11(20)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Ochrona sieci oszczędzi wielu zmartwień

Dwa lata na froncie walki z cyberprzestępczością

Cyber(nie)bezpieczeństwo polskiej energetyki

Jak edukować klientów w okresie Black Friday

Zabezpieczanie aplikacji to więcej niż technologia
Wywiad z Adrianem Sroką

SPIS TREŚCI

SZANOWNI PAŃSTWO,

październik był miesiącem, w którym pokazaliśmy moc współpracy, której przyświecał cel uświadamiania i edukacji dotyczącej inżynierii społecznej. Dlaczego taki temat? Bo było to hasło przewodnie Europejskiego Miesiąca Cyberbezpieczeństwa. Październik od 11 lat jest czasem, kiedy ENISA przypomina Europejczykom o niebezpieczeństwach czyhających w sieci.

W Polsce inicjatywę tę koordynuje NASK, który mocno nas wspierał w naszych działaniach. Razem z nami jako patron było również Centralne Biuro Zwalczania Cyberprzestępczości, a także firmy - nasi partnerzy, którzy przygotowali z nami specjalne wydanie poświęcone głównie inżynierii społecznej a także cały szereg informacji, które publikowaliśmy przez cały miesiąc w social mediach.

Podsumowanie naszego projektu znajdziesz w grudniowym wydaniu, a o czym przeczytacie tym razem? Odsłaniamy kulisy roli sektora prywatnego w obronie bezpieczeństwa narodowego i dzielimy się strategiami na bezpieczne zakupy online, niezbędnymi w sezonie wyprzedażowym. Przybliżamy też istotę testów socjotechnicznych i najnowsze metody walki z cyberprzestępczością, które zyskują na znaczeniu.

Jeśli chcecie, by Wasz firmowy ekspercki artykuł znalazł się na łamach najbliższych wydań, skontaktuj się z nami: redakcja@securitymagazine.pl

Zapraszam do lektury.

Rafał Stępniewski

SZCZEGÓŁY STR. 100

POROZUMIENIE DLA CYBERBEZPIECZEŃSTWA

NASK i Instytut Energetyki podpisały porozumienie dotyczące współpracy w obszarze cyberbezpieczeństwa i wykorzystania technik sztucznej inteligencji w sektorze energetycznym. Współpraca będzie skupiać się na przygotowaniu sektora energetycznego do identyfikacji cyberzagrożeń, wdrażaniu zabezpieczeń oraz obsłudze incydentów. Dodatkowo, obie instytucje zamierzają współpracować nad rozwiązaniami bazującymi na sztucznej inteligencji dla odnawialnych źródeł energii i transformacji przemysłu energetycznego.

WSPÓŁPRACA WOJSKO-PRZEMYSŁ

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) otwiera drzwi dla firm specjalizujących się w nowoczesnych technologiach. Jeśli Twoja firma działa w obszarze kryptologii, cyberbezpieczeństwa, IT lub łączności, DKWOC chce z Tobą współpracować. Na stronie wojskowej pojawił się formularz "Dla Firm", dzięki któremu przedsiębiorcy mogą zgłaszać swoje innowacyjne pomysły. Kluczowe obszary to sztuczna inteligencja, cyberbezpieczeństwo, technologie kwantowe oraz bezpieczeństwo systemów IT. Współpraca ma na celu lepszą wymianę informacji z sektorem cywilnym oraz rozwój technologii kluczowych dla Sił Zbrojnych RP.

Dodatkowo, inicjatywa ta ma na celu wzmocnienie współpracy pomiędzy wojskiem a sektorem prywatnym, co przyczyni się do zwiększenia bezpieczeństwa kraju w cyberprzestrzeni. Współpraca z firmami pozwoli również na szybsze wdrażanie nowych technologii w Siłach Zbrojnych RP. Jest to krok w kierunku modernizacji i adaptacji do współczesnych wyzwań w dziedzinie obronności.

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"

DOŁĄCZ DO CBZC

Masz pasję do technologii i chcesz pomagać w zapewnianiu bezpieczeństwa w cyberprzestrzeni? Służba w CBZC może być dla Ciebie idealnym wyborem.

Centralne Biuro Zwalczania Cyberprzestępczości to jednostka organizacyjna Policji, która posiada komórki w każdym mieście wojewódzkim w kraju, skupiająca się na zapobieganiu, ściganiu i zwalczaniu przestępczości w cyberprzestrzeni. Służba w CBZC to nie tylko praca przed komputerem. To też udział w wielu operacjach, szkoleniach krajowych i międzynarodowych. Najnowsze rozwiązania z zakresu informatyki śledczej, czynności operacyjne i procesowe. Praca w takim środowisku jest niezwykle ekscytująca i daje możliwość rozwoju zawodowego w różnych aspektach.

Co daje służba w CBZC?

1. Gwarancję stałego rozwoju i poszerzania swoich umiejętności.
2. Perspektywę rozwiązywania skomplikowanych problemów, analizowania dowodów cyfrowych i pracę z wykwalifikowanymi specjalistami na szczeblu krajowym i międzynarodowym.
3. Stabilność zawodową. Na stanowisku związanym z bezpośrednim zwalczaniem cyberprzestępczości oprócz policyjnego wynagrodzenia przysługuje specjalne świadczenie, które wynosi pomiędzy ok. 5100 zł - 9500 zł brutto.

Jesteś zainteresowany walką z cyberprzestępczością? Służba w CBZC może być dla Ciebie pasjonującym wyzwaniem. Da Ci możliwość realnej poprawy bezpieczeństwa innych w sieci oraz rozwijania swoich umiejętności.

Dołącz do walki z cyberprzestępczością i pomóż w tworzeniu bezpiecznej przyszłości w wirtualnym świecie! Wstąp do CBZC! #stanpodobrejstronie

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"

PRACA W NASK

Chcesz pracować w miejscu, gdzie nowoczesna technologia łączy się z humanistycznym podejściem? Gdzie możesz być na pierwszej linii obrony w świecie cyberbezpieczeństwa?

NASK w Warszawie otwiera drzwi dla specjalistów takich jak Ty! Jako część Zespołu Analiz Strategicznych, będziesz miał wpływ na kształtowanie strategii i regulacji w dziedzinie cyberbezpieczeństwa. Twoje analizy i rekomendacje będą miały realny wpływ na bezpieczeństwo cyfrowe naszego kraju.

Twoja rola w NASK będzie nie tylko analityczna. Będziesz miał okazję nawiązywać międzynarodowe kontakty w branży, współpracować z kluczowymi graczami rynku technologicznego oraz redagować treści na portalu CyberPolicy.
Jeśli biegle mówisz w języku angielskim, posiadasz umiejętności analityczne, doświadczenie w redagowaniu tekstów i wykształcenie wyższe (szczególnie w dziedzinie nauk społecznych lub humanistycznych), to jesteś idealnym kandydatem!

W zamian NAKS oferuje konkurencyjne wynagrodzenie, atrakcyjne benefity oraz szansę na rozwój w zespole pełnym pasjonatów. Oferta wynagrodzeniowa zaczyna się od 6000, a kończy na 11000 zł, dodatkowo premia za Twoje zaangażowanie i wkład w projekty.
Chcesz stać się częścią elitarnej grupy specjalistów w NASK? **Aplikuj**.

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

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

Redakcja "Security Magazine"

PATRONAT
SECURITY MAGAZINE

JUBILEUSZOWA EDYCJA

ADVANCED THREAT SUMMIT 2023

Zapraszamy do udziału w wyjątkowym wydarzeniu - Konferencji Advanced Threat Summit - najważniejszej konferencji cybersecurity w Polsce! Spotykamy się 22 i 23 listopada w Warszawie lub online, 24 listopada online.

Od dekady, co roku roku AT Summit gromadzi kilkusetosobowe, fachowe grono przedstawicieli przedsiębiorstw, banków oraz instytucji finansowych i publicznych z całego świata.
To będzie prawdziwy festiwal cyberbezpieczeństwa! Dołącz, aby poznać najnowsze trendy oraz nawiązać wartościowe kontakty!
Tej edycji towarzyszy Konkurs Advanced Threat Summit. W ramach konkursu nagrodzimy m.in. najlepsze organizacje oraz projekty z obszaru cyberbezpieczeństwa w Polsce.
Podczas wydarzenia omówimy aktualne wyzwania w dziedzinie cyberbezpieczeństwa w Polsce. W tym roku skupimy się na konsekwencjach rozprzestrzeniania się cyberbezpieczeństwa poza jej tradycyjnym obszarem. Cyberbezpieczeństwo stało się mainstreamowym zagadnieniem, dotykającym praktycznie każdej działalności biznesowej i prywatnej.

AT Summit jest najlepszym miejscem do wymiany doświadczeń i dobrych praktyk!
O wpływie współczesnej AI i uczenia maszynowego na kwestie bezpieczeństwa IT opowie **Gynvael Coldwind z HexArcana Cybersecurity.**
W tajniki w różnych wymiarów cyberwojny wprowadzą nas: **Tamara Hendriksen oraz Jort Kollerie z Orange Cyberdefense.**
Richard Stiennon z IT-Harvest zaprezentuje globalny rynku dostawców cyberbezpieczeństwa.
O zastosowaniu Secure Software Development Lifecycle – DevSecOps opowie **Marcin Schubert z Santander Bank Polska.**

EKSPERCI I AGENDA >>>

Dzięki udziałowi ATS otrzymasz 19 punktów CPE.

REZERWUJĄC BILET DO 10.11. Z KODEM PROMOYJNYM„SECURITYMAGAZYN10” OTRZYMASZ 10% RABATU!

PATRONAT
SECURITY MAGAZINE

RAPORT #CYBERMADEINPOLAND

MAPA POLSKIEGO CYBERBEZPIECZEŃSTWA

Jaki jest polski rynek cyberbezpieczeństwa? Jak zmieni się w ciągu najbliższych 5 lat? Nad tymi pytaniami pochylili się eksperci z firm zgromadzonych w Klastrze #CyberMadeInPoland. W raporcie pokazują potencjał polskiego rynku cyberbezpieczeństwa i opisują wyzwania przyszłości.

Każdego roku odnotowywany jest wzrost cyberataków, nie dziwi więc fakt, że zapotrzebowanie na usługi cyberbezpieczeństwa jest najwyższe od lat i w każdym kwartale rośnie. Temu trendowi sprzyja coraz większa świadomość zagadnień bezpieczeństwa IT. Trudno o lepszy moment, by zbudować efektywny przemysł cyberbezpieczeństwa w Polsce.

- *Kiedy trzy lata temu zdecydowaliśmy się na powołanie klastra #CyberMadeInPoland, przyświecał nam cel: wspierać dynamiczny rozwój rynku cyberbezpieczeństwa w Polsce. Po kilku latach działalności i współpracy z wieloma podmiotami budującymi ten ekosystem możemy stwierdzić, że rynek rośnie dynamicznie, a perspektywy są wzrostu są obiecujące* - powiedział **Łukasz Gawron, prezes Klastra.**

Pod parasolem marki #CyberMadeInPoland zgromadzonych jest blisko 50 polskich firm tworzących rozwiązania dla cybersecurity. Razem zdecydowali zebrać odpowiedzi na pytania dotyczące kształtu polskiego rynku cyber oraz jego przyszłości w raporcie „Polski Rynek Cyberbezpieczeństwa 2023-2028".

Autorami są eksperci, prezesi i założyciele firm cyberbezpieczeństwa, doświadczeni praktycy i konsultanci.

Tematyka raportu to mapa polskiego sektora cyberbezpieczeństwa, analiza ekosystemu polskiego rynku cyber, analiza SWOT polskiego rynku, Perspektywa CISO na polski rynek cybersecurity, wpływ strategii i polityk międzynarodowych na polski rynek cybersecurity

RAPORT POBIERZESZ TUTAJ

PATRONAT

SECURITY MAGAZINE

#CyberMadeInPoland

POLSKI RYNEK CYBERBEZPIECZEŃSTWA 2023-2028

PREMIERA: 23 PAŹDZIERNIKA 2023

WYRÓŻNIJ SIĘ W BRANŻY
BEZPIECZEŃSTWA

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

redakcja@securitymagazine.pl
+48 518 609 987

www.securitymagazine.pl

PATRONAT
SECURITY MAGAZINE

CYBERBEZPIECZEŃSTWO ENERGETYKI

FAKTY CZY MITY?

6 grudnia w Warszawie spotkamy się na 7. Konferencji „Inteligentna Energetyka" – Cyber(NIE)bezpieczeństwo polskiej energetyki – fakty czy mity? Prelegenci poruszą zagadnienia związane z cyberbezpieczeństwem polskiej energetyki.

Aby zadbać o cyberbezpieczeństwo energetyki, konieczne jest wdrażanie kompleksowych strategii i działań obejmujących świadomość pracowników, regulacji, zarządzania ryzykiem, a także współpraca międzysektorowa, inwestycje w technologie, monitorowanie i reagowanie na incydenty oraz edukacja społeczeństwa.
O tym, jak poprzez holistyczne podejście i stałe dążenie do doskonałości w obszarze cyberbezpieczeństwa, możemy zapewnić ochronę infrastruktury energetycznej przed coraz bardziej zaawansowanymi zagrożeniami cybernetycznymi, opowiedzą prelegenci 7. Konferencji „Inteligentna Energetyka".

Zakres tematyczny

Głównym celem tegorocznej edycja wydarzenia jest wywołanie dialogu rynkowego przez obalenie lub udowodnienie tez:

- **Teza I:** Polska energetyka może czuć się cyberbezpiecznie
- **Teza II:** Wytwórcy energii na celowniku
- **Teza III:** OSD i OSP na granicy cyberodporności
- **Teza IV:** Systemy łączności w energetyce do podsłuchania.

Wydarzenie otworzy pokaz przedstawiający obecną sytuację w energetyce związaną z cyberbezpieczeństwem. Opowiedzą o niej podczas wystąpienia: „Trendy i wyzwania dotyczące cyberzagrożeń" – Patryk Gęborys, Partner, i Kamil Pszczółkowski, Senior Manager Cyber Security, EY Polska. Drugą prelekcję wygłosi dr Magdalena Krawczyk, Adwokat, która skupi się na omówieniu aktualnie obowiązujących w Polsce regulacji prawnych dotyczących cyberbezpieczeństwa, jak m.in. dyrektywa CRA, CER, NIS2, AI Act, nowelizacja KSC.

Wśród prelegentów konferencji wystąpią też: Marek Seeger, Information Security Manager, SMA Solar Technology AG, Jacek Grzechowiak, Właściciel, RiskResponse, Piotr Szczerek, Kierownik B+R, dział IoT, ANDRA Sp. z o.o., Piotr Wądołowski, CTO, ESMETRIC GROUP Sp. z o.o., Adam P. Grodecki, CX CTO i Paweł Niedzielski, Dyrektor ds. Sprzedaży, Nokia Solutions and Networks Sp.z o.o., Piotr Stępniewicz, Dyrektor Sprzedaży – Telekomunikacja & Cyberbezpieczeństwo, MCX PRO Sp. z o.o.

Raport rynkowy

Na podstawie uzyskanych wniosków z panelu dyskusyjnego powstanie raport rynkowy, który będzie dostępny w wersji cyfrowej do bezpłatnego pobrania na stronie wydarzenia i na portalu Smart-Grids.pl.

REJESTRACJA DO 15.11.

7. KONFERENCJA

INTELIGENTNA ENERGETYKA

Cyber(NIE)bezpieczeństwo polskiej energetyki – fakty czy mity?

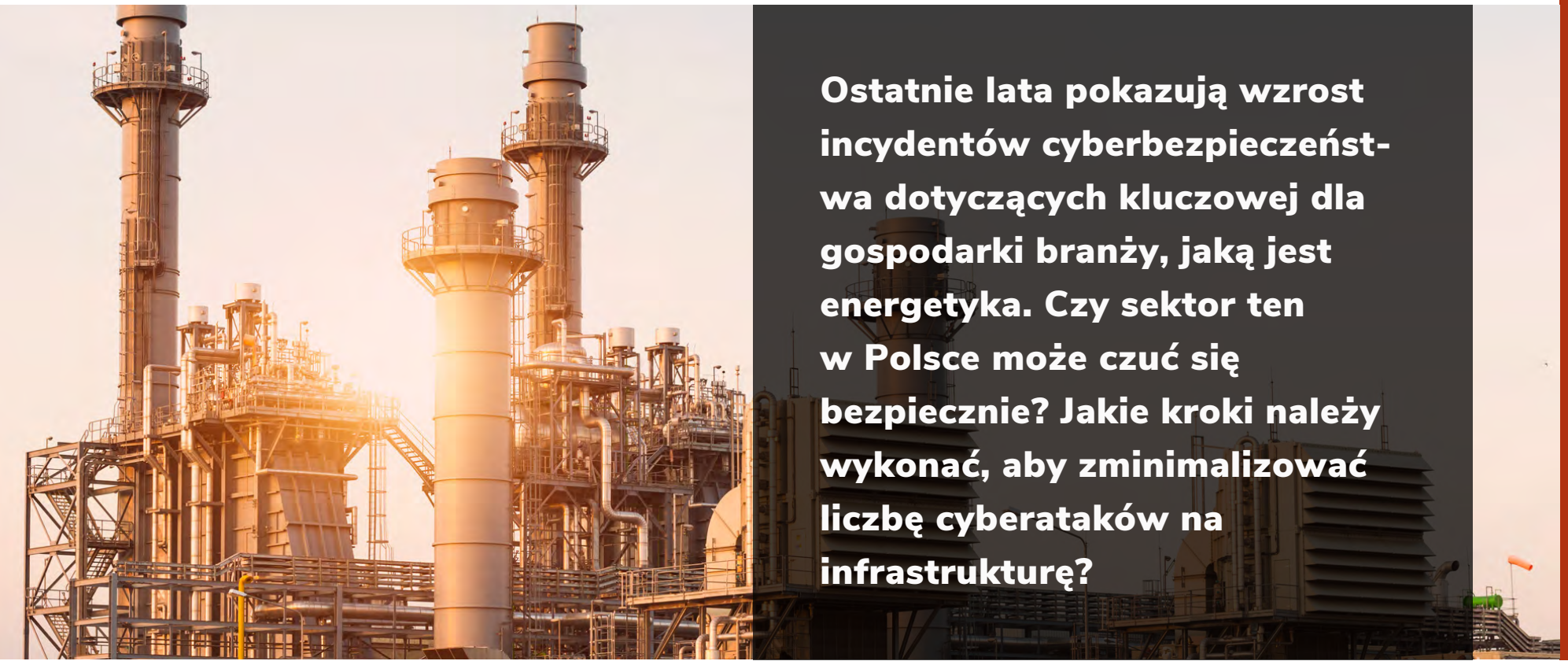
6 grudnia 2023, Warszawa

ZAREJESTRUJ SIĘ JUŻ DZIŚ:

www.inteligentnaenergetyka.pl

CYBER(NIE)BEZPIECZEŃSTWO POLSKIEJ ENERGETYKI

Izabela Żylińska
Konferencja "Inteligentna Energetyka"



Ostatnie lata pokazują wzrost incydentów cyberbezpieczeństwa dotyczących kluczowej dla gospodarki branży, jaką jest energetyka. Czy sektor ten w Polsce może czuć się bezpiecznie? Jakie kroki należy wykonać, aby zminimalizować liczbę cyberataków na infrastrukturę?

STATYSTYKI CYBERATAKÓW POZOSTAJĄ NIEUBŁAGANE

Cyberataki na sektor energetyczny stanowią poważne zagrożenie dla infrastruktury energetycznej i funkcjonowania gospodarki krajowej. W ostatnich latach na świecie zdarzyło się wiele tego typu incydentów, które miały na celu zakłócenie wytwarzania i dostaw energii elektrycznej, zniszczenie urządzeń czy kradzież poufnych informacji. Z informacji za 2022 r., jakie opublikował CERT Polska wynika, że w analizowanym czasie zespół obsłużył 4320 incydentów cyberbezpieczeństwa związanych z energetyką, co stanowiło prawie 10,89% wszystkich zarejestrowanych incydentów.

Pięć z nich uznano za poważne, czyli takie, których wystąpienie miało istotny skutek zakłócający świadczenie usługi kluczowej. Wzrost statystyk w porównaniu do 2021 r. był nieznaczny (zarejestrowano 4084 incydentów dla sektora energii (13,85% całości), w tym trzy poważne według "Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego internetu"), jednak przypadków naruszeń może być dużo więcej. Dane dotyczące cyberataków są bowiem często trudne do ustalenia z powodu ich charakteru, a wiele z nich może pozostać niezgłoszonych lub nieodkrytych.

Problem z cyberatakami potwierdza najnowszy Raport KPMG pt. „Barometr cyberbezpieczeństwa.

Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu", do udziału w którym zaproszono osoby odpowiedzialne za bezpieczeństwo IT w tym również w firmach z branży energetycznej. Z publikacji dowiadujemy się, że w 2022 r. 58% wszystkich ankietowanych przedsiębiorstw z Polski odnotowało przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa, 12% zanotowało 30 i więcej incydentów bezpieczeństwa, 33% zauważyło wzrost intensywności prób cyberataków, a 20% odnotowało wzmożoną aktywność cyberprzestępców w związku z toczącym się za naszą granicą konfliktem zbrojnym w Ukrainie.

7 KROKÓW DO POPRAWY STANU CYBERBEZPIECZEŃSTWA W ENERGETYCE

Jak widać, analizując statystyki tylko z dwóch źródeł, możemy już zaobserwować wzrost działalności cyberprzestępców. Nie bez powodu też na koniec sierpnia premier Mateusz Morawiecki podpisał zarządzenia, które przedłużyły do 30 listopada 2023 r. obowiązywanie stopni alarmowych: 3. stopnia CHARLIE-CRP, 2. stopnia BRAVO na terenie całego kraju oraz 2. stopnia BRAVO wobec polskiej infrastruktury energetycznej, mieszczącej się poza granicami Rzeczypospolitej Polskiej. Aby energetyka w Polsce mogła czuć się cyberbezpiecznie, konieczne jest więc wdrożenie szeregu środków i działań mających na celu ochronę infrastruktury przed atakami cybernetycznymi. Wśród kluczowych kroków, które mogą przyczynić się do poprawy stanu cyberbezpieczeństwa w sektorze energetycznym, wymienia się:

Świadomość i szkolenia

Wzrost świadomości i kompetencji pracowników stanowi priorytetowy element ochrony przed atakami. Mając to na uwadze, w zakresie cyberbezpieczeństwa należy odpowiednio przeszkolić wszystkich pracowników w sektorze energetycznym, począwszy od zarządzających aż po personel techniczny i biurowy. Szkolenia powinny obejmować m.in. identyfikację zagrożeń, zasady higieny cyfrowej (tzw. cyber-BHP), przetestowanie procedury reagowania na incydenty, świadomość ryzyka związanego z atakami cybernetycznymi oraz

kwestie odpowiedzialności personalnej za niedopełnienie obowiązków.

Wdrażanie standardów i regulacji

Dla wzmocnienia ochrony infrastruktury w sektorze energetycznym bardzo istotne jest wprowadzenie odpowiednich regulacji i standardów. W ostatnich latach w prawodawstwie Unii Europejskiej pojawiło się wiele nowych aktów, jak m.in. Critical Entities Resilience Directive **(**CER), Digital Operational Resilience Act (DORA), Network and Information Systems Directive 2 (NIS2), Artificial Intelligence Act (AI Act).

Określanie standardów cyberbezpieczeństwa może m.in. obejmować wymogi dotyczące zabezpieczeń sieciowych, zarządzania dostępem, audytów bezpieczeństwa, procedur reagowania na incydenty, jak również listę dostawców wysokiego ryzyka i tworzenie modeli certyfikacji urządzeń oraz komponentów.

Odpowiednie zarządzanie ryzykiem

Przedsiębiorstwa energetyczne powinny regularnie przeprowadzać analizy ryzyka związane z cyberbezpieczeństwem, identyfikować potencjalne zagrożenia i wdrażać proporcjonalne środki zaradcze. W tym kontekście istotne staje się zapewnienie ciągłego monitorowania i audytów systemów w celu wykrywania ewentualnych słabości oraz podejmowania działań naprawczych w czasie zbliżonym do rzeczywistego.

Współpraca międzysektorowa i międzynarodowa

Ważnym elementem zapewnienia cyberbezpieczeństwa w energetyce jest współpraca międzysektorowa oraz międzynarodowa. Współpraca między sektorem publicznym, prywatnym, dostawcami usług telekomunikacyjnych, operatorami usług kluczowych i innymi partnerami może przyczynić się do wymiany informacji, identyfikacji zagrożeń oraz opracowania skutecznych strategii ochrony. Współpraca na poziomie międzynarodowym umożliwia natomiast wymianę doświadczeń i najlepszych praktyk w zakresie cyberbezpieczeństwa.

Inwestycje w technologie i infrastrukturę

Przedsiębiorstwa energetyczne powinny inwestować w nowoczesne technologie i infrastrukturę, które umożliwią skuteczną ochronę systemów energetycznych przed atakami cybernetycznymi. Może to obejmować zastosowanie zaawansowanych rozwiązań bezpieczeństwa sieciowego,

w tym zapory sieciowe / firewall nowej generacji, systemy wykrywania intruzów, monitorowanie ruchu sieciowego oraz szyfrowanie danych. Aktualizacja i regularne „łatanie" oprogramowania oraz systemów operacyjnych są również kluczowymi działaniami mającymi na celu zabezpieczenie przed znanymi podatnościami.

Ciągłe monitorowanie i reagowanie na incydenty

Dziś energetyka nie powinna zastanawiać się, czy będzie miała cyberatak, lecz kiedy on nastąpi. Dla skutecznej ochrony infrastruktury energetycznej kluczowe jest więc wdrożenie systemów monitorowania, które będą wykrywać nieprawidłowości i potencjalne ataki. Reagowanie na incydenty powinno obejmować szybką identyfikację, izolację i naprawę systemów, a także zbieranie i analizę danych dotyczących incydentu w celu zapobieżenia przyszłym atakom.

W dobie szybkiej ewolucji zagrożeń standardowe podejście oparte na sygnaturach nie jest już skuteczne. Eksperci radzą, aby równolegle wykorzystywać uczenie maszynowe, analizę behawioralną, algorytmy uczenia głębokiego, bazy sygnatur oraz ekspercką wiedzę operacyjną.

Edukacja społeczeństwa

Informowanie społeczeństwa o zagrożeniach, dobrych praktykach bezpieczeństwa cyfrowego oraz sposobach ochrony danych może przyczynić się do podniesienia ogólnej świadomości, także zaangażowania w tym obszarze, co wpłynie korzystnie również na sektor energetyki. Ważne, aby sektor wspornie przeprowadził kampanię informacyjną i zaczął aktywnie zwalczać fałszywe reklamy zachęcające do inwestowania.

JAK W PRAKTYCE WYGLĄDA CYBERBEZPIECZEŃSTWO W ENERGETYCE?

Na to pytanie odpowiedzą Prelegenci 7. Konferencji „Inteligentna Energetyka", która odbędzie się pod hasłem „Cyber(nie)bezpieczeństwo polskiej energetyki – fakty czy mity?" już 6 grudnia 2023 w Warszawie. **Zapraszamy do udziału w spotkaniu!**

ZAMÓW

AUDYT BEZPIECZEŃSTWA

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

DOWIEDZ SIĘ WIĘCEJ!

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

POTENCJAŁ I ROLA SEKTORA PRYWATNEGO W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO. 24. KONFERENCJA BRANŻY OCHRONY

PATRONAT
SECURITY MAGAZINE

Fot. PIO (6)

Technologie służące narodowemu bezpieczeństwu, współpraca z mieszkańcami i partycypacja społeczna w tworzeniu bezpiecznych przestrzeni, praca zdalna w branży ochrony czy potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego w obecnej sytuacji geopolitycznej to kilka wybranych tematów, które poruszono podczas 24. Konferencji Branży Ochrony,

Technologie służące narodowemu bezpieczeństwu, współpraca z mieszkańcami i partycypacja społeczna w tworzeniu bezpiecznych przestrzeni, bezpieczeństwo społeczności, organizacja cyberbezpieczeństwa, praca zdalna w branży ochrony oraz potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego w obecnej sytuacji geopolitycznej to tylko kilka wybranych tematów, które poruszono podczas 24. Konferencji Branży Ochrony, która odbyła się 28 - 29 września 2023 w Jachrance. Organizatorem była Polska Izba Ochrony Osób i Mienia, współorganizatorem przedsięwzięcia: Akademia WSB z Dąbrowy Górniczej, Partnerami Honorowymi: Targi e Securex, oraz Partnerzy merytoryczni: Stowarzyszenie Polskich Specjalistów Bombowych, Centrum Prewencji Terrorystycznej ABW, Kancelaria RK Legal, Safety Project, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron”.

Konferencje oficjalnie otworzył Prezes Zarządu Polskiej Izby Ochrony Marcin Pyclik oraz prof. dr. hab. Bernard Wiśniewski, przedstawiciel współorganizatora Akademii WSB.

Patronat Security Magazine.

24. Konferencja Branży Ochrony

W trakcie konferencji oprócz merytorycznych wystąpień odbył się panel dyskusyjny nt. udziału prywatnego sektora ochrony w systemie bezpieczeństwa Państwa, w których uczestniczyli m.in. płk SOP dr Jarosław Cymerski, Paweł Płużyczka - Koordynator ds bezpieczeństwa Igrzysk Europejskich w Krakowie w 2023 r, Prezes Stowarzyszenia Polskich Specjalistów Bombowych Adam Niemczyk czy Pułkownik rezerwy SZ RP były dowódca Jednostki Wojskowej GROM, Piotr Gąstał.

Dyskusja stanowiła wprowadzenie do merytorycznych wykładów, w których uczestnicy 24. Konferencji Branży Ochrony mogli poznać najnowsze rozwiązania technologiczne użyteczne dla narodowego bezpieczeństwa. Tradycyjnie konferencja łączyła wymiar naukowy i praktyczny, umożliwiając wymianę doświadczeń wielu środowisk, prezentując kierunki rozwoju sektora security w Polsce i na świecie.

Więcej informacji na stronie: www.konferencjapio.pl

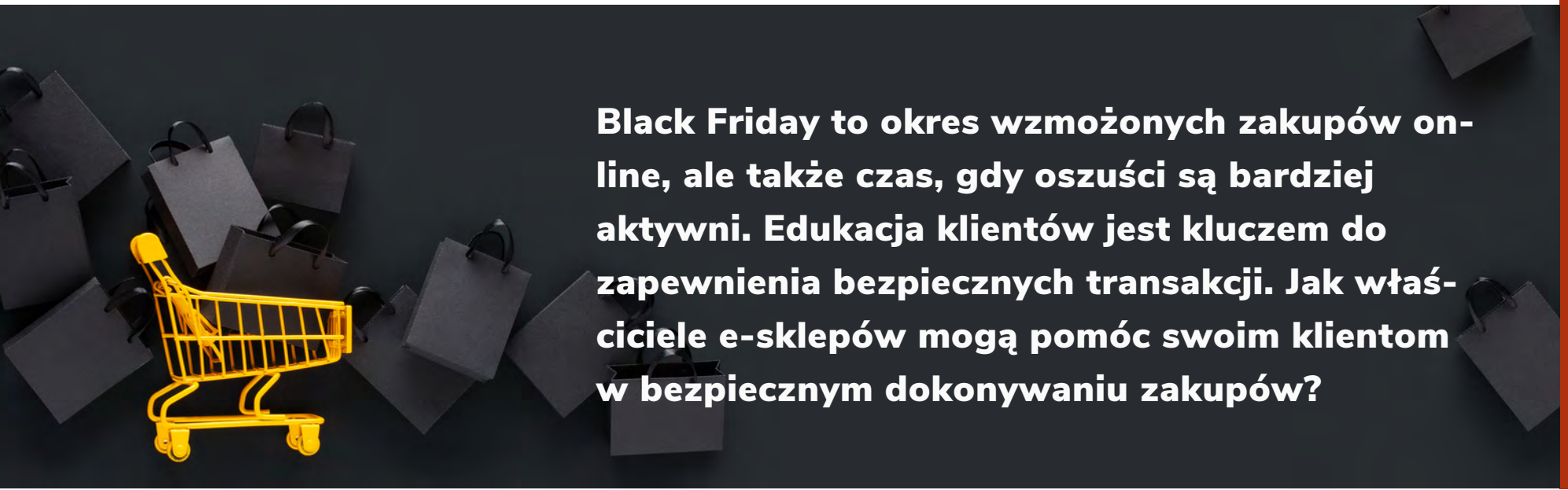
Polska Izba Ochrony jest organizacją samorządu gospodarczego działającą na podstawie ustawy o izbach gospodarczych oraz zgodnie z własnym Statutem usankcjonowanym przez Sąd Rejestrowy. Izba zrzesza na zasadach dobrowolności przedsiębiorców prowadzących działalność gospodarczą w zakresie ochrony osób i mienia, projektowania, produkcji, obrotu towarowego i usług w zakresie technicznych urządzeń, środków i systemów ochrony osób i mienia, doradztwa w dziedzinie bezpieczeństwa osób i mienia, usług detektywistycznych. Polska Izba Ochrony reprezentuje interesy gospodarcze zrzeszonych w niej podmiotów w zakresie ich działalności wytwórczej, handlowej i usługowej, w szczególności wobec organów państwowych.


Rzetelny Regulamin®
Kompleksowa obsługa prawna Twojego e-commerce

BEZPIECZNE ZAKUPY ONLINE. JAK EDUKOWAĆ KLIENTÓW W OKRESIE BLACK FRIDAY

ChatGPT

Redakcja
SECURITY MAGAZINE



Black Friday to okres wzmożonych zakupów online, ale także czas, gdy oszuści są bardziej aktywni. Edukacja klientów jest kluczem do zapewnienia bezpiecznych transakcji. Jak właściciele e-sklepów mogą pomóc swoim klientom w bezpiecznym dokonywaniu zakupów?

CYBERPRZESTĘPCZOŚĆ W CIENIU BLACK FRIDAY

Cyberprzestępcy wykorzystują ważne wydarzenia, aby przeprowadzać swoje kampanie. Sytuacje, w których konsumenci chętnie udostępniają informacje o swoich kartach kredytowych i innych danych osobowych sklepom internetowym, stwarzają dla nich idealną okazję do ataku. Takim wydarzeniem jest Black Friday.

Czarny Piątek stał się globalnym zjawiskiem, przyciągającym miliony klientów do sklepów zarówno stacjonarnych, jak i internetowych. To wydarzenie, które pierwotnie miało miejsce w Stanach Zjednoczonych Ameryki w dniu po Święcie Dziękczynienia, szybko zdobyło popularność na całym świecie, stając się jednym z najważniejszych dni w kalendarzu handlowym. Ale wraz z rosnącą popularnością Black Friday, rośnie również liczba zagrożeń związanych z cyberprzestępczością. Stał się on głównym celem dla cyberprzestępców, oszustów i scammerów.

Cyberprzestępcy wykorzystują różne metody, takie jak inżynieria społeczna, manipulacja pracownikami i zaniedbania w zakresie cyberbezpieczeństwa. W okresie takich dni handlowych jak Black Friday i Cyber Monday, organizacje, które nie są przygotowane, mogą stać się celem dewastujących cyberataków.

Co więcej, ze względu na ogromny wzrost e-zakupów w trakcie tych świąt, sprzedawcy stają się doskonałym celem z uwagi na dużą liczbę transakcji kartami kredytowymi.

Dlaczego jeszcze Black Friday jest tak atrakcyjny dla cyberprzestępców?

- Wielka liczba transakcji. W dniu Black Friday sklepy internetowe odnotowują rekordową liczbę transakcji. Dla cyberprzestępców oznacza to większą szansę na "łowienie" nieświadomych ofiar.
- Presja czasu. Wielu klientów, w pośpiechu za okazjami, może nie zwracać uwagi na typowe oznaki oszustwa, takie jak podejrzane adresy URL czy brak certyfikatu SSL na stronie.
- Zwiększona aktywność e-mailowa. Sklepy często wysyłają klientom informacje o promocjach i ofertach specjalnych. Oszuści wykorzystują to, tworząc fałszywe e-maile promocyjne, które kierują do zainfekowanych stron lub zawierają złośliwe załączniki.

Oszustwa przybierają różne formy, a ich skutki mogą być dotkliwe zarówno dla e-sklepów, jak również dla ich klientów. Wszystkie te zagrożenia powinny być powodem do niepokoju zarówno dla sprzedawców, jak i dla klientów podczas tych świąt handlowych.

Najbardziej bezpośrednią formą oszustwa jest próba wyłudzenia pieniędzy od ofiar. Oszuści mogą, na przykład, podszywać się pod e-sklepy czy banki lub inne instytucje finansowe, wysyłając wiadomości e-mail z prośbą o aktualizację danych bankowych lub potwierdzenie transakcji. Kiedy ofiary wpisują swoje dane na fałszywej stronie, przestępcy uzyskują dostęp do ich kont i dokonują nieautoryzowanych transakcji.

Innym powszechnym oszustwem jest **sprzedaż podróbek lub produktów niższej jakości** pod marką renomowanego producenta. Klienci, myśląc, że dokonują zakupu autentycznego produktu, otrzymują artykuł, który jest daleki od opisu. W wielu przypadkach takie produkty mogą być nie tylko gorszej jakości, ale także niebezpieczne dla użytkowników.

Kolejna technika to phishing. Oszuści tworzą fałszywe strony internetowe sklepów lub wiadomości e-mail, które wyglądają jak prawdziwe, celem wyłudzenia od ofiar wrażliwych informacji, takich jak nazwy użytkowników, hasła czy dane karty kredytowej. Te informacje mogą być następnie wykorzystywane do kradzieży tożsamości, nieautoryzowanych transakcji finansowych lub dostępu do kont online.

Ataki za pomocą złośliwego oprogramowania, czyli malware, mogą być bardziej skomplikowane. Oszuści mogą wysyłać wiadomości e-mail z załącznikami lub linkami, które, gdy są otwierane lub klikane, instalują złośliwe oprogramowanie na komputerze ofiary. Takie oprogramowanie może śledzić aktywność użytkownika, kradnąc wrażliwe dane, lub nawet zablokować dostęp do systemu, żądając okupu za jego odblokowanie.

Współpraca z ekspertami ds. bezpieczeństwa, regularne aktualizacje oprogramowania oraz wdrażanie zaawansowanych rozwiązań zabezpieczających mogą pomóc w ochronie przed cyberzagrożeniami.

STATYSTYKI MÓWIĄ SAME ZA SIEBIE

Według danych Narodowego Centrum Cyberbezpieczeństwa (National Cyber Security Centre - NCSC) w Wielkiej Brytanii ofiary oszustw online straciły średnio £1,000 ($1,176, ponad 4100 zł) każdy podczas ubiegłorocznego sezonu zakupów w ostatnim kwartale roku. To alarmujące statystyki, które pokazują, jak ważne jest zachowanie ostrożności podczas dokonywania zakupów online.

Z kolei ponad 112 milionów konsumentów w USA trafiło do amerykańskich sklepów stacjonarnych w ostatni weekend listopada, co stanowi wzrost o około 17% w porównaniu z 2021 r. Ogromna fala zakupów i wydatków spowodowała tak dużą aktywność sieciową, że oszuści byli w stanie wślizgnąć się do niektórych firm prawie niezauważeni.

Dlatego tak ważne jest, aby dbać o cyberbezpieczeństwo przez cały rok, aby mieć plan na wydarzenia takie jak Black Friday i Cyber Monday. Wiemy przecież, jak wiele szkód może wyrządzić organizacja, która nie jest przygotowana na konsekwencje ataku.

Cyberprzestępcy podążają za pieniędzmi, ponieważ około 90% cyberataków jest motywowanych finansowo. Straty finansowe, uszczerbek na reputacji i niezgodne z prawem grzywny mogą wynikać z niezauważonego naruszenia cyberbezpieczeństwa.

Dla firm ważniejsze niż kiedykolwiek jest podjęcie niezbędnych środków ostrożności, które zapewnią bezpieczeństwo ich sieci i danych konsumentów w weekendy Black Friday i Cyber Monday.

FAŁSZYWE STRONY SKLEPÓW

Cyberprzestępcy, chcąc wykorzystać renomę oraz zaufanie do marki e-sklepu, tworzą kopie strony e-commerce. Te kopie są na tyle przekonujące, że nawet doświadczeni użytkownicy mogą zostać wprowadzeni w błąd. Głównym celem tych fałszywych stron jest wyłudzenie danych logowania, informacji o karcie kredytowej lub nawet skłonienie klienta do dokonania zakupu, po czym pieniądze są kradzione, a produkt nigdy nie jest wysyłany.

Oprócz bezpośrednich strat finansowych klientów, fałszywe strony sklepów mogą poważnie uszkodzić reputację również Twojego sklepu. Klienci, którzy zostali oszukani, mogą nie zdawać sobie sprawy, że byli na fałszywej stronie oraz obwiniać Twoją firmę za wszelkie problemy. To może prowadzić do negatywnych opinii, spadku zaufania i w konsekwencji do spadku sprzedaży.

Jak chronić swoją markę i klientów?

- **Certyfikaty SSL.** Upewnij się, że Twoja strona korzysta z certyfikatu SSL, który zapewnia bezpieczne połączenie i pokazuje klientom, że Twoja strona jest autentyczna. Ikona kłódki w pasku adresu jest jednym ze wskazówek dla klientów, że są na prawdziwej stronie.
- **Edukacja klientów.** Regularnie informuj swoich klientów o potencjalnych zagrożeniach i daj im wskazówki, jak rozpoznać autentyczną stronę Twojego sklepu.

- Możesz to zrobić poprzez newslettery, posty na mediach społecznościowych czy specjalne komunikaty na Twojej stronie. Edukuj klientów na temat znaczenia sprawdzania adresu URL przed dokonaniem zakupu. Jeśli adres strony nie jest znany lub wygląda podejrzanie, lepiej jest unikać dokonywania zakupów.
- **Monitorowanie internetu.** Istnieją narzędzia i usługi, które monitorują internet w poszukiwaniu kopii Twojej strony. Dzięki temu możesz szybko zidentyfikować i podjąć działania przeciwko fałszywym stronom.
- **Transparentność w komunikacji.** Upewnij się, że wszelka Twoja komunikacja z klientem, zwłaszcza dotycząca płatności, jest jasna i przejrzysta. Unikaj wysyłania linków bezpośrednio do stron logowania lub płatności w e-mailach.
- **Ostrzeżenia przed fałszywymi e-mailami promocyjnymi.** W okresie Black Friday wiele sklepów wysyła e-maile promocyjne. Niestety, oszuści również korzystają z tej techniki, wysyłając fałszywe e-maile w celu przekierowania klientów na szkodliwe strony. Właściciele sklepów powinni informować klientów o tym zagrożeniu i zachęcać ich do bezpośredniego odwiedzania strony sklepu, zamiast klikać w linki zawarte w e-mailach.
- **Promowanie bezpiecznych metod płatności.** Zachęcanie klientów do korzystania z bezpiecznych metod płatności może pomóc w ochronie ich danych finansowych. Ponadto, korzystanie z kart kredytowych zamiast debetowych może zapewnić dodatkową warstwę ochrony w przypadku oszustwa.
- **Współpraca z instytucjami.** W przypadku wykrycia fałszywej strony, niezwłocznie zgłoś to odpowiednim instytucjom i organom ścigania. Współpracując z nimi, możesz przeciwdziałać cyberprzestępczości oraz chronić swoją markę.

Edukacja klientów jest kluczowa, dlatego właściciele e-sklepów muszą podjąć odpowiednie kroki, aby edukować swoich klientów na temat potencjalnych zagrożeń.

Obejmuje to informowanie o typowych metodach oszustwa, takich jak fałszywe e-maile promocyjne, strony phishingowe czy podejrzane oferty. Właściciele e-sklepów powinni również zachęcać klientów do korzystania z silnych haseł i włączania dwuetapowej weryfikacji tam, gdzie to możliwe.

KOMENTARZ REDAKCJI DO ARTYKUŁU

Choć w 98% jest tworem wygenerowanym przez sztuczną inteligencję, wymagał sporego wysiłku ludzkiego, aby stał się wiarygodnym źródłem informacji. Jest formą eksperymentu polegającego na oddaniu niemal w całości etapu tworzenia treści związanej z cyberbezpieczeństwem: od propozycji tytułu, po konspekt i wygenerowanie treści.

Jakie wnioski?

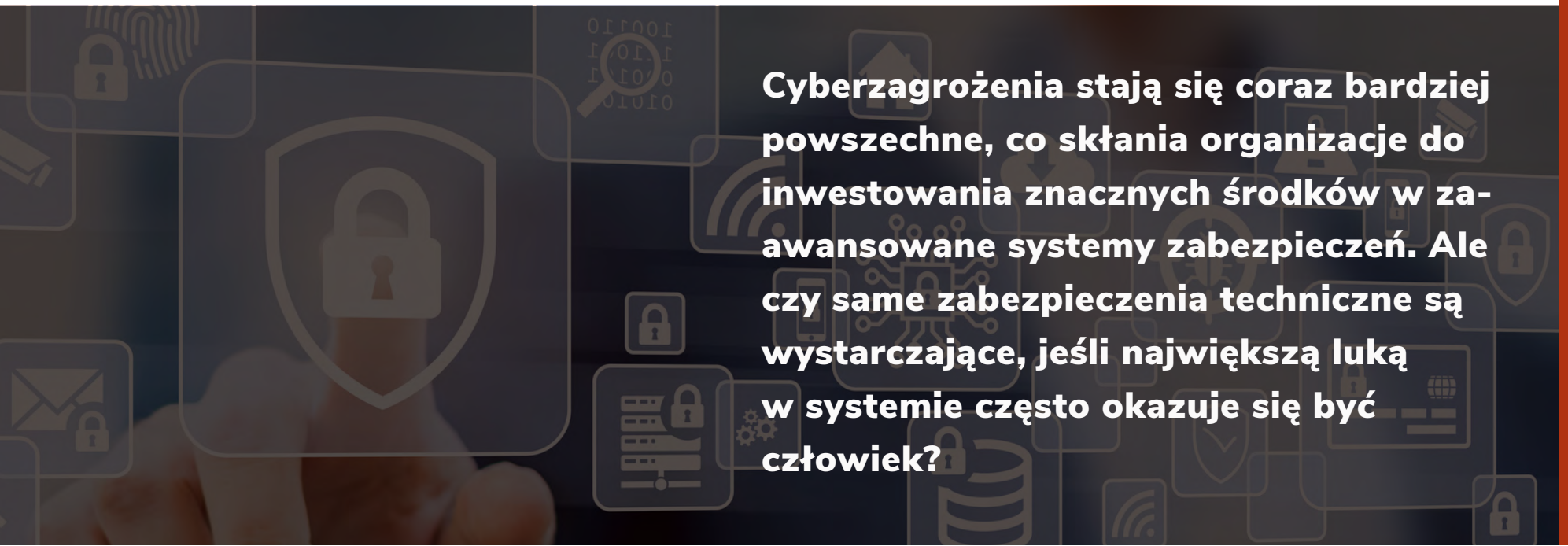
- *Mimo precyzyjnego wskazania w prompcie grupy docelowej, ChatGPT w pierwotnej wersji skierował treść do konsumentów, nie do firm,*
- *Mimo wskazania, by opierał się na źródłach wiedzy, używał fikcyjnych informacji związanych z analizami i statystykami, przypisując je istniejącym firmom badającym rynek.*
- *Istotne tematy, mimo wskazania, na co ma zwrócić uwagę, pomijał, skupiając się na ogólnikach, które wiele razy powtarzał.*
- *Praca człowieka to poprawki gramatyczne, logiczne i weryfikacja faktów. Łącznie praca człowieka nad treścią mieszczącą się w ok. 8 tys. znaków zajęła około 1,5 godziny.*

Jak oceniasz efekty?

Napisz do nas: **redakcja@securitymagazine.pl**

DLACZEGO TESTY SOCJOTECHNICZNE SĄ TAK WAŻNE?

Oleksii Doroshenko
Redsaber Security



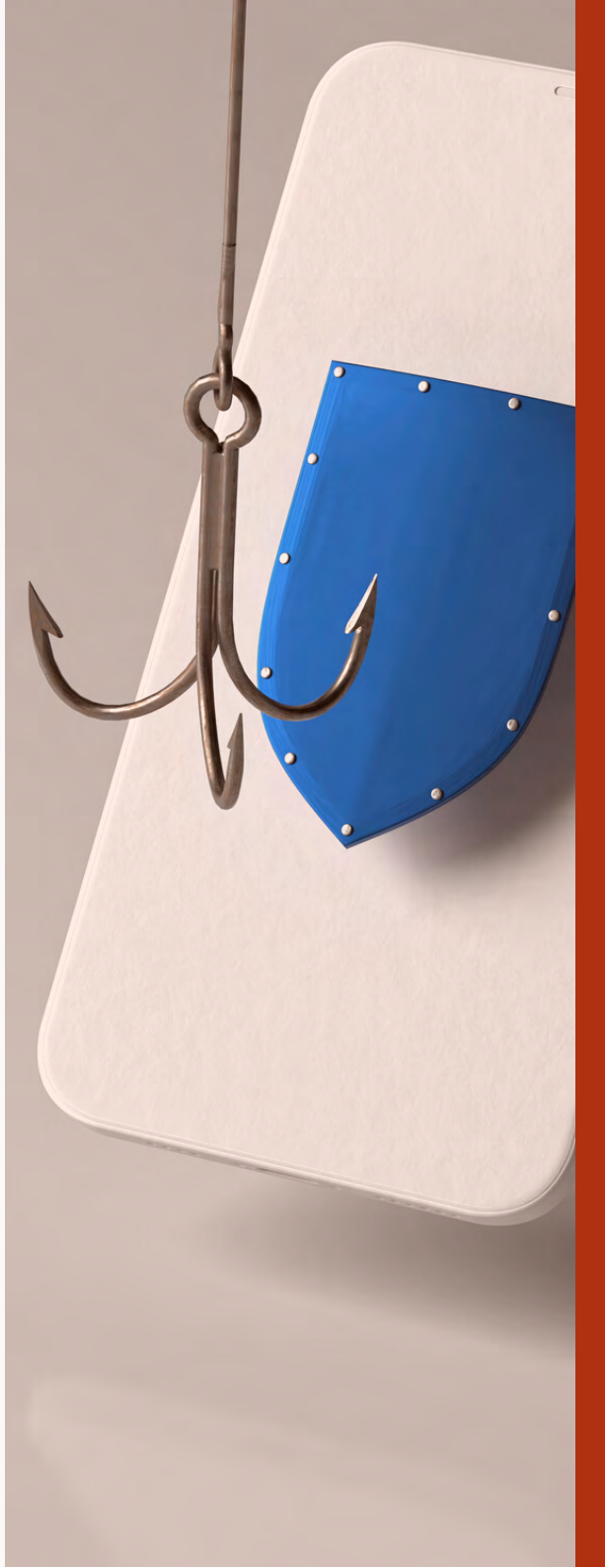
Cyberzagrożenia stają się coraz bardziej powszechne, co skłania organizacje do inwestowania znacznych środków w zaawansowane systemy zabezpieczeń. Ale czy same zabezpieczenia techniczne są wystarczające, jeśli największą luką w systemie często okazuje się być człowiek?

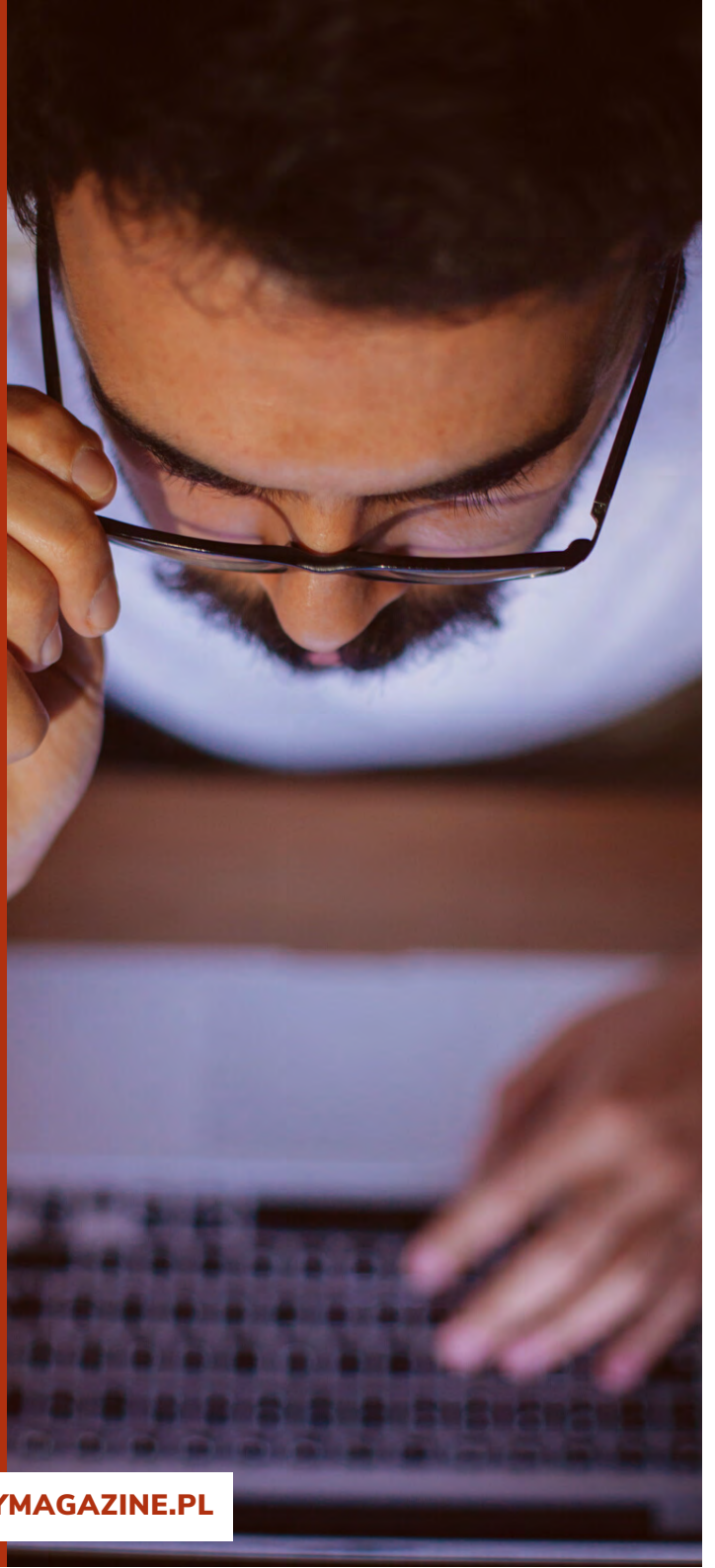
Ataki socjotechniczne, bazujące na manipulacji i eksploatacji ludzkich emocji oraz decyzji, zyskują na znaczeniu. Socjotechnika, choć znana od dawna, w nowoczesnej, cyfrowej rzeczywistości powoduje nieproporcjonalnie duże szkody. Statystyki mówią za siebie. Zgodnie z danymi raportu CERT Polska z 2022 roku, phishing był najczęściej zgłaszanym rodzajem incydentu. Z informacji Safetica wynika, że aż 80% firm traci dane w wyniku błędów pracowników lub ich świadomego działania Zaawansowany rozwój sztucznej inteligencji, nie wróży nic dobrego, a ataki będą coraz bardziej wyrafinowane.

JAK BRONIĆ SIĘ PRZED ATAKAMI SOCJOTECHNICZNYMI?

Chociaż rzadko kiedy udaje się powstrzymać wszystkie ataki, można podjąć kroki w celu zmniejszenia prawdopodobieństwa ich powodzenia. Kluczowe jest zrozumienie, że ostateczną linią obrony często jest właśnie człowiek. Z tego powodu tak ważne jest przeprowadzanie testów socjotechnicznych, które nie tylko identyfikują słabe punkty w ludzkim elemencie bezpieczeństwa, ale również edukują i zwiększają świadomość zagrożeń wśród pracowników.
Pracownik może na własnej skórze poczuć jak wygląda zaawansowany atak socjotechniczny, a najlepszą formą edukacji jest praktyka. Lepiej, żeby pracownik dał się nabrać podczas testu socjotechnicznego i wyciągnął z tego wnioski, niż żeby został oszukany podczas rzeczywistego ataku i skompromitował system firmy.

Po każdym teście ważne jest, żeby pokazać wyniki, wyciągnąć wnioski i przeprowadzić na tej podstawie szkolenie pracowników. Testy i szkolenia należy prowadzić regularnie, bo techniki manipulacji ewoluują i regularne aktualizacje wiedzy są kluczowe.





KULTURA ORGANIZACYJNA POPRAWIAJĄCA CYBERBEZPIECZEŃSTWO

Cyberhigiena wynika w dużej mierze z kultury organizacji i atmosfery pracy. Nie można karać pracowników za to, że kliknęli w złośliwy link. Jeśli pojawią się takie przypadki, kolejni pechowcy ze wstydu i obawy przed konsekwencjami nie będą zgłaszali incydentów, które nie zawsze zostaną wychwycone przez systemy bezpieczeństwa. A stąd już tylko krok do bardzo poważnych konsekwencji...

Pracownicy powinni wiedzieć, jak wyglądają procedury i w jaki sposób zgłaszać, że padli ofiarą cyberataku. Zamiast karać lepiej nagradzać - system nagród za zgłaszanie podejrzanych maili czy incydentów może bardzo pozytywnie wpłynąć nie tylko na poziom wiedzy pracowników, ale także na ich poczucie odpowiedzialności za bezpieczeństwo całej infrastruktury. Mogą to być drobne nagrody, które jednak skłonią ich do zaangażowania się w weryfikację przychodzącej korespondencji, a to znacznie poprawi bezpieczeństwo. W dużych organizacjach do rozważenia może być również wewnętrzna grywalizacja w obszarze bezpieczeństwa IT.

TESTY SOCJOTECHNICZNE. CO, JAK I DLACZEGO?

Jak dokładnie testy socjotechniczne pomagają w obronie przed cyberatakami? Testy te symulują różne scenariusze ataków socjotechnicznych, takie jak phishing, preteksting czy tailgating.

Zakres testów socjotechnicznych może być szeroki, od wysyłania zwykłych maili na skrzynki pocztowe pracowników, po próbę dostania się na teren firmy. Taka symulacja to najlepszy sposób, aby zidentyfikować słabe punkty i podatności wśród pracowników, a później móc je wzmocnić. Wyniki testów pozwalają pracownikom zobaczyć, jak łatwo można dać się oszukać, a co za tym idzie – jakie konsekwencje mogą wyniknąć z ich błędów. To znacznie wzmaga czujność.

PRZEBIEG TESTU SOCJOTECHNICZNEGO W 5 KROKACH

Testy socjologiczne przebiegają zgodnie ze schematem, w którym powtarzają się następujące etapy:

1. **Ustalenie zakresu prac**. Testy socjotechniczne powinny być zaplanowane z wyprzedzeniem i wykonane tylko po zatwierdzeniu wszystkich ustaleń po obu stronach. Ustala się zakres prac i terminy wykonania testów.

2. **Scenariusze i symulacje**. Na tym etapie strona atakująca przeprowadza rozpoznanie oraz projektuje scenariusz ataku. Po zebraniu danych wywiadowczych musi zaplanować jakich technik użyć, aby test był jak najlepiej dopasowany do specyfiki klienta.

3. **Egzekucja testu**. Po zatwierdzeniu planu zaczyna się część praktyczna. W zależności od typu testu atakujący może podkładać fałszywe nośniki danych w miejscu pracy, może telefonować do poszczególnych pracowników w celu wyłudzenia danych, albo przeprowadzić klasyczną kampanię phishingową zachęcającą do podania wrażliwych danych lub pobrania złośliwego załącznika.

4. **Gromadzenie danych i analiza.** Najważniejszy etap, jeżeli chodzi o wyciąganie wniosków po teście. W tym momencie powstaje raport z symulowanego ataku, zbierane są wszelkie statystyki i identyfikowane są słabe punkty. Jest to najważniejszy etap, ponieważ na bazie tych informacji widać, co (lub w tym przypadku bardziej: kto) w danej organizacji wymaga wzmocnienia.

5. **Edukacja i działania naprawcze.** Po teście, gdy wiadomo już, na jakie techniki pracownicy są najbardziej podatni, jakie systemy

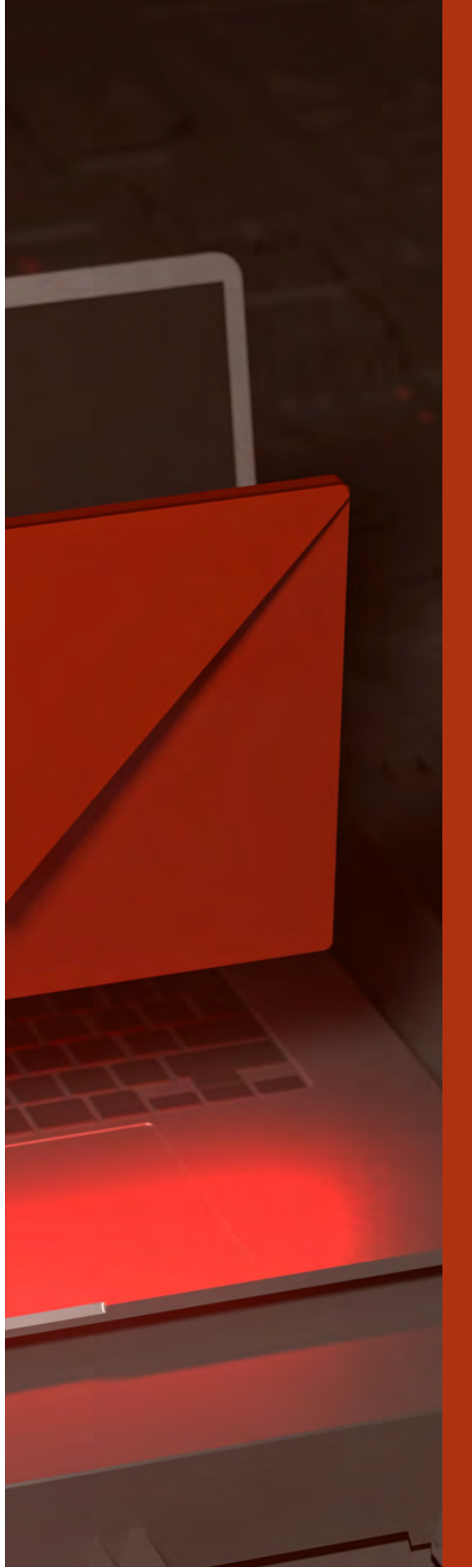
bezpieczeństwa zawodzą, można zabrać się za edukację i wprowadzić działania naprawcze. Na tym etapie przeprowadza się spersonalizowane szkolenia dla pracowników i wdraża się technologie, które pomagają w utrzymaniu bezpieczeństwa.

Jeden test, oczywiście, nie wystarczy, by zapewnić pełne bezpieczeństwo organizacji. Zagrożenia się zmieniają, a hakerzy stają się coraz sprytniejsi. Nie zapominajmy również o tym, że pracownicy rotują, a nowy skład nie zawsze posiada odpowiedni poziom wiedzy o zagrożeniach. Najważniejsze, aby aktualizować i sprawdzać wiedzę pracowników na bieżąco. Zakłada się, że, aby pracownicy byli na bieżąco z zagrożeniami, testy i szkolenia powinno się przeprowadzać raz na kwartał.

TESTY SOCJOTECHNICZNE Z REDSABER SECURITY

Zabezpieczenie infrastruktury technicznej to tylko połowa zasobów niezbędnych do wygrania bitwy o cyberbezpieczeństwo. Drugą, równie ważną częścią organizacji są ludzie - ich wiedza i świadomość zagrożeń.

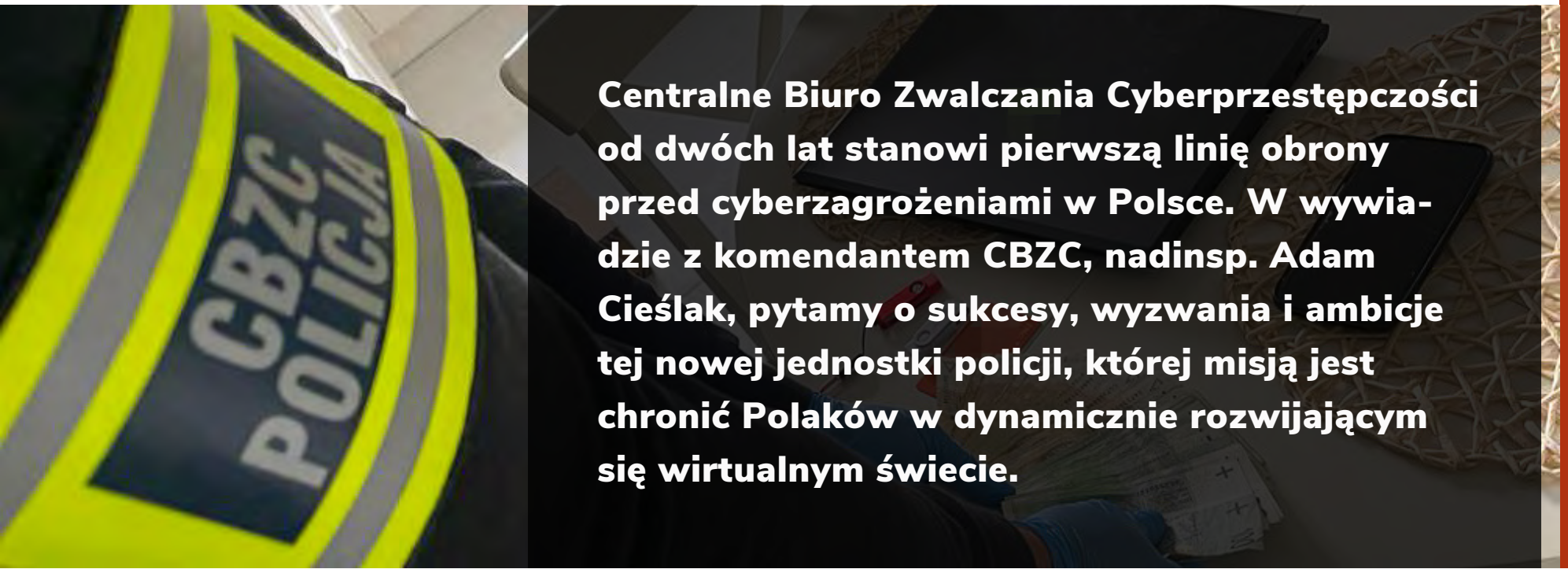
Redsaber Security specjalizuje się w dziedzinie testów socjotechnicznych, dostarczając skuteczne rozwiązania na miarę potrzeb testowanej organizacji. Wykorzystujemy realistyczne symulacje, aby zdiagnozować słabe punkty w świadomości i zachowaniach pracowników, co jest kluczowym elementem w zapewnieniu pełnego spektrum cyberbezpieczeństwa. Po identyfikacji potencjalnych luk oferujemy dedykowane szkolenia i edukację, mając na celu podniesienie ogólnego poziomu bezpieczeństwa. Zapewniamy ciągłość i adaptacyjność wobec zmieniających się warunków i zagrożeń, aby wzmocnić cyberbezpieczeństwo Twojej firmy.



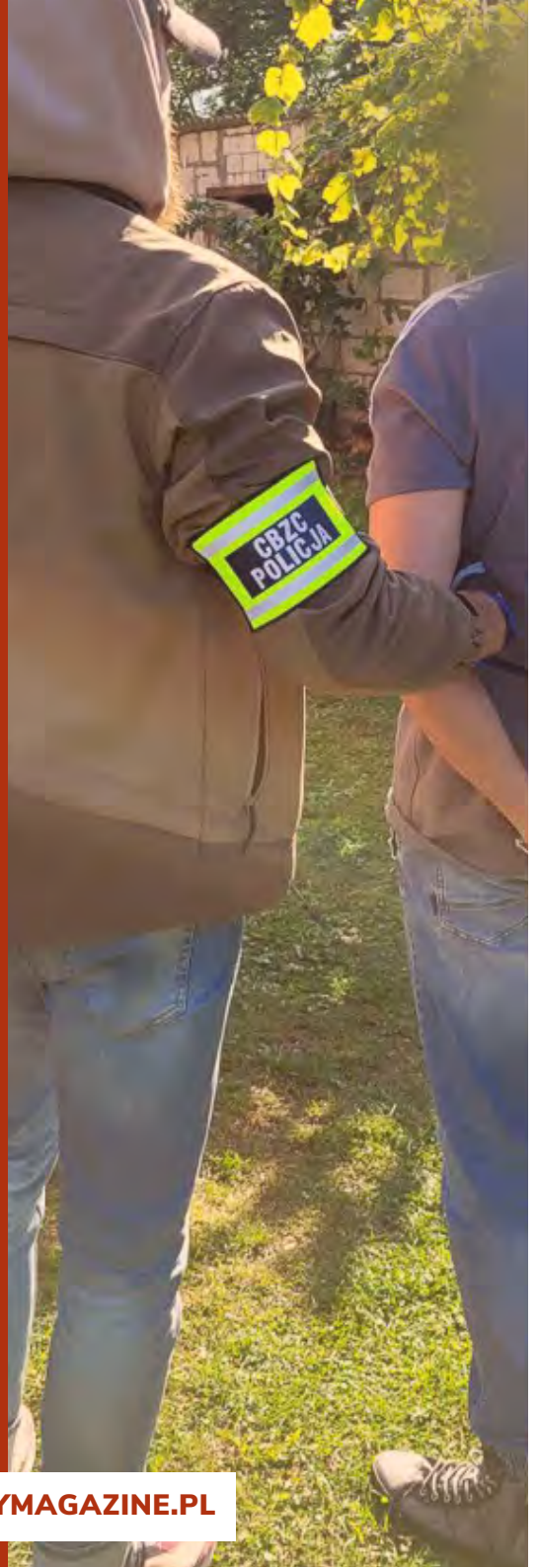

Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

DWA LATA NA FRONCIE WALKI Z CYBERPRZESTĘPCZOŚCIĄ

nadinsp. Adam Cieślak
Centralne Biuro Zwalczania Cyberprzestępczości



Centralne Biuro Zwalczania Cyberprzestępczości od dwóch lat stanowi pierwszą linię obrony przed cyberzagrożeniami w Polsce. W wywiadzie z komendantem CBZC, nadinsp. Adam Cieślak, pytamy o sukcesy, wyzwania i ambicje tej nowej jednostki policji, której misją jest chronić Polaków w dynamicznie rozwijającym się wirtualnym świecie.



Niebawem miną dwa lata od powołania do życia Centralnego Biura Zwalczania Cyberprzestępczości. Jakie wyzwania okazały się najbardziej wymagające dla Biura w tym czasie?

nadinsp. Adam Cieślak: CBZC formalnie powstało 12 stycznia 2022 roku. Pierwsze pół roku istnienia Biura to ciężki okres prac organizacyjnych, formowania struktur Biura, rekrutacji Policjantów z pionu cyber oraz innych jednostek Policji. Za faktyczny start Biura przyjmujemy datę 12 lipca 2022 roku. To w tym dniu blisko 70 % policjantów pełniących służbę w komórkach ds. zwalczania cyberprzestępczości w KGP i w komendach wojewódzkich przeszło do CBZC, a wraz z nimi część prowadzonych przez nich spraw zarówno operacyjnych jak i procesowych.

Od samego początku wyzwań było bardzo wiele. Tworzenie Biura w początkowym okresie spoczywało na barkach kilku a następnie kilkunastu osób. Do tych zadań zaliczało się między innymi opracowanie wszelkiej dokumentacji wymaganej przepisami, koncepcji pracy Biura, utworzenie założeń strukturalnych, przygotowanie testów i procedury weryfikacyjnej dla kandydatów do CBZC, przygotowanie koncepcji budowy siedzib dla CBZC zarówno w centrali, jak i w terenie, opracowanie specyfikacji do zakupów sprzętu komputerowego, oprogramowania, licencji.

Obecnie liczba wyzwań rośnie z każdym dniem, natomiast trzy najważniejsze to: rekrutacja i pozyskiwanie nowych funkcjonariuszy, kwestie logistyczne związane z budową siedzib CBZC oraz trzecia - zadbanie o to, aby biuro zajmowało się najbardziej poważnymi zagrożeniami w cyberprzestrzeni poprzez właściwy dobór spraw, podniesienie poziomu pracy operacyjnej oraz rozwój funkcjonariuszy.

Jakie działania edukacyjne i prewencyjne podjęło CBZC w tym czasie w celu podniesienia świadomości społeczeństwa w zakresie cyberbezpieczeństwa?

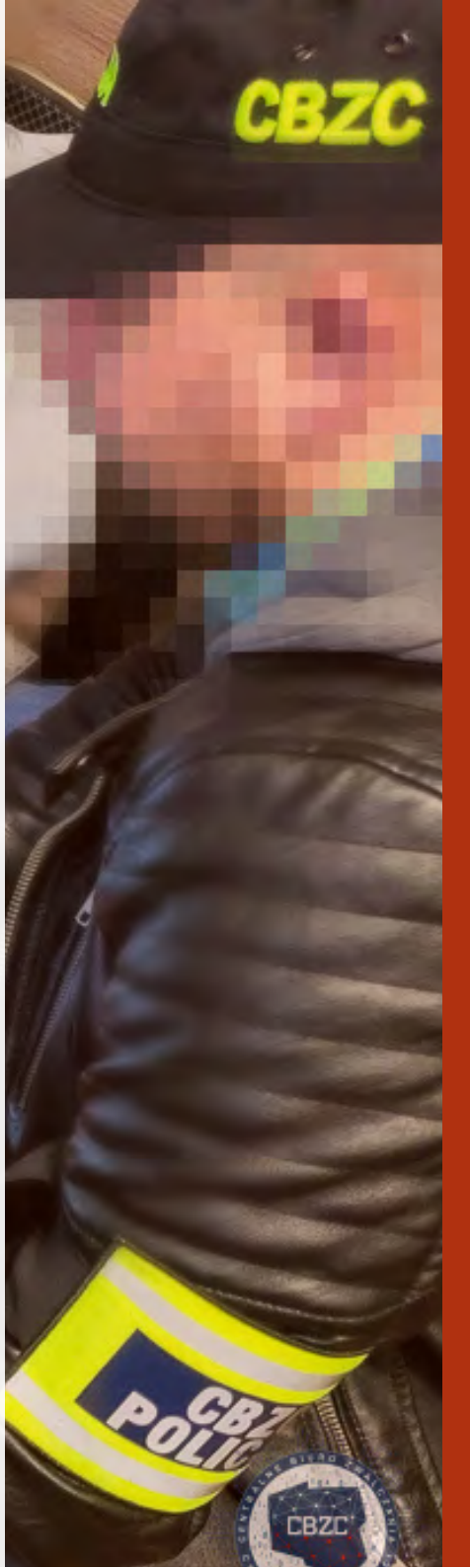
A.C.: Od początku istnienia CBZC stawiamy duży nacisk na działania informacyjno – profilaktyczne. Na początku grudnia 2022 powołaliśmy w CBZC Zespół ds. Zapobiegania Cyberprzestępczości. Nasze działania są wielopłaszczyznowe. Skupiają się w głównej mierze na uświadamianiu społeczeństwa jak nie stać się ofiarą cyberprzestępców.

Ponieważ najwięcej przestępstw to oszustwa internetowe, CBZC aktywnie włącza się w cykl kampanii prowadzonych wspólnie z Bankowym Centrum Cyberbezpieczeństwa Związku Banków Polskich – FINCERT.PL oraz NASK-iem, w których informujemy o najczęściej występujących sposobach oszustw w sieci, o zagrożeniu spoofingiem, przedstawiamy zasady bezpiecznych zakupów w Internecie, pokazujemy, jak oszuści wykorzystują aktualne wydarzenia w kraju i za granicą do tworzenia nowych kampanii phishingowych.

Uruchomiliśmy stronę internetową i profile na FB, LinkedIn oraz na platformie X gdzie zamieszczamy różnego rodzaju porady i informacje o aktualnych zagrożeniach w sieci. Stworzyliśmy materiały wideo przestrzegające przed najczęstszymi zagrożeniami w sieci. Policjanci CBZC biorą udział w różnego rodzaju webinariach oraz spotkaniach profilaktycznych. Mamy świadomość, że podnoszenia poziomu wiedzy użytkowników Internetu znacząco wpływa na skalę cyberprzestępczości.

Jakie są więc najczęstsze rodzaje cyberprzestępstw zgłaszane do CBZC?

A.C.: CBZC jest jednostką organizacyjną Policji działającą na obszarze całego kraju. Według mnie, największym zagrożeniem są oszustwa internetowe, których skala



zarówno w Polsce, jak i na całym świecie jest ogromna. Prowadzimy najpoważniejsze oraz najbardziej złożone postępowania. Często postępowania te są łączone z terenu całej Polski z uwagi na rodzaj przestępstwa, np. wielu pokrzywdzonych działalnością fałszywego sklepu internetowego czy oszukańczej platformy inwestycyjnej.

Poza wymienionymi wyżej przestępstwami wskazałbym jeszcze oszustwa typu BEC (business email compromise), oszustwa na platformach sprzedażowych czy tzw. oszustwa nigeryjskie. Poważnym problemem są też ataki ransomware, ataki DDoS oraz przestępstwa związane z seksualnym wykorzystywaniem osób małoletnich. Wiele z tych spraw ma charakter międzynarodowy i wymaga ustaleń poza granicami kraju.

A jakie są największe zagrożenia dla cyberbezpieczeństwa w Polsce?

A.C.: W Centralnym Biurze Zwalczania Cyberprzestępczości zagrożenia dzielimy na 3 główne obszary. Pierwszym z nich jest Cyber-dependent crime – zaawansowane technicznie przestępstwa, które nie mogą być popełnione bez wykorzystania technologii informatycznych. Należą do nich np. hacking, ransomware, ataki DDoS, malware, bulletproof hosting Drugim obszarem jest Cyber-enabled crime, czyli tradycyjne przestępstwa, które można popełnić bez komputera, ale w pewnych okolicznościach są możliwe do popełnienia na szeroką skalę dzięki wykorzystaniu sieci Internet. Należą do nich takie przestępstwa jak oszustwa internetowe, fałszywe e-sklepy, przestępstwa inwestycyjne często z wykorzystaniem technologii deepfake i sztucznej inteligencji.

Trzecim obszarem są przestępstwa dotyczące szczególnie bezbronnej grupy ofiar, a mianowicie dzieci. Mowa o wykorzystywaniu seksualnym dzieci w sieci Internet. Zauważamy znaczny wzrost tego przestępstwa od momentu wybuchu pandemii covid-19 i zmieniającej się sytuacji geopolitycznej na świecie.

Jakie są największe sukcesy CBZC w walce z cyberprzestępczością?

A.C.: Od początku istnienia CBZC przeprowadziliśmy już wiele operacji zarówno na terenie Polski, ale również poza granicami naszego państwa, ściśle współpracując w tym zakresie z Europolem i organami ścigania na całym świecie.

W większości przypadków o naszych działaniach można przeczytać na stronie internetowej lub profilach w social mediach. Wśród zrealizowanych operacji pozwolę sobie wspomnieć choćby operację „COOKIE MONSTER", która miała na celu przejęcie i zamknięcie rynku przestępczego Genesis Market.

Operację „POWER OFF" dotyczącą likwidacji infrastruktury przestępczej, przy pomocy której dokonywano ataków DDoS na systemy informatyczne na całym świecie.

Operacje „Anastazja" i „Barbossa" skierowane wobec sprawców przestępstw o podłożu seksualnym. W efekcie naszych czynności zatrzymano 93 osoby podejrzane o popełnienie powyższych przestępstw, 30 z nich zostało tymczasowo aresztowanych. W wyniku 169 przeszukań mających miejsce na terenie całej Polski zabezpieczono komputery i nośniki pamięci zawierające ponad 185,5 tys. plików video i zdjęć przedstawiających seksualne wykorzystywanie dzieci.

CBZC cały czas się rozwija i prowadzi intensywne rekrutacje. Jakie kwalifikacje są wymagane od osób chcących dołączyć do CBZC? Jakie są główne wyzwania w rekrutacji do CBZC?

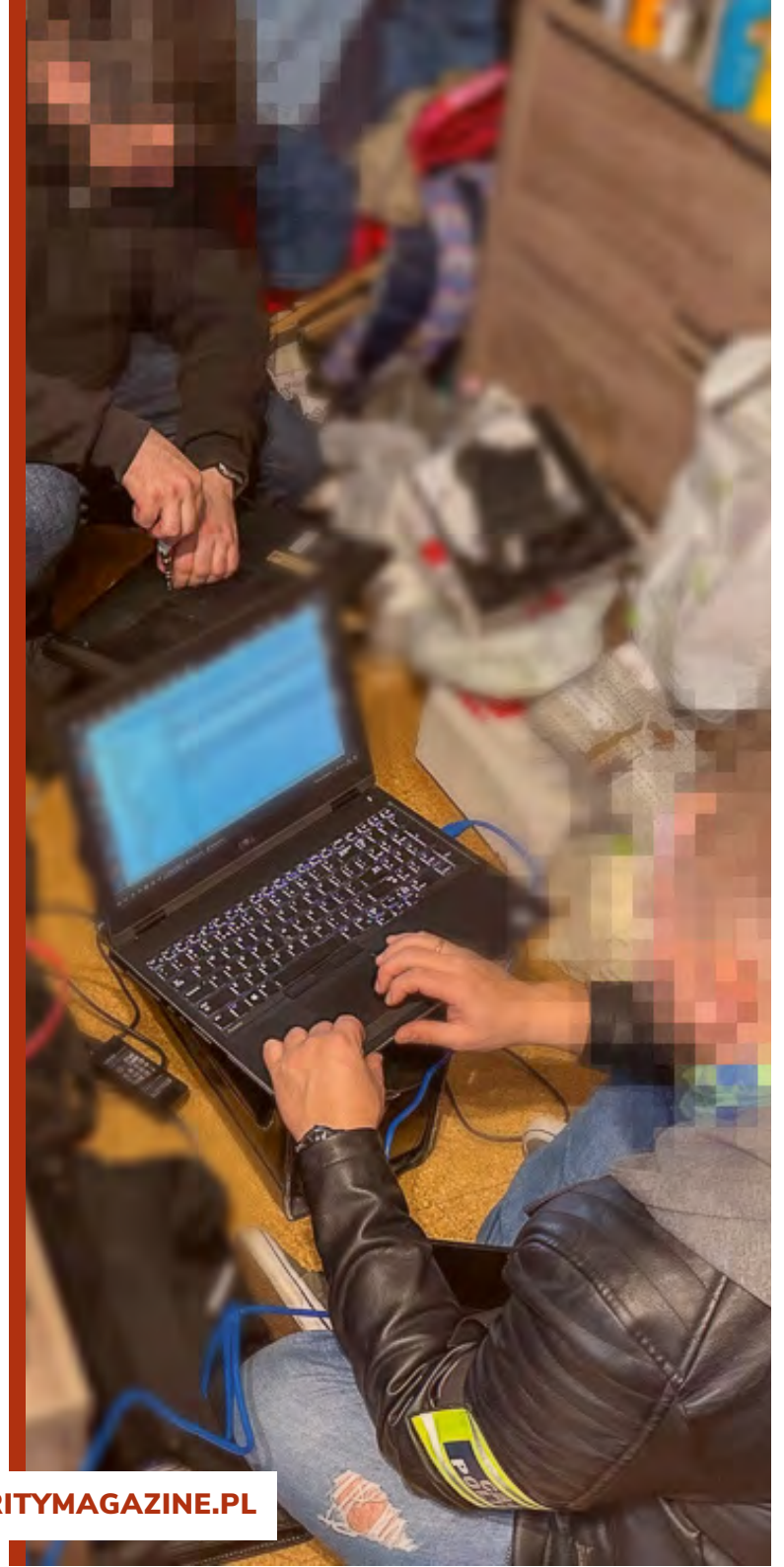
A.C.: Do służby przyjmowane są głównie osoby z wiedzą oraz umiejętnościami z zakresu informatyki i nowoczesnych technologii teleinformatycznych. Postępowanie kwalifikacyjne nie zawiera testu sprawności fizycznej oraz testu wiedzy ogólnej, natomiast obejmuje sprawdzenie wiedzy i umiejętności z zak-

resu informatyki, funkcjonowania systemów informatycznych, systemów teleinformatycznych, sieci teleinformatycznych oraz znajomości języka obcego obejmującej te dziedziny.
Stan etatowy Centralnego Biura Zwalczania Cyberprzestępczości wynika z założeń ustawy powołującej CBZC, która zakłada, że każdego roku etatów w tym Biurze będzie przybywać.
W bieżącym roku wynosi 800 etatów, w 2024 roku wyniesie 1300 etatów a docelowo w 2025 będzie to 1800 etatów.

Od listopada 2022 roku trwa kampania promocyjna zachęcająca do wstąpienia do służby. Od jej rozpoczęcia podania o przyjęcie złożyło ponad 370 osób. Proces rekrutacji do CBZC jest wieloetapowy i oprócz wspomnianych wyżej testów wiedzy są to również badania lekarskie, badania na poligrafie, badania psychologiczne oraz procedura dostępu do informacji niejawnych. Niestety dużo osób nie przeszło poszczególnych etapów postępowania, najwięcej testu wiedzy. W momencie wydawania tego artykułu pierwsze osoby, które pozytywnie ukończyły cały proces rekrutacji są w naszych szeregach.

Jakie są największe wyzwania w zakresie świadomości społecznej dotyczącej cyberprzestępczości?

A.C.: Obecne realia życia bardzo sprzyjają działaniom przestępczym, głównie poprzez stopniową utratę czujności potencjalnych ofiar. Ograniczenia kontaktów osobistych, praca zdalna, zdalne nauczanie, spowodowało przeniesienie kontaktów w obszar telekomunikacji, a głównym medium stał się Internet.



Tym samym zwielokrotniła się ilość informacji wymienianych przez wiadomości sms, komunikatory internetowe, czy pocztę elektroniczną. W takim natłoku elektronicznego morza informacji przestaje się weryfikować każdą informację z osobna. Coraz częściej „klika się" w niesprawdzone linki w korespondencji elektronicznej, coraz rzadziej weryfikujemy nadawcę wiadomości lub dokumenty w formie zdigitalizowanych obrazów, czyli popularnych skanów, których podrobienie lub spreparowanie nie jest rzeczą trudną. Kluczową rolę w mechanizmie przestępstw pełni socjotechnika stosowana przez sprawców przestępstw.

Obserwujemy, że ich ofiarami są ludzie w różnym wieku, o różnym wykształceniu, wykonującym różne zawody. Centralne Biuro Zwalczania Cyberprzestępczości w dalszym ciągu będzie kładło nacisk na uświadamianie jak największej liczby osób o aktualnych sposobach wykorzystywanych przez oszustów internetowych oraz o sposobach jak nie stać się ofiarą cyberprzestępców. Będzie to zarówno udział w kampaniach społecznych przestrzegających przed aktualnymi zagrożeniami, jak i dalszy udział funkcjonariuszy CBZC w różnego rodzaju webinariach oraz spotkaniach profilaktycznych.

Jakie są główne cele współpracy między NASK a CBZC, o której czytaliśmy w jednym z ostatnich artykułów Biura?

A.C.: Współpraca między NASK-iem a Centralnym Biurem Zwalczania Cyberprzestępczości realizowana była regularnie jeszcze przed podpisaniem porozumienia.

Funkcjonariusze CBZC są współautorami wielu publikacji realizowanych przez NASK, współprowadzili webinary jak również przekazywali dane statystyczne i angażowali się w wiele przedsięwzięć o charakterze edukacyjnym.

Współpraca jest realizowana na wielu płaszczyznach jednak głównie skupiać się będzie na wymianie informacji o technikach i sposobach działań przestępców, na wymianie doświadczeń i pomysłów w tworzeniu oraz użytkowaniu technologii informatycznych, a także na realizacji wspólnych projektów i przedsięwzięć związanych ze zwalczaniem cyberprzestępczości, szkoleń czy działań prewencyjnych poprzez podejmowanie wspólnych przedsięwzięć edukacyjnych, profilaktycznych oraz informacyjnych.

Jakie są plany CBZC na najbliższą przyszłość w kontekście zwalczania cyberprzestępczości w Polsce?

A.C.: Przede wszystkim wzrost zatrudnienia policjantów z odpowiednimi umiejętnościami, wiedzą techniczną i znajomością języków obcych szczególnie w komórkach terenowych Biura. Ze wzrostem zatrudnienia ściśle związany jest rozwój infrastruktury Biura. Mam tutaj na myśli budowę nowych siedzib oraz zakup specjalistycznego sprzętu i oprogramowania. Niezbędne jest również ciągłe podnoszenie poziomu kwalifikacji policjantów CBZC.
Bardzo ważnym aspektem pod kątem przyszłości jest rozwój współpracy międzynarodowej, głównie w obszarze operacyjnym.

Dziękuję za rozmowę i życzę kolejnych sukcesów.

Fot. CBZC (7)

PUBLIKUJ OGŁOSZENIA OFERT PRACY

SZUKASZ SPECJALISTY Z BRANŻY SECURITY?

ZACZNIJ REKRUTOWAĆ Z NAMI

Znajdź najlepszych w branży z "Security Magazine"!

Publikuj ogłoszenia o pracę i dotrzyj do tysięcy wykwalifikowanych profesjonalistów z sektora security.

Celuj w specjalistów z branży

Wysoka widoczność wśród kandydatów

Skróć czas rekrutacji

Napisz do nas: redakcja@securitymagazine.pl **Zadzwoń:** +48 518 609 987

SECURITYMAGAZINE.PL

USTAWIANIE PRZETARGÓW. WYKRYWANIE I ZAPOBIEGANIE

Rafał Lachowicz
Specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji

Proces udzielania zamówień niejednokrotnie bywa areną podejrzanych praktyk, ofiarą których padają przedsiębiorstwa ogłaszające przetargi. Oferenci, chcąc zdobyć upragniony kontrakt, nie zawsze skupiają się na przygotowaniu najlepszej oferty. Często zamiast tego szukają nieuczciwych dróg na skróty.

Filozofia przetargów - bez względu na to, czy są one realizowane z zastosowaniem ustawy Prawo zamówień publicznych czy prowadzone w oparciu o wewnętrznie opracowane procedury – wydaje się prosta: przedsiębiorstwo rozpoznaje potrzebę, ustala sposób jej zaspokojenia, ogłasza chęć nabycia towaru lub usługi, określa minimalne warunki i kryteria oceny ofert, ocenia złożone oferty i w konsekwencji tej oceny wybiera najlepszą.

Zainteresowani realizacją zamówienia przygotowują oferty w taki sposób, by jak najbardziej spełniały wszystkie określone w ogłoszeniu warunki, a oferta odpowiadająca potrzebom, charakteryzująca się najlepszym stosunkiem ceny do jakości, wygrywa.

Z dysponentem najlepszej oferty podpisywany jest kontrakt, w wyniku realizacji którego przedsiębiorstwo zaspokaja zidentyfikowaną wcześniej potrzebę.

KORUPCJA W PROCESIE ZAMÓWIEŃ

Czasami praktyka wygląda jednak nieco inaczej. Bywa, że oferenci próbują zwiększyć swoje szanse w przetargu za pomocą nieuczciwych praktyk. Zgodnie z wynikami badań firmy EY, opublikowanymi w dokumencie pn. Uczciwość pod lupą. Przyszłość zarządzania zgodnością. 15 Światowe Badania Nadużyć Gospodarczych, 11% pracowników odpowiedzialnych za realizację przetargów jest zdania, że wręczanie korzyści majątkowej w celu zdobycia pożądanego kontraktu jest powszechną praktyką w ich branży, a 13% z nich uważa za zasadne oferowanie gotówki ce-

lem zdobycia lub utrzymania kontraktu. Jednocześnie, jak wynika z ubiegłorocznej edycji Report to the Nations ACFE, aż 50% przypadków wykrytych nadużyć stanowi korupcja.

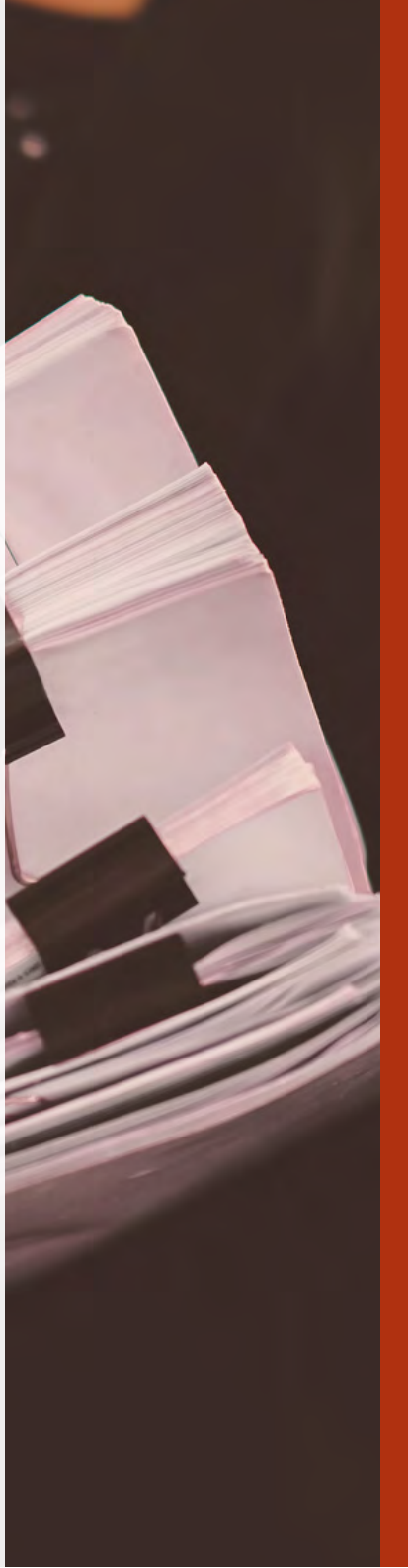
Można zatem zaryzykować tezę, że zjawisko zmowy korupcyjnej, zawieranej pomiędzy pracownikiem przedsiębiorstwa ogłaszającego przetarg a nieuczciwym oferentem, ma charakter jeśli nawet nie powszechny, to przynajmniej niepokojąco częsty.

Pracownicy, do których w analizowanym przypadku kierowane są propozycje korupcyjne, to osoby odpowiedzialne za każdy etap procedury przetargowej, zatem: pracownicy pionów zaopatrzenia i zamówień, pracownicy bezpośrednio kontaktujący się z oferentami oraz pracownicy odpowiedzialni za zawieranie zobowiązań finansowych w imieniu przedsiębiorstwa. Metody, jakimi mogą się posługiwać w celu ustawienia przetargu, są uzależnione od przydzielonych im zakresów obowiązków i przyznanych kompetencji. Im są one większe, tym większą mają oni możliwość manipulacji przetargiem.

Obowiązujące w przedsiębiorstwach procedury przetargowe mogą się od siebie różnić w zależności od wielkości czy sposobu organizacji przedsiębiorstwa, w każdym z nich można jednak wyróżnić trzy podstawowe etapy: przygotowanie zapytania ofertowego, ogłoszenie zapytania ofertowego oraz ocena i wybór oferty.

PRZYGOTOWANIE ZAPYTANIA OFERTOWEGO

Nieuczciwe zachowania, jakie mogą wystąpić na etapie przygotowanie zapytania ofertowego, to najczęściej: zgłoszenie przez pracownika konieczności dokonania zamówienia określonej usługi lub towaru mimo braku rzeczywistej potrzeby przeprowadzenia takiego zamówienia, nieujawnione spotkania oferentów z pracownikami odpowiedzial-



nymi za przetargi, przygotowanie zapotrzebowania w taki sposób, by sztucznie podzielić zamówienie na kilka mniejszych i uniknąć tym samym zastosowania obowiązującego trybu dla zamówień o większej wartości, dopasowanie warunków udzielenia zamówienia do konkretnego oferenta, przygotowanie zapytania ofertowego we współpracy z konkretnym oferentem, wskazanie w ofercie parametrów technicznych lub jakościowych możliwych do spełnienia tylko przez jednego oferenta, przesadne komplikowanie opisu przedmiotu zamówienia oraz towarzyszącej mu dokumentacji, mające na celu zniechęcenie do składania konkurencyjnych ofert oraz takie określenie warunków udziału w zamówieniu i kryteriów oceny, że do przetargu zgłosić się może tylko jeden, konkretny oferent, który jako jedyny je spełnia.

OGŁOSZENIE ZAPYTANIA OFERTOWEGO

Najpopularniejsze nadużycia, do jakich dochodzi na etapie ogłoszenia zapytania ofertowego, to: nieupublicznienie zapytania ofertowego mimo wymogów wynikających z obowiązujących procedur, opublikowanie zapytania ofertowego po terminie składania ofert (ze sfałszowaniem daty jego publikacji), wysyłanie zapytań ofertowych do fikcyjnych oferentów, utrzymywanie nieuprawnionych kontaktów z wybranym oferentem w trakcie procedury przetargowej, publikowanie zapytania ofertowego w terminie niemożliwym do przygotowania i złożenia oferty, publikowanie zapytania ofertowego w przeddzień szeregu dni wolnych od pracy (długi weekend, przerwa świąteczna) czy publikowanie zapytania ofertowego w miejscach, co do których istnieją niewielkie szanse, że trafią na nie pozostali oferenci.

OCENA I WYBÓR OFERT

Na etapie oceny i wyboru ofert dochodzić może do następujących praktyk: udostępnianie wybranemu oferentowi treści pozostałych ofert, co pozwala na przygotowanie bardziej konkurencyjnej oferty, umożliwienie konkretnemu oferentowi złożenia oferty po wskazanym w ogłoszeniu terminie (najczęściej po zapoznaniu go z treścią pozostałych ofert), umożliwienie konkretnemu oferentowi uzupełnienia lub poprawienia oferty, ocena i przyjęcie do realizacji oferty, która nie spełnia wymaganych parametrów technicznych lub jakościowych oraz ukrycie (lub zniszczenie) ofert, które uzyskały lepszą ocenę niż oferta pozostającego w zmowie oferenta.

SYGNAŁY OSTRZEGAWCZE I WYKRYWANIE

Mimo powszechności zjawiska zmów korupcyjnych,

zawieranych pomiędzy skorumpowanymi pracownikami przedsiębiorstw ogłaszających przetargi a nieuczciwymi oferentami oraz mimo ilości sytuacji, w których do nadużyć w procesie zamówień może w konsekwencji takiej zmowy dochodzić, żadne przedsiębiorstwo nie jest skazane na pozostanie bierną ofiarą tych nieuczciwych działań. Istnieje bowiem wiele sygnałów ostrzegawczych, wskazujących, że ogłaszany przetarg może być realizowany ze szkodą dla przedsiębiorstwa. Mogą być nimi nietypowe zachowania pracowników, niestandardowe operacje finansowe lub podejrzanie wyglądające dokumenty.

Najpoważniejszym sygnałem ostrzegawczym, mogącymi świadczyć o ustawionym przetargu, jest wystąpienie jednej lub wielu opisanych już wcześniej sytuacji na którymkolwiek z etapów postępowania przetargowego.

Pozostałe sygnały ostrzegawcze, ściśle związane z procesem zamówień, to: nienotowana wcześniej częstotliwość występowania zapotrzebowania na określoną grupę towarów lub usług, unikanie trybów konkurencyjnych, nieuzasadniony pośpiech podczas ogłoszenia przetargu, nieuzasadnione zwlekanie z ogłoszeniem przetargu, niechęć do rezygnacji z nieuzasadnionych przedmiotem zamówienia wymogów i kryteriów oceny, częste skargi odrzucanych oferentów na przejrzystość i uczciwość przeprowadzanych postępowań, ciągłe kierowanie zamówień do jednego oferenta lub wąskiej grupy oferentów, wybór oferentów o wątpliwej reputacji, skargi użytkowników na niską jakość dostarczanych towarów lub usług, krótkie, odbiegające od przyjętych w przedsiębiorstwie terminy opłacania faktur konkretnego wykonawcy zamówienia, rezygnacja z uzasadnionych zapisami kontraktu kar umownych czy też odbiór zamówienia mimo zauważalnych wad w jego realizacji.

Trzeba przy tym pamiętać, że sygnały ostrzegawcze nie stanowią dowodu na wystąpienie zmowy pomiędzy pracownikiem przedsiębiorstwa a oferentem. Są to jedynie po-

szlaki wskazujące na to, że do takiej zmowy mogło dojść. Powinny jednak budzić niepokój i być sumiennie weryfikowane, zwłaszcza wtedy, gdy pojawiają się w większej ilości.

Umiejętność identyfikowania sygnałów ostrzegawczych oraz zdolność ich weryfikacji jest najskuteczniejszą metodą wykrywania zmów korupcyjnych. Ignorowanie ich, czy to ze względu na zaufanie do pracowników, czy też z powodu zwykłej ignorancji, jest prostym przepisem na nieuchronne problemy.

ZAPOBIEGANIE

Zdecydowanie łatwiej – potwierdzi to każdy lekarz – jest jednak zapobiegać niż leczyć. Dlatego też, o ile umiejętność wykrywania ustawionych przetargów jest ważna, to znacznie ważniejsza jest umiejętność zapobiegania im.

Sposobem na to jest opracowanie oraz wdrożenie w przedsiębiorstwie takiej polityki przetargowej, która jeśli nawet nie uniemożliwi nieuczciwych praktyk (nikt nie jest w stanie przewidzieć każdego możliwego mechanizmu przestępczego), to przynajmniej radykalnie ograniczy możliwość ich występowania.

Podstawą przygotowania polityki przetargowej musi być świadomość, że proces zamówień zawsze będzie obszarem o wysokim ryzyku wystąpienia praktyk korupcyjnych. Dlatego też polityka taka – poza opisaniem trybów przetargowych i ich zasad - powinna szczegółowo wskazywać zakres kompetencji każdego pracownika, rolę, jaką pełni on w procesie zamówień oraz ścieżki postępowań w określonych okolicznościach. W szczególności powinna definiować sposób zachowania w sytuacjach, które mogą narażać pracownika na ryzyko: spotkania z potencjalnymi wykonawcami czy otrzymywanie od nich prezentów.

Przy opracowaniu polityki przetargowej można wzorować się na już istniejących rozwiązaniach lub skorzystać z doświadczenia i wiedzy ekspertów.

Istotne jest, by polityka ta uwzględniała indywidualne cechy przedsiębiorstwa, jego wielkość oraz strukturę organizacyjną tak, by zapewniając przejrzystość i uczciwość prowadzonych postępowań przetargowych, nie ograniczała jednocześnie możliwości ich realizacji.

Polityka® Bezpieczeństwa

ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE

SPRAWDŹ OFERTĘ

GRADACJA ZABEZPIECZEŃ. CO I KIEDY MA SENS?

Katarzyna Bieńkowska
Silny&Salamon

Lata praktyki w zabezpieczaniu łańcucha dostaw pozwalają dokonać nieoczywistych, a jednocześnie optymalnych wyborów. Znam sytuacje, w których już samo umieszczenie najprostszych plomb zabezpieczających w widocznym miejscu, stanowiło wystarczającą barierę dla prób naruszenia. Dlatego też właściwe rozpoznanie potrzeb klienta i dokonanie audytu zabezpieczenia łańcucha dostaw z udziałem doświadczonego partnera pozwalają świadomie przeanalizować realne wyzwania i dobrać właściwe dla firmy rozwiązania.

Warto rozpocząć od znalezienia odpowiedzi na kilka kluczowych pytań, które odnoszą się do funkcji plomby, czy ma spełniać tylko funkcję zabezpieczającą, czy też informacyjną, a także, co i gdzie ma ona zabezpieczać. Ważna jest również decyzja czy ma być wielorazowa czy nie, jak bardzo zaawansowana, a także czy ma być częścią szerszego systemu oznaczeń w firmie. To punkt wyjścia, który pomoże określić, jaki poziom zabezpieczeń jest niezbędny, by zapewnić sprawne procesy logistyczne.

Na różne potrzeby odpowiadają różne rozwiązania, a wiedza o nich pozwala dobrać te skuteczne i efektywne kosztowo. Czasem okazuje się, że rozwiązania zabezpieczające stosowane standardowo lub z przyzwyczajenia nie odpowiadają realnym potrzebom, które zmieniają się na przykład wraz z uwarunkowaniami gospodarczo-społecznymi. Dawniej wystarczyło zamknąć pojazd z transportem, a dziś przy rozbudowanej dystrybucji i wielu rozproszonych lokalizacjach, wszystkie pojemniki z towarami muszą być odpowiednio zamknięte i oznaczone.

Towary będące regularnie na celowniku złodziei, takie jak m.in. wyroby tytoniowe, artykuły AGD czy kosmetyki, będą wymagały wielostopniowych zaawansowanych zabezpieczeń i monitoringu. O tym jak ważnym elementem w łańcuchu dostaw jest bezpieczeństwo produktów w transporcie drogowym, wiedzą nie tylko firmy działające w tym obszarze, ale świadczą też dane regularnie raportowane przez stowarzyszenie TAPA (Transported Asset Protection Association) obejmujące 41 państw regionu EMEA. W samym tylko wrześniu (stan na 20.09.2023) zaraportowano 43 incydentów kradzieży wewnątrz łańcucha dostaw, w których straty wyniosły ponad 5,8 mln euro. Co ważne 70,1% to straty poniesione na terenie niezabezpieczonych placów parkingowych.

W obszarze ładunków o wysokiej wartości sprawdzają się plomby elektroniczne z wbudowanymi modułami GPS, GSM, RFID, BT, które zapewniają dokłady monitoring transportu. To np. system TrackLock 2.0 (plomba elektroniczna wraz z platformą), który działa w koncepcji IoT, dostarczając natychmiastowo informacji o położeniu, przebiegu trasy i statusie w każdym punkcie drogi.

Umożliwia przyznanie dostępu do towarów tylko osobom upoważnionym, dzięki uzbrajaniu plomby na kilka sposobów: przy użyciu kart RFID, platformy web, aplikacji mobilnej, SMS, BT lub kodu PIN.

Rozwiązanie można zintegrować z dowolnym systemem zarządzania, co stanowi bazę do optymalizacji procesów, dzięki łatwemu dostępowi do statystyk i analiz w czasie rzeczywistym. Nowoczesne systemy oparte na rozwiązaniach IoT, pozwalające na skuteczne zabezpieczenie naczep i ładunków, usprawniają procesy firm logistycznych.

Przy zaawansowanych rozwiązaniach zabezpieczających trzeba mieć na uwadze opłacalność takiej inwestycji, dlatego doświadczony doradca powinien wesprzeć klienta przy doborze właściwego, a także wyliczenia ROI.

UNIKALNA KOMBINACJA ROZWIĄZAŃ ZABEZPIECZAJĄCYCH

By zaprojektować dobrze zabezpieczony łańcuch dostaw, poza otwartością na wdrażanie nowych technologii, niezbędna jest umiejętność integrowania ich z klasycznymi rozwiązaniami, czyli plombami tradycyjnymi wyposażonymi w mechanizmy zabezpieczające. Kategorią plomb, które bardzo dobrze chronią środki transportu, magazyny, pojemniki, beczki są metalowe plomby linkowe. Pozwalają one wprowadzić dodatkowe elementy, takie jak trwałe nadruki laserowe z numeracją, logotypami czy kodami kreskowymi. Wiedza jak łączyć te rozwiązania, przyczynia się do oszczędności, a także elastycznego i szybkiego działania w procesach logistycznych.

Niejednokrotnie solidne plomby plastikowe sprawdzają się tam, gdzie konieczne jest zabezpieczenie transportu produktów, np. umieszczonych w workach. Wciąż jednak wiele firm działających w obszarze materiałów sypkich nie wie, że warto sięgnąć po np. plombę ze zwiększoną liczbą kolców. Praktyczne rozwiązanie, które opracowaliśmy dla jednego z naszych klientów, stanowi solidną ochronę przed ubytkiem zawartości worka. Nie zsuwa się z niego, a duża flaga umożliwia naniesienie dodat-

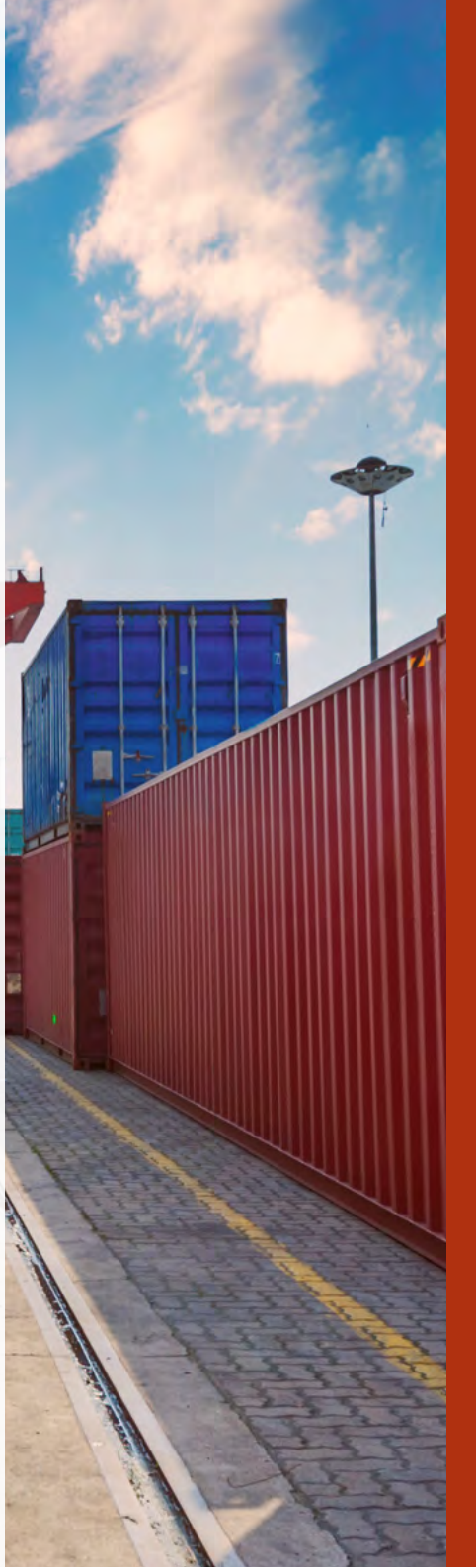
kowych informacji lub naklejanie etykiet.

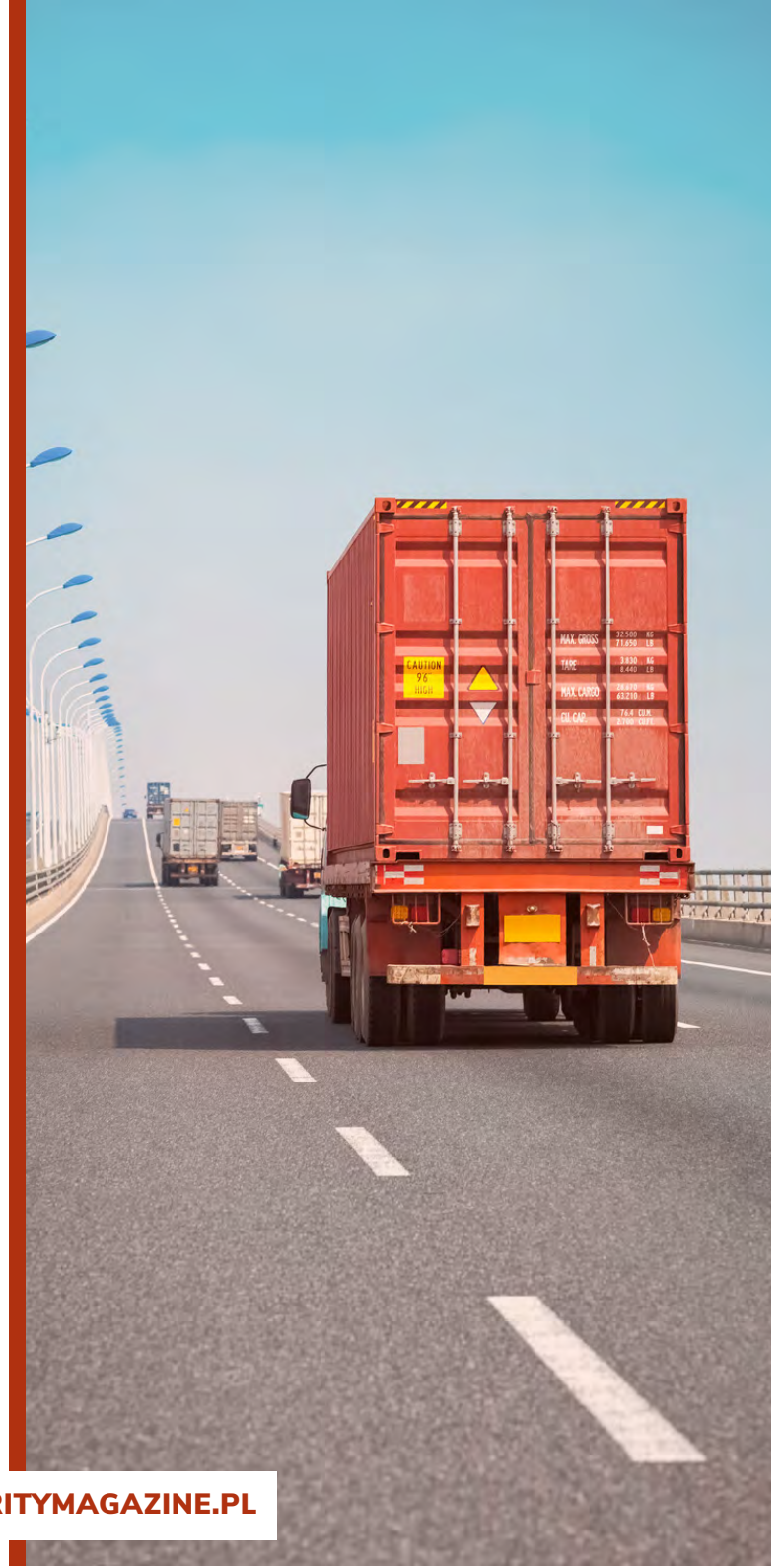
Jak się okazuje różnorodność gotowych plomb plastikowych, metalowych czy wielorazowych elektronicznych nie zawsze wystarcza, by znaleźć skuteczne zabezpieczenia. Są miejsca, w których nie można skorzystać z tradycyjnych plomb, ponieważ brakuje elementów, np. oczek do przełożenia plomby.

To powierzchnie płaskie i gładkie, takie jak drzwi do magazynów, biur, kontenerów, szaf, szuflad, gdzie konieczna jest informacja, czy ktoś je otworzył. W takich sytuacjach sprawdzają się plomby naklejkowe w postaci samoprzylepnych etykiet. Spełniają one rolę identyfikacyjną informując o naruszeniu, rozumianym jako otwarcie drzwi pomieszczeń, jak i ingerencji w pojemnik, beczkę lub karton. To podstawowe zastosowania tych niewielkich i praktycznych zabezpieczeń.

Co ciekawe, nasi klienci stosują też te rozwiązania, by pełniły rolę pieczęci na opakowaniach, ale i plomb informacyjnych, gwarancyjnych czy inwentaryzacyjnych. Plomby naklejkowe, zwane też etykietami proste w zastosowaniu zabezpieczenia, sprawdzą się w archiwizacji dokumentów. Łatwo nimi zakleić i oznaczyć teczki, segregatory oraz kartony. Pomagają chronić przedmioty i pomieszczenia przed próbami ingerencji, są też łatwe w aplikacji i usunięciu.

Na rynku znajduje się wiele rozwiązań z zakresu bezpieczeństwa, a mimo to często ciężko znaleźć odpowiednie. Zachęcam wtedy do dokładnej analizy biznesowej problemu, a następnie stworzenia wraz z naszym zespołem projektowym nietypowego, dedykowanego rozwiązania w postaci unikalnego produktu.





DOŚWIADCZENIE SPRZYJA OSZCZĘDNOŚCIOM

Rozwiązania cyfrowe oparte o najnowocześniejsze technologie to najwyższy poziom zabezpieczeń, który dostarcza informacji służących do optymalizacji procesów w firmach.

Ich dopełnieniem są fizyczne zabezpieczenia dające klientom poczucie pewności, że towary i miejsca są chronione przed manipulacją, nieuprawnionym wejściem czy kradzieżą. Dlatego do wydajnego podniesienia bezpieczeństwa w łańcuchu dostaw niezbędna jest przekrojowa wiedza i doświadczenie o zastosowaniu produktów w praktyce, by dobrać te właściwe, skuteczne, a zarazem efektywne kosztowo.

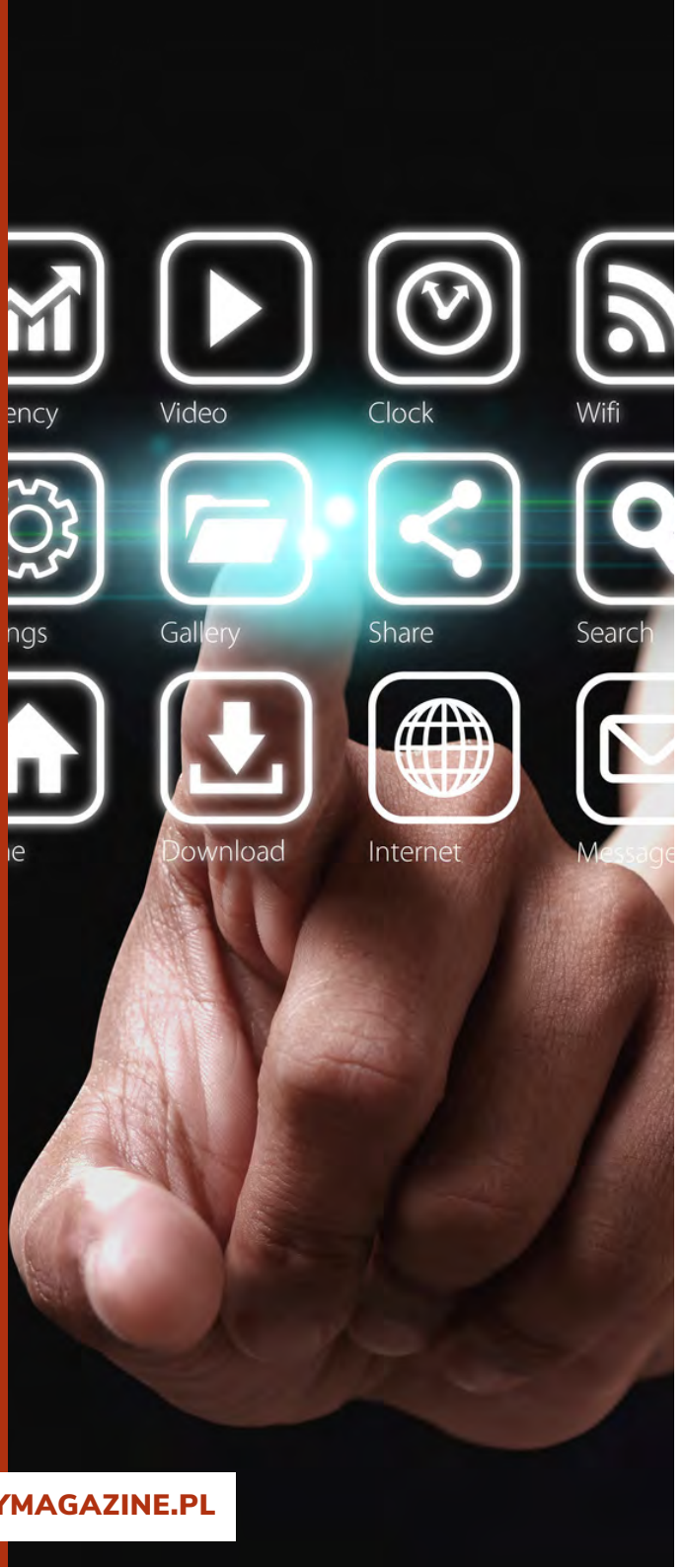
Dlatego zawsze gorąco zachęcam do korzystania z wiedzy ekspertów, którzy pomogą dopasować optymalny do potrzeb poziom zabezpieczeń, a także będą służyć wsparciem w wyliczeniu zwrotu z takiej inwestycji. Jestem przekonana, że sięgnięcie po ekspertyzę często będzie stanowiło większą oszczędność niż samodzielny wybór.

ZABEZPIECZANIE APLIKACJI TO WIĘCEJ NIŻ TECHNOLOGIA. WYWIAD Z ADRIANEM SROKĄ

Adrian Sroka
Architekt bezpieczeństwa

Architekt bezpieczeństwa oraz konsultant IT, Adrian Sroka, w rozmowie z redakcją "Security Magazine" wyjaśnia, jak odpowiednie projektowanie aplikacji i świadomość użytkowników są kluczowe dla zapewnienia ich bezpieczeństwa, kiedy zagrożeń cyfrowych jest coraz więcej.

Zabezpieczanie aplikacji to więcej niż technologia. Wywiad z Adrianem Sroką



Czym zajmuje się obszar bezpieczeństwa aplikacji?

Adrian Sroka: Można powiedzieć, że praca nad bezpieczeństwem aplikacji ma na celu takie zaprojektowanie systemów, by zarówno użytkownik jak i jego dane były bezpieczne. To dbanie o bezpieczeństwo można realizować na wiele sposobów, np. edukując użytkowników. Niestety jest to trudne i mało efektywne, ponieważ po pierwsze nie zawsze mamy stałych czy powracających użytkowników/Klientów, a po drugie nie wszystkich jesteśmy w stanie wyedukować, nawet wtedy, gdy bardzo byśmy się starali.

Znacznie efektywniejsze jest z kolei takie zaprojektowanie i zabezpieczenie systemów, żeby użytkownicy nie musieli tak wiele myśleć o swoim bezpieczeństwie. Wiadomo, nie można w ten sposób zredukować ryzyka do zera, ale można je skutecznie zmniejszyć do akceptowalnego poziomu. Dla przykładu, jeśli wprowadziliśmy logowanie dwuskładnikowe, to uratujemy naszego użytkownika nawet w sytuacji, gdy padnie on ofiarą ataku phishingowego i poda komuś swoje dane logowania do naszego systemu.

Jakie są główne zagrożenia dla aplikacji?

A. S.: Obecnie bardzo popularnymi zagrożeniami są ataki na łańcuch dostawczy — czyli to wszystko, z czego jest budowana (i w jaki sposób jest budowana) finalna aplikacja. Atakujący dzięki temu mogą uzyskać efektywną dźwignię. Kompromitując jeden element łańcucha dostawczego oprogramowania, mogą zainfekować/ zaatakować wiele różnych firm, korzystających z tego elementu.

Przykładem może tu być korzystanie z narzędzi do automatyzacji wdrożeń i weryfikacji kodu. Po udanym ataku (lub zalezieniu luki) w takim narzędziu, każda firma, która z nich korzysta, może stać się łatwym celem ataku.

Najpopularniejszy branżowy przykład tego typu ataku to luka w log4j. Problem w jednej bibliotece skutkował podatnością zależną w 35 tysiącach innych bibliotek, co stanowi **8% całego zbioru bibliotek publicznych Java**.

Jak więc można zadbać o ten obszar w firmie?

A. S.: Najważniejsze jest holistyczne podejście. Wytwarzanie oprogramowania to dość skomplikowana dziedzina, która obejmuje wiele perspektyw takich jak projektowanie, dewelopment, utrzymanie. Do tego dochodzi wiele różnych technologii i środowisk (chmura, aplikacje webowe, mobilne, itp.).

Każdy z tych elementów ma ogromny wpływ na bezpieczeństwo całego systemu. Nie wystarczy uwzględnić bezpieczeństwa na etapie projektowania, jeśli deweloperzy nie dbają o nie w swojej codziennej pracy nad tworzeniem kodu. Nie wystarczą testy penetracyjne, jeżeli nasza aplikacja jest skomplikowana, bo nie wychwycą one np. problemów bezpieczeństwa powiązanych z logiką.

Jakie są obecnie trendy w obszarze bezpieczeństwa aplikacji?

A. S.: Obecnie coraz częściej w celu redukcji kosztów i zwiększenia efektywności dbania o bezpieczeństwo aplikacji stosuje się podejście shift left. Kiedyś głównym punktem zadbania o bezpieczeństwo były testy penetracyjne wykonywane zwykle tuż przed wdrożeniem aplikacji lub cyklicznie. To powodowało wiele problemów organi-

zacyjnych. Dlatego też teraz nacisk przenosi się na wcześniejsze etapy dewelopementu. Im wcześniej pomyślimy o zaaplikowaniu bezpieczeństwa do codziennej pracy analityków i deweloperów, tym łatwej i finalnie taniej będzie je wprowadzić.

Uwzględnienie elementów bezpieczeństwa dla funkcjonalności na etapie projektu jest dużo tańsze niż dodanie ich dopiero po wykryciu błędu. A co dopiero, gdy błąd ten zostanie wykorzystany na produkcji.

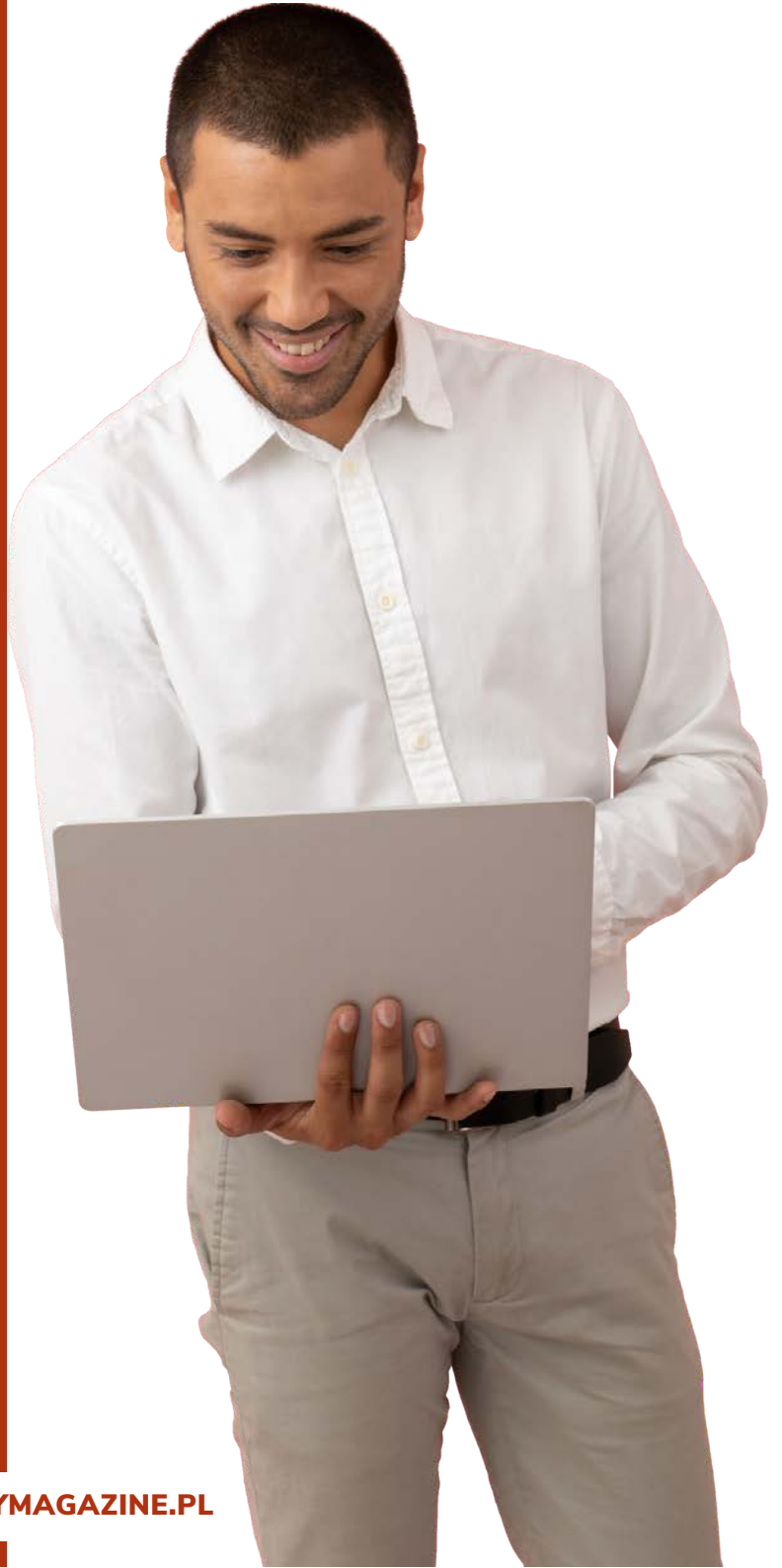
Kolejnym trendem jest DevSecOps. To krok dalej, czyli wprowadzenie automatycznych miar i testów, dzięki którym upewnimy się, że spełniamy oczekiwany poziom bezpieczeństwa. W ten sposób możemy uwzględniać troskę o bezpieczeństwo w procesie wytwarzania oprogramowania najwcześniej, jak to tylko możliwe. Jak widać duży nacisk w obecnych trendach kładzie się na ludzi i na wdrażanie bezpieczeństwa, począwszy od nich.

Bezpieczeństwo, czyli najpierw ludzie, ale jak to wprowadzić?

A. S.: Wiele firm, zaczynając przygodę z bezpieczeństwem aplikacji, bierze udział w różnorakich szkoleniach podnoszących świadomość tego tematu.

To dobry pomysł. Jednak tylko na początek, gdy poziom wiedzy i zainteresowania pracowników tymi tematami jest stosunkowo niski. Praktyka pokazuje, że pracownicy dość szybko zapominają o tym, czego nauczyli się na szkoleniach. Dlaczego? Ponieważ dostają w krótkim czasie potężną dawkę wiedzy (często szkolenia są bardzo dobrze przygotowane pod względem merytorycznym), ale nie mają przestrzeni, by chociaż część nowo poznanych praktyk od razu wprowadzić w życie.

Dlatego też obecnie popularnym trendem jest tworzenie międzyzespołowych społeczności skupionych na rozwijaniu bezpieczeństwa wewnątrz organizacji. Nazywa się je Security Champions. Ponieważ jak już mówiliśmy, dbanie o bezpieczeństwo wymaga spojrzenia z wielu perspektyw, taka społeczność jest zbiorem osób z różnych zespołów o różnych rolach. Celem społeczności jest rozwój umiejętności np. poprzez szkolenia, wymianę wiedzy i doświadczeń, tworzenie forum do wspólnego rozwiązywania problemów oraz przede wszystkim zadbanie o ciągłą ekspozycję na temat bezpieczeństwa. Co przekłada się na to, że pracownicy stale zaangażowani w bezpieczeństwo, sami pilnują tego typu tematów już od samego początku procesu wytwarzania.



Nie wszystkie firmy mogą sobie pozwolić na tworzenie i utrzymywanie wyspecjalizowanych społeczności wewnątrz firmy. To wymaga dużego zaangażowania i wiedzy.

Przykładem wsparcia firm w tworzeniu bezpiecznych systemów może być społeczność **Security Champions**, której celem jest pomaganie pracownikom w podejmowaniu dobrych decyzji i wybieraniu właściwych rozwiązań poprzez przybliżanie trendów czy omawianie zagrożeń z zakresu bezpieczeństwa.

Od czego zacząć?

A. S.: Od przestrzeni czasowej w wyznaczaniu terminów, by pracownicy mogli zacząć stosować wiedzę w praktyce. Czyli aby mogli modelować zagrożenia (Threat modelling) czy zwracać uwagę na bezpieczeństwo w czasie Code Review.

Z biegiem czasu, omawiane na spotkaniach problemy bezpieczeństwa, będą coraz bardziej skomplikowane. Wiedza oraz świadomość w firmie będą rosły, a na testach penetracyjnych (z których wcale rezygnować nie należy) wykrywanych podatności będzie coraz mniej.

Dziękuję za inspirującą rozmowę.

-20%

SECURITY MAGAZINE

JESIENNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

WAŻNY DO

10.12.2023

KONTAKT I SZCZEGÓŁY: REDAKCJA@SECURITYMAGAZINE.PL

SECURITYMAGAZINE.PL

ZEROWE ZAUFANIE, ANOMINIZACJA DANYCH I ELEKTRONICZNE PODPISY

Redakcja
SECURITY MAGAZINE

Świat biznesu stoi na progu coraz większych wyzwań. Kwestie związane z cyber-bezpieczeństwem się kompli-kują. Dlatego jeśli prowadzisz firmę – musisz być w stanie mierzyć się z potencjalnymi zagrożeniami. Niejedno-krotnie w tej kwestii bardzo mogą pomóc Ci startupy z całego świata.

DOSTĘP ZEROWEGO ZAUFANIA – GOODACCESS

Czeski startup GoodAccess specjalizuje się w dziedzinie bezpiecznego dostępu do zasobów biznesowych. Organizacja oferuje niedrogie rozwiązania dostępu do sieci o zerowym zaufaniu, które są nie tylko łatwe we wdrożeniu, ale także proste w zarządzaniu i obsłudze. To szczególnie ważne w dobie pracy hybrydowej i zdalnej. Dzięki temu zapewnisz bezpieczny dostęp do swoich systemów biznesowych, danych oraz usług.

To jednak nie koniec, bo GoodAccess oferuje też inne usługi. Mowa tutaj np. o dedykowanej bramie VPN, statycznym adresie IP, centralnym pulpicie nawigacyjnym, filtrowaniu DNS, uwierzytelnianiu wieloskładnikowym, kontroli dostępu do sieci, dzienniku dostępu, białej liście adresów IP oraz jednokrotnym logowaniu. Te rozwiązania mogą pomóc Ci w zapewnieniu cyberbezpieczeństwa w Twojej firmie.

Warto podkreślić, że rozwiązanie dostępu do sieci o zerowym zaufaniu GoodAccess zostało wyróżnione przez TechRadar jako jedno z najlepszych rozwiązań ZTNA (Zero Trust Network Access). Dodatkowo w ramach swojej misji, GoodAccess wprowadził w 2022 r. pierwszą na świecie darmową biznesową sieć VPN. Pomaga ona firmom zapewnić bezpieczny dostęp zdalny bez żadnych ograniczeń.

Co więcej – wśród partnerów GoodAccess można wymienić m.in. WordPress, Salesforce, phpMyAdmin, Microsoft IIS, Apache, ZOHO, Microsoft Azure, Magento, PrestaShop, Opencart czy REDAMP Security. Dodatkowo oferta GoodAccess jest dostępna w ponad 120 krajach – w tym w Polsce.

ANONIMIZACJA DANYCH – NYMIZ

Hiszpański startup Nymiz wykorzystuje sztuczną inteligencję do wspomagania ochrony danych osobowych. Misją organizacji jest dbanie o prywatność ludzi, niezależnie od czasu i miejsca i wspieranie Twojej firmy w tym procesie.

Nymiz skupia się na dostarczaniu dodatkowej warstwy bezpieczeństwa na poziomie danych. Proces anonimizacji lub pseudonimizacji danych ma na celu zapobieganie sytuacjom, w których poufne informacje (np. Twoich klientów) mogłyby zostać wykradzione w wyniku naruszenia cyberbezpieczeństwa lub błędu ludzkiego. Proces anonimizacji danych pozwala na oddzielenie informacji osobo-

wych od danych identyfikujących, co gwarantuje bezpieczne przetwarzanie informacji. Co istotne, proces pseudonimizacji umożliwia identyfikację podmiotu w odniesieniu do danych sklepu, bez konieczności uwzględniania danych identyfikujących daną osobę.

W dodatku Nymiz zobowiązuje się do przestrzegania aktualnych przepisów regulacyjnych dotyczących prywatności i ochrony danych, takich jak RODO, CCPA czy LGPD. Dzięki temu firma zapewnia swoim klientom, że ich dane są bezpieczne i zgodne z obowiązującymi przepisami. Dane są anonimizowane np. poprzez zastępowanie ich gwiazdkami czy żetonami.

Startup posługuje się regułami i słownikami uzyskanymi w wyniku przetwarzania niezliczonych dokumentów z pomocą technologii NLP (Natural Language Processing). Dzięki temu sztuczna inteligencja, która dba o anonimizację czy pseudoanonimizację dokumentów – doskonale rozumie, gdzie są zawarte dane osobowe i że to właśnie te należy chronić.

Nymiz kieruje swoją ofertę głównie do administracji publicznej, służby zdrowia i usług medycznych czy prawniczych, ale nie ogranicza się wyłącznie do tych branż. Jeśli tylko Twoja firma jakkolwiek przetwarza dane osobowe – zwłaszcza w dużych ilościach – Nymiz może okazać się niezwykle pomocny w zadbaniu o ich bezpieczeństwo.

PODPISY ELEKTRONICZNE – EID EASY

Estoński startup eID Easy oferuje rozwiązanie mające na celu uprościć oraz zabezpieczyć procesy związane z podpisami elektronicznymi. Or-

ganizacja specjalizuje się w zapewnieniu bezpiecznej infrastruktury dla podpisów cyfrowych, które spełniają międzynarodowe przepisy i standardy.

Każdy kraj ma swoje własne przepisy i urzędy certyfikacji i jest to wyzwanie dla każdego, kto stawia na ekspansję międzynarodową. Rozproszenie różnych rozwiązań do podpisów elektronicznych z różnych krajów i dostawców usług zaufania stało się poważnym wyzwaniem dla firm.

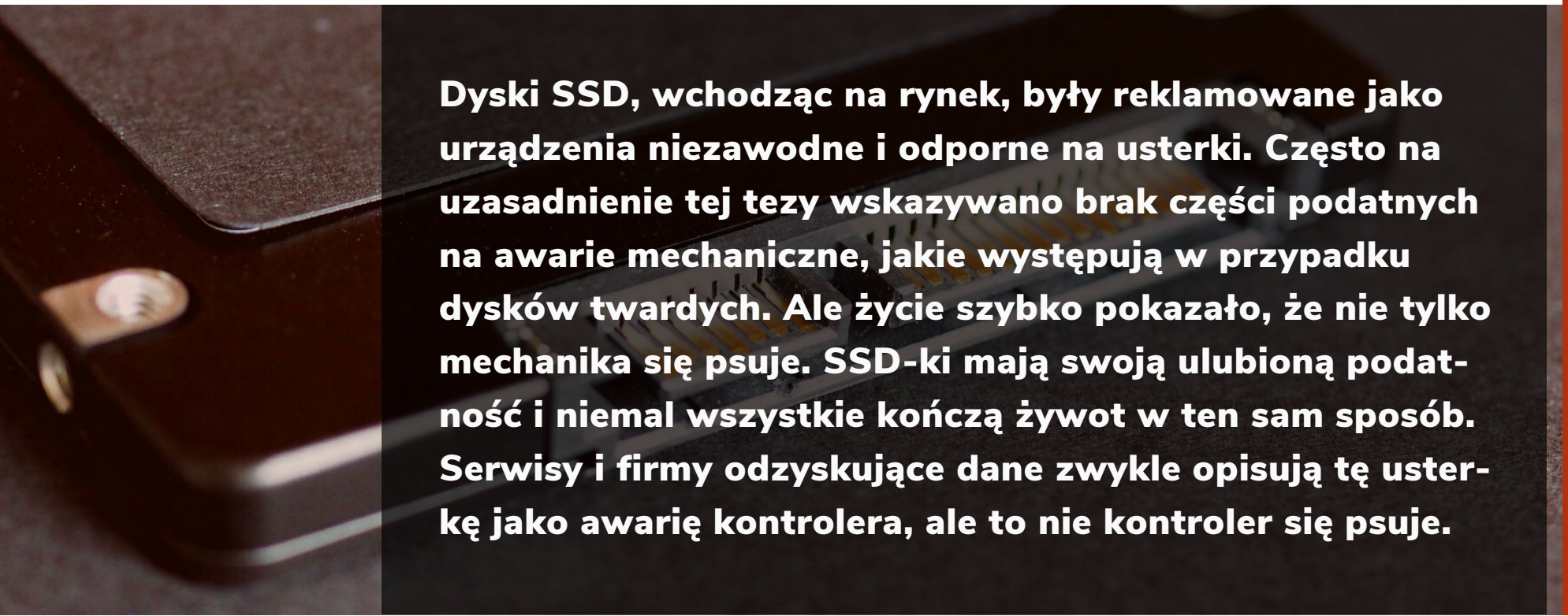
eID Easy dąży do wyeliminowania tego problemu poprzez agregację i standaryzację lokalnych i uznanych metod podpisów elektronicznych, które już zweryfikowały tożsamość użytkownika. Dzięki temu Twoja firma minimalizuje problemy związane z procesem podpisywania i jednocześnie obniża koszty konserwacji, co pozytywnie wpływa na czas i efektywność operacji.

Zazwyczaj proces wdrożenia rozwiązań związanych z podpisami cyfrowymi jest kosztowny, długotrwały i wymaga specjalistycznej wiedzy. eID Easy, mając dostęp do najlepszych ekspertów i kontakty z urzędami certyfikacji i dostawcami usług zaufania, umożliwi Twojej firmie szybkie i łatwe rozpoczęcie korzystania z podpisów elektronicznych. To wszystko jest możliwe dzięki prostemu procesowi integracji, który pozwala na natychmiastowe uruchomienie rozwiązania.

To przykłady tylko niektórych startupów technologicznych, które mogą przyspieszyć procesy w Twojej firmie, czy wesprzeć ją w zakresie cyberbezpieczeństwa. Warto korzystać z nowoczesnych rozwiązań, bo dzięki nim zapewniasz bezpieczeństwo sobie, swoim klientom i zasobom.

NAJCZĘSTSZE PRZYCZYNY AWARII SSD

Paweł Kaczmarzyk
Serwis komputerowy Kaleron



Dyski SSD, wchodząc na rynek, były reklamowane jako urządzenia niezawodne i odporne na usterki. Często na uzasadnienie tej tezy wskazywano brak części podatnych na awarie mechaniczne, jakie występują w przypadku dysków twardych. Ale życie szybko pokazało, że nie tylko mechanika się psuje. SSD-ki mają swoją ulubioną podatność i niemal wszystkie kończą żywot w ten sam sposób. Serwisy i firmy odzyskujące dane zwykle opisują tę usterkę jako awarię kontrolera, ale to nie kontroler się psuje.

PRZECHOWYWANIE DANYCH W SSD-KACH

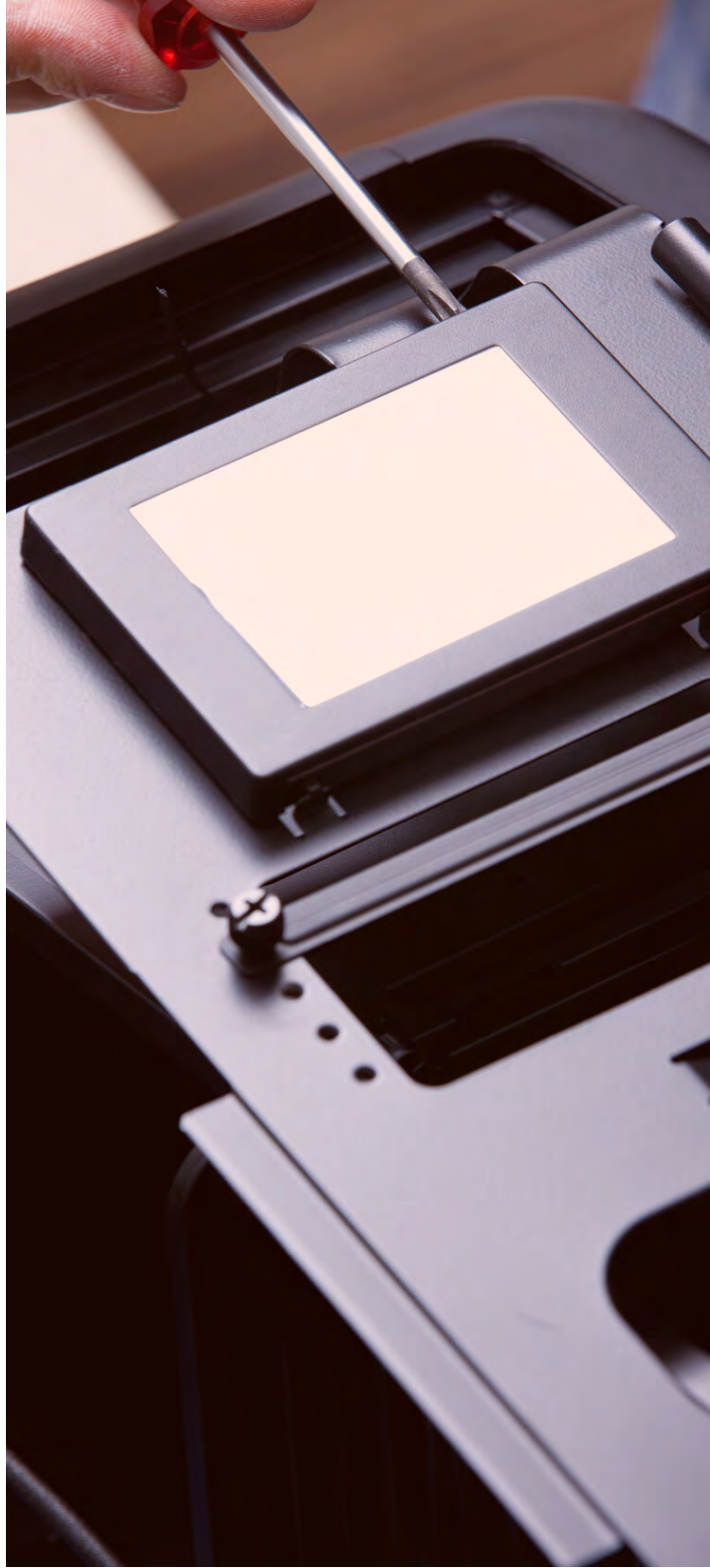
Dyski SSD przechowują dane w układach Flash-NAND, spotykanych również w innych urządzeniach, jak np. pendrivy i karty pamięci. Dlatego informacje o przyczynach awaryjności SSD-ków można w prosty sposób odnieść i do innych nośników. Układy NAND zawierają bardzo duże liczby zmodyfikowanych tranzystorów polowych typu npn z kanałem zubażanym. Modyfikacja polega na wyodrębnieniu w tych tranzystorach odseparowanych elektrycznie obszarów – bramek pływających.

Bramka pływająca jest pułapką na elektrony pozwalającą przechowywać umieszczony w niej ładunek także po odłączeniu zasilania. Ładunek ten zachowuje się tak, jakby do bramki tranzystora zostało przyłożone napięcie, czyli w najprostszym wariancie przechowujących po jednym bicie w tranzystorze pamięci typu SLC (Single Level Cell) całkowicie zamyka kanał tranzystora. Dlatego zazwyczaj naładowaną bramkę tranzystora interpretuje się jako logiczne zero, a bramkę pustą – jako logiczną jedynkę.

PODSTAWOWE OPERACJE W UKŁADACH FLASH-NAND

W układach Flash-NAND możemy wykonywać trzy rodzaje operacji. Odczyt, zapis i kasowanie. Odczyt jest wykonywany przez pomiar napięcia między źródłem, a drenem tranzystora. Jest to operacja bezpieczna i nieszkodliwa dla układów, w odróżnieniu od operacji kasowania i programowania. Ponieważ programować możemy jedynie puste bramki pływające, tranzystory zaprogramowane wcześniej przed przyjęciem nowej porcji danych muszą zostać skasowane (muszą z nich zostać usunięte elektrony).

Zarówno programowanie, jak i kasowanie bramek pływających zazwyczaj wykonuje się z wykorzystaniem kwantowego zjawiska tunelowania Fowlera – Nordheima. Zjawisko to wykorzystuje falowe właściwości elektronów, ale żeby je wymusić, konieczne jest podniesienie napięcia między źródłem, a bramką do poziomu kilkunastu V.



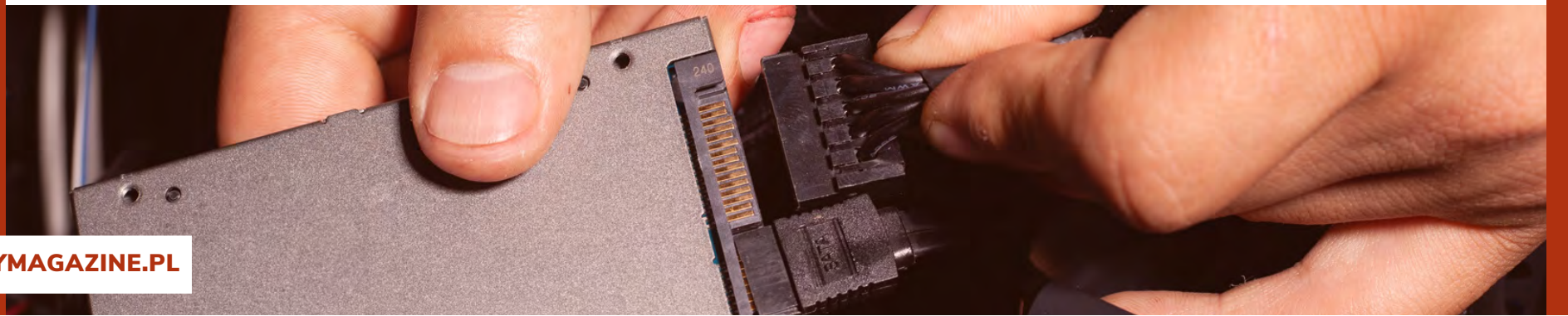
Powoduje to straty energii skutkujące wydzielaniem ciepła oraz obciąża izolator, prowadząc do jego degradacji. W miarę postępującej degradacji izolatora dochodzi do ucieczki elektronów i upływności danych. Dlatego żywotność układów Flash-NAND określa się liczbą cykli programowania i kasowania.

Ponieważ współcześnie produkowane układy pamięci mają żenująco niską żywotność, producenci odeszli od podawania tego parametru, zastępując go lepiej wyglądającym parametrem TBW (Total Bytes Written). Jeśli chcesz ustalić, jaką żywotność mają układy w Twoim SSD-ku, możesz to zrobić w bardzo prosty sposób. Wystarczy, że podzielisz parametr TBW przez pojemność swojego nośnika. Prawda, że wyszła niezbyt imponująca wartość?

TECHNOLOGIA PAMIĘCI WIELOSTANOWYCH

Wspomniane wyżej pamięci SLC obecnie są już bardzo rzadko spotykane. Przez lata były stopniowo wypierane przez układy zawierające 2 (MLC- Multi Level Cell), 3 (TLC – Triple Level Cell), a ostatnio nawet 4 (QLC – Quad Level Cell) bity w tranzystorze. Więcej bitów w każdym tranzystorze, to lepszy stosunek pojemności do ceny gotowego produktu. Czy zatem możemy spodziewać się niebawem pamięci zawierających po 5 bitów na tranzystor?

Kiedy inżynierowie zauważyli możliwość precyzyjnego sterowania częściowym przymykaniem kanału tranzystora przez umieszczenie w bramce pływającej określonego ładunku, księgowym ten pomysł się bardzo spodobał. I dopóki przechowywaliśmy w tranzystorze 2 bity, potrzebowaliśmy jedynie 4 rozróżnialnych poziomów naładowania. Dlatego układy MLC wciąż mogły oferować całkiem sensowną trwałość i niezawodność przy znacznie niższej cenie od układów SLC.
Problemy zaczęły wyraźnie narastać wraz z wpro-



wadzeniem układów TLC. Wymagane w nich 8 rozróżnialnych poziomów naładowania spowodowało wyraźne pogorszenie stosunku sygnału do szumu oraz zwiększenie liczby występujących w nich błędów bitowych. Skutkowało to koniecznością zastosowania silniejszych kodów korekcji ECC oraz bardziej złożonych algorytmów kodowania danych. Problem ten jeszcze bardziej pogłębił się w przypadku pamięci QLC.

Prócz pogorszenia stosunku do szumu w układach wielostanowych występuje jeszcze jeden problem. Programowanie tranzystorów odbywa się etapami, co przyśpiesza degradację izolatorów bramek pływających. I o ile układy SLC wytrzymywały nawet ponad 100.000 operacji kasowania/ zapisu, a MLC typowo kilkanaście tysięcy takich operacji, to dla pamięci TLC parametr ten wynosi zaledwie kilka tysięcy (dla obecnie produkowanych układów typowo ok. 1500 cykli), a dla QLC – ok. 600.

ZMNIEJSZANIE ROZMIARU TRANZYSTORA

Ponieważ głównym czynnikiem wpływającym na cenę układu scalonego jest jego powierzchnia, inżynierowie dążą do zmniejszania rozmiarów poszczególnych elementów i zwiększenia gęstości ich upakowania w układzie.

Dotyczy to nie tylko procesorów i kart graficznych, ale i układów NAND-owych. Zmniejszanie rozmiaru tranzystora skutkuje też zmniejszaniem grubości izolatora bramki pływającej oraz wielkości samej bramki.

Cieńszy izolator, to większe ryzyko uszkodzenia, szybsza degradacja i łatwiejsza ucieczka elektronów. Zalecana grubość izolatora wynosi ok. 4 nm. W przypadku układów wykonywanych w litografii kilkunastu nm jego grubość spada do ok. 2 nm. Istotny wzrost awaryjności tych układów w stosunku do wcześniejszych generacji jest w znacznym stopniu spowodowany właśnie przez zbyt niską trwałość izolatorów bramek pływających.

Mniejsza bramka pływająca, to także mniejsza możliwość umieszczania w niej elektronów. Elektrony nie mogą być upychane w bramce pływającej w dowolnej liczbie. Są one umieszczane na powłokach walencyjnych znajdujących się wewnątrz bramki atomów, których liczba ogranicza możliwą do umieszczenia w bramce liczbę elektronów. W przypadku układów wykonywanych w litografii kilkunastu nm w bramce pływającej można umieścić zaledwie ok. 1000 elektronów. Jeśli podzielimy tę liczbę przez wymaganą dla układów QLC liczbę 16 odróżnialnych poziomów naładowania, zobaczymy, że już

kilkadziesiąt elektronów może przesądzić o wystąpieniu błędu bitowego.

Zmniejszanie procesu litografii, to także większe trudności wykonawcze i większe wymagania technologiczne. Wyzwaniem jest chociażby sam fakt operowania coraz krótszymi falami światła, czy konieczność wykonywania procesu napylania w warunkach wysokiej próżni. Przy tak niskich wymiarach tranzystorów różnice mogą robić nie tylko nawet nieznaczne zanieczyszczenia, ale i niedokładności wykonawcze na poziomie pojedynczych atomów.
Przeniesienie tych procesów z warunków laboratoryjnych do masowej produkcji wiąże się z większą skalą odpadów produkcyjnych i większym ryzykiem awaryjności niedostatecznie przetestowanych układów w początkowym okresie ich eksploatacji.

3-D NAND

Innym stosowanym przez producentów sposobem zwiększania gęstości zapisu są układy wielowarstwowe 3D-NAND. Układy te zbudowane są z od kilkudziesięciu do kilkuset warstw umieszczanych jedna nad drugą. Pozwala to znacząco zwiększyć upakowanie danych w układzie, jednak i to rozwiązanie nie jest wolne od wad.
Najważniejszym problemem jest ciepło wydzielane podczas operacji kasowania i zapisu. Wprawdzie układ można chłodzić przy pomocy radiatora i to się od pewnego czasu

robi, ale radiator odprowadza ciepło tylko z powierzchni układu. A ono ma tendencję do akumulowania się pomiędzy warstwami. I to właśnie odprowadzanie ciepła spomiędzy warstw stanowi dla producentów największe wyzwanie.

Drugim problemem są zjawiska indukcyjne występujące pomiędzy sąsiednimi tranzystorami. Wprawdzie nie są one nowością i występowały już wcześniej, jednak ich wpływ nie był aż tak istotny, dopóki tranzystory były ułożone w jednej płaszczyźnie. Znaczenie pól elektrycznych indukowanych przez sąsiednie ładunki jest przy tym tym istotniejsze, im mamy mniejsze tranzystory, im gęściej chcemy je upakować i im więcej bitów chcemy w nich umieścić. A to są najważniejsze kierunki rozwoju układów NAND-owych.

ADRESOWANIE DANYCH W SSD-KACH

Komunikując się z SSDkami wysyłamy im polecenia zapisu lub odczytu określonych sektorów. Ale same układy NAND-owe nie adresują danych w sektorach. Ich podstawowymi jednostkami adresowania są strony, jako minimalne jednostki odczytu i programowania (stanowią odpowiednik od 1 do 32 sektorów LBA) i liczące od kilku do kilkuset stron bloki, jako minimalne jednostki kasowania. W przypadku obu tych jednostek adresowania stałą tendencją jest zwiększanie ich rozmiarów. Kontroler pośredniczy pomiędzy wewnętrzną adresacją układów NAND, a używaną na zewnętrznym interfejsie adresacją LBA, wykorzystując tablice oprogramowania układowego nazywane translatorem.

Translator przechowuje informację pozwalającą ustalić, w której fizycznej jednostce którego układu znajdują się poszukiwane sektory. W odróżnieniu od dysków twardych, w nośnikach półprzewodnikowych fizyczne położenie poszczególnych jednostek LBA stale się zmienia.

Jest to związane z brakiem możliwości bezpośredniego nadpisywania danych i koniecznością umieszczania ich w skasowanych blokach. Informacja translatora zmienia się często, bo przy każdym zapisie na dysk. Dlatego musi być umieszczona w układach NAND i dlatego jest narażona na te same ryzyka wystąpienia błędów, co i inne dane umieszczone w tych układach.

Kiedy zapisujemy do SSDka nowe dane, są one umieszczane w dostępnej lokalizacji i tej lokalizacji

przypisywane są adresy LBA związane z tymi danymi. Natomiast strony zawierające zdezaktualizowaną zawartość tych sektorów tracą powiązanie z adresacją LBA i są oznaczane jako przeznaczone do skasowania. Jak zapewne się domyślasz, translator jest bardzo ważny dla prawidłowego działania SSD-ka. Co by się mogło stać, gdyby jego zawartość uległa uszkodzeniu?

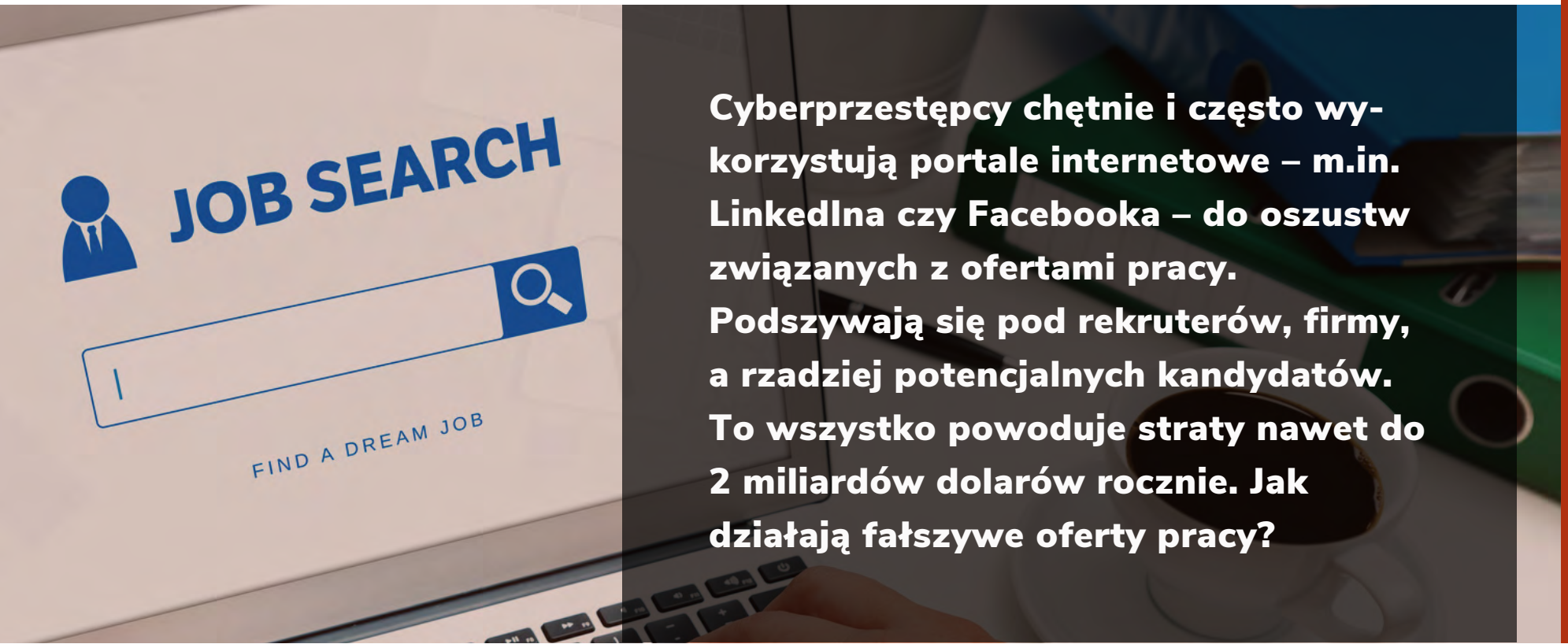
I to jest właśnie odpowiedź na pytanie o najczęstszą przyczynę awarii SSD-ków. Kiedy translator zawiera błędy, kontroler traci możliwość poprawnego adresowania danych. Na wszelki wypadek odcina dostęp do NAND-ów. W takiej sytuacji SSD przedstawia się tzw. paszportem technologicznym. Zwykle zamiast modelu widniejącego na obudowie wyświetla nam się model kontrolera albo jakiś związany z nim ciąg znaków, jak np. SATAFIRM S11. Deklarowana pojemność jest dziwnie mała, lub wręcz zerowa. Kiedyś w dyskach Intela zamiast numeru seryjnego często pojawiał się kod błędu. Znaczna część SSD-ków w przypadku awarii tego typu zawiesza się i w ogóle nie odpowiada.

Nie zawsze przyczyną awarii muszą być błędy akurat translatora.

Oprogramowanie układowe odpowiada też za inne funkcje, np. za zarządzanie defektami i eliminowanie z eksploatacji uszkodzonych bloków. Czasem może dojść do uszkodzenia innych części oprogramowania układowego. Ale to właśnie błędy oprogramowania układowego odpowiadają za niemal wszystkie awarie SSD-ków. Dlaczego więc w diagnozach dowiadujemy się, że uszkodzeniu uległ kontroler, choć tak naprawdę sam układ jest sprawny? Może dlatego, że jest fizycznie namacalny, a mało komu się chce tłumaczyć nietechnicznym klientom rolę oprogramowania układowego w działaniu SSD-ka.

FAŁSZYWE OFERTY PRACY TO ZMORA INTERNETU

Redakcja
SECURITY MAGAZINE



Cyberprzestępcy chętnie i często wykorzystują portale internetowe – m.in. LinkedIna czy Facebooka – do oszustw związanych z ofertami pracy. Podszywają się pod rekruterów, firmy, a rzadziej potencjalnych kandydatów. To wszystko powoduje straty nawet do 2 miliardów dolarów rocznie. Jak działają fałszywe oferty pracy?

FAŁSZYWE OFERTY PRACY TO PLAGA

W ciągu ostatnich kilku lat cyberprzestępcy coraz śmielej poczynają sobie w kontekście oszustw. Rozwój rynku pracy – zwłaszcza tej zdalnej i cyfryzacji procesu rekrutacji – dolał tylko oliwy do ognia w wykorzystaniu tego rynku do kolejnych oszustw. Cyberprzestępcy niezwykle często podszywają się pod znane firmy, headhunterów, agencje pracy, a niekiedy i kandydatów. Po co? W celu pozyskania danych, dostępów, a czasem i pieniędzy. Problem jest na tyle duży, że na swoich stronach internetowych ostrzegają przed nim nawet Komisja Europejska, jak i FBI.

Jednak przechodząc do rzeczy – jak dowiadujemy się z badań Password Manager w latach 2020–2021 liczba zgłoszonych przypadków oszustw związanych z fałszywymi ofertami pracy wzrosła prawie trzykrotnie. I sporą cegłę do tego dołożyła pandemia, która spowodowała przeniesienie się sporej części komunikacji do internetu.

Password Manager postanowił przeprowadzić ankietę wśród 663 Amerykanów i okazało się, że 38% z nich natrafiało na fałszywe oferty pracy, 32% zostało oszukanych i aplikowało na nieistniejące miejsce pracy. Z kolei 15% z nich skradziono dane osobowe, a 9% przekazało oszustom swoje pieniądze (22% przyznało, że stracili od 500 do 1000 dolarów). Co najgorsze – 84% wszystkich osób, które aplikowały na fałszywą ofertę prawie do samego końca nie miały pojęcia, że jest to oszustwo.

LINKEDIN RAJEM DLA CYBERPRZESTĘPCÓW?

Gdzie najczęściej natrafiali na fałszywe oferty? Na 1. miejscu znalazł się serwis Craigslist (47%), Indeed (44%) i Facebook (44%). LinkedIn znalazł się „dopiero” na 5. miejscu z wynikiem 23%, tuż za ZipRecruiter – niecałe 25%.

Choć LinkedIn nie miał wysokiej pozycji w badaniu Password Manager, to już w ankiecie NordLayer sytuacja prezentuje się nieco inaczej. Według badania przeprowadzonego przez tę organizację aż 67% małych firm (zatrudniających do 10 osób) poniosło straty finansowe w wyniku oszustwa na LinkedInie. Z kolei większe firmy częściej były narażone na utratę reputacji.

Dlaczego LinkedIn jest takim „łakomym kąskiem” dla cyberprzestępców? To ze względu na jego rosnącą popularność i to, jak ważnym portalem w kontekście poszukiwania pracy się stał. Dość powiedzieć, że według danych NordLayer, co sekundę na LinkedInie składane jest nawet 117 aplikacji. A to stwarza idealne wręcz warunki dla oszustów wykorzystujących firmy i kandydatów.

NAWET 2 MILIARDY DOLARÓW STRAT

Zgodnie z danymi Better Business Bureau, oszustwa związane z rekrutacją sieją prawdziwe spustoszenie w świecie przedsiębiorczości. Coroczne straty wyceniane są nawet na 2 miliardy dolarów. W samym tylko I kwartale 2023 r. nastąpił 250% wzrost liczby oszustw związanych z rekrutacją w porównaniu z 2022 r.

Są to nie tylko straty w postaci wyłudzenia pieniędzy czy danych osobowych, ale również straty wizerunkowe.

Przykład? Według wspomnianej wcześniej ankiety Password Manager 50% osób, które widziały fałszywe oferty pracy, twierdzą, że te rzekomo pochodziły od korporacji. Z kolei 85% wskazywało na małe firmy. Pod jaką korporację cyberprzestępczy podszywali się najczęściej? Pod Amazona (54%). Na 2. miejscu znalazł się Walmart (34%), a na 3. UPS (31%). Nie trudno sobie wyobrazić, jak poważne straty może to wygenerować w kontekście wizerunkowym, wśród tych dużych, jak i małych firm.

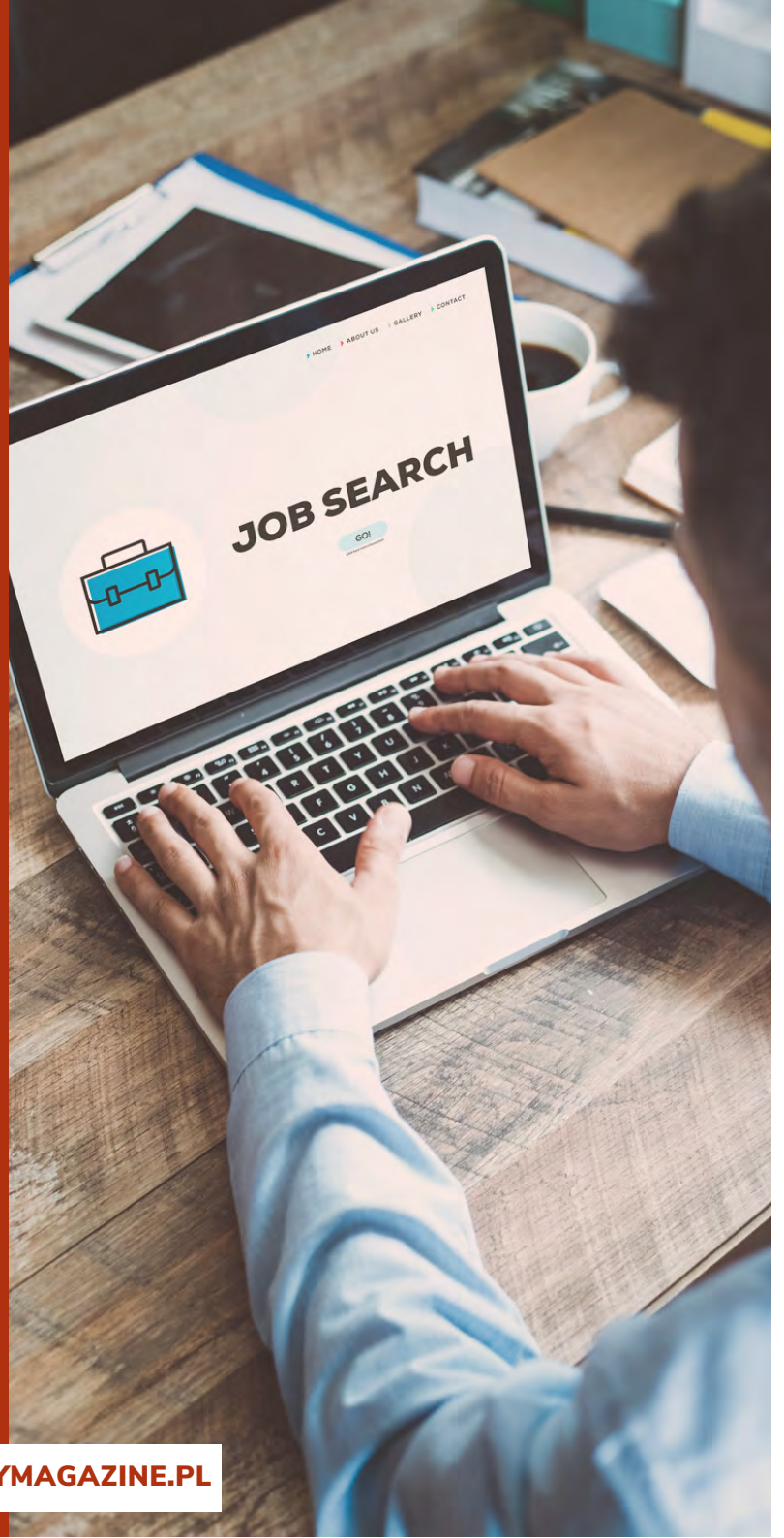
Może to się okazać szczególnie dotkliwe dla przedsiębiorstw, które są na giełdzie, bo wpłynie to również na ich akcje. A także dla tych, które już obecnie borykają się z kryzysem wizerunkowym w kontekście zatrudnienia – np. wspomniany wcześniej Amazon.

DODAWANIE FAŁSZYWYCH OFERT JEST PROSTE

LinkedIn stał się tak lubianą przez cyberprzestępców platformą również ze względu na to, jak paradoksalnie łatwo można się podszywać tam pod inne firmy. Bardzo często fałszywe oferty pracy pojawiają się na tej platformie na profilach rzekomych rekruterów. Albo ci wysyłają wiadomości do swoich potencjalnych ofiar. Mimo to można łatwo stworzyć profil podszywający się pod rzeczywistą firmę. I choć LinkedIn stara się walczyć z tym zjawiskiem i aktywnie to moderuje, to nadal łatwo to obejść.

Jednak jakiś czas temu Harman Singh, ekspert ds. cyberbezpieczeństwa, pracujący w Cyphere wskazał, że każdy może zamieścić pod firmową nazwą na LinkedIn ogłoszenie o pracę. I będzie ono wyglądać dokładnie tak samo, jak to stworzone przez prawdziwy profil.

Firma BleepingComputer postanowiła sprawdzić, czy to prawda. Stworzyli fałszywą ofertę pracy na LinkedIn z zupełnie innego profilu, pod który podpięli nowy adres mailowy, niepowiązany z ich przedsiębiorstwem. Wynik? Potencjalni kandydaci błyskawicznie zaczęli wysyłać CV na fałszywą ofertę, a ta przekierowywała aplikacje na rzeczony mail. Co gorsze – BleepingComputer nie było w stanie usunąć fałszywej oferty, zgłaszając ją ze swojego prawdziwego profilu. Mogli jedynie napi-



sać do zespołu bezpieczeństwa LinkedIn i prosić o jej usunięcie. Gdy o sprawie zrobiło się głośno i trafiła do mediów branżowych na całym świecie, przedstawiciel LinkedIna wydał oświadczenie, w którym wskazał, że zamieszczanie fałszywych ofert pracy to złamanie zasad korzystania z ich usługi.

Stwierdził, że używają różnych narzędzi, zarówno automatycznych, jak i ręcznych, aby wykrywać i usuwać takie fałszywe oferty pracy. Co więcej, pracują nad poprawą wykrywania takich oszustw, w tym sprawdzają e-maile służbowe przed publikacją na LinkedIn. I rzeczywiście się to dzieje. Wystarczy tylko spojrzeć na to, że w okresie od stycznia do czerwca 2022 r. LinkedIn usunął aż 22 miliony fałszywych kont.

CYBERPRZESTĘPCY UWIARYGADNIAJĄ SIĘ

Oszuści, którzy wykorzystują procesy rekrutacyjne, by oszukiwać kandydatów czy firmy, najczęściej stosują wiadomości i maile phishingowe, ale niekiedy proces przeprowadzają tak dokładnie, że chętnie biorą udział w rozmowach telefonicznych czy wideoczatach – niejednokrotnie dokładnie imitując podobne procesy firm, pod które się podszywają. Najczęściej wabią kandydatów perspektywą dobrych zarobków czy dogodnych warunków.

Niejednokrotnie pod koniec takich rozmów pojawia się pro-

śba o skan dokumentów osobistych.

Również same oferty są często bardzo dobrze napisane, na co zwraca uwagę m.in. OLX w swoim Kurierze Specjalnym. Tam Zuzanna Pawłowska wskazała, że oszuści często stosują się do zasad poprawnej polszczyzny oraz dbają o wiarygodność ogłoszenia. Jako sytuacje, w których powinna nam się zapalić czerwona lampka, wymieniła prośbę o wysyłanie skanów dokumentów na etapie rekrutacji, wpłacanie zaliczek np. na materiały szkoleniowe, zakup niezbędnego sprzętu do pracy, podpisanie poufnych dokumentów, kontakt z kandydatem przez komunikatory, ukrywanie nazwy firmy, zatrważająco wysokie zarobki czy zawiły opis stanowiska.

Niekiedy jednak cyberprzestępcy potrafią posunąć się o jeszcze kilka kroków dalej. Ekspert ds. cyberbezpieczeństwa Sagar Neupane opisał kiedyś prawdziwą historię kobiety, której oszust zaoferował pracę osobistej asystentki. Ta miała najpierw przejść okres próbny, w którym zajmowała się rezerwacją lotów, hoteli itp. Po pomyślnym przejściu rzeczonego okresu oszust stwierdził, że pomoże kobiecie złożyć wniosek wizowy i ta musi wysłać mu pieniądze. Obiecał, że wszystkie koszty związane z owym procesem i jej relokacją zwróci, gdy ta będzie na miejscu. Tego jednak nie zrobił. Kobieta straciła zarówno czas, jak i pieniądze.

OSZUŚCI CELUJĄ TEŻ W ZATRUDNIONYCH

W kontekście cyberoszustw związanych z fałszywymi ofertami pracy często mówi się o osobach, które aktywnie jej poszukują. To jednak zaledwie wycinek grup docelowych, w które stają na celowniku cyberprzestępców. Fałszywe oferty mogą dostawać także osoby, które są obecnie zatrudnione oraz wcale nie poszukują pracy. Dobrze pokazuje to akcja grupy Lazarus, która w I kwartale 2023 r. zaatakowała pracowników jednej z polskich firm zbrojeniowych.

Do osób pracujących w rzeczonej organizacji wysłano fałszywe oferty pracy z załącznikami PDF zainfekowanymi złośliwym oprogramowaniem RAT o nazwie ScoringMathTea. W tym przypadku nie chodziło tyle o pieniądze, co o wykradzenie danych, uzyskanie dostępów, dyskredytację i chaos.

Zdarza się bowiem, że cyberprzestępcy w ten sposób chcą zaszkodzić konkretnym firmom czy organizacjom. Zwłaszcza tym, które mają szczególne znaczenie strategiczne w danym sektorze czy kraju. Nie była to zresztą odosobniona akcja Lazarusa. Północnokoreańska grupa w podobny sposób zaatakowała też indyjską firmę zajmującą się zarządzaniem danych.

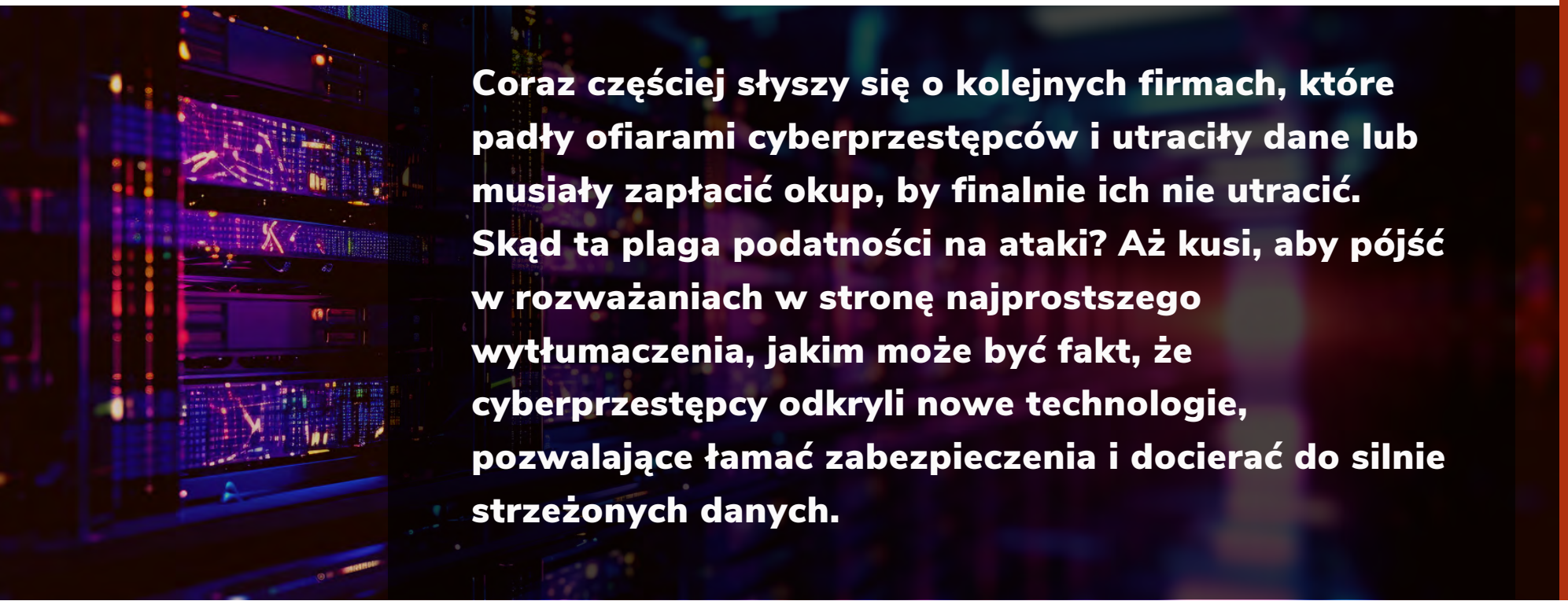
CHROŃ SIEBIE I SWOICH PRACOWNIKÓW

Aby uniknąć wpadnięcia w pułapkę oszustów na LinkedInie czy innych portalach, gdzie mogą pojawić się fałszywe oferty pracy, trzeba zachować szczególną ostrożność. Warto też rozmawiać o tym ze swoimi pracownikami, którzy mogą np. być obecnie w okresie wypowiedzenia albo nawet w ogóle nie szukać nowej pracy, lecz i tak mogą paść ofiarom wiadomości phishingowych czy zainfekowanych załączników. W końcu tego typu oszustwa mogą być podyktowane nie tylko chęcią zdobycia pieniędzy od potencjalnych kandydatów czy ich danych osobowych, ale też być formą dyskredytacji reputacji firmy, czy próbą pozyskania ważnych dostępów lub informacji o niej. Co pokazuje przykład Lazarusa.

Choć platformy i portale takie jak LinkedIn, starają się z nimi walczyć, to jest to poważne wyz-wanie. Potencjalni kandydaci mogą tracić przez cyberprzestępców swoje dane osobo-we, pieniądze i czas. Z kolei firmy reputacje, a czasem i także istotne informacje lub dostępy, gdy obecny jej pracownik kliknie podejrzany załącznik, link lub skusi się na propozycję nie do odrzucenia.

OCHRONA SIECI. NIEDOCE-NIANY ASPEKT, KTÓRY OSZ-CZĘDZI WIELU ZMARTWIEŃ

Przemysław Stróżniak
Perceptus Sp z o. o.



Coraz częściej słyszy się o kolejnych firmach, które padły ofiarami cyberprzestępców i utraciły dane lub musiały zapłacić okup, by finalnie ich nie utracić. Skąd ta plaga podatności na ataki? Aż kusi, aby pójść w rozważaniach w stronę najprostszego wytłumaczenia, jakim może być fakt, że cyberprzestępcy odkryli nowe technologie, pozwalające łamać zabezpieczenia i docierać do silnie strzeżonych danych.

Nasze doświadczenia w pracy z klientami pokazują jednak, że niestety nie musieli odkrywać nowych rozwiązań i rozwijać zaawansowanej technologii. To firmy nadal nie posiadają wystarczających zabezpieczeń. Poznaj prawdziwą historię, dowiedz się jak uniknąć zaszyfrowania danych w firmie przez złośliwe oprogramowanie.

OCHRONA SIECI I BACKUP - MUST HAVE PRZY PRACY ZDALNEJ

Ostatnie lata naznaczone epidemią SARS-CoV-2 w biznesie spowodowały silną popularyzację pracy zdalnej. Jest to zrozumiałe, ponieważ jest to rozwiązanie dogodne zarówno dla pracowników, jak i pracodawców.

Niestety, nie zawsze ułatwienia technologiczne do takiej pracy są przygotowywane zgodnie z zasadami cyberbezpieczeństwa. W wielu przypadkach zdalne połączenia z firmową siecią dla pracowników nie są w żaden sposób zabezpieczone. Zdalny pulpit pracownika do logowania z zewnątrz łatwo namierzyć, ponieważ jest on widoczny w sieci. Cyberprzestępcy wyszukują takie niezabezpieczone zdalne dostępy, a mając namiary na adres, pod którym można się zalogować, testują możliwe hasła, np. metodą bruteforce lub atakiem słownikowym. Po złamaniu hasła droga do firmowej sieci stoi otworem.

Często zaszyfrowanie plików nie następuje od razu. Atakujący nie ujawniają się i weryfikują, czy oraz jak wykonywane są backupy danych w sieci. Dopiero po zainfekowaniu wszystkich dostępnych kopii zasobów następuje szyfrowanie danych.
Właściwie skonfigurowane połączenie do pracy zdalnej, zintegrowane z ochroną sieci i backupem z wykorzystaniem migawek mogą skutecznie zabezpieczyć organizację przed problemami z zaszyfrowaniem danych. Dobrą praktyką jest również okresowe testowanie kopii zapasowych, ich posiadanie jest ważne, ale równie ważna jest weryfikacja czy można z nich skorzystać w razie potrzeby.

INTEGRACJA Z OBECNĄ INFRASTRUKTURĄ TO NIE WSZYSTKO

Kiedy firma decyduje się na inwestycje w zabezpieczenie swojej sieci, kluczowym aspektem, który często jest niedoceniany, jest uwzględnienie planów rozwoju organizacji.

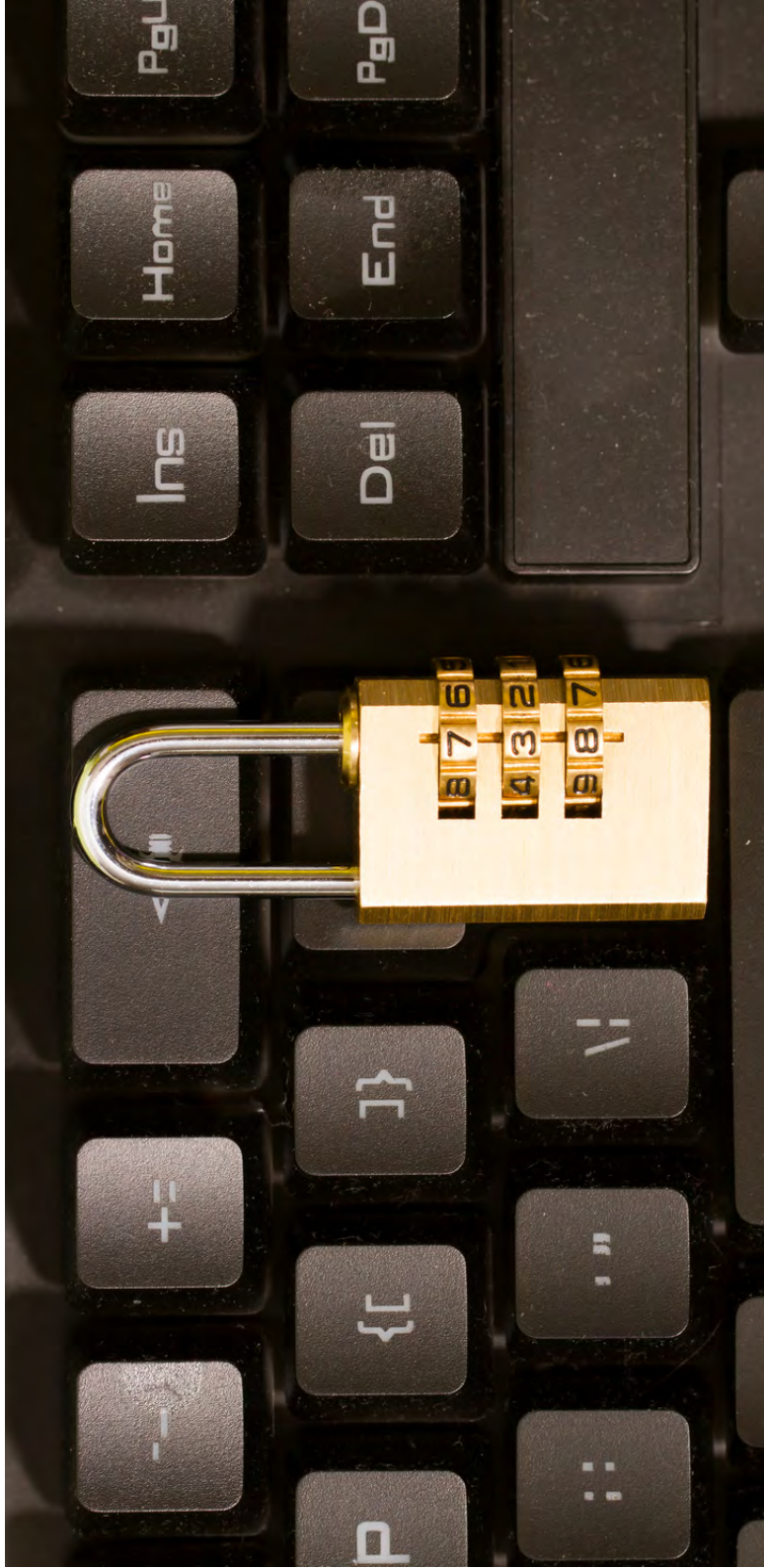
Wybór odpowiednich urządzeń realizujących tę potrzebę nie powinien być jedynie reakcją na bieżące zagrożenia, ale także strategicznym posunięciem, które uwzględnia przyszłe potrzeby firmy.

Warto zastanowić się, jakie cele organizacja planuje osiągnąć w ciągu kilku najbliższych lat. Czy firma planuje rozszerzyć swoją działalność, wprowadzić nowe usługi, czy też rozwijać się globalnie? Każdy z tych scenariuszy może wpłynąć na wymagania związane z bezpieczeństwem sieci.

Dlaczego? Oto przykład - jeśli firma planuje ekspansję na nowe rynki, może okazać się, że będzie potrzebować zwiększenia przepustowości sieci, a to determinuje wybór urządzeń z odpowiednimi parametrami technicznymi.
Z kolei rozwijanie nowych usług internetowych może wymagać bardziej zaawansowanych rozwiązań w obszarze filtrowania ruchu sieciowego lub ochrony przed atakami DDoS.

Jednym z kluczowych błędów, jakie są popełniane podczas wyboru UTM/NGFW, jest inwestowanie w rozwiązania, które są dostosowane tylko do obecnych potrzeb, bez uwzględnienia długoterminowych strategii rozwoju. W efekcie, po kilku latach takie rozwiązania mogą okazać się niewystarczające, co generuje koszty związane z ich wymianą, których można byłoby uniknąć prowadząc odpowiednią analizę na początku inwestycji.

Właśnie z tego powodu przed wyborem urządzeń do zabezpieczania sieci warto przeprowadzić analizę i dostosować rozwiązania do długoterminowych planów rozwoju organizacji.



JAK WYBRAĆ UTM / NGFW DO TWOJEJ FIRMY?

Urządzenia UTM łączą w sobie różne funkcje zabezpieczające sieć wewnętrzną, takie jak firewall, antywirus, antyspam, filtracja treści web, analiza protokołów sieciowych, dostęp VPN oraz wykrywanie i zapobieganie włamaniom: IDS/IPS.
Dzięki temu jedno urządzenie może zapewnić kompleksową ochronę przed różnymi zagrożeniami, eliminując potrzebę stosowania wielu osobnych rozwiązań. Dlatego tak ważne jest, by wybrać optymalne urządzenie dla swojej infrastruktury.

Błędy popełnione na etapie wyboru rozwiązania mogą skutkować znacznym wzrostem TCO infrastruktury, czyli jej kompleksowego kosztu. Urządzenie o zbyt małej wydajności nie jest w stanie analizować ruchu sieciowego w czasie rzeczywistym, co wprowadza opóźnienia w pracy sieci.. To może negatywnie wpłynąć na wydajność pracy w organizacji. Naprawa takiego błędu po zakupie wymaga wymiany na lepsze urządzenie lub rozbudowy za pomocą licencji umożliwiającej zwiększenie wydajności tzw. „pay-as-you-go”.

Pay-as-you-go może być korzystniejszym rozwiązaniem, ponieważ często jest to tańsza forma rozbudowy w stosunku do całkowitej wymiany rozwiązania na nowe, a także pozwala rozłożyć koszty w czasie.

Nie każdy producent jednak dopuszcza taką opcję rozbudowy posiadanego urządzenia. Której formy nie wybierzemy, rozwiązania pozwalające na zwiększenie wydajności generują dodatkowe koszty.

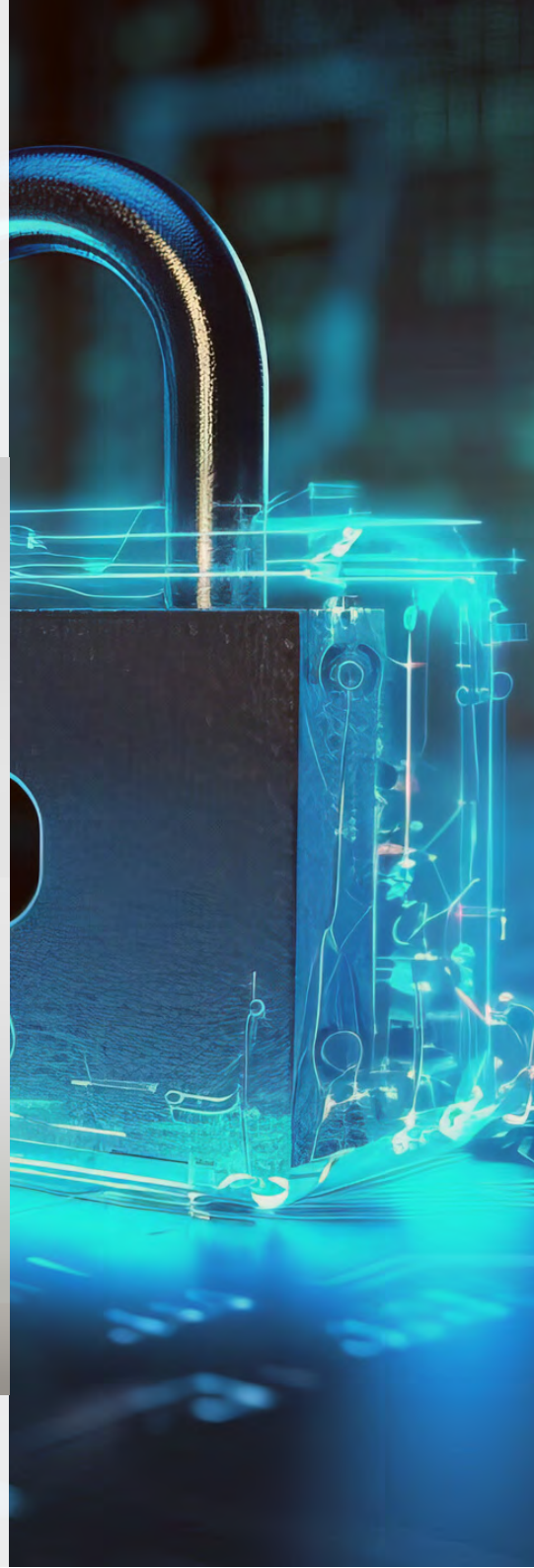
Perceptus od 15 lat integruje rozwiązania IT i dlatego wiemy, jak trudne jest czasem właściwe dobranie urządzenia. By to ułatwić, udostępniliśmy bezpłatne narzędzie, które pozwala na dobranie odpowiedniego urządzenia na podstawie wymaganych minimalnych parametrów rozwiązania przez organizację.

JAK TWORZYLIŚMY PORÓWNYWARKĘ UTM?

Oczywiście, nasza porównywarka nie zapewnia 100% dopasowania rozwiązania do twoich potrzeb. Konfiguracja polecanych rozwiązań opiera się na informacjach na temat minimalnych wymagań uzupełnianych w trakcie krótkiej ankiety przez użytkownika.

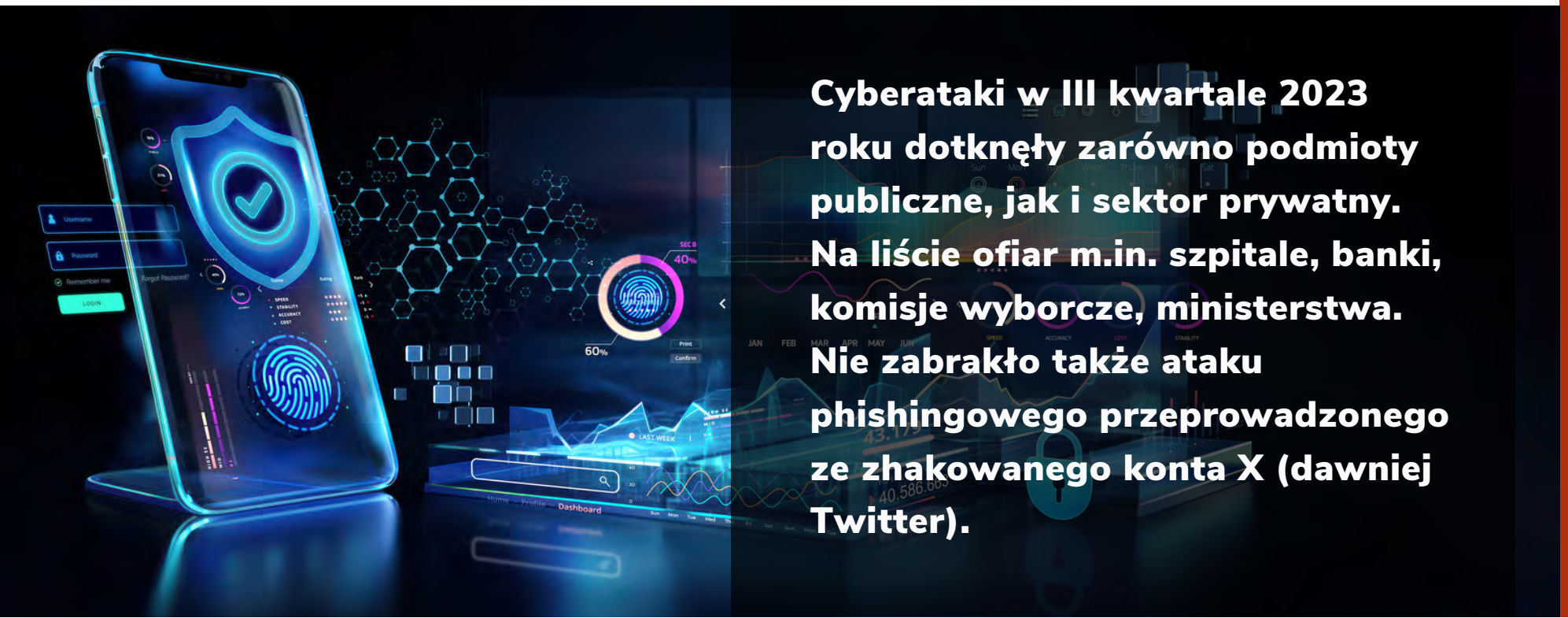
Na bazie tych wskazań dobierane są rozwiązania zapewniające określone parametry techniczne. Te parametry wytypowaliśmy na podstawie analizy dokumentacji technicznej wybranych rozwiązań, najczęściej spotykanych na rynku.

Jeśli szukasz rozwiązania zabezpieczającego sieć - sprawdź porównanie UTM od Perceptus - zeskanuj kod QR, który przeniesie Cię na stronę internetową z porównywarką.



CYBERATAKI W III KWARTALE 2023 ROKU

Redakcja
SECURITY MAGAZINE



Cyberataki w III kwartale 2023 roku dotknęły zarówno podmioty publiczne, jak i sektor prywatny. Na liście ofiar m.in. szpitale, banki, komisje wyborcze, ministerstwa. Nie zabrakło także ataku phishingowego przeprowadzonego ze zhakowanego konta X (dawniej Twitter).

ZAGROŻONE MINISTERSTWA NORWESKIE

W trzecim kwartale 2023 roku doszło do szeregu cyberataków. Ofiarami były nie tylko giganci, ale także instytucje publiczne, o czym na własnej skórze przekonał się rząd norweski. Zgodnie z tym, co przekazał Erik Hope, dyrektor organizacji ds. bezpieczeństwa i usług w norweskich ministerstwach, dwanaście ministerstw padło ofiarą cyberataku. Zagrożenie wyryto poprzez „nietypowy" ruch sieciowy, polegający na braku dostępu do poczty elektronicznej i kilku usług sieciowych. Do ataku doszło, ponieważ cyberprzestępcy wykorzystali lukę w oprogramowaniu jednej z firm, która świadczy usługi na rzecz norweskiego rządu.

W lipcu doszło także do poważnego cyberataku na Indonezyjską Dyrekcję Generalną ds. Imigracji w Ministerstwie Prawa i Praw Człowieka. W wyniku przestępstwa wyciekły dane paszportowe ponad 34 milionów Indonezyjczyków, które zawierały pełne imiona i nazwiska mieszkańców Indonezji, płeć, numer paszportów, daty urodzenia oraz daty ważności i wydania dokumentów. Autor cyberataku pozyskane nielegalnie informację zamieścił w dark web za 10 tys. dolarów. Organy ścigania w dalszym ciągu badają incydent.

DOSTĘP DO DANYCH WRAŻLIWYCH NA TIGO I HOT TOPIC

Początkiem trzeciego kwartału 2023 roku pojawiły się także informację o tym, że na Tigo, chińskiej platformie do czatów video, doszło do wycieku danych osobowych ponad 700 tys. osób. Do sieci trafiły takie informacje jak: imiona i nazwiska użytkowników, ich nicki, płeć, adresy e-mail, adresy IP, zdjęcia oraz prywatne wiadomości.

1 sierpnia portal Hot Topic ogłosił, że od lutego do czerwca 2023 r. został dotknięty falą ataków polegających na fałszowaniu danych uwierzytelniających. Według sprzedawcy „podejrzana aktywność związana z logowaniem" na jego platformie z nagrodami doprowadziła do wykrycia cyberataków. Dochodzenie wykazało, że cyberataki miały miejsce między 7 lutego a 21 czerwca 2023 r. i mogły umożliwić odpowiedzialnym za to złośliwym podmiotom dostęp do wrażliwych informacji klientów. Hakerzy wielokrotnie wykorzystali skradzione dane uwierzytelniające, aby uzyskać nieautoryzowany dostęp do platformy Hot Topic Rewards. Umożliwiło im to dostęp do informacji o klientach, w tym imion i nazwisk, adresów pocztowych, dat urodzenia, numerów telefonów i historii zamówień. Dostęp do częściowych informacji o karcie płatni-

czej (cztery ostatnie cyfry) mógł również zostać uzyskany, jeśli ofiara zapisała na swoim koncie dane karty. Po dochodzeniu w sprawie naruszenia danych Hot Topic ustalił, że w ataku użyto legalnych danych uwierzytelniających, ale uzyskano je z „nieznanego źródła zewnętrznego", a nie z samego Hot Topic.

W NIEBEZPIECZEŃSTWIE WŁOSKIE BANKI I AMERYKAŃSKIE SZPITALE

Sierpień niebezpieczny okazał się także dla włoskich banków, które zostały odłączone od sieci z powodu ukierunkowanych ataków typu rozproszona odmowa usługi (DDoS). Agenzia per la Cybersicurezza Nazionale (ACN) podała, że co najmniej pięć banków w całym kraju stało się celem cyberataków. Według ACN „stwierdzono reaktywację kampanii rozproszonych ataków typu »odmowa usługi« (DDoS) prowadzonych przez prorosyjskie grupy przeciwko krajowym podmiotom instytucjonalnym". ACN stwierdziło, że za ataki odpowiedzialny jest rosyjski gang NoName.

Trzeci kwartał 2023 roku okazał się także niebezpieczny dla jednego ze szpitali w USA. Mowa tu o Prospect Medical Holdings, który padł ofiarą cyberataku opartego na oprogramowaniu ransomware. Atak dotknął 16 szpitali w Kalifornii, Connecticut, Pensylwanii i Rhode Island, a także 166 przychodni i klinik. W wyniku zagrożenia niektóre placówki musiały wstrzymać działalność i przekierować pacjentów do innych szpitali. Federalne Biuro Śledcze (FBI) wszczęło dochodzenie w sprawie cyberataku, który został potwierdzony jako związany z oprogramowaniem ransomware.

ATAK NA DISCORD.IO

W trzecim kwartale 2023 roku zaatakowano platformę Discord.io. W wyniku cyberataku ujawniono dane osobowe ponad 760 tys. użytkowników. Cyberprzestępca, który przesłał dane, posługujący się pseudonimem „Akhirah", udostępnił cztery rekordy użytkowników z bazy danych jako dowód ich autentyczności. Discord.io potwierdziło również, że dane były pozyskane zgodne z prawem.

W odpowiedzi na naruszenie Discord.io zamknął wszystkie swoje operacje i usługi oraz wszczął dochodzenie w sprawie naruszenia. Dochodzenie ujawniło, że cyberprzestępca uzyskał dostęp do bazy danych poprzez lukę w kodzie witryny, co umożliwiło mu pobranie całej bazy Discord.io i wystawienie jej na sprzedaż.

NARUSZENIE MOVEIT Z NOWYMI OFIARAMI

Naruszenie MOVEit nadal pochłania ofiary, z których najważniejszą – przynajmniej pod względem liczby indywidualnych ofiar – była Better Outcomes Registry & Network, w ramach której odkryto, że „osobiste informacje na temat zdrowia około 3,4 miliona osób – głównie tych poszukujących opieki w ciąży i noworodków urodzonych w Ontario w okresie od stycznia 2010 r. do maja 2023 r." zostało zagrożonych.

Inne niedawno zidentyfikowane ofiary MOVEit to:

- **należąca do Microsoftu firma Nuance** zajmująca się technologią opieki zdrowotnej, która wydała powiadomienie o naruszeniu w imieniu 13 organizacji z branży opieki zdrowotnej;

- **National Student Clearinghouse,** która w imieniu 900 szkół wydała powiadomienie o naruszeniu danych;
- **CareSource – dostawca planów Medicaid i Medicare** – który poinformował, że ujawniono informacje dotyczące 212 193 osób.

Skala naruszenia MOVEit pozostaje nieokreślona, ale według niektórych szacunków liczba organizacji, których to dotyczy, wynosi ponad 2000, a liczba indywidualnych ofiar – ponad 60 milionów. Jest prawdopodobne, że w nadchodzących tygodniach i miesiącach nadal będziemy mieli do czynienia z ujawnieniami naruszeń związanych z MOVEit Transfer.

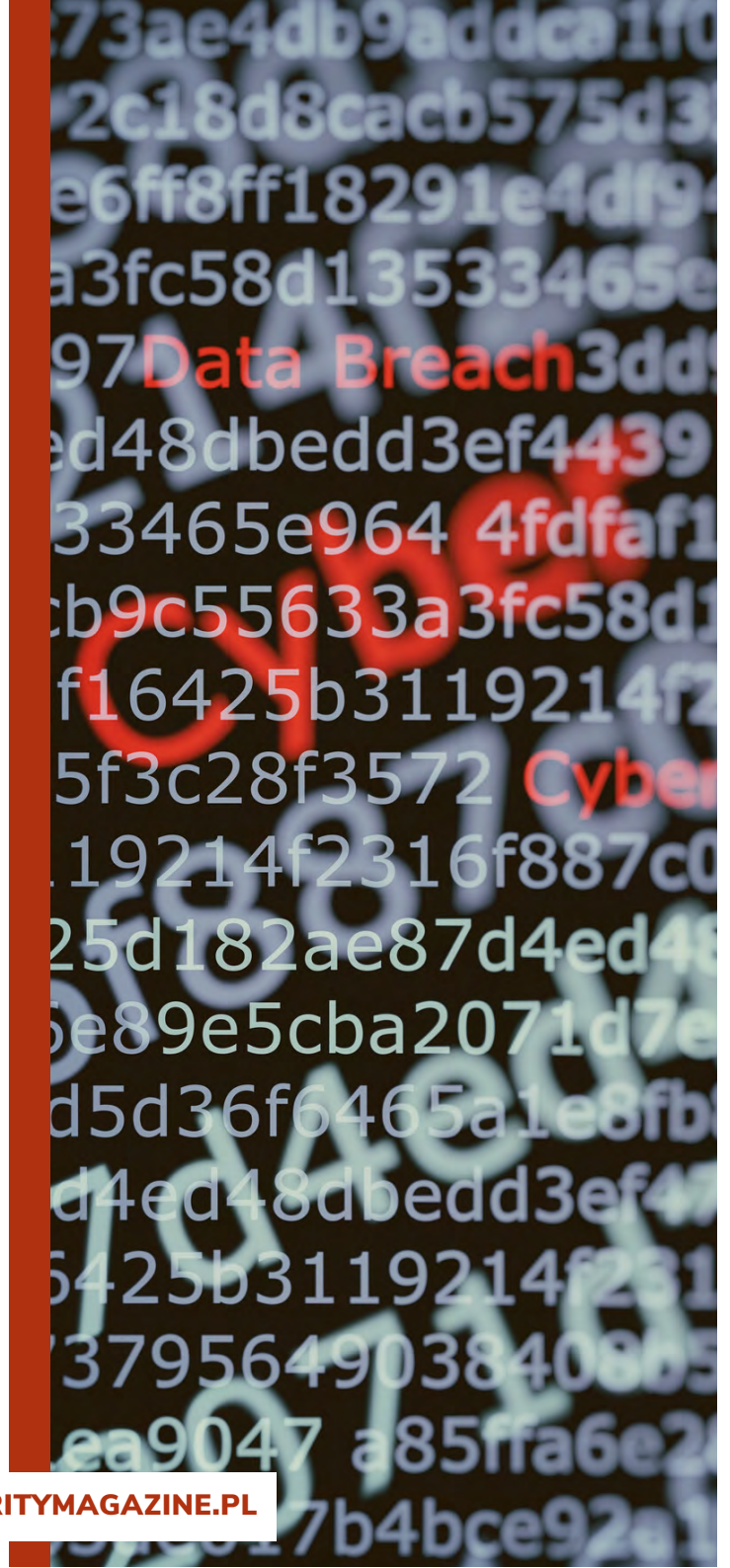
ATAK PHISHINGOWY ZE ZHAKOWANEGO KONTA X

Atak phishingowy przeprowadzony ze zhakowanego konta X (dawniej Twitter), współzałożyciela zdecentralizowanego blockchaina Ethereum i kryptowaluty Ether, Vitalika Buterina, doprowadził do straty ponad 691 000 dolarów.

Podejrzana aktywność na koncie Buterina 9 września doprowadziła do wykrycia naruszenia i schematu phishingu. Korzystając z wpływów Buterina w społeczności kryptowalut, hakerzy próbowali ukraść kryptowalutę i NFT jego zwolennikom, publikując post, który oferował bezpłatne pamiątkowe NFT w celu „świętowania przybycia Proto-Danksharding do Ethereum".

W rzeczywistości post zawierał link phishingowy, który wymagał od ofiary połączenia swoich portfeli blockchain ze stroną phishingową przed otrzymaniem NFT. Umożliwiło to złośliwym programom opróżnienie portfeli ofiar. Platforma wymiany kryptowalut CoinEx z siedzibą w Hongkongu odnotowała stratę 70 milionów dolarów w kryptowalutach w wyniku cyberataku przeprowadzonego na nią 12 września.

Firma podzieliła się wiadomością o cyberataku za pośrednictwem postu na swoim koncie X. Firma wyjaśniła w nim, że cyberatak został wykryty po tym, jak jej system kontroli ryzyka „wykrył anomalne wypłaty z kilku adresów gorących portfeli używanych do przechowywania aktywów giełdy CoinEx". Platforma wymiany kryptowalut bezpośrednio skontaktowała się ze złośliwymi podmiotami w sprawie cyberataku, również za pośrednictwem postu na X, próbując z nimi negocjować.



WNIOSKI

Powyższe przykłady dobitnie pokazują, że od cyberataków wolne nie są ani podmioty państwowe, ani prywatne. Dlatego tak ważne jest, aby wśród swoich pracowników na bieżąco aktualizować wiedzę na temat tego, w jaki sposób kradzione są dane w sieci, a gdy już do takiego ataku dojdzie, jak wtedy reagować.

Jeżeli chce się dobrze chronić dane, zarówno firmy, jak i podmioty publiczne, powinny dużą uwagę przywiązywać do zachowania odpowiednich procesów. Chodzi tutaj m.in. o kwestie dostępu, regularne monitorowanie urządzeń podpiętych do sieci czy szybkie reagowanie na zagrożenie, aby maksymalnie zminimalizować jego skutki.

Należy również pamiętać, że cyberprzestępcy stosują coraz bardziej wyrafinowane sposoby kradzieży danych. Dlatego czujność, wiedza o cyberzagrożeniach oraz odpowiednie systemy bezpieczeństwa, to zmniejszenie ryzyka cyberataku, który może być brzemienny w skutkach.

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

NADINSP. ADAM CIEŚLAK
komendant
Centralne Biuro Zwalczania Cyberprzestępczości

Absolwent Wyższej Szkoły Policji w Szczytnie oraz Uniwersytetu Wrocławskiego. W Policji od 1995 r. Od 2004 r. służył w Centralnym Biurze Śledczym Policji, a od 2016 r. na stanowisku Zastępcy Komendanta CBŚP. Od 2021 r. Pełnomocnik Komendanta Głównego Policji do przygotowania rozwiązań organizacyjno-prawnych związanych z utworzeniem Centralnego Biura Zwalczania Cyberprzestępczości. 1 maja 2022 r. powołany przez Ministra Spraw Wewnętrznych i Administracji na Komendanta CBZC.

PRZEMYSŁAW STRÓŻNIAK
Inżynier ds. Sieci i Systemów Teleinformatycznych
Perceptus Sp z o. o.

Od ponad 7 lat zajmuje się sieciami komputerowymi, bezpieczeństwem sieci oraz rozwiązaniami serwerowymi. W Perceptus projektuje infrastrukturę sieciową, wdraża i administruje rozwiązaniami sieciowymi, serwerami, prowadzi testy infrastruktury IT (hardware/software) i bierze udział w opracowywaniu koncepcji projektów rozwojowych w zakresie nowych technologii informatycznych.

ADRIAN SROKA
Security Architect

Architekt bezpieczeństwa i konsultant IT. Z pasją tworzy nowe rozwiązania oraz udoskonala istniejące, podnosząc jednocześnie ich techniczną, jak i funkcjonalną wartość. W pracy stosuje podejście oparte na współpracy i wiedzy. Zorientowany na zbliżanie do siebie bezpieczeństwa i dewelopmentu.

OLEKSII DOROSHENKO
Business Development Manager
Redsaber Security

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

EKSPERCI WYDANIA

IZABELA ŻYLIŃSKA

Organizatorka
Konferencja Inteligentna Energetyka

Magister inżynier robotyki. Od 2008 r. związana z branżowymi mediami technicznymi o tematyce automatyka, robotyka, energetyka, inteligentne miasta i regiony. Wydawca czasopism: Smart Grids Polska, INTELTECH, Inteligentne Miasta i Regiony. Organizatorka Konferencji "Inteligentna Energetyka".

KATARZYNA BIEŃKOWSKA

Prezes Zarządu
Silny&Salamon

Od początku kariery związana z Silny&Salamon, gdzie od podszewki poznawała specyfikę branży zabezpieczeń, rozwijając markę rzetelnego i niezawodnego partnera w biznesie. Od 2018 roku prezes zarządu, wcześniej w roli wiceprezesa i dyrektora handlowego rozwijała sprzedaż w spółce.

RAFAŁ LACHOWICZ

Specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji

Kierownik Działu Kontroli oraz Koordynator ds. Nadużyć Finansowych w Urzędzie Marszałkowskim Województwa Dolnośląskiego. Certyfikowany specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji. Specjalizuje się w obszarze przeciwdziałania i wykrywania nadużyć finansowych.

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.

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

Skontaktuj się z nami

redakcja@securitymagazine.pl

+48 22 390 91 05
+48 518 609 987

Deadline:
wydanie grudniowe: do 20.11
wydanie styczniowe: do 10.12

KATALOG FIRM

intellias

INTELLIAS POLSKA SP. Z.O.O

Zabłocie Business Park
Zabłocie 43B
30-701 Kraków

Dane kontaktowe
@ info-krakow@intellias.com

Specjalizacje

C++	Java	DevOps	JavaScript
AQA	.NET	Python	Scala
IoT	UX/UI	Cloud	BigData

Firma Intellias jest globalnym partnerem technologicznym firm z listy Fortune 500 i liderów branży. Intellias pomaga firmom w Europie, Ameryce Północnej, na Bliskim Wschodzie oraz w regionie Azji i Pacyfiku we wdrażaniu innowacyjnych rozwiązań cyfrowych.

Została wpisana na listę Global Outsourcing 100 przez IAOP oraz otrzymała nagrody od Inc. 5000, nagrody Forbesa i GSA UK.

Dzięki ponad 20-letniemu doświadczeniu i stabilnej pozycji na rynku firma zapewnia swoim klientom pomoc w dążeniu do sukcesu. W naszych polskich biurach, które ulokowane są w Krakowie, Warszawie, Wrocławiu oraz Łodzi pracuje aktualnie ponad 300 specjalistów.

W tym roku Intellias zdobył tytuł Top Tech Employer przyznawany przez portal IT – BulldogJob oraz tytuł Great Place to Work 2023.

NIEZAWODNY GLOBALNY PARTNER

Od ponad dwudziestu lat gromadzimy najlepsze umysły inżynieryjne na całym świecie, aby tworzyć rozwiązania cyfrowe nowej generacji dla firm z listy Fortune 500. Chcemy być niezawodnymi partnerami nie tylko dla naszych klientów, ale także dla siebie nawzajem. Pielęgnujemy kulturę dbania o siebie, w której wspieramy się nawzajem, próbujemy nowych sposobów działania, popełniamy błędy i uczymy się na nich. Nasze projekty są inteligentne i innowacyjne, a nasze zespoły życzliwe i pełne szacunku. Myślimy globalnie, ale zawsze działamy po ludzku.

21 lat dostarczania doskonałej technologii

3200 specjalistów i specjalistek na pokładzie

60% senior inżynierów i inżynierek w projektach

130+ klientów globalnie

ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ

Wydanie 2/2022
POBIERZ

Wydanie 3/2022
POBIERZ

Wydanie 4/2022
POBIERZ

Wydanie 5/2022
POBIERZ

Wydanie 6/2022
POBIERZ

Wydanie 7/2022
POBIERZ

Wydanie 8/2022
POBIERZ

Wydanie 9/2022
POBIERZ

Wydanie 1(10)/2023
POBIERZ

Wydanie 2(11)/2023
POBIERZ

Wydanie 3(12)/2023
POBIERZ

Wydanie 4(13)/2023
POBIERZ

Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

Wydanie 7(16)/2023
POBIERZ

Wydanie 8(17)/2023
POBIERZ

Wydanie 9(18)/2023
POBIERZ

Wydanie 10(19)/2023
POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

ul. Nowogrodzka 42 lok. 12
00-695 Warszawa

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

Redaktor Naczelny: Rafał Stępniewski

Redaktor prowadząca: Monika Świetlińska

Redakcja: Damian Jemioło, Joanna Gościńska, Katarzyna Leszczak
Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL