczeństwa, z którymi muszą mierzyć się przedsiębiorstwa?

Tomasz Kowalski: Przedsiębiorstwa w Europie mierzą się teraz z nowymi regulacjami unijnymi mającymi na celu zwiększenie poziomu cyberbezpieczeństwa państw członkowskich.

Mówię o rozporządzeniu DORA, które dotyczy sektora finansowego, oraz dyrektywie NIS 2, obejmującej swoim zasięgiem podmioty kluczowe dla funkcjonowania państw, w tym energetykę, transport, opiekę zdrowotną, administrację publiczną, produkcję, bankowość czy zarządzanie usługami ICT.

Czasu na wdrożenie wytycznych dotyczących bezpieczeństwa cybernetycznego jest już niewiele. Warto pamiętać, że za wdrożenie przepisów DORA i NIS 2 odpowiedzialny jest zarząd przedsiębiorstwa. Przed firmami zatem sporo pracy, zwłaszcza że wymogi unijne obejmują szeroki zakres działań – od audytu, po wdrożenie odpowiednich rozwiązań, aż po szkolenia pracowników i podnoszenie ich świadomości.

A jakie trendy w zakresie zarządzania tożsamościami cyfrowymi w Polsce Pan obserwuje?

T.K.: Z dużym zaciekawieniem obserwuję działania dużych instytucji, takich jak banki czy telekomy, których celem jest wyróżnienie się na rynku. To jest trudny sektor, który zwykle konkuruje ceną. Natomiast od niedawna organizacje te pos-

tawiły na inne wartości pozwalające im przyciągać do siebie nowych klientów. Wartości takie jak bezpieczeństwo. Media szeroko komentowały wdrożenie przez ING kluczy U2F. To było na pewno kosztowne przedsięwzięcie, bo klucze te są fizycznymi urządzeniami, niemniej zwróciło uwagę mediów i zostało entuzjastycznie przyjęte przez rynek.

W mojej ocenie trend wyróżniania się na tle konkurencji właśnie poprzez podnoszenie bezpieczeństwa konsumentów będzie się nasilać. Świadomość społeczna dotycząca zagrożeń rośnie. Ludzie chcą chronić swoje dane i pieniądze, dlatego na pewno chętniej wybiorą dostawcę usług, który zapewni im wyższy poziom bezpieczeństwa. Nie wykluczam, że niedługo któryś z telekomów zaoferuje swoim klientom zabezpieczenie wszystkich kanałów dostępu do danych uwierzytelnianiem odpornym na phishing. To byłaby zmiana na skalę nie tylko polską, ale i światową.

Jakie praktyki związane z zarządzaniem dostępem do danych uważa Pan za kluczowe dla ochrony przedsiębiorstw przed cyberatakami?

T.K.: Firmy bez wątpienia powinny wykorzystywać uwierzytelnianie odporne na phishing. To oznacza odchodzenie od wciąż popularnych SMS-ów i aplikacji i wdrażanie w ich miejsce FIDO, czyli standardu uwierzytelniania online zastępującego hasła, oraz passkeys, czyli kluczy uniwersalnych. Stare metody 2FA dają tylko fałszywe poczucie bezpieczeństwa. W rzeczywistości średnio zaawansowany intruz jest w stanie rozpracować SMS 2FA za pomocą kilku tutoriali dostępnych na YouTube. Nie mówię tego po to, aby kogokolwiek straszyć. Właśnie nagrywamy webinar z ekspertem cyberbezpieczeństwa Mateuszem Chrobokiem, w którym pokazujemy, jak w 15 minut złamać uwierzytelnianie dwuskładnikowe oparte na SMS-ach. To jest nie tylko możliwe, ale i dość proste do przeprowadzenia.

Całe szczęście tego typu 2FA można szybko zastąpić odpornym na phishing uwierzytelnianiem wieloskładnikowym opartym na biometrii i kryptografii, czyli FIDO. Podczas webinaru również wyjaśniamy, jak to zrobić. W naszych social mediach będziemy informować w najbliższych tygodniach, gdzie można zobaczyć ten materiał.

Jakie rekomendacje mógłby dać Pan firmom, które dopiero zaczynają myśleć o wdrożeniu skomplikowanych systemów zarządzania tożsamościami?

T.K.: Dziś najważniejsza jest elastyczność, stąd firmy powinny szukać takich rozwiązań, które nie związą im rąk. Dostawcy często wprowadzają ograniczenia i blokady, które nie pozwalają w pełni wykorzystać potencjału technologii, którą wdrażają.

Ważne jest zatem wybieranie takich narzędzi, które są wszechstronne i elastyczne, czyli działają i ze starszymi aplikacjami, i z mobilnymi oraz webowymi. Które można szybko i w łatwy sposób modyfikować i rozbudowywać – czyli na bieżąco dostosowywać je do wciąż zmieniających się potrzeb przedsiębiorstwa.

Jakie są najczęstsze błędy, które firmy popełniają w zakresie zarządzania dostępem i jak można ich unikać?

T.K.: Problemem jest to, że przedsiębiorstwa nie poświęcają wystarczająco dużo czasu na znalezienie optymalnych rozwiązań. Na przykład, na rynku narzędzi zapewniających silne uwierzytelnianie są także takie, które pozwalają na kompleksowe wzmocnienie uwierzytelniania w całej firmie – dla wszystkich pracowników i klientów. Są też takie, które pokrywają ten temat tylko częściowo. Brak dokładnego researchu sprawia, że firmy połowicznie rozwiązują swoje problemy lub wybierają technologie, które nie zapewniają najwyższego poziomu ochrony.

Czy Secfense IdP jest odpowiedzią na rosnące potrzeby firm w zakresie zarządzania tożsamościami w złożonych środowiskach IT?

T.K.: Tak, przede wszystkim dlatego że wiele dużych firm korzysta dziś z kilku różnych narzędzi IAM, chociażby ze względu na ich dopasowanie do aplikacji używanych przez pracowników. Np. Microsoft Entra ID (dawniej Azure AD) lepiej integruje się z usługami Microsoft, OneLogin ma silną integrację z Amazon Web Services (AWS) itd.

Migracja tożsamości między poszczególnymi systemami IAM jest jednak problematyczna. Zwykle wiąże się z chaosem organizacyjnym, przeciążeniem działu helpdesk oraz dodatkowymi kosztami. Kosztowne jest też utrzymywanie różnych rozwiązań IAM. Zwłaszcza jeśli dodanie do nich potrzebnej firmie funkcji, np. dostępu warunkowego opartego na ryzyku, wiąże się z zakupem wyższego pakietu, oferującego także wiele funkcjonalności, z których przedsiębiorstwo wcale nie będzie korzystać.

Secfense Identity Provider pozwala rozwiązać ten problem, bo działa jak przełącznik między różnymi systemami IAM i daje firmie pełną kontrolę nad tożsamością. Dzięki niemu to organizacja decyduje, którzy użytkownicy różnych aplikacji są uwierzytelniani w np. Entra ID, a którzy w Okta czy OneLogin. Firma może dowolnie konfigurować ustawienia tożsamości tak, aby przynosiły korzyści biznesowe, oraz samodzielnie decydować, z jakiej usługi IAM będą korzystać poszczególne aplikacje.

Co więcej, Secfense IdP pozwala korzystać z najlepszych funkcjonalności bezpieczeństwa, takich jak dostęp warunkowy, mechanizm wykrywania botów czy biometria behawioralna, bez konieczności modyfikacji dotychczas stosowanych pakietów usług. Umożliwia też wprowadzenie w organizacji uwierzytelniania bezhasłowego opartego na standardzie FIDO.

Idąc dalej zapytam, jaka jest, Pana zdaniem, przyszłość uwierzytelniania bezhasłowego i jakie korzyści może przynieść ono przedsiębiorstwom?

T.K.: Myślę, że od tego nie ma odwrotu, jednak adopcja uwierzytelniania bezhasłowego zajmie więcej czasu, niż pierwotnie przypuszczaliśmy. Tak bywa z nowymi technologiami.

Spójrzmy na sztuczną inteligencję. Jeszcze kilka miesięcy temu baliśmy się, że za chwilę zabierze nam wszystkim pracę. Teraz mało kto tak myśli. AI jest, rozwija się sprawnie, pomaga w różnych zadaniach, ale nie powinniśmy być raczej zmartwieni tym, że za 5 lat zastąpi nas kolejna wersja chata GPT.

Podobnie z passwordless. Kiedy w 2017 pojawił się U2F, a później FIDO, wróżyliśmy w Secfense, że koniec haseł jest bliski. Dziś modyfikujemy nasze prognozy. Wciąż uważamy, że hasła w internecie muszą odejść, z roku na rok są bowiem coraz mniej skuteczne i coraz bardziej uciążliwe. Zmiana ta jednak nie nastąpi od razu. Natomiast nie mam wątpliwości, że firmy, które jako pierwsze przejdą na passwrodless, bardzo szybko będą czerpać z tego korzyści. Nie będą musiały się bowiem zajmować ciągłą walką z cyberprzestępcami, z phishingiem. Dzięki temu zyskają czas i zasoby na inne zadania. Dodatkowo wyróżnią się w oczach klientów, co może okazać się dużą przewagą konkurencyjną.

Jakie są plany rozwoju Secfense w kontekście IdP i jakie nowe funkcjonalności można spodziewać się w najbliższej przyszłości?

T.K.: Rozwiązanie, które oferujemy, czyli broker Secfense, to niewidzialna warstwa między użytkownikiem i aplikacją. Jest to naturalne miejsce dla wzmocnienia bezpieczeństwa, stąd właśnie tu wstawiamy silne i odporne na phishing bezhasłowe uwierzytelnianie.

Jednak jest to również punkt, w którym z powodzeniem można wstawić inne funkcjonalności, dziś na stałe wpisane w przeróżne aplikacje czy infrastrukturę firmy. Docelowo Secfense będzie więc dostarczał różne funkcjonalności z różnych obszarów bezpieczeństwa, wykraczające poza uwierzytelnianie i tożsamość, ale zawsze łatwe do wdrożenia, elastyczne i ułatwiające działanie firmy w coraz bardziej skomplikowanym technologicznie świecie.

Życzę sukcesów i dziękuję za rozmowę.


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

PRAWO A AI. ODPOWIEDZIALNOŚĆ I OCHRONA

Redakcja
SECURITY MAGAZINE

LAWMORE

Czy do tekstu lub obrazu wygenerowanego przez AI można posiadać prawa autorskie? Czy można opatentować wynalazki, których współtwórcą jest sztuczna inteligencja? I w końcu, kto bierze odpowiedzialność za wytwory algorytmów, które narażają na straty konsumentów? Odpowiedzi w dokumencie "Prawne aspekty Gen AI" szukali Dominika Wcisło, Aleksandra Maciejewicz, Milena Balcerzak i Bartłomiej Serafinowicz z LAWMORE.

Odpowiedzi są dość skomplikowane, podobnie jak obecna sytuacja prawna w kontekście AI. Co zatem warto wiedzieć o sztucznej inteligencji, aby nie narazić siebie i swojego biznesu na poważne konsekwencje prawne?

AI WYGRAŁO PRESTIŻOWY KONKURS

Kilka miesięcy temu było głośno o niemieckim fotografie Borisie Eldagsenie. Artysta wziął udział w prestiżowym konkursie Sony World Photography Awards 2023, w którym przyznano mu nagrodę w otwartej kategorii "Creative". Szybko okazało się, że autorem wyróżnionego zdjęcia nie jest Eldagsen, tylko sztuczna inteligencja, która bazowała na trzydziestoletnim doświadczeniu niemieckiego fotografa. Co prawda, Eldagsen wycofał się z konkursu, ale jego twórcze działanie dorzuciło kolejną „cegiełkę” do dyskusji na temat prawnych aspektów wykorzystania AI.

Dlaczego? Bo narzędzia, które wspiera sztuczna inteligencja coraz częściej wykorzystuje się w pracy zawodowej, co później ma przełożenie, chociażby na kwestie związane z prawem autorskim, czy patentowym. Nieumiejętne korzystanie z nowych technologii może sporo kosztować, dlatego warto przyjrzeć się bliżej niektórym kwestiom prawnym w kontekście używania sztucznej inteligencji.

CZYM JEST AI?

Nim przejdziemy do rozważań prawnych, na początku należy wyjaśnić, czym jest sztuczna inteligencja i jak ona się „uczy”. Obecna definicja mówi, że AI to algorytm, który posiada zdolność uczenia się. Mowa tu o tzw. uczeniu maszynowym, gdzie system wykonuje zadania na podstawie dostarczonych danych, co zastępuje klasyczne programowanie.

Proces uczenia maszynowego składa się z czterech etapów:

1. wprowadzenie źródła danych;
2. użycie danych do uzyskania rezultatu;
3. porównanie rezultatu z danymi kontrolnymi;
4. zapamiętanie rezultatów i użycie ich do kolejnej iteracji związanej z przetwarzaniem wprowadzonego zbioru danych.

Bazując na tej definicji AI rodzi się zatem pytanie, komu przysługuje prawo autorskie do dzieł, które powstały przy wsparciu np. takich narzędzi jak: ChatGPT, MidJourney, czy CoPilot?

Czy tworząc tekst lub obraz przy wsparciu AI możemy sobie do takiego utworu rościć prawa?

AI A PRAWO AUTORSKIE

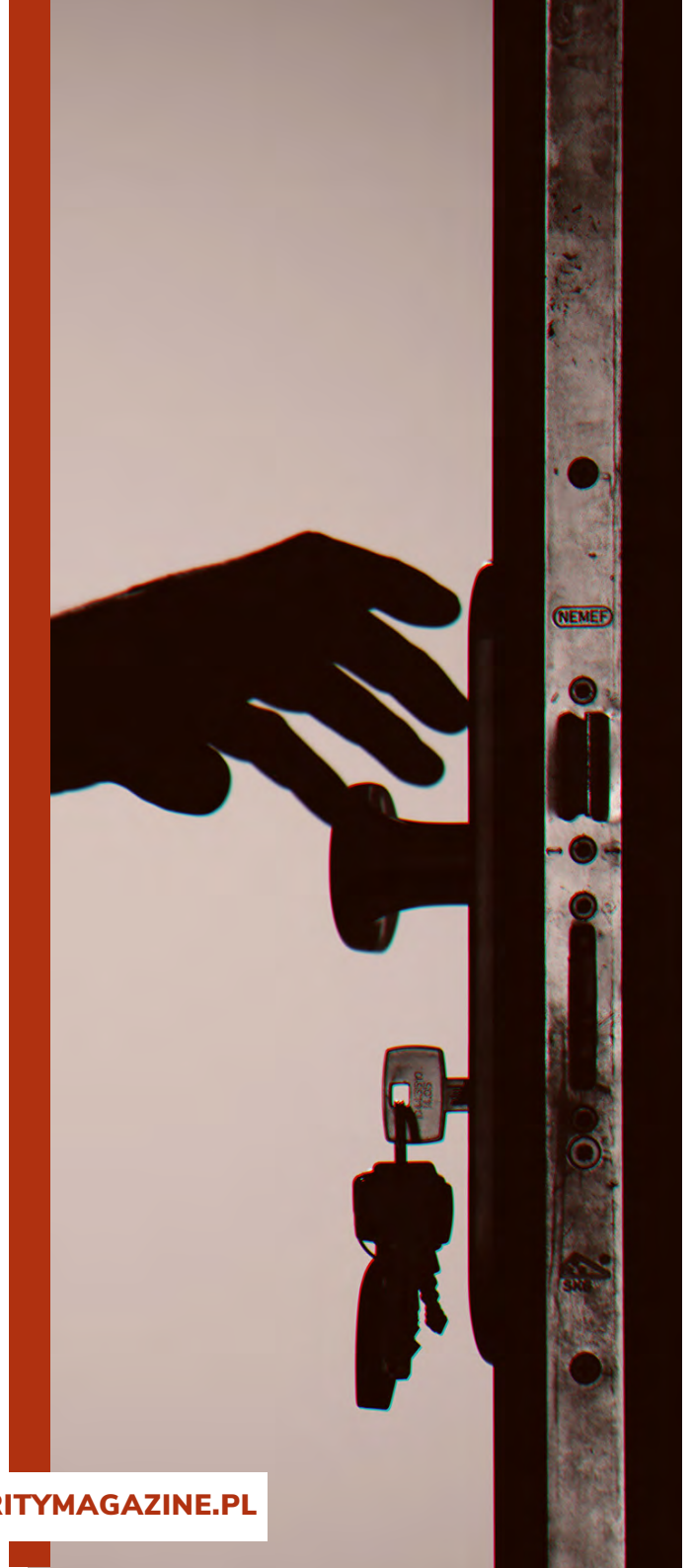
W takich przypadkach zwykle podnosi się, że zgodnie z prawem polskim, utworem podlegającym ochronie prawnej jest jedynie przejaw twórczej działalności człowieka. Co oznacza, że efekt działania „maszyny" nie stanowi utworu w myśl prawa autorskiego, więc dzieło stworzone przez AI nie podlega ochronie. Inaczej nieco wygląda sprawa, gdy mowa tu o pracy programisty. Co prawda może on posiadać prawo autorskie do kodu źródłowego, ale już nie do wytworów sztucznej inteligencji.

A co z użytkownikami, którzy dostarczają dane do narzędzia AI? Co do zasady, oni również nie będą posiadać praw autorskich do dzieła, ponieważ nie oni decydują o jego ostatecznym kształcie.

AI JAKO ASYSTENT?

Szukając wskazówek jak interpretować działanie AI w kontekście powstawania utworów można sięgnąć do orzecznictwa Sądu Najwyższego w sprawach gdy oceniał on pracę asystenta twórcy.

W sprawie, w której asystentka fotografa rościła sobie prawa autorskie do zdjęć, które technicznie zostały wykonane przez nią, ale to jej szef decydował o całej wizji artystycznej i sposobie wykonania zdjęć, Sąd Najwyższy uznał, że jej praca polegała na wykonaniu czynności pomocniczych, a co za tym idzie, nie można jej uznać za współautor-



kę fotografii.

Decyzję tę argumentowano tym, że współtwórczość w rozumieniu prawa autorskiego nie zachodzi, gdy współpraca nie ma charakteru twórczego lecz pomocniczy. Nie ma tu znaczenia fakt, że wykonywanie czynności pomocniczych wymagały wysokiego stopnia wiedzy fachowej, zręczności oraz inicjatywy osobistej.

Analogicznie można ocenić działanie AI – tj. jako pewnego rodzaju „pomocnika" twórcy.
W takich przypadkach, dla pewności, warto sobie jednak zadać trzy pytania:

- Czy dzieło, które powstało przy użyciu sztucznej inteligencji jest wynikiem twórczej działalności?
- Czy ma ono indywidualny charakter?
- Czy dzieło zostało ustalone w jakiejkolwiek postaci, pozwalającej na jego percepcję?

Odpowiedzi na powyższe pytania są w stanie pomóc ustalić czy powstałe dzieło jest utworem w rozumieniu polskiej ustawy o prawie autorskim.

PRAWO AMERYKAŃSKIE I BRYTYJSKIE

Inaczej do kwestii pomocy AI podchodzi prawo amerykańskie. Niedawno Urząd Praw Autorskich (USCO) wydał wytyczne dotyczące rejestracji utworów/praw autorskich w kontekście pracy wygenerowanej przez sztuczną inteligencję. Wśród nich znajdziemy m.in. zapis, który jasno mówi, że jeśli użytkownicy nie sprawują ostatecznej twórczej kontroli nad tym, jak system interpretuje prompty

i generuje materiał, to powstałe dzieło jest wytworem technologii, a nie człowieka.

Wyjątek stanowią sytuacje, gdy człowiek, wygenerowany przez AI materiał, przetworzy w wystarczająco kreatywny sposób. Wówczas ochronie prawnej podlegają te elementy, które są wytworem ludzkiej pracy.

Z kolei w Wielkiej Brytanii od lat funkcjonuje pojęcie tzw. utworów generowanych maszynowo. Są one objęte ochroną prawną, a prawa autorskie przysługują osobie, która podjęła niezbędne działania do jego wykonania.

CZY AI DOPUSZCZA SIĘ PLAGIATU?

Korzystanie z dzieł wygenerowanych przez sztuczną inteligencję w kontekście prawa autorskiego generuje jeszcze jedno ryzyko. Chodzi o naruszenie praw autorskich osób trzecich. Mając świadomość, że sztuczna inteligencja bazuje na nieograniczonej liczbie danych z sieci, istnieje duże prawdopodobieństwo, że wytwory AI będą plagiatem. Podobnie sprawa ma się z kodami źródłowymi na wolnych licencjach. Jeśli wykorzystywane są one do trenowania modeli AI, to istnieje prawdobieństwo naruszenia warunków licencji tego kodu.

AI A PRAWO WŁASNOŚCI PRZEMYSŁOWEJ

Debata nad wytworami AI w kontekście prawa nie odnosi się jedynie do prawa autorskiego, ale również do prawa własności przemysłowej. Z analizy, chociażby Europejskiego Urzędu Patentowego wynika, że przedmiotem patentu nie może być urządzenie lub narzędzie. To oznacza, że wpisywanie jej do zgłoszenia patentowego to pisanie się na problemy. Być może w takiej sytuacji warto siebie wpisać jako wynalazcę, a to czy rozwiązanie zostało stworzone przy pomocy AI potraktować jako sprawę drugorzędną.

Ponadto prawo własności przemysłowej mówi wprost, że za wynalazek nie uważa się w szczególności programów komputerowych i metod matematycznych. Odstępstwami od tej przesłanki są sytuacje, w których można wykazać tzw. dalszy efekt techniczny, czyli efekt, który wykracza poza „normalne” oddziaływanie fizyczne między programem komputerowym a komputerem, na którym oprogramowanie jest uruchamiane.

W przypadku metody matematycznej trzeba wy-

kazać, że zastrzeżenie dotyczy nie tylko czysto abstrakcyjnej metody matematycznej, ale wymaga też środków technicznych. Przy czym podczas oceniania wkładu metody matematycznej w technicznych charakter wynalazku, należy wziąć pod uwagę czy metoda ta, w kontekście wynalazku, wywołuje efekt techniczny służący celowi technicznemu.

RYZYKA PO STRONIE KONSUMENTÓW A AI

Dynamiczny rozwój sztucznej inteligencji powoduje, że z narzędzi wspieranych przez AI (głównie tych, które pomagają stworzyć tekst lub obraz) coraz częściej korzystają konsumenci. Z czasem skala będzie większa, ale już dziś można zdefiniować szereg zagrożeń, które wiążą się z wykorzystaniem sztucznej inteligencji przez konsumenta. Oto one:

- ryzyko manipulacji;
- wprowadzenie w błąd;
- dezinformacja;
- naruszenie prywatności.

Obecna rzeczywistość prawna konsumenta przed wytworami AI chroni na zasadach ogólnych. W związku z tym, w celu skutecznego dochodzenia roszczeń dany podmiot musi udowodnić:

- wysokość poniesionej szkody;
- winę osoby trzeciej;
- związek przyczynowy między działaniem lub zaniechaniem osoby a powstałą szkodą.

Takie uregulowanie zasad odpowiedzialności w kontekście AI powoduje, że obecnie dochodzenie roszczeń jest ekstremalnie trudne. Dlatego Komisja Europejska w 2022 roku opublikowała projekt dyrektywy w sprawie dostosowania przepisów dotyczącej pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji.

Dyrektywa ta wyróżnia: system sztucznej inteligencji i system sztucznej inteligencji wysokiego ryzyka. W odniesieniu do tego drugiego KE państwom członkowskim nakazuje wprowadzenie przepisów umożliwiających zabezpieczenie oraz ujawnienie dowodów dotyczących działania systemu sztucznej inteligencji wysokiego ryzyka. Ponadto dokument zakłada wprowadzenie wzruszalnego domniemania istnienia związku przyczynowego w przypadku winy. Proponowane przez Komisję przepisy mają ułatwić dochodzenie roszczeń odszkodowawczych związanych z działaniem AI.

KTO PONOSI ODPOWIEDZIALNOŚĆ?

Kolejną sprawą, którą należy poruszyć, jest kwestia odpowiedzialności za szkody, które może wyrządzić wytwór sztucznej inteligencji konsumentowi. Czy leży ona po stronie programisty, producenta, a może samego użytkownika?

Jeśli chodzi o programistę, tu w większości przypadków jego odpowiedzialność będzie ponoszona wyłącznie względem podmiotu, który zlecił mu pracę nad AI. Należy też pamiętać, że w przypadku, gdy program będzie posiadał ukryte błędy, które wyrządzają szkody wśród użytkowników, wówczas w niektórych przypadkach możliwe jest dochodzenie roszczeń od programisty przez producenta/dystrybutora w ramach tzw. odpowiedzialności regresowej.

W przypadku podmiotu wprowadzającego system na rynek obowiązuje odpowiedzialność zarówno kontraktowa jak i deliktowa.

Z kolei sam użytkownik ponosi odpowiedzialność deliktową. Chodzi tu np. o takie sytuacje gdy przy pomocy AI generuje on nieprawdziwy tekst o danej osobie i publikuje go jako treść zgodną z prawdą.

AI ACT

Kolejnym europejskim dokumentem regulującym kwestie AI jest AI Act, którego celem jest zapewnienie działania systemów sztucznej inteligencji w UE w sposób bezpieczny, przejrzysty, etyczny oraz kontrolowany przez człowieka.

AI Act ma za zadanie wprowadzić przepisy m.in. dotyczące wprowadzania do obrotu, oddawania do użytku oraz wykorzystywania systemów sztucznej inteligencji w całej Unii Europejskiej. Jednocześnie na jego mocy ustanowione mają zostać zakazy dotyczące określonych praktyk związanych z wykorzystaniem sztucznej inteligencji, szczególne wymogi dotyczące systemów AI wysokiego ryzyka, jak również wymogi w zakresie przejrzystości - w szczególności co do narzędzi AI mających wchodzić w interakcje z osobami fizycznymi. Rozporządzenie obejmuje również wymogi jakości zbiorów danych treningowych, walidacyjnych oraz testowych używanych do trenowania systemów AI, a także kwestie monitorowania narzędzi AI po ich wprowadzeniu do obrotu i nadzoru nad rynkiem. Komisja przyjęła w AI Act założenie, że narzędzia sztucznej inteligencji powinny zostać skategoryzowane pod względem ryzyka dla praw oraz wolności człowieka jakie wiąże się z ich używaniem, a im wyższe ryzyko, tym więcej obowiązków i obostrzeń.

WNIOSKI

Mając do czynienia z szybkim rozwojem algorytmów sztucznej inteligencji, a jednocześnie z brakiem aktualnych i wdrożonych rozwiązań prawnych dotyczących stricte AI trzeba szczególnie dokładnie oceniać ryzyko związane z używaniem, tworzeniem i wdrażaniem narzędzi AI.

Dlatego w sytuacji, kiedy sięgamy po sztuczną inteligencję w swoim projekcie, zawsze warto kierować się kierować się takimi zasadami działania jak transparentność, rozliczalność i bezpieczeństwo.

Tekst powstał na podstawie e-booka "Prawne aspekty Gen AI" autorstwa: Dominiki Wcisło, Aleksandry Maciejewicz, Mileny Balcerzak, Bartłomieja Serafinowicza., do pobrania ***TUTAJ****.*

ZAMÓW

AUDYT BEZPIECZEŃSTWA

I PRZEKONAJ SIĘ,
JAK OPTYMALIZACJA
PRZETWARZANIA DANYCH
MOŻE DAĆ
CI PRZEWAGĘ
KONKURENCYJNĄ

DOWIEDZ SIĘ WIĘCEJ!

Polityka® Bezpieczeństwa

NAJCZĘŚCIEJ SPOTYKANE USTERKI DYSKÓW TWARDYCH

Paweł Kaczmarzyk
Serwis komputerowy
Kaleron

Kiedy pojawia się temat usterek nośników danych, w pierwszej chwili przychodzą nam na myśl usterki mechaniczne i stukające dyski twarde. I przez dziesięciolecia faktycznie problemy związane z podsystemem mechanicznym dysków twardych były najważniejszą, najbardziej bolesną przyczyną awarii nośników danych.

Jeszcze 20 lat temu uszkodzenia elektroniczne można było naprawić przekładając śrubokrętem PCB od takiego samego dysku. Ale czasy się zmieniają i zmieniają się też nośniki danych oraz ich usterki.

ROLA OPROGRAMOWANIA UKŁADOWEGO W PRACY DYSKU TWARDEGO

W swoich początkach dyski twarde były stosunkowo prostymi urządzeniami. Podsystem mechaniczny odpowiadał za zapis i odczyt sygnału na powierzchniach magnetycznych talerzy i był sterowany przez relatywnie prosty kontroler. Dane były kodowane z wykorzystaniem metody FM (Frequency Modulation – modulacja częstotliwości) w późniejszym okresie zmodyfikowaną do MFM w celu uzyskania większej gęstości zapisu. Tym niemniej gęstość ta była na tyle mała, że dla wykrywania impulsów sygnału w zupełności wystarczała detekcja szczytów (peak-detection). Adresowanie danych polegało na bezpośrednim odwoływaniu się do fizycznych sektorów – tzw. adresacja CHS – od Cylinder, Sector, Head – czyli cylinder (grupa ścieżek o tym samym promieniu), sektor i głowica (jednoznacznie identyfikująca powierzchnię talerza).

Wiele zaczęło się zmieniać w latach '80. Upowszechnienie komputerów osobistych spowodowało wzrost zapotrzebowania na dyski, które można by było w takich komputerach montować. To czas otwarcia architektury komputerów IBM-PC, okres powstawania setek różnych producentów podzespołów, spośród których nieliczni działają do dziś, a wielu zdołało opracować jedynie pojedyncze modele produktów, oraz powstawania standardów zapewniających wzajemną kompatybilność podzespołów produkowanych przez różnych producentów. Światem dysków twardych do dziś rządzą dwa standardy – ATA i SCSI, które zostały opracowane w połowie lat '80.

TRANSLACJA ADRESACJI LOGICZNEJ NA FIZYCZNĄ

Istotną zmianą wprowadzoną przez standardy ATA i SCSI była adresacja w logicznych blokach – LBA (Logical Block Addressing). Adresacja ta polega na nadaniu wszystkim sektorom dysku numerów porządkowych od 0 kolejno aż do ostatniego, którego numer wynika pojemności dysku. Pozwoliło to odciążyć systemy plików i oprogramowanie od radzenia sobie z rosnącą różnorodnością dysków charakteryzujących się różną liczbą talerzy, ścieżek oraz sektorów na ścieżkę. Ale fizycznie wciąż trzeba te sektory odnajdywać. I to zadanie zostało scedowane na oprogramowanie układowe dysku.

Podsystem zajmujący się przeliczaniem adresacji LBA na adresację fizyczną dysku nazywa się translatorem. Działanie translatora powiązane jest także z obsługą defektów oraz operacjami remapowania (realokacji) uszkodzonych sektorów.

Dodatkowe skomplikowanie podsystemu translacji występuje w dyskach SMR, które zostały pokrótce opisane w **Security Magazine w numerze 6(15) 2023**. W przypadku tych dysków uszkodzenia translatora są prawdziwą plagą i dotyczą zwłaszcza drugiego poziomu translacji. I w przypadku dysków SMR podsystem translacji jest bardziej wrażliwy na wszelkie błędy podczas próby jego naprawy. Stąd przed jakąkolwiek próbą regeneracji translatora należy bezwzględnie zabezpieczyć stan wyjściowy.

Szczegóły działania translatorów dysków różnych producentów są różne i zmieniają się z kolejnymi generacjami modeli. Różnią się też szczegóły usterek, jakie mogą w nich wystąpić oraz objawy takich usterek. Częstym objawem uszkodzenia translatora jest rozpoznanie dysku z zerową pojemnością.
W przypadku urządzeń WD można też spotkać dyski rozpoznawane z poprawnym modelem i pra-

widłową pojemnością, które przy próbie odczytu sektorów zwracają błąd IDNF (nieprawidłowy identyfikator sektora). W przypadku bardzo dużej liczby takich błędów, często występujących na całej pojemności dysku, nie jest to uszkodzenie sektorów samych w sobie, a modułu oprogramowania układowego odpowiadającego za ich prawidłowe odnajdowanie.

Uszkodzenia translatora są bardzo często występują w dyskach Seagate pokolenia F3. W internecie łatwo można odnaleźć instrukcję naprawy tego uszkodzenia, jednak pochodzi ona z początkowego okresu produkcji tych dysków („czarna seria" 7200.11) i nie uwzględnia niuansów późniejszej ewolucji translatora. Poza tym w procedurze tej brakuje etapu zabezpieczenia translatora (pliku systemowego 0x28 – polecenie terminala T>r28).

W przypadku nieadekwatnego zastosowania tej procedury (bez odpowiedniej diagnostyki, w przypadku innego uszkodzenia lub nowszych modeli) istnieje ryzyko spowodowania uszkodzenia dysku polegającego na tym, że od pewnego sektora wszystkie kolejne przy próbie ich odczytu zwracają błąd nieprawidłowej sumy kontrolnej (UNC).

Także i w tym przypadku same sektory mogą być sprawne, a błędy spowodowane są nieprawidłowym ich adresowaniem. Objaw wynika z tego, że dyski Seagate pokolenia F3 przy obliczaniu sumy kontrolnej uwzględniają dla każdego sektora jego aktualny numer LBA.

Błąd podsystemu translacji powoduje, że od momentu jego wystąpienia nieprawidłowo wywoływane są wszystkie kolejne sektory, przez co ich sumy kontrolne są niezgodne.

ZARZĄDZANIE DEFEKTAMI

Produkcja wolnych od defektów talerzy dysków twardych jest niemożliwa. Dlatego konieczna jest ich odpowiednia obsługa. Dawno temu, przy niskiej gęstości zapisu i relatywnie małej liczbie defektów na etykietach dysków można było spotkać tabelki z wydrukowaną listą adresów uszkodzonych sektorów, które należało omijać. Taka tabelka zawierała też wolne miejsca, w które można było ołówkiem dopisać kolejne defekty, które mogły pojawić się w trakcie eksploatacji.

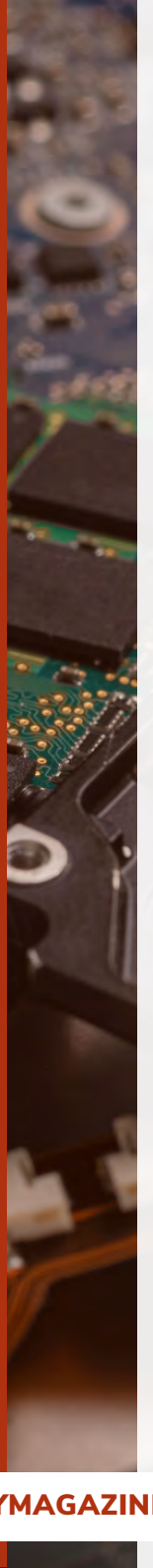
Omijanie uszkodzonych defektów było wówczas zadaniem systemów plików, które do tej pory obsługują funkcje pozwalające na odpowiednie zamarkowanie klastrów zawierających uszkodzone

sektory, aby nawet nie próbować umieszczać w nich plików. Ale wraz ze wzrostem gęstości zapisu i pojemności nośników rośnie także i liczba defektów, z którymi coś trzeba zrobić. Wprowadzenie adresacji LBA było doskonałą okazją, by oprogramowaniu układowemu przekazać kolejne zadanie.

Każdy dysk ma pewną liczbę defektów produkcyjnych – sektorów, które nie przechodzą testów fabrycznych. Ponieważ te sektory są uszkodzone, nie ma sensu przypisywać im adresów LBA. Są one rejestrowane na podstawowej liście defektów (lista P, odpowiednik adresów wydrukowanych na wspomnianej wyżej etykietce) i omijane przez translator przy nadawaniu numerów LBA.

Z kolei uszkodzone sektory, które pojawią się w czasie eksploatacji, są zapisywane na przyrostowej liście defektów (lista G, odpowiednik pustych rubryk w tabelce, do której można dopisywać nowe sektory). W wielu modelach dysków zarządzanie defektami jest bardziej skomplikowane, ale szczegółowe opisanie tego zagadnienia wykracza poza ramy niniejszego artykułu.

W przypadku uszkodzenia sektora w czasie eksploatacji dysku jest on remapowany. Operacja ta polega na wpisaniu adresu fizycznego tego sektora na wspomnianą wyżej przyrostową listę defektów oraz przypisaniu jego adresu LBA innemu sektorowi leżącemu na ścieżce rezerwowej.

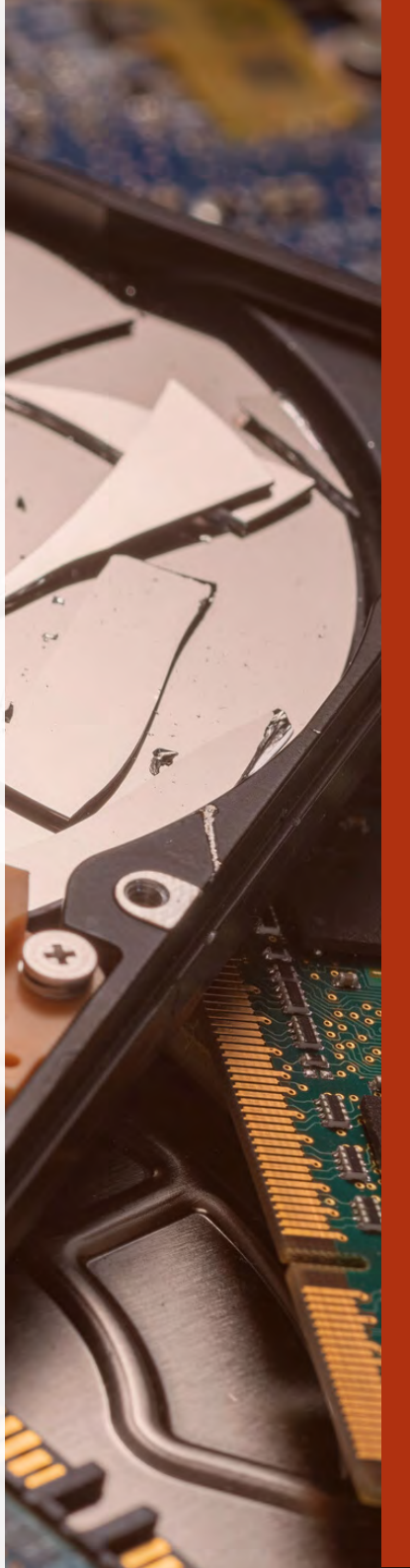


Początkowo operację remapowania trzeba było wymuszać ręcznie, ale ok. 20 lat temu została ona zautomatyzowana. Sam fakt autorealokacji uszkodzonych sektorów poza kontrolą użytkownika budził wówczas duże kontrowersje ze względu na bezpieczeństwo danych oraz obawy co do możliwości przegapienia objawów degradacji powierzchni.

Automatyzacja procesu remapowania uszkodzonych sektorów wymagała zaimplementowania algorytmów optymalizujących ten proces. Z jednej strony zbyt szybkie reakcje i remapowanie od razu każdego sektora sprawiającego jakikolwiek problem mogły doprowadzić do obniżenia wydajności dysku i przedwczesnego wyczerpania puli sektorów zapasowych. Z drugiej – konsekwencjami reakcji spóźnionych mogły być destabilizacja struktur logicznych i uszkodzenie danych.

Wówczas w oprogramowaniu układowym dysków zaczęły się pojawiać listy sektorów niestabilnych. Trafiały tam sektory, które sprawiały problemy swoim zachowaniem, ale jeśli te problemy miały charakter incydentalny (to były jeszcze czasy mało odpornego na efekt superparamagnetyzmu zapisu równoległego oraz powszechnego wykorzystania niskiej klasy zasilaczy podających bardzo niestabilne napięcia), nie były remapowane. Operacja realokacji była przeprowadzana dopiero wtedy, kiedy z danym sektorem wiązały się powtarzalne problemy, co świadczyło, że stoi za nimi coś więcej od jedynie nieprawidłowego namagnesowania.

Listy związane z obsługą defektów również mogą być przyczyną awarii dysku. Jeśli wystąpią błędy w ich zawartości, mogą być one pierwotną przyczyną uszkodzenia translatora. Problemem jest też przepełnianie list. Jeśli któraś z list się przepełni, próby dopisania do niej kolejnych adresów kończą się niepowodzeniem, ale obsługa takiego błędu zajmuje czas i zwykle powoduje zawieszanie dysku. W szczególności dotyczy to



przepełniania listy sektorów niestabilnych (lista relo, moduł 0x32) dysków WD, co skutkuje bardzo wolną odpowiedzią dysku na otrzymywane polecenia.

W przypadku wystąpienia problemu objawiającego się zawieszaniem dysku podczas pracy należy wyłączyć opcję autorealokacji. Wskazane jest także wyczyszczenie listy sektorów niestabilnych. Po wykonaniu tych czynności należy wykonać kopię posektorową i odzyskać dane z kopii. Sam dysk z takimi objawami nadaje się tylko do utylizacji, gdyż jednoznacznie świadczą one o daleko posuniętej degradacji powierzchni.

INNE PROBLEMY OPROGRAMOWANIA UKŁADOWEGO

W dyskach twardych mogą wystąpić także inne problemy oprogramowania układowego, ale szczegółowe wyczerpanie tematu, to materiał na kilka tomów, a nie na artykuł. W przypadku niektórych uszkodzeń, jak wspomniane wyżej zagadnienia dotyczące podsystemu translacji i zarządzania defektami, problem dotyczy modułów unikatowych dla każdego egzemplarza dysku, o które trzeba walczyć, jak o niepodległość.

Czasem uszkodzenia są o tyle łatwiejsze do naprawy, że mogą dotyczyć fragmentów kodu wykonywalnego, które można skopiować z innego dysku. Niektóre uszkodzenia dotyczą modułów mało istotnych dla działania dysku, jak np. logi systemu SMART.

SMART służy do monitorowania stanu dysku i ostrzegania użytkownika w przypadku wykrycia symptomów wskazujących na zbliżającą się awarię. Ale dla samego działania dysku i dostępu do danych nie jest on niezbędny i błędy w jego obszarze przeważnie nie rzutują na pracę dysku. Inaczej rzecz się miała we wczesnych modelach Seagatów pokolenia F3, gdzie przepełnienie logów SMART prowadziło do zawieszania dysku przy jego uruchomieniu i utraty dostępu do danych. Aby rozwiązać ten problem, należy wyczyścić SMART (polecenie terminala 1>N1). Przy okazji warto zwrócić uwagę, że wyczyszczenie logów SMART jest operacją bezpieczną dla zawartości dysku i jego funkcjonowania, także względnie prostą do przeprowadzenia. Dlatego nie powinno się nim sugerować, kupując dyski z rynku wtórnego. Czyszczenie logów SMART jest też standardowym elementem procedury serwisowej producentów dysków twardych. Stąd bez trudu można znaleźć oferty dysków sprzedawanych jako nowe, choć oznaczenia na etykietach typu „Certified Repaired" lub „Refurbished" jednoznacznie wskazują, że są to dyski poserwisowe.

Polityka® Bezpieczeństwa

ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE

SPRAWDŹ OFERTĘ

WYCIEKI DANYCH W FIRMACH. CZY CZŁOWIEK JEST NAJWIĘKSZYM ZAGROŻENIEM?

Rafał Stępniewski
Rzetelna Grupa

Bezpieczeństwo danych jest kluczowym elementem funkcjonowania każdej firmy. Rafał Stępniewski, specjalista w dziedzinie bezpieczeństwa, prezes Rzetelnej Grupy, redaktor naczelny "Security Magazine" analizuje najczęstsze przyczyny wycieków oraz podkreśla rolę człowieka w tym procesie. Jakie działania mogą pomóc firmom w zabezpieczeniu się przed potencjalnymi zagrożeniami?

Jakie są najczęstsze przyczyny wycieków danych w firmach?

Rafał Stępniewski: To najczęściej brak świadomości, ignorowanie lub bagatelizowanie zagrożeń, nie stosowanie się do procedur, nie wyciąganie wniosków z wpadek swoich lub innych, nadmierna pewność siebie i nieuwaga, ale też nadmierne zaufanie do dostawców lub partnerów biznesowych.

Większość przyczyn wynika z wewnątrz. Ktoś kliknął w link, włożył pendrive z niewiadomego źródła, zainstalował darmowe świetne oprogramowanie na swoim urządzeniuu - bo mógł, ktoś odłożył na później aktualizację oprogramowania, bo nie ma czasu, bo laptop będzie wolniej działał lub usługa serwerowa będzie niedostępna albo, co gorsza, update może spowodować jej niedziałanie np. naszego sklepu lub CRM, a nie mamy środowiska testowego, by to sprawdzić.

Pomijam tak oczywiste przyczyny, jak wyrzucanie wydruków z danymi do kosza na śmieci, albo proste czy przewidywalne hasła dostępowe, używane w wielu systemach - czasem hasła uniwersalne tj, takie same, bo łatwiej zapamiętać jedno hasło i logować się nim np. do CRM, do banku, portali społecznościowych itp.

Nie bez powodu człowiek jest najsłabszym ogniwem w całym procesie bezpieczeństwa. Gubi nas rutyna i nieuwaga oraz zaufanie do tego, co czasem bezrefleksyjnie czytamy lub wi-

dzimy.

Od paru lat trend Zero Trust nabiera na znaczeniu. Oczywiście, duże firmy coraz częściej stosują takie podejście, ale wśród małych i średnich jest to często pojęcie abstrakcyjne. Skala, zakres oraz możliwości wdrażania metodologii Zero Trust w takich firmach jest inne, ale samo podejście do myślenia o bezpieczeństwa w firmie w taki sposób może wiele zmienić na plus.

Które sektory są najbardziej narażone na wyciek danych? Czy jest na to jakaś reguła?

R.S.: Nie ma dzisiaj firmy, która nie jest narażona na atak czy też na wyciek informacji. Musimy pamiętać o tym, że większość ataków jest automatyczna. Wystarczy wybrać daną podatność, wybrać skuteczną i efektywną metodę ataku i rozpocząć szukanie potencjalnych ofiar. Zdarzają się, oczywiście, spektakularne ataki na duże korporacje i firmy, które z reguły planuje się skrupulatnie, ale jeżeli mówimy o małych i średnich przedsiębiorcach, to tu działa automat i szukanie tych, którzy nie są wystarczająca zabezpieczeni. Oni są bardziej podatni na takie automatyczne ataki niż duże korporacje.

Skala jest inna i potencjalne zyski dla przestępcy są inne. Mając na uwadze skalę jednej zaatakowanej firmy, ale mnożąc to przez ilość potencjalnych ofiar ataków i większą efektywność względem kosztów, jakie musi ponieść taki haker, jest to równie atrakcyjny obszar działania. Branża nie ma tu większego znaczenia.

Niestety, panuje mit w tym zakresie - nie jestem dużą firmą z milionami USD dochodu, więc jestem bezpieczny - nikt mnie nie będzie atakował, bo nie ma w tym interesu. Jest to błędne podejście. Wystarczy zadać sobie pytania: co zrobię, kiedy

stracę całkowicie dane z kluczowego systemu informatycznego, jaki funkcjonuje w mojej firmie, albo co się stanie, gdy ktoś mi te dane wykradnie - jak będzie wyglądał kolejny dzień w mojej firmie, jak wpłynie to na ciągłość działania mojej firmy.

W jaki sposób firmy mogą monitorować oraz wykrywać potencjalne wycieki danych w czasie rzeczywistym?

R.S.: Są, oczywiście, takie możliwości. W rozsądnym budżecie można zakupić oprogramowanie do firmy, które będzie za nas pilnować w czasie rzeczywistym, czy nie mamy wycieku. Dotyczy to strony serwerowej, jak i stacji roboczych naszych pracowników. Są programy, które wykrywają niepożądany ruch na zasadzie geolokalizacji. Jeżeli nasz komputer chce wysyłać pakiety danych do krajów o podwyższonym ryzyku, program taki zablokuje ten ruch oraz wyśle ostrzeżenie.

Ochronić nas to może przed sytuacją, gdy padniemy ofiarą zarówno phisingu, czyli na przykład klikniemy link w otrzymanym mailu i będziemy przekierowani na stronę na serwerach nie znajdujących się w bezpiecznej strefie. Również w przypadku zainfekowania komputera malware lub innymi, oprogramowanie wykryje niepożądany ruch i zablokuje go.

W przypadku serwerów, tu również możemy mieć narzędzia monitorujące niestandardowe zachowania, które zostaną zablokowane na poziomie sieciowym. Monitorować możemy zarówno system operacyjny, połączenia przychodzące i wychodzące, a także bazę danych w zakresie ilości danych jakie są z niej pobierane.

Dzisiejsze narzędzia dodatkowo są wspierane coraz częściej przez AI, które pozwala na analizę zachowań naszego systemu i użytkowników, w celu zapobiegania tego typu niepożądanym zjawiskom w czasie rzeczywistym.

Jakie konsekwencje grożą firmom za niewłaściwe przechowywanie danych?

R.S.: Zaczynając od tych najbardziej oczywistych, jakimi są kary administracyjne, w przypadku niedochowania należytej staranności w zakresie spełniania przepisów sektorowych, w tym między innymi RODO. Tu ze względu na skalę zaniedbań i oporu w zakresie współpracy z organami, kary mogą sięgać w zależności od wielkości biznesu nawet kilku milionów złotych.

Kolejnym aspektem są potencjalne pozwy lub kary umowne wynikające z kontraktów, których nie będziemy mogli realizować albo które wręcz mogą wymagać od nas zachowania poufności.

Inny aspekt konsekwencji to problemy z ciągłością działania firmy i utrata wiarygodności na rynku względem klientów lub kontrahentów. Budowany przez lata wizerunek i zaufanie może być zaprzepaszczony w ciągu paru chwil na skutek zaniechań i wpadki.

O ile kwestie kar i ryzyko ich nałożenia można oszacować, to w przypadku kosztów, jakie będzie musiała firma ponieść na odbudowanie zaufania, może być problem z oszacowaniem - zwłaszcza przez pryzmat konkurencji, która może wykorzystać naszą słabość w danej chwili.

Jakiego typu szkolenia powinni przechodzić pracownicy, by zminimalizować ryzyko wycieku danych?

R.S.: Mając na uwadze, że to człowiek jest najsłabszym ogniwem szeroko rozumianego bezpieczeństwa, rola szkoleń pracowników jest bardzo ważna. Szkolenia powinny obejmować swoim zakresem zarówno budowanie świadomości, jak i pogłębianie wiedzy, jaką powinni dysponować pracownicy.

Zakres takich szkoleń powinien obejmować między innymi podstawy teoretyczne, ale również część praktyczną.

W teorii możemy wiedzieć, czym jest np. phishing, ale ważne jest aby w praktyce wiedzieć, jak się przed nim bronić. Istotne jest również to by wiedzieć, jak postępować w sytuacji, jeśli padniemy ofiarą takiego phishingu - tu powinny zadziałać procedury opracowane wewnątrz danej firmy, a pracownicy powinni je znać i nie powinni mieć obaw w zakresie ich stosowania.

Mam tu na myśli sytuację, gdzie pracownik woli nie przyznać się do tego, że nastąpiło jakieś naruszenie, ponieważ boi się konsekwencji. Ważne jest, aby zbudować odpowiednią kulturę organizacji w tym zakresie i przestawić myślenie zarówno na poziomie szeregowym, jak i kadry zarządzającej. Priorytetem jest bezpieczeństwo firmy i jej zasobów.

Istotnym elementem szkoleń są kontrolowane testy, tj. sprawdzanie odporności organizacji na wybrane wektory ataków. Odbywa się to w sposób kontrolowany, a pracownicy są poddawani takim testom, nie będąc świadomym. Dla firmy jest to bardzo cenne doświadczenie i w rezultacie może okazać się dużo tańsze niż prawdziwy atak. W ten sposób firma może zidentyfikować obszary, jakie należy zabezpieczyć, na co położyć nacisk w szkoleniach pracowników.

Kolejnym ważnym elementem są zmiany w zakresie sposobów ataków i nowych zagrożeń. U swoich podstaw ataki bazują na sprawdzonych metodach i tu się zmienia niewiele, ale formy i sposoby ewoluują. Pracownicy powinni być na bieżąco z trendami, a rolą osób odpowiedzialnych za bezpieczeństwo jest dopilnowanie tego, by pracownicy firmy byli świadomi nowych form ataków.

Jakie kroki powinna podjąć firma po wykryciu wycieku danych? Dlaczego tak wiele firm nie robi nic po wycieku?

R.S.: Jeżeli firma padła ofiarą ataku powinna uruchomić procedury na tę okoliczność. Jeżeli nie ma wypracowanych metod działania w tego typu sytuacjach, wówczas mamy do czynienia z chaosem, stratą cennego czasu, a ryzyko dalszych szkód może diametralnie rosnąć.

Procedura postępowania w dużym uproszczeniu powinna polegać na zabezpieczeniu źródła wycieku, zbieraniu jak największej ilości informacji o okolicznościach, a także o zakresie informacji jakie wyciekły. Kolejnym krokiem jest oszacowanie skali wycieku, szacowaniu ryzyk dla firmy, jakie mogą z tego wynikać, analiza informatyczna oraz prawna. Te wszystkie rzeczy powinny dziać się niemal równolegle. Koniecznym jest współpraca wielu obszarów kompetencyjnych w firmie, a cel powinien być jeden - minimalizacja strat oraz zachowanie ciągłości prowadzonego biznesu. Najgorszą rzeczą, jaka może się wydarzyć w tym momencie, to skupianie się na przerzucaniu się winą albo ignorowanie problemu.

Odpowiadając na drugie pytanie - nie powiedziałbym, że firmy bagatelizują wycieki. Wiele firm nie wie, jak ma postępować i działa na zasadzie gaszenia pożaru. Skupiają się wówczas jedynie na wybranych elementach np. odzyskania danych z backupu - o ile takie mają - załataniu “dziury”, przez którą doszło do wycieku. Bardzo często pomijają inne ważne aspekty tj. analiza i ryzyko prawne, ryzyko ponownego wycieku, ryzyko biznesowe wynikające z wycieku. Często firmy mają problem z oszacowaniem zakresu wycieku tj. jakie informacje i dane wyciekły oraz jak długo osoby trzecie miały nieuprawniony dostęp.

Często brakuje również konsekwencji w dalszych działaniach. Mamy wyciek, usunęliśmy jego źródło i na tym często jest koniec. Nie przychodzi refleksja, jak w przyszłości nie dopuszczać do tego sytuacji, a jeżeli przyjdzie to w niewystarczającym zakresie. Mam na myśli np. jedynie zakup jakiegoś oprogramowania, które ma być złotym środkiem oraz ma firmę zabezpieczyć w danym obszarze. Niestety, nie jest to gwarancja, że nie przydarzy się to ponownie.

Powodów tego jest wiele - inny wektor ataku, brak regularnych testów skuteczności danego rozwiązania, brak kompleksowego szeroko rozumianego podejścia do bezpieczeństwa.

I na zakończenie, czy zaniedbania w zakresie bezpieczeństwa informacji mogą mieć poważne konsekwencje dla firmy?

R.S.: Informacja dziś stanowi często zasób firmy - na równi z maszyną produkcyjną, budynkiem, biurkiem. Mogą nią być zarówno dane klientów, umowy, warunki współpracy, receptury, know-how. Zasoby fizyczne zabezpieczamy, poddajemy konserwacji oraz regularnym przeglądom, a pracowników szkolimy jak mają ich używać zgodnie z zasadami oraz przeznaczeniem.

Można pójść dalej - maszyna i budynek mogą okazać się bezużyteczne, jeżeli nie będziemy mieli klientów i systemów IT do obsługi procesów z tym związanych. Czy patrząc na informację w firmie przez ten pryzmat, możemy sobie pozwolić na zaniedbania w zakresie bezpieczeństwa?

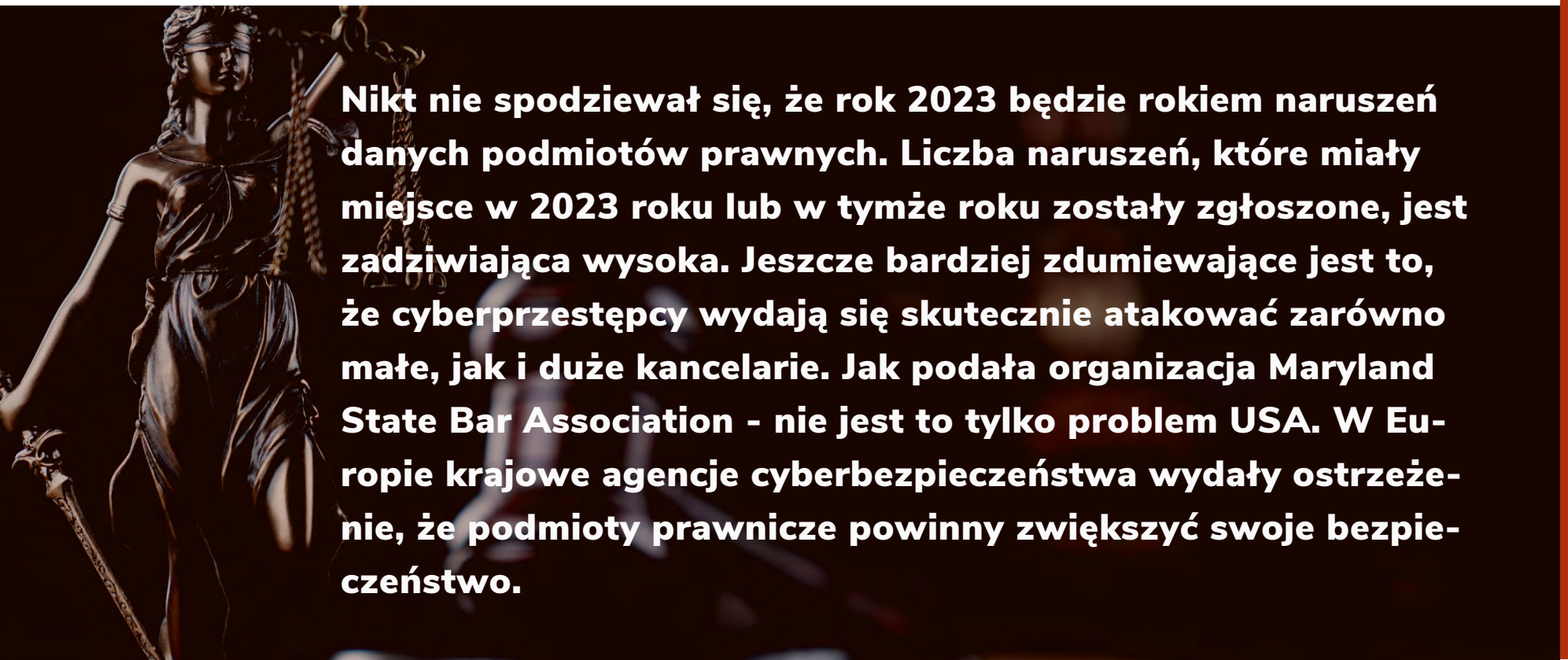
I z tym pytaniem zostawiamy naszych Czytelników.

Dziękuję za rozmowę.


Rzetelny Regulamin®
Kompleksowa obsługa prawna Twojego e-commerce

CYBERZAGROŻENIA W BRANŻY PRAWNICZEJ

Redakcja
SECURITY MAGAZINE



Nikt nie spodziewał się, że rok 2023 będzie rokiem naruszeń danych podmiotów prawnych. Liczba naruszeń, które miały miejsce w 2023 roku lub w tymże roku zostały zgłoszone, jest zadziwiająca wysoka. Jeszcze bardziej zdumiewające jest to, że cyberprzestępcy wydają się skutecznie atakować zarówno małe, jak i duże kancelarie. Jak podała organizacja Maryland State Bar Association - nie jest to tylko problem USA. W Europie krajowe agencje cyberbezpieczeństwa wydały ostrzeżenie, że podmioty prawnicze powinny zwiększyć swoje bezpieczeństwo.

ZMIENIAJĄCY SIĘ KRAJOBRAZ CYBERZAGROŻEŃ

Jeszcze w 2017 roku, według ankiety ABA Legal Technology, aż 22% podmiotów prawnych doświadczyło włamań lub naruszeń danych. Szczególnie narażone były małe kancelarie z 10-49 prawnikami (35% doświadczyło ataków) oraz średniej wielkości kancelarie z 50-99 prawnikami (33% doświadczyło włamań). Chociaż nie wszystkie te ataki prowadziły do nadużycia danych o klientach, to stanowiły one znaczące zagrożenie w zakresie nieautoryzowanego dostępu do ich wrażliwych danych.

W miarę jak technologia ewoluuje, tak samo robią cyberprzestępcy, dostosowując swoje metody ataku do nowych technologii i praktyk. Współczesne ataki są bardziej zaawansowane i ukierunkowane, co sprawia, że są trudniejsze do wykrycia i zwalczania. Podmioty prawne, które przechowują wrażliwe dane klientów, takie jak informacje finansowe, dane osobowe oraz poufne dokumenty, stały się atrakcyjnym celem dla cyberprzestępców.

- Cyberbezpieczeństwo w branży prawnej nie jest już luksusem, ale koniecznością. Liczba ataków wciąż rośnie, ale świadomość klientów na temat cyberzagrożeń - również. Dlatego podmioty prawne muszą podjąć konkretne kroki, aby chronić swoje dane i reputację. To nie tylko kwestia technologii, ale także kultury organizacyjnej i edukacji - powiedział **Rafał Stępniewski, prezes firmy Rzetelna Grupa oferującej usługi prawne dla biznesu, redaktor naczelny "Security Magazine" i właściciel marki Polityka Bezpieczeństwa.**

Dodał, że dziś podmioty prawne są skarbnicami wrażliwych informacji, które, jeśli zostaną naruszone, mogą mieć katastrofalne skutki zarówno dla klien-

tów, jak i dla samego podmiotu: - *Kancelarie muszą być bardziej czujne niż kiedykolwiek wcześniej oraz inwestować w zaawansowane rozwiązania związane z cyberbezpieczeństwem. Współpraca z ekspertami w dziedzinie bezpieczeństwa jest nie tylko zalecana, ale zwyczajnie obowiązkowa.*

Branża prawna stoi obecnie przed wyzwaniami związanymi z cyberbezpieczeństwem, które nie były wcześniej tak wyraźnie widoczne.

W USA w 2023 roku do lipca złożono aż pięć pozwów zbiorowych przeciwko kancelariom prawnym (choć dwa z nich zostały wycofane). Podstawa? Kancelarie prawne nie miały właściwych zabezpieczeń, aby chronić swoje dane przed cyberatakami.

"Zaskoczyło nas, jak wiele mniejszych firm zgłosiło naruszenia danych w 2023 r. Z pewnością muszą zwiększyć swoje zaangażowanie w cyberbezpieczeństwo, zwłaszcza w świetle mnożących się pozwów zbiorowych. W ubiegłym roku nastąpił 154% wzrost federalnych pozwów zbiorowych dotyczących naruszenia danych. Średnia pozwów przed tym trendem wynosiła 13 miesięcznie - obecnie wzrosła do 33 miesięcznie" - podała amerykańska organizacja prawnicza Maryland State Bar Association.

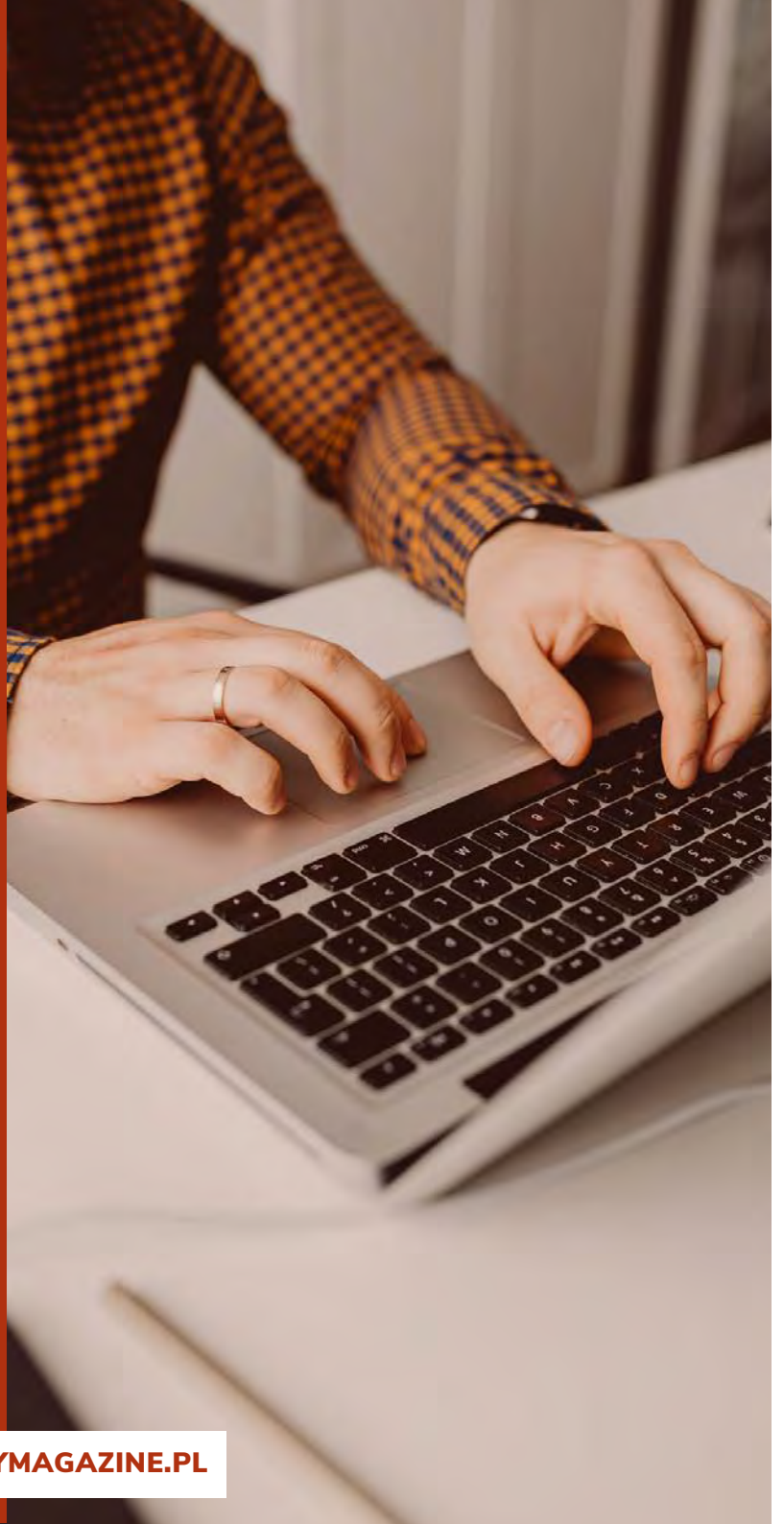
Ponadto Checkpoint Research poinformował w kwietniu tego roku, że cyberataki wzrosły o 7% w pierwszym kwartale 2023 roku w porównaniu z pierwszym kwartałem 2022 roku. Co ciekawe, jeden na każde 40 ataków był skierowany przeciwko kancelarii prawnej.

NAJCZĘSTSZE CYBERZAGROŻENIA W BRANŻY

Przechowywanie wrażliwych informacji klientów, zarówno indywidualnych, jak i korporacyjnych, sprawia, że kancelarie są atrakcyjnym celem dla różnego rodzaju ataków. Poznanie i zrozumienie najczęstszych cyberzagrożeń jest kluczowe, by zapewnić im skuteczną ochronę i utrzymać zaufanie klientów.

Ataki typu phishing

Phishing to technika, w której przestępcy próbują zdobyć wrażliwe informacje, takie jak dane logowania lub informacje o kartach kredytowych, poprzez podszywanie się pod wiarygodne źródło. Podmioty prawne, które regularnie przesyłają i odbierają wrażliwe informacje od klientów, są szcze-



gólnie narażone na tego typu ataki. Przestępcy często tworzą fałszywe e-maile, które wyglądają jak autentyczne wiadomości od klientów, próbując skłonić pracowników kancelarii do ujawnienia poufnych informacji lub kliknięcia na zarażone linki.

Zhakowane konta e-mail

Kiedy przestępcy zdobywają dostęp do konta e-mail pracownika kancelarii, mogą wykorzystać go do kradzieży wrażliwych informacji, przeprowadzenia ataków na innych pracowników lub klientów, a nawet do manipulowania toczącymi się sprawami. Ponieważ wiele kancelarii prawnych polega na komunikacji e-mailowej w swojej codziennej pracy, zhakowane konta e-mail mogą prowadzić do poważnych naruszeń danych.

Ransomware

Ransomware to rodzaj złośliwego oprogramowania, które szyfruje dane na komputerze ofiary, uniemożliwiając dostęp do nich, dopóki nie zostanie zapłacony okup. Podmioty prawne, które przechowują wrażliwe informacje klientów, są atrakcyjnym celem dla przestępców stosujących ransomware. Nawet jeśli zdecyduje się zapłacić okup, nie ma gwarancji, że dane będą odszyfrowane lub że przestępcy nie będą próbowali ponownie zaatakować w przyszłości.

Naruszenie danych

Kancelarie prawne przechowują ogromne ilości wrażli-

wych informacji, od danych osobowych klientów po poufne dokumenty prawne. Naruszenie tych danych może prowadzić do poważnych konsekwencji prawnych, finansowych i reputacyjnych. Wycieki danych mogą wynikać z wielu przyczyn, od ataków zewnętrznych po błędy ludzkie wewnątrz organizacji.

Zarzuty zaniedbania

Cyberbezpieczeństwo stało się kluczowym zagadnieniem, dlatego podmioty prawne muszą być bardziej ostrożne niż kiedykolwiek wcześniej. Jeśli nie podejmują odpowiednich środków ostrożności, aby chronić dane swoich klientów, mogą zostać oskarżone o zaniedbanie. Takie zarzuty prowadzą do poważnych konsekwencji prawnych, w tym do pozwów zbiorowych i wysokich odszkodowań.

Przykładami zaniedbań w tym zakresie są te, które doczekały się choćby decyzji prezesa **Urzędu Ochrony Danych Osobowych**. I choć nie dotyczą one bezpośrednio cyberataków, to są efektem zaniedbań, które jednak się zdarzają. I tak:

- w czerwcu 2021 roku zapadła decyzja prezesa UODO dotycząca naruszenia ochrony danych osobowych przez Fundację Promocji Mediacji i Edukacji Prawnej Lex Nostra, która nie zgłosiła naruszenia w ciągu 72 godzin oraz nie zawiadomiła o tym fakcie osób, których dotyczyło naruszenie. Dane fundacja utraciła w związku z kradzieżą teczek zawierających te dane, ale uznała, że nie jest to sprawa priorytetowa. Kara wyniosła prawie 14 tys. zł.
- w maju tego roku prezes Urzędu Ochrony Danych Osobowych nałożył administracyjną karę pieniężną w wysokości ponad 23 tys. zł na Rzecznika Dyscyplinarnego Izby Adwokackiej w Warszawie w związku z naruszeniem przepisów RODO poprzez niewdrożenie odpowiednich środków technicznych oraz organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych osobowych.
- również w maju tego roku prezes UODO nałożył na Prokuraturę Rejonową administracyjną karę pieniężną w wysokości 20 tys. zł za niezawiadomienie organu o naruszeniu ochrony danych osobowych oraz niezawiadomienie osób, których dane objęto naru-

szeniemniem. Prokuratura przekazała lokalnemu dziennikarzowi w ramach odpowiedzi na wniosek złożony w trybie ustawy o dostępie do informacji publicznej niezanonimizowanej dokumentacji z zakończonego postępowania. Dziennikarz ten opublikował je w lokalnym serwisie internetowym, anonimizując wcześniej dane osobowe.

NAJCZĘSTSZE BŁĘDY PODMIOTÓW PRAWNYCH W ZAKRESIE CYBERBEZPIECZEŃSTWA

Chociaż wiele z nich inwestuje w zaawansowane technologie zabezpieczające, nadal popełniają one pewne podstawowe błędy, które mogą narażać je na poważne ryzyko. Najczęstsze błędy w tym zakresie to:

- **Zbyt duże poleganie na zabezpieczeniach zewnętrznych.** Jednym z najczęstszych błędów popełnianych przez kancelarie prawne jest zakładanie, że jedynym sposobem na minimalizację szkód wynikających z ataków cybernetycznych jest wdrożenie zewnętrznych technologii zabezpieczających, takich jak zapory ogniowe czy oprogramowanie antywirusowe. Chociaż takie zabezpieczenia są niezbędne, ich skuteczność jest ograniczona, jeśli atakujący znajdzie sposób na ich obejście.
- **Korzystanie z otwartych modeli zabezpieczeń.** Wiele kancelarii prawnych korzysta z otwartych modeli zabezpieczeń, które udostępniają wszystkim pracownikom swobodny dostęp do wrażliwych informacji klientów. W dzisiejszym środowisku bezpieczeństwa ryzyko związane z takim modelem, w którym przestępca zdobywający dane uwierzytelniające dowolnego użytkownika ma dostęp do wszystkich informacji klienta kancelarii, jest zbyt duże.

- **Brak polityki przechowywania danych.** Wielu kancelariom prawnym brakuje polityki przechowywania danych. Firmy, które nie mają takich polityk, często zachowują wszystkie dokumenty i inne dane klienta, które posiadają. Może to prowadzić do nadmiernego gromadzenia danych, umożliwiając cyberprzestępcom kradzież wrażliwych dokumentów klienta z przeszłości.
- **Brak odpowiedniego szkolenia i świadomości**. Jednym z najczęstszych błędów popełnianych przez kancelarie prawne jest niedostateczne szkolenie i budowanie świadomości wśród pracowników, również tych, którzy prawnikami nie są. Ataki typu phishing czy inne zaawansowane metody są skuteczne, gdy pracownicy nie są świadomi zagrożeń i nie wiedzą, jak się przed nimi chronić.
- **Brak silnej technologii zarządzania informacjami.** Kancelarie prawne mogą ograniczyć szkody wynikające z ataków, które przeniknęły przez ich zabezpieczenia zewnętrzne, wdrażając silne technologie zarządzania informacjami. Takie technologie umożliwiają podmiotom prawnym zapewnienie, że użytkownicy muszą się odpowiednio uwierzytelnić, aby uzyskać dostęp do informacji, oraz że mogą uzyskiwać dostęp tylko do informacji, które są dla nich istotne.

Konsekwencją braku reakcji lub niesprostaniu wyzwaniom związanym z atakami wymierzonymi w stronę kancelarii prawnej, jest też utrata zaufania klientów.

- Zaufanie w kontekście relacji klient - kancelaria prawna to nie tylko podstawa, a wręcz filar, na którym opiera się cała współpraca. Tam, gdzie w grę wchodzą nie tylko skomplikowane kwestie prawne, ale przede wszystkim ludzkie losy, historie i tajemnice, zaufanie staje się walutą, której wartości nie

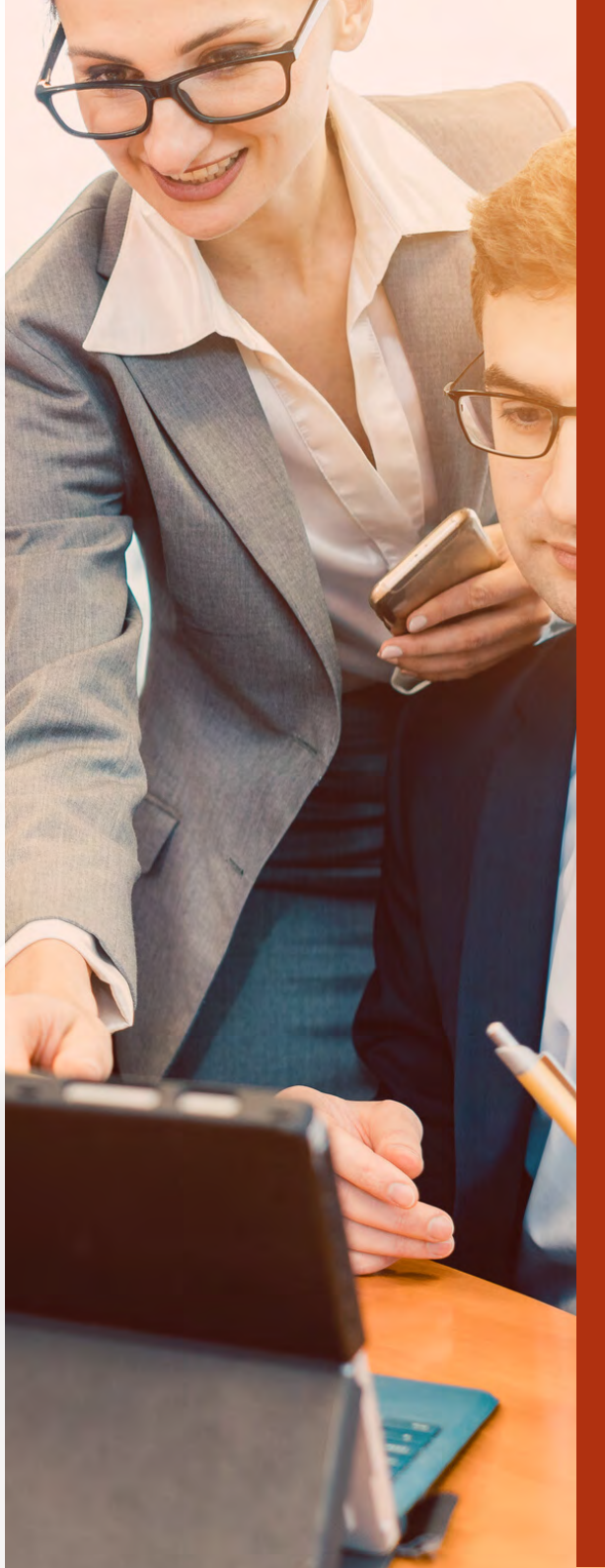
można przecenić. Klienci powierzają prawnikom nie tylko swoje sprawy, ale często najgłębsze sekrety, wierząc, że są one odpowiednio chronione i wykorzystane wyłącznie w celu ochrony ich interesów. Kiedy dane mogą zostać zhakowane, a informacje trafiać w niepowołane ręce, zaufanie do kancelarii prawnej obejmuje również przekonanie o jej kompetencjach w zakresie cyberbezpieczeństwa. Wniosek z tego jest taki, że bez zaufania trudno wyobrazić sobie skuteczną i owocną współpracę w dziedzinie prawa. To nie tylko kwestia profesjonalizmu, ale przede wszystkim ludzkiego wymiaru relacji prawnik-klient - powiedziała **Anna Stępniewska, radca prawny, dyrektor działu prawnego spółki Rzetelna Grupa.**

JAK PRZED CYBERATAKAMI MOŻE CHRONIĆ SIĘ BRANŻA PRAWNA?

Aby to zaufanie utrzymać, kancelarię należy chronić przed cyberzagrożeniami, a w przypadku ich wystąpienia, w sposób profesjonalny bronić się przed nimi. Dlatego cyberbezpieczeństwo w branży prawnej, jak w każdej innej, nie może być jednorazowym procesem. Wymaga dostosowywania wewnętrznych systemów i zabezpieczeń oraz czujnych praktyk w celu szybkiego wykrywania i reagowania na naruszenia.

Przykłady technologii i narzędzi, które podmioty prawne powinny rozważyć:

- **Polityka Akceptowalnego Użytkowania**. AUP wyraźnie określa zasady, których pracownicy muszą przestrzegać w odniesieniu do sieci firmy, oprogramowania, komputerów, laptopów i urządzeń mobilnych. Pomaga to zrozumieć pracownikom ich obowiązki w zakresie technologii i edukować ich w zakresie identyfikacji potencjalnych cyberzagrożeń.



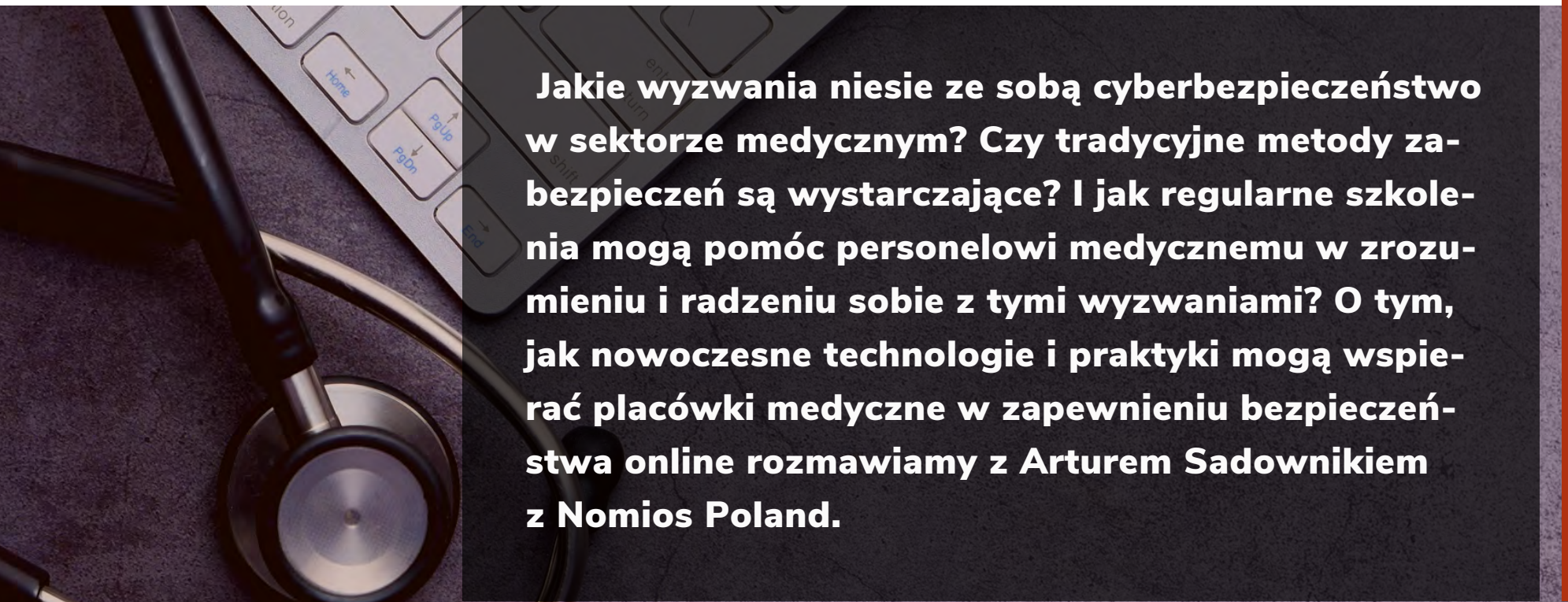
- **technologia oparta na chmurze.** Chociaż wiele kancelarii prawnych wciąż obawia się przenoszenia swoich danych do chmury, prawda jest taka, że rozwiązania oparte na chmurze są znacznie bezpieczniejsze niż oprogramowanie zainstalowane lokalnie. Dostawcy rozwiązań SaaS mają zespoły dedykowane wyłącznie zapewnieniu, że ich infrastruktura IT jest jak najbardziej bezpieczna.
- **plan reagowania na incydenty.** Każdy podmiot prawny powinien być przygotowany na ewentualność naruszenia bezpieczeństwa. Skuteczny plan reagowania na incydenty powinien zawierać kroki takie jak: klasyfikacja rodzaju/rozmiaru incydentu, początkowe raportowanie, eskalacja incydentu, informowanie dotkniętych osób i organizacji, badanie i zbieranie dowodów, łagodzenie dalszych ryzyk i wdrażanie środków naprawczych.
- **szyfrowanie.** Jest to bezpłatne lub niskokosztowe rozwiązanie do ochrony przed nieautoryzowanym dostępem do danych. Szyfrowanie plików i e-maili jest coraz bardziej popularne wśród kancelarii prawnych, zwłaszcza tych większych.
- **ocena bezpieczeństwa**. Regularne przeglądy własnych podatności i korzystanie z usług firm zewnętrznych do przeprowadzania ocen bezpieczeństwa może ujawnić potencjalne luki w zabezpieczeniach kancelarii.
- **narzędzia do zarządzania hasłami.** Takie narzędzia, jak KeePassXC czy Dashlane, pomagają w przechowywaniu i generowaniu silnych haseł, co jest kluczowe dla ochrony wrażliwych informacji.
- **rozwiązania do tworzenia kopii zapasowych**. Z uwagi na rosnącą liczbę ataków ransomware, posiadanie solidnych kopii zapasowych jest kluczowe. Kancelarie prawne powinny korzystać z rozwiązań online, takich jak EaseUS czy Paragon Backup & Recovery, aby regularnie tworzyć kopie zapasowe swoich danych.

WNIOSKI

Podmioty prawne są szczególnie narażone na ataki cybernetyczne ze względu na wrażliwość przechowywanych przez nie informacji. Chociaż niemożliwe jest całkowite zabezpieczenie się przed atakami, wiele kancelarii popełnia proste błędy, które zwiększają ryzyko udanego włamania i szkód wynikających z takich naruszeń.

MOŻE OPRÓCZ ZDROWIA ZACZNIEMY SOBIE ŻYCZYĆ RÓWNIEŻ BEZPIECZEŃSTWA?

Artur Sadownik
Nomios Poland



Jakie wyzwania niesie ze sobą cyberbezpieczeństwo w sektorze medycznym? Czy tradycyjne metody zabezpieczeń są wystarczające? I jak regularne szkolenia mogą pomóc personelowi medycznemu w zrozumieniu i radzeniu sobie z tymi wyzwaniami? O tym, jak nowoczesne technologie i praktyki mogą wspierać placówki medyczne w zapewnieniu bezpieczeństwa online rozmawiamy z Arturem Sadownikiem z Nomios Poland.

Jakie są największe wyzwania związane z cyberbezpieczeństwem w placówkach medycznych?

Artur Sadownik: Zagadnienia dotyczące ochrony systemów i danych przetwarzanych w placówkach medycznych zawsze były nietrywialne i wymagały często stosowania nietrywialnych rozwiązań. Systemy i urządzenia wykorzystywane w placówkach medycznych, podobnie jak w przypadku pozostałych sektorów, są coraz bardziej złożone i coraz bardziej cyfrowe.

W odróżnieniu do normalnego biznesu, w którym mamy do czynienia z ochroną komputerów, serwerów, drukarek i innego sprzętu tradycyjnie wiązanego z klasycznym biurem i zdalnym dostępem do niego, w przypadku placówek medycznych działamy dodatkowo z bardzo zaawansowanymi urządzeniami monitorującymi, obrazującymi, testującymi, itp. Działają one pod kontrolą jakiegoś oprogramowania, będąc w istocie mniej lub bardziej zaawansowanymi komputerami czy sterownikami przemysłowymi, z pogranicza światów OT i IoT.

I tu pojawia się problem z tym, jak te zaawansowane systemy skutecznie zabezpieczać, począwszy od ich separacji, bo zwykle one pracują w jednej rozległej sieci z komputerami biurowymi, czy kioskami dla klientów, poprzez aktualizację podatności systemów i oprogramowania na nich zainstalowanych, czy choćby monitorowaniu i zarządzaniu dostępem do tych systemów.

Specjalistyczne systemy i urządzenia wykorzystywane w medycynie powinny być stale aktualizowane, tak jak każde inne komputery działające w sieci. W praktyce nie jest to łatwe – albo to są zamknięte platformy, albo nie ma na takie operacje przyzwolenia czy czasu. W efekcie są one narażone na rozmaite zagrożenia, które mogą do nich przeniknąć drogą sieciową, czy też poprzez nośniki danych, wykorzystywane chociażby do przenoszenia wyników badań.

Trzeba także wyraźnie zaznaczyć, że dużą część placówek medycznych ta cyfrowość i nowoczesność zwyczajnie zaskoczyła – nikt tam zwykle nie planował zbudowania sieci oraz systemów ochrony w sposób, który znamy z sektora komercyjnego. Do tego często istotniejszym priorytetem dla zarządzających, dysponujących ograniczonymi środkami, było wyposażenie danej placówki w kolejne urządzenie zapewniające realizację określonych potrzeb czysto medycznych, niż wdrażanie skutecznych systemów bezpieczeństwa.

Jakie są główne różnice między zabezpieczeniami teleinformatycznymi w instytucjach medycznych a innymi sektorami? Czy są specyficzne wymagania lub regulacje, które placówki medyczne muszą spełnić?

A.S.: Zabezpieczenia teleinformatyczne, które stosujemy w instytucjach medycznych zwykle są bardzo podobno do tych, które stosujemy w typowych firmach z sektora enterprise, czy sektora przemysłowego. Trudno sobie dzisiaj wyobrazić firmę, w której nie trzeba byłoby chronić brzegu sieci przed nieuprawnionym dostępem z zewnątrz za pomocą nowoczesnych zapór ogniowych, ruchu internetowego, generowanego przez pracowników, stacji i serwerów przed niechcianym (złośliwym) oprogramowaniem, czy też poczty elektronicznej. Dodatkowo dochodzą systemy ochrony aplikacji i stron internetowych, na przykład, z informacjami dotyczącymi danej organizacji oraz jej klientów (np. wynikami badań). W przypadku specjalistycznego, skomputeryzowanego sprzętu medycznego zaczynamy przemieszczać się ze świata klasycznego do bardziej przemysłowego i tutaj w zależności od dostępnych możliwości zaczynamy stosować dedykowane do tej klasy rozwiązań systemy ochrony oraz monitorowania.

Co do wymagań i regulacji, w przypadku placówek medycznych poruszamy się w Polsce głównie wokół wymagań stawianych przez wytyczne RODO/GDPR i KSC/NIS z ich kolejnymi aktualizacjami. Pomagają one zwrócić uwagę na konkretne obszary do priorytetowego pokrycia odpowiednimi środkami bezpieczeństwa, przy wykorzystaniu środków własnych danej placówki, czy też funduszy publicznych na ten cel (np. z NFZ).

Zmieniając nieco temat, jakie są najważniejsze funkcje systemów kopii zapasowych oraz jak wpływają one na ciągłość działania placówek medycznych?

A.S.: Jak zwykło się mawiać wśród specjalistów IT – firmy dzielą się na te, które robią kopie zapasowe, i te które będą je robiły, bo się w pewnym momencie przekonają, że są

one bardzo istotne. Chyba nie ma takiej osoby wśród nas, która przypadkowo nie skasowałaby jakiegoś istotnego pliku albo nadpisała wersję, do której chciałaby powrócić. Nawet w przypadku takich, powiedzmy często małej wagi przypadków, możliwość odzyskania odpowiedniej wersji pliku jest bardzo pożądana. A co dopiero, kiedy zmierzymy się z awarią systemu dyskowego w komputerze, serwerze, czy zaawansowanym urządzeniu medycznym? Nie wspominam o przypadkach intencjonalnego zaszyfrowania zasobów dyskowych przez cyberprzestępców. Skutki każdego z tych przypadków można niwelować, gdy posiadamy odpowiedni backup danych i konfiguracji.

W przypadku placówek medycznych mówimy o zbiorach danych pacjentów, wraz z wynikami badań, czy też konfiguracji poszczególnych systemów pomagających leczyć oraz ocalać życie, gdzie czas zwłoki w podjęciu działań może prowadzić do nieodwracalnych zmian zdrowotnych, czy wręcz śmierci pacjentów. Stąd wykonywanie kopii zapasowych ma bardzo istotne znaczenie dla ciągłości funkcjonowania danej placówki medycznej.

Jakie są kluczowe cechy systemów typu firewall i jak one wspierają ochronę danych pacjentów oraz infrastruktury medycznej?

A.S.: Nowoczesne systemy firewall zapewniają możliwość odseparowania sieci, w której zainstalowana jest infrastruktura medyczna oraz bazy danych pacjentów od Internetu. Dzięki nim z jednej strony nieuprawnione osoby z zewnątrz nie mogą się łączyć z systemami wewnątrz sieci danej placówki, z drugiej zaś – firewalle zapewniają możliwość precyzyjnej kontroli kto, kiedy, na jakich zasadach oraz z jakich zasobów Internetu może korzystać.

Wiele rozwiązań tego typu zapewnia także skanowanie ruchu na okoliczność

Może oprócz zdrowia zaczniemy sobie życzyć również bezpieczeństwa?

różnego rodzaju zagrożeń, czy też blokowanie stron internetowych, które mogą potencjalnie nieść zagrożenie.

Dodatkowo za pomocą zapór ogniowych możliwe jest podzielenie sieci na segmenty funkcjonalne (np. osobny segment dla komputerów biurowych, osobny dla infrastruktury medycznej danego oddziału), co w konsekwencji może utrudnić potencjalnemu cyberprzestępcy na swobodne przenikanie przez sieć całego przedsiębiorstwa i przejmowanie infrastruktury medycznej po przejęciu komputera jednego z pracowników.

Jakie są trzy najważniejsze obszary, na które placówki medyczne powinny zwrócić uwagę w kontekście cyberbezpieczeństwa, i jakie rozwiązania oferuje Nomios w tych obszarach?

A.S.: Wskazanie konkretnych trzech obszarów, od których należy priorytetowo rozpocząć przygodę z cyberbezpieczeństwem w placówkach medycznych nie jest łatwe ze względu na skomplikowanie ich środowisk, ale jeśli musiałbym wybierać, to zacząłbym od zabezpieczenia wszystkich systemów komputerowych, łącznie z serwerami i urządzeniami medycznymi, które to umożliwiają za pomocą rozwiązań klasy EDR.

Rozwiązania te wykrywają podejrzaną aktywność na chronionym systemie, identyfikują złośliwe oprogramowanie oraz pomagają identyfikować i czyścić z zagrożeń potencjalnie zara-

żone stacje.

Kolejnym obszarem byłaby ochrona kanałów internetowych, a w szczególności poczty elektronicznej, która jak mówiłem wcześniej, jest najłatwiejszym kanałem do skutecznego wykorzystania przez cyberprzestępców.

Trzecim – zarządzanie podatnościami, czyli skanowanie całej infrastruktury pod kątem możliwości zainfekowania poszczególnych jej elementów z wykorzystaniem znanych podatności (kolokwialnie – dziur) w oprogramowaniu oraz wdrożenie procesu aktualizacji, zmniejszając ryzyko przejmowania systemów przez cyberprzestępców.

Jakie technologie i metody są wykorzystywane w systemach poczty elektronicznej wraz z systemem bezpieczeństwa do zapobiegania atakom phishingowym i złośliwemu oprogramowaniu?

A.S.: Poczta elektroniczna jest obecnie najczęściej wykorzystywanym kanałem do zarażenia komputera ofiary, z którego potem można wykonywać ataki na kolejne systemy przyłączone wewnątrz sieci firmowej. Stąd też niezbędne jest wykorzystywanie do ochrony tego kanału odpowiednio skutecznych rozwiązań. Zwykle łączą one w sobie kilka elementów, takich jak ochrona przed spamem (niechcianą korespondencją), ochrona przed niechcianym oprogramowaniem (ang. malware) czy funkcjonalność weryfikowania linków i plików przesyłaną pocztą elektroniczną, na przykład, za pomocą rozwiązań klasy sandbox (uruchamianie kodu w wyizolowanym środowisku, w celu zidentyfikowania potencjalnie złośliwego zachowania i wyeliminowania zagrożeń).

Wspomniane tu rozwiązania, działające w sposób automatyczny, mimo dokładania wszelkich starań przez producentów zabezpieczeń, nie dają stuprocentowego zabezpieczenia przed atakami kierowanymi pocztą elektroniczną do pracowników danej organizacji. Stąd niezbędnym wydaje się być uruchomienie procesu szkoleniowego, uświadamiającego pracowników o zagrożeniach płynących z wykorzystywania kanałów internetowych oraz o sposobach rozróżniania treści fałszywych od tych, które rzeczywiście powinny trafić do ich skrzynek pocztowych. Większość dzisiejszych udanych ataków na organizacje zaczyna się od kliknięcia w link udający normalną stronę, czy też otwarcia pliku z – wydawałoby się – istotną dla nas informacją. Króluje tu prosta zasada: nie spodziewałem się czegoś

takiego, to podejrzliwie sprawdzam, czy na pewno nie jest to jakaś próba wykorzystania mojej nieuwagi. Nie otwieram plików pochodzących od nieznanych nadawców, a już tym bardziej – nie klikam w linki z wiadomości pocztowych. Bezpieczniej jest je po prostu przepisać niż potem długo żałować ich użycia.

Na koniec, zapytam, jakie są korzyści z regularnych szkoleń z zakresu cyberbezpieczeństwa dla personelu medycznego? Jak Nomios może pomóc w ich organizacji?

A.S.: W ofercie Nomios posiadamy zautomatyzowane systemy szkoleniowe, zapewniające stałe podnoszenie świadomości pracowników odnośnie zagrożeń płynących ze świata cyfrowego. Dodatkowo, po ustaleniu zakresu szkolenia, możemy przygotować dedykowane warsztaty z wybranych zagadnień cyberbezpieczeństwa, jak również szkolenia produktowe, powiązane z rozwiązaniami z naszego portfolio.

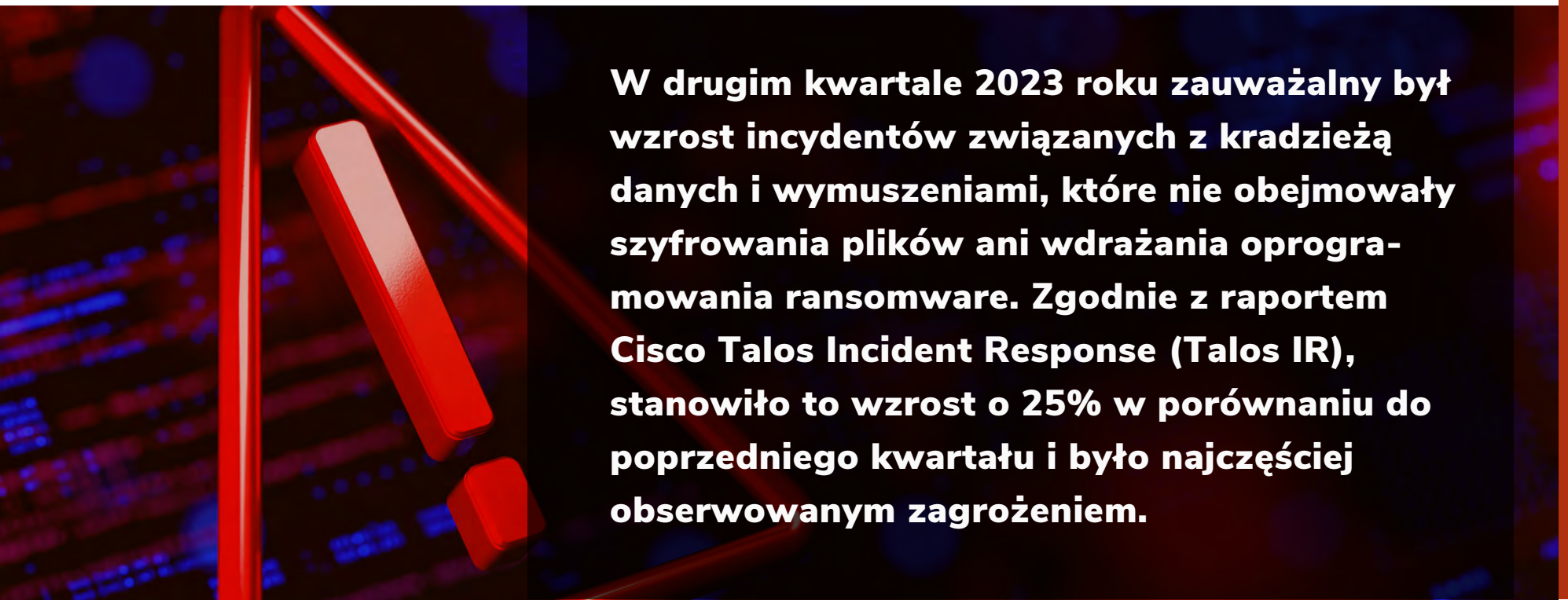
Korzyścią płynącą z przeprowadzania takich szkoleń i warsztatów jest na pewno bezpieczeństwo danych nas dotyczących, o które powinniśmy zabiegać i jego wymagać. Może od dzisiaj zaczniemy oprócz zdrowia życzyć sobie również bezpieczeństwa?

To całkiem racjonalne podejście.
Serdecznie dziękujemy za rozmowę.

Może oprócz zdrowia zaczniemy sobie życzyć również bezpieczeństwa?

CYBERZAGROŻENIA II KWARTAŁU 2023. ZMIENIAJĄCE SIĘ TRENDY

Redakcja
SECURITY MAGAZINE



W drugim kwartale 2023 roku zauważalny był wzrost incydentów związanych z kradzieżą danych i wymuszeniami, które nie obejmowały szyfrowania plików ani wdrażania oprogramowania ransomware. Zgodnie z raportem Cisco Talos Incident Response (Talos IR), stanowiło to wzrost o 25% w porównaniu do poprzedniego kwartału i było najczęściej obserwowanym zagrożeniem.

KRADZIEŻ DANYCH I WYMUSZENIA NA CZELE ZAGROŻEŃ

W drugim kwartale 2023 roku, cyberprzestępcy coraz częściej decydowali się na strategię polegającą na kradzieży danych i wymuszeniach, zamiast tradycyjnych ataków ransomware. W tym typie ataku, sprawcy kradną dane ofiary i grożą ich wyciekiem lub sprzedażą, chyba że ofiara zapłaci określoną sumę pieniędzy. To eliminuje potrzebę wdrażania oprogramowania ransomware lub szyfrowania danych.

Takie działania odróżniają się od metody podwójnego wymuszenia ransomware, w której przeciwnicy najpierw wykradają dane, a następnie szyfrują pliki na serwerach ofiary. Następnie żądają one zapłaty za otrzymanie klucza do odszyfrowania, a także za gwarancję, że skradzione dane nie zostaną opublikowane lub sprzedane.

W przypadku kradzieży danych i wymuszeń, cyberprzestępcy wykorzystują fakt, że wiele firm jest bardziej zaniepokojonych perspektywą wycieku wrażliwych danych, niż utratą dostępu do nich. Wyciek takich danych może mieć poważne konsekwencje, takie jak naruszenie przepisów o ochronie danych, utrata zaufania klientów, a nawet potencjalne kary prawne.

W związku z tym, firmy muszą podjąć dodatkowe środki w celu ochrony swoich danych. Obejmuje to nie tylko zabezpieczenia techniczne, takie jak silne hasła i szyfrowanie danych, ale także szkolenia dla pracowników na temat bezpieczeństwa informacji i regularne audyty bezpieczeństwa.

Muszą też zainwestować w narzędzia i procedury, które pomogą im szybko wykryć potencjalne naruszenia, zidentyfikować skradzione dane i podjąć

odpowiednie kroki w celu ich odzyskania. To może obejmować takie działania jak monitorowanie ruchu sieciowego, regularne przeglądy logów systemowych, a także utworzenie planu reagowania na incydenty, który określa, jak firma powinna reagować na potencjalne naruszenia bezpieczeństwa.

- *To nowe podejście do cyberprzestępczości wymaga od firm zmiany perspektywy. Muszą one zrozumieć, że ochrona danych to nie tylko kwestia zapobiegania atakom, ale też zapewnienia, że w przypadku naruszenia, skutki dla firmy będą jak najmniejsze* - skomentował **Rafał Stępniewski, redaktor naczelny "Security Magazine".**

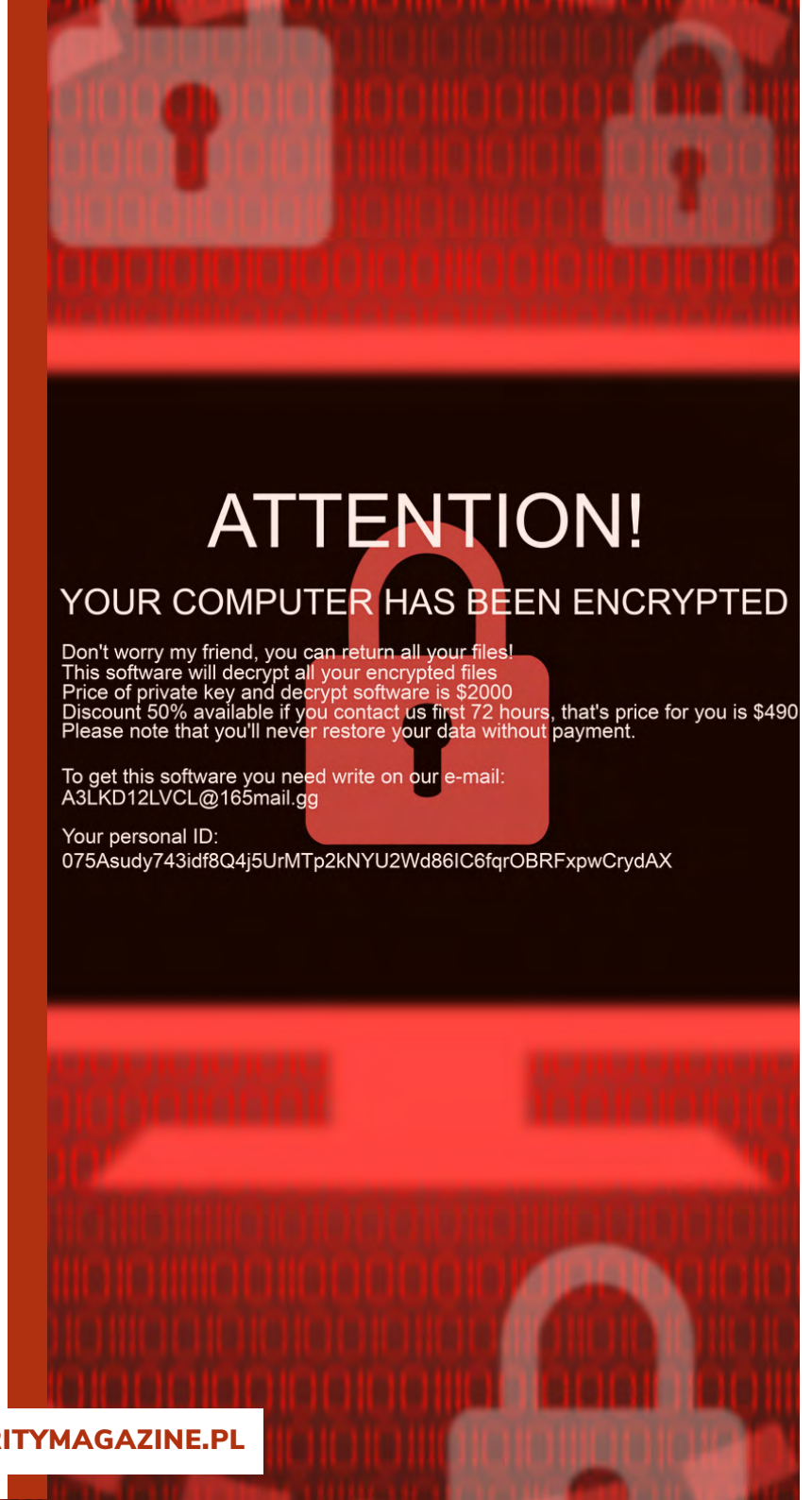
Kradzież danych i wymuszenia stały się najważniejszym zagrożeniem dla firm w drugim kwartale 2023 roku. Firmy muszą dostosować swoje strategie bezpieczeństwa, aby sprostać temu nowemu wyzwaniu. Jak podkreślił Rafał Stępniewski, "cyberbezpieczeństwo to nie tylko ochrona przed utratą dostępu do danych, ale przede wszystkim ochrona przed ich wyciekiem."

RANSOMWARE NADAL NA DRUGIM MIEJSCU

Mimo rosnącej popularności ataków polegających na kradzieży danych i wymuszeniach, ransomware nadal pozostaje poważnym zagrożeniem. W drugim kwartale 2023 roku, ransomware stanowił drugie najczęściej obserwowane zagrożenie, odpowiadając za 17% wszystkich zaangażowań. To stanowi niewielki wzrost w porównaniu do 10% w poprzednim kwartale, co pokazuje, że mimo zmiany taktyki niektórych cyberprzestępców, ransomware nadal jest poważnym problemem.

W tym kwartale, grupa Cisco Talos Incident Response (Talos IR) zaobserwowała kilka rodzin ransomware, które były aktywne w poprzednich kwartałach, w tym LockBit i Royal. Te rodziny ransomware są znane z wykorzystywania zaawansowanych technik, takich jak szyfrowanie plików na serwerach ofiary i wymuszanie okupu za ich odszyfrowanie.

Talos IR zaobserwował też kilka nowych rodzin ransomware, które pojawiły się po raz pierwszy w tym kwartale. Wśród nich były 8Base i Money-Message.



Te nowe rodziny ransomware pokazują, że cyberprzestępcy ciągle inwestują w rozwój nowych narzędzi i technik, aby skuteczniej przeprowadzać swoje ataki.

- Mimo że obserwujemy zmianę taktyki niektórych cyberprzestępców, ransomware nadal pozostaje poważnym zagrożeniem. Firmy muszą nadal inwestować w zabezpieczenia przeciwko ransomware, takie jak regularne tworzenie kopii zapasowych danych, szkolenia pracowników z zakresu bezpieczeństwa informacji oraz utrzymanie swojego oprogramowania na bieżąco, aby zapobiec wykorzystaniu znanych luk bezpieczeństwa - zaznaczył Rafał Stępniewski.

Mimo rosnącej popularności ataków polegających na kradzieży danych i wymuszeniach, ransomware nadal jest poważnym zagrożeniem dla firm. Firmy muszą być świadome tego zagrożenia i podjąć odpowiednie kroki, aby się przed nim zabezpieczyć.

SKOMPROMITOWANE DANE UWIERZYTELNIAJĄCE NA CZELE

W drugim kwartale 2023 roku, najczęściej obserwowanym sposobem zdobywania początkowego dostępu do systemów były skompromitowane dane uwierzytelniające lub prawidłowe konta. Stanowiły one prawie 40% wszystkich zaangażowań, co pokazuje, jak ważne jest utrzymanie bezpieczeństwa danych uwierzytelniających.

Jednakże, identyfikacja sposobu, w jaki dane uwierzytelniające zostały skompromitowane, była trudna. Wiele razy, dane te były uzyskiwane z urządzeń poza widocznością firmy, takich jak zapisane dane uwierzytelniające na osobistym urządzeniu pracownika. To pokazuje, jak ważne jest zapewnienie bezpieczeństwa nie tylko w obrębie infrastruktury IT firmy, ale także poza nią.

- Skompromitowane dane uwierzytelniające są jednym z najłatwiejszych sposobów na zdobycie dostępu do systemów firmy. Dlatego tak ważne jest, aby firmy zainwestowały w narzędzia i procedury, które pomogą im monitorować i chronić te dane. To może obejmować takie działania jak wymuszanie silnych haseł, regularne zmiany haseł, a także użycie autentykacji wieloskładnikowej - podkreślił redaktor naczelny “Security Magazine”.

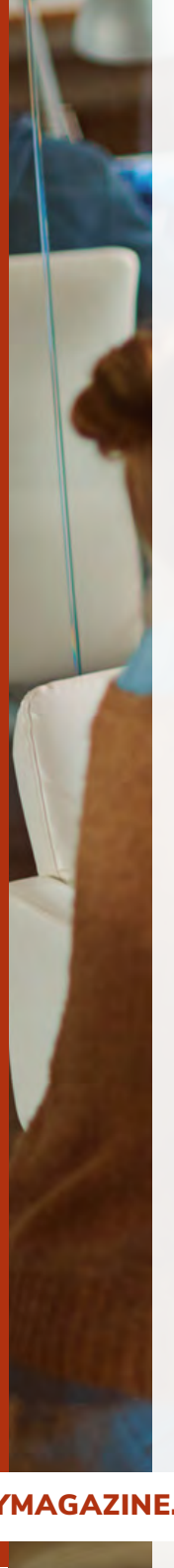
Skompromitowane dane uwierzytelniające są jednym z największych zagrożeń dla bezpieczeństwa firm. Firmy muszą podjąć odpowiednie kroki, aby chronić te dane i zapobiec ich kompromitacji.

SEKTOR ZDROWIA NADAL NAJBARDZIEJ NARAŻONY

Kontynuując trend z poprzedniego kwartału, sektor opieki zdrowotnej był najbardziej narażony na ataki cyberprzestępców w drugim kwartale 2023 roku. Stanowił on 22% całkowitej liczby zaangażowań w reakcję na incydenty. To pokazuje, jak ważne jest dla firm z tego sektora, aby podjąć odpowiednie kroki w celu zabezpieczenia swoich systemów i danych.

Sektor opieki zdrowotnej jest szczególnie atrakcyjny dla cyberprzestępców ze względu na wrażliwość danych, które przetwarza. Dane pacjentów, takie jak informacje o stanie zdrowia, dane osobowe i finansowe, są niezwykle cenne i mogą być wykorzystane do różnych celów, od wymuszeń po kradzież tożsamości.

- Sektor opieki zdrowotnej musi podjąć szczególne środki ostrożności, aby chronić dane pacjentów. Wymaga to nie tylko zabezpieczeń technicznych, ale także szkoleń dla personelu medycznego i administracyjnego, aby zrozumieć i przestrzegać najlepszych praktyk w zakresie bezpieczeństwa informacji - zauważył nasz rozmówca.



Bezpośrednio za sektorem opieki zdrowotnej, usługi finansowe były drugim najbardziej narażonym sektorem, co pokazuje, że cyberprzestępcy nadal skupiają swoje wysiłki na sektorach, które przetwarzają wrażliwe dane.

ZMIANA TAKTYKI CYBERPRZESTĘPCÓW. OD BLOKOWANIA DO KRADZIEŻY DANYCH

Cyberprzestępcy nieustannie dostosowują swoje metody ataku, aby zwiększyć swoje szanse na sukces i potencjalne zyski. W ostatnich latach obserwujemy istotną zmianę w ich taktyce. Kiedyś głównym celem ataku było zablokowanie dostępu do danych poprzez ich zaszyfrowanie i żądanie okupu za odszyfrowanie. Teraz, coraz częściej, celem jest kradzież tych danych.

Ta zmiana taktyki oznacza, że firmy muszą dostosować swoje strategie obronne. Ochrona przed ransomware nadal jest ważna, ale teraz firmy muszą również skupić się na zapobieganiu kradzieży danych. To może obejmować takie działania jak monitorowanie ruchu sieciowego, regularne przeglądy logów systemowych, a także wdrożenie zaawansowanych narzędzi do wykrywania intruzów.

- Zmiana taktyki cyberprzestępców oznacza, że firmy muszą dostosować swoje strategie obronne. To nie jest łatwe zadanie, ale jest absolutnie niezbędne. Firmy muszą zrozumieć, że cyberbezpieczeństwo to nie tylko ochrona przed utratą dostępu do danych, ale przede wszystkim ochrona przed ich wyciekiem - podkreślił Rafał Stępniewski.

Kradzież danych może mieć daleko idące konsekwencje dla firm. Oprócz potencjalnej utraty zaufania klientów i szkód dla reputacji, firmy mogą też

ponieść poważne konsekwencje prawne i finansowe. W zależności od jurysdykcji, firmy są zobowiązane do powiadomienia klientów o wycieku danych, a także mogą być narażone na kary finansowe.

CYBERBEZPIECZEŃSTWO TO NIE TYLKO TECHNOLOGIA

Cyberbezpieczeństwo to także kwestia ludzi i procesów. Wszyscy pracownicy firmy, niezależnie od stanowiska i roli, muszą być świadomi zagrożeń oraz wiedzieć, jak postępować, aby zapobiec incydentom związanym z bezpieczeństwem.

Pracownicy bywają najsłabszym ogniwem w łańcuchu bezpieczeństwa. Mogą nieświadomie kliknąć na link w e-mailu phishingowym, używać słabych haseł lub udostępniać wrażliwe informacje niepowołanym osobom. Dlatego tak ważne jest, aby firmy inwestowały w szkolenia z zakresu bezpieczeństwa dla swoich pracowników.

- Firmy muszą zrozumieć, że każdy pracownik jest częścią ich strategii bezpieczeństwa. Szkolenia z zakresu bezpieczeństwa powinny być regularnie przeprowadzane i aktualizowane, aby pracownicy byli na bieżąco z najnowszymi zagrożeniami i najlepszymi praktykami - powiedział redaktor naczelny "Security Magazine".

Oprócz szkoleń, firmy muszą również zwrócić uwagę na swoje procesy. To obejmuje takie aspekty jak zarządzanie dostępem, monitorowanie systemów, regularne przeglądy bezpieczeństwa i reagowanie na incydenty. Wszystkie te elementy powinny być częścią kompleksowej strategii bezpieczeństwa firmy.

Cyberzagrożenia są dynamicznym i ewoluującym obszarem. Firmy muszą być na bieżąco z najnowszymi trendami i zagrożeniami, by skutecznie chronić swoje aktywa cyfrowe.

SECURITYMAGAZINE.PL

BEZPIECZNA CHMURA, IOT I OCHRONA PRZED CYBERATAKAMI

Redakcja
SECURITY MAGAZINE

Cyberzagrożenia czyhają na nas na każdym kroku. A celem każdej firmy powinno być umiejętne obronienie się przed nimi. Poznaj trzy startupy, które zapewnią bezpieczeństwo Twojej organizacji.

BEZPIECZEŃSTWO W CHMURZE

W obecnym dynamicznym i zglobalizowanym środowisku biznesowym korzystanie z technologii chmurowych stało się nieodzownym elementem innowacyjności i efektywności. Tym bardziej że organizacje przechowują i przetwarzają coraz więcej gigabajtów danych. Jednak wraz z korzyściami płynącymi z chmury pojawiają się również nowe wyzwania związane z cyberbezpieczeństwem. Kalifornijski startup Lacework stara się zaadresować te kwestie.

Organizacja oferuje Polygraph® Data Platform, czyli rozwiązanie w dziedzinie bezpieczeństwa dla chmury, które automatyzuje i usprawnia jej ochronę. Platforma ta pozwala na gromadzenie, analizowanie oraz skorelowanie danych w różnych środowiskach chmurowych, takich jak AWS, Azure, GCP i Kubernetes. Dzięki temu klienci otrzymują precyzyjne informacje na temat istotnych zdarzeń związanych z bezpieczeństwem w chmurze, co pozwala im skutecznie reagować na zagrożenia.

Jednym z kluczowych aspektów tego rozwiązania jest jego zdolność do analizy i korelacji danych, co pozwala na wykrycie nawet subtelnych i złożonych zagrożeń. Platforma ta identyfikuje nie tylko oczywiste ataki, ale także podejrzane wzorce zachowań, które mogą wskazywać na zaawansowane cyberataki.

Ważną cechą rozwiązania od startupu jest zdolność Polygraph® Data Platform do integrowania różnych rozwiązań bezpieczeństwa w jednej platformie. To oznacza, że firmy nie muszą angażować się w skomplikowane integracje i zarządzanie wieloma narzędziami. Zamiast tego, mogą skupić się na efektywnej ochronie swoich zasobów, korzystając z całościowego podejścia do bezpieczeństwa w chmurze.

PRZECIWDZIAŁANIE RANSOMWARE

Cyberataki, takie jak np. ransomware są coraz poważniejszym problemem w świecie biznesu. Dlatego startup Deep Instinct umożliwia ochronę opartą o tzw. deep learning przed złośliwym oprogramowaniem. Rozwiązanie to ma skracać czas reakcji na ataki (w tym zero-day) do czasu poniżej 20 ms.

Startup ponadto dostarcza dokładną klasyfikację złośliwego oprogramowania według typu zagrożenia. To znaczy, że narzędzie nie tylko eliminuje

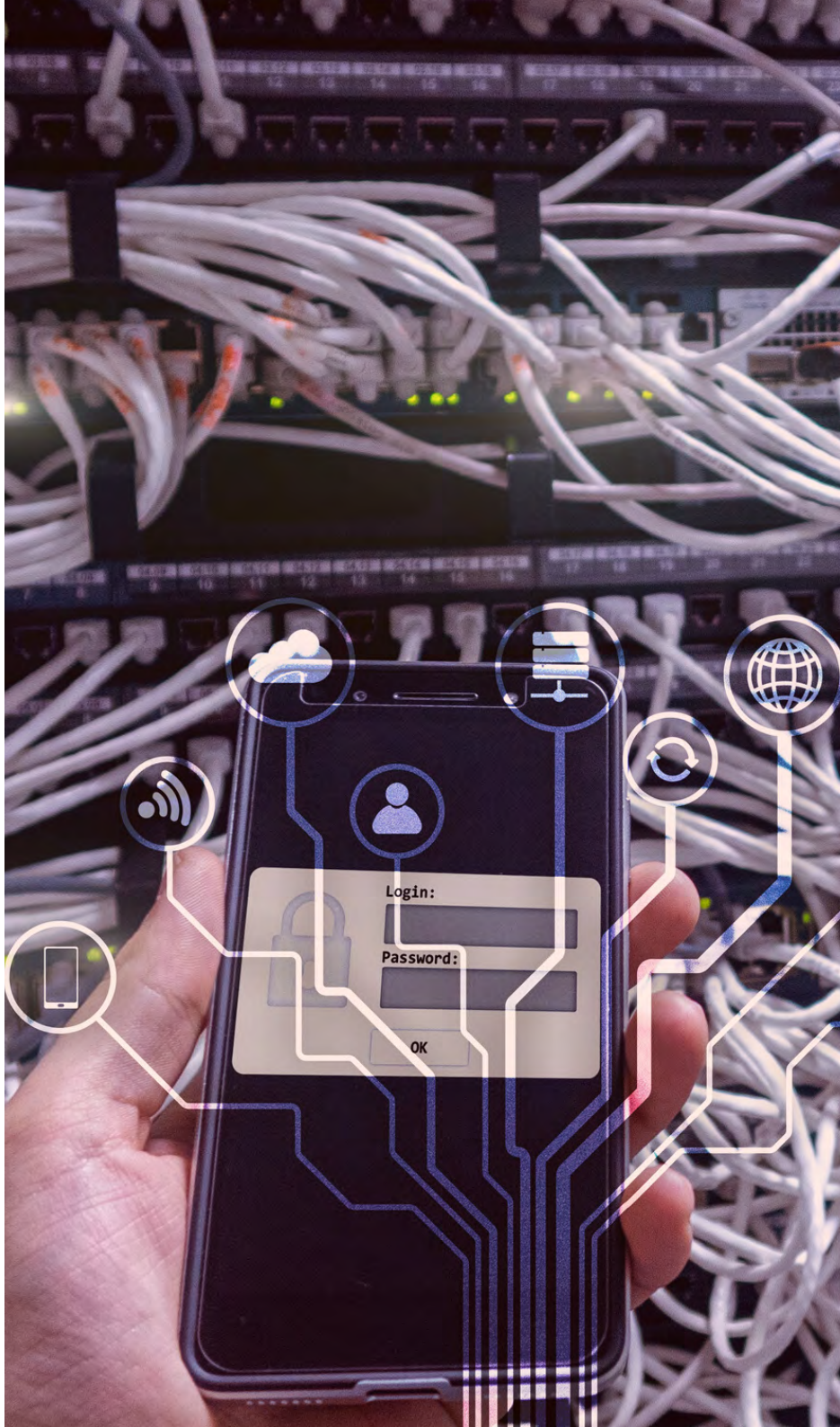
atak, ale również precyzyjnie identyfikuje, z jakim konkretnym rodzajem złośliwości mieliśmy do czynienia – czy to ransomware, spyware, czy inna forma szkodliwego oprogramowania. Dzięki temu organizacja może precyzyjniej reagować na zagrożenia.

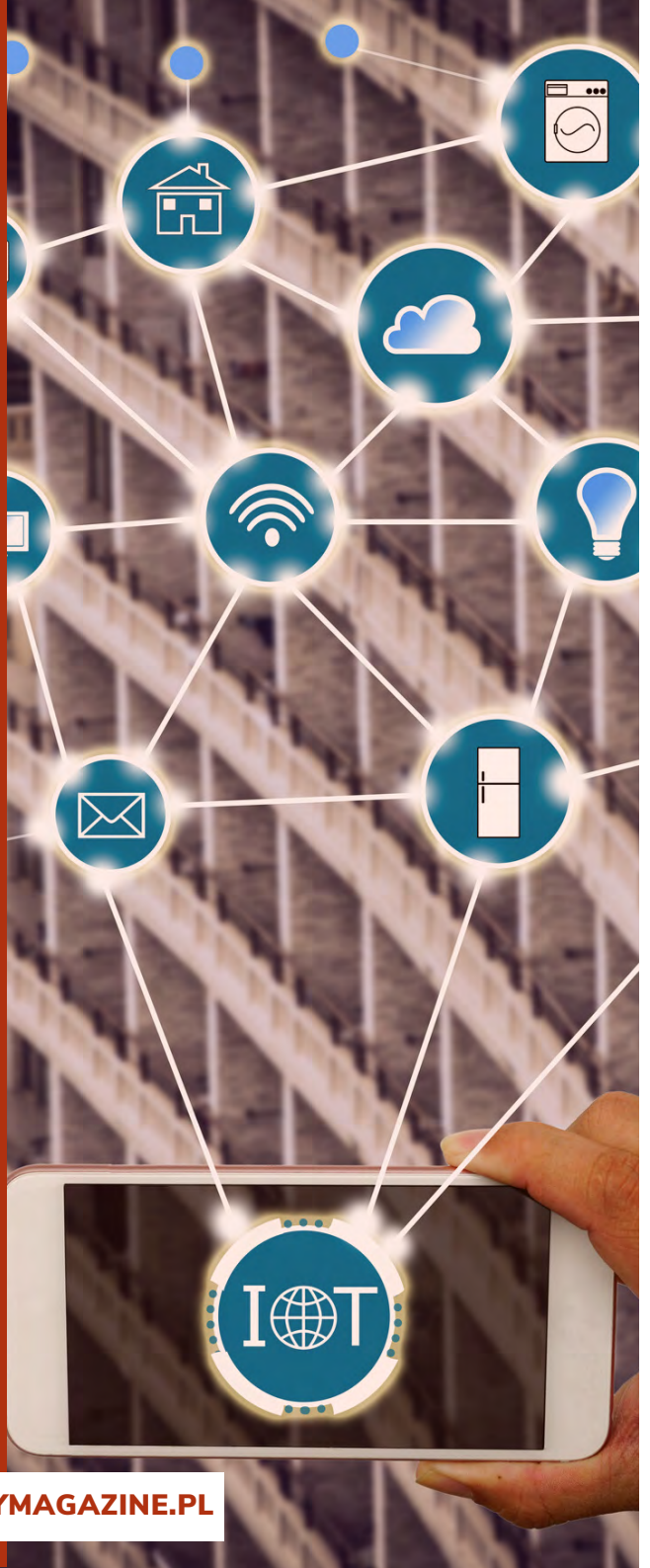
Jednym z najważniejszych atutów oferowanego przez Deep Instinct rozwiązania jest jego zdolność do przewidywania i zapobiegania atakom zeroday. Tradycyjne narzędzia ochrony punktów końcowych często polegają na identyfikowaniu i reagowaniu na ataki, które już wykazują swoje działanie. W przypadku zagrożeń zeroday takie podejście może być niewystarczające. Deep Instinct chwali się jednak, że umożliwia przeciwdziałanie tym atakom.

Startup twierdzi, że technologia ta została oparta o doświadczeń i obserwacji z 15 różnych krajów, a także dogłębnemu zbadaniu rynku tzw. Ransomware-as-a-Service. Wśród klientów startupów znajdują się już duże technologiczne podmioty, takie jak Nvidia, LG czy Samsung.

OCHRONA URZĄDZEŃ IOT

W naszych organizacjach coraz częściej pojawiają się produkty, które mają całodobowy dostęp do internetu, tj. tzw. internet rzeczy (IoT). Są one jednocześnie nierzadko





narażone na cyberataki.

Startup Claroty oferuje rozwiązanie, które zapewnia ochronę systemów cyberfizycznych w środowiskach przemysłowych, służbie zdrowia oraz korporacjach. Za pomocą swojej platformy, startup dąży do zapewnienia pełnej kontroli, zarządzania ryzykiem i wykrywania zagrożeń w rozległych i złożonych infrastrukturach organizacji.

Centralnym elementem oferty Claroty jest Unified Platform, która umożliwia organizacjom zintegrowanie się z istniejącą infrastrukturą klientów w obszarach rozszerzonego internetu rzeczy (XIoT), obejmujących środowiska przemysłowe (OT i IIoT), opieki zdrowotnej (IoMT) i korporacyjne (IoT). Platforma umożliwia organizacjom pełen wgląd w swoje środowisko, zarządzanie ryzykiem i identyfikowanie słabych punktów oraz zapewnia bezpieczny zdalny dostęp do urządzeń.

Innym produktem startupu jest Claroty xDome. Czyli modułowe i elastyczne rozwiązanie oparte na modelu SaaS. To narzędzie wspierają organizację w zakresie cyberbezpieczeństwa, oferujące nie tylko kontrolę nad infrastrukturą, ale także wsparcie w zarządzaniu zagrożeniami.

Claroty Edge, to z kolei narzędzie do wykrywania zasobów. Dostarcza ono organizacjom pełny wgląd w ich środowisko w zaledwie kilka minut. To kluczowe dla skutecznego monitorowania i reagowania na zagrożenia. Z kolei w kontekście zdalnego dostępu Claroty Secure Remote Access (SRA) oferuje rozwiązanie zapewniające bezpieczny zdalny dostęp dla personelu wewnętrznego, jak i zewnętrznego.

Ostatnim produktem startupu jest Claroty Continuous Threat Detection (CTD). Zapewnia ono pełną kontrolę bezpieczeństwa w środowiskach firm. Dzięki niemu organizacje mogą monitorować i identyfikować zagrożenia związane z internetem rzeczy.

To tylko część startupów związanych z cyberbezpieczeństwem, które oferują swoje usługi firmom. Nie ma co ukrywać – wraz z rozwojem technologii zagrożeń przybywa. Rozwija się też czarny rynek, który udostępnia mniej zdolnym cyberprzestępcom narzędzia do wyrządzania szkód organizacjom. A celem każdej firmy powinna być poprawa swojego bezpieczeństwa w tym zakresie.

EKSPERCI WYDANIA

ANNA STĘPNIEWSKA
Dyrektor działu prawnego
Rzetelna Grupa

Członek Zarządu i Dyrektor Działu Prawnego Rzetelna Grupa. Radca prawny z branżą e-commerce związana od ponad 15 lat. Doświadczenie zdobywała w polskich i zagranicznych korporacjach. Obecnie specjalizuje się we wprowadzaniu firm na rynek e-commerce i ich obsługą prawną w szerokim zakresie, w tym ochroną prawno-autorską i prawnej ochrony marki czy też RODO.

ANNA KWAŚNIK
ekspertka w Dziale Budowania Świadomości Cyberbezpieczeństwa
PIB-NASK

Absolwentka Instytutu Profilaktyki Społecznej i Resocjalizacji na Uniwersytecie Warszawskim. Autorka materiałów popularyzacyjno-edukacyjnych z zakresu cyberbezpieczeństwa, różnych zagrożeń i oszustw internetowych, jak również trenerka z zakresu profilaktyki niebezpiecznych zachowań w internecie, nowoczesnych technologii oraz zagadnień związanych z cyberhigieną.

TOMASZ KOWALSKI
CEO i współzałożyciel
Secfense

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

ARTUR SADOWNIK
CTO, Board Member
Nomios Poland

Z branżą IT związany od ponad 20 lat. Swoje doświadczenie zdobywał w firmach z sektora finansowego oraz cybersecurity. Obecnie odpowiada m.in. za rozwój w obszarze bezpieczeństwa IT, pełniąc funkcję Dyrektora Technicznego w wiodącej firmie zajmującej się cyberbezpieczeństwem. Przez 10 lat specjalizował się wdrażaniem i doradztwem w zakresie systemów SIEM.

EKSPERCI WYDANIA

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

Redaktor naczelny "Security Magazine" oraz serwisów: dziennikprawny.pl i politykabezpieczenswa.pl. Manager z 20-letnim doświadczeniem w branżach IT&T i zarządzaniu. Autor wielu publikacji m.in. z zakresu bezpieczeństwa.

PAWEŁ KACZMARZYK
Prezes Zarządu
Serwis komputerowy Kaleron

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

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ

Wydanie 2/2022
POBIERZ

Wydanie 3/2022
POBIERZ

Wydanie 4/2022
POBIERZ

Wydanie 5/2022
POBIERZ

Wydanie 6/2022
POBIERZ

Wydanie 7/2022
POBIERZ

Wydanie 8/2022
POBIERZ

Wydanie 9/2022
POBIERZ

Wydanie 1(10)/2023
POBIERZ

Wydanie 2(11)/2023
POBIERZ

Wydanie 3(12)/2023
POBIERZ

Wydanie 4(13)/2023
POBIERZ

Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

Wydanie 7(16)/2023
POBIERZ

Wydanie 8(17)/2023
POBIERZ

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

Redaktor prowadzący: Monika Świetlińska

Redakcja: Damian Jemioło

Projekt, skład i korekta: Monika Świetlińska

Wszelkie prawa zastrzeżone.

Współpraca i kontakt: redakcja@securitymagazine.pl

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

Redakcja ma prawo do korekty i edycji nadesłanych materiałów celem dostosowani ich do wymagań pisma.

SECURITYMAGAZINE.PL