2(23)/2024

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

To ostatnie wydanie w PDF

Zapraszamy od marca na www.securitymagazine.pl

Szczegóły str. 7

SPIS TREŚCI

SZANOWNI PAŃSTWO,

niebawem minie druga rocznica powstania "Security Magazine". Z tego miejsca chcę wyrazić głęboką wdzięczność za Wasze nieustające wsparcie i zaangażowanie, które umożliwiło nam nieprzerwane dzielenie się najważniejszymi informacjami i analizami z obszaru cyberbezpieczeństwa.

W trakcie dwuletniej działalności naszego magazynu byliśmy świadkami wielu incydentów bezpieczeństwa, które potwierdziły, iż żadna organizacja nie jest w pełni zabezpieczona przed atakami. Dlatego nasza misja “w służbie bezpieczeństwu” jest wciąż aktualna.

W nadchodzącym roku zobowiązujemy się do kontynuowania naszej misji w zupełnie nowej odsłonie. Co to oznacza? Wydanie, które teraz Państwo czytacie, jest ostatnim w formacie PDF. Od marca magazyn będzie dostępny za pośrednictwem strony www.securitymagazine.pl, a o szczegółach będziemy informować na bieżąco w naszych social mediach.

Wszystkie dotychczasowe wydania, a było ich 23, będą dostępne na wspomnianej stronie. Wszystkich zainteresowanych współpracą w nowej formule zapraszam do kontaktu. Na życzenie prześlemy Państwu naszą zupełnie nową ofertę współpracy biznesowej.

Zachęcam do lektury naszego drugiego jubileuszowego wydania oraz śledzenia naszych kanałów na LinkedIn oraz Facebook.

Rafał Stępniewski

SZCZEGÓŁY STR. 112

NASK I KOMPUTER KWANTOWY

Projekt EPIQUE, finansowany przez Komisję Europejską kwotą ponad 10 mln euro, ma na celu stworzenie europejskiego komputera kwantowego opartego na fotonice. Państwowy Instytut Badawczy NASK, wraz z 17 innymi partnerami, bierze udział w tym ambitnym przedsięwzięciu.

Komputery kwantowe, uznawane za jedną z najbardziej obiecujących technologii przyszłości, mogą rozwiązywać problemy nieosiągalne dla obecnych superkomputerów. Projekt EPIQUE skupia się na technologiach fotonicznych, wykorzystujących fotony jako kubity, co oferuje zalety, takie jak niska dekoherencja kubitów i łatwość integracji z sieciami światłowodowymi. Celem projektu jest opracowanie trzech prototypów fotonicznych komputerów kwantowych, pracujących na dziesiątkach kubitów, jako krok w kierunku stworzenia platformy obliczeń kwantowych z ponad 1 tys. kubitów. Wyniki mogą wpłynąć na inne obszary technologii kwantowych, takie jak metrologia czy komunikacja kwantowa. EPIQUE jest częścią inicjatywy Quantum Flagship, mającej na celu rozwój europejskiego komputera kwantowego, z budżetem około 1 miliarda euro.

CBZC W PROJEKCIE NOTIONES

Projekt NOTIONES - iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS", wspierany przez Centralne Biuro Zwalczania Cyberprzestępczości, ma stworzyć sieć specjalistów z dziedziny bezpieczeństwa, w tym cyberbezpieczeństwa, do wymiany doświadczeń i integracji nowych technologii, jak AI i uczenie maszynowe. Przez 5 lat wyniki projektu będą prezentowane np. na konferencjach, wpływając na badania w bezpieczeństwie i wywiadzie.

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"

UNIJNY SCHEMAT EUCC

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) opracowała pierwszy schemat certyfikacji cyberbezpieczeństwa w ramach unijnego ramowego programu certyfikacji cyberbezpieczeństwa, zatwierdzony przez Komisję Europejską. Schemat, znany jako Europejski Schemat Certyfikacji Cyberbezpieczeństwa na Wspólne Kryteria (EUCC), ma na celu podniesienie poziomu cyberbezpieczeństwa produktów, usług i procesów ICT na rynku UE przez ustanowienie kompleksowego zestawu reguł, wymagań technicznych, standardów i procedur. Schemat EUCC, oparty na sprawdzonym systemie oceny Wspólnych Kryteriów SOG-IS, już stosowanym w 17 państwach członkowskich UE, oferuje dwa poziomy zapewnienia w zależności od poziomu ryzyka związanego z zamierzonym użyciem produktu, usługi lub procesu. Jest to pierwszy krok w kierunku harmonizacji certyfikacji cyberbezpieczeństwa w UE, zastępujący krajowe schematy certyfikacji i umożliwiający dostawcom ICT wykazanie zapewnienia poprzez proces oceny zrozumiały w całej UE. Schemat EUCC ma również zachęcić dostawców do przestrzegania wymagań certyfikacji cyberbezpieczeństwa, co wpłynie na rynek certyfikacji cybernetycznych.

REKRUTACJA DO CYBERWOJSKA

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

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

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

Redakcja "Security Magazine"

PATRONAT
SECURITY MAGAZINE

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

8. EDYCJA InfraSEC FORUM
ICS SCADA OT IIOT

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

Dlaczego warto uczestniczyć?

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

Dla kogo?

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

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

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

SZCZEGÓŁY I REJESTRACJA

SECURITYMAGAZINE.PL

DWA LATA “SECURITY MAGAZINE”. CZAS NA ZMIANY

Redakcja
SECURITY MAGAZINE

Od dawna wiadomo, że kwestia bezpieczeństwa w przedsiębiorstwach, instytucjach publicznych i organizacjach bywa bagatelizowana, co niekoniecznie wynika z ignorancji, ale z ograniczonego dostępu do specjalistycznej wiedzy w tym obszarze. Dlatego "Security Magazine" ma służyć Państwu wsparciem w zdobywaniu wiedzy na temat bezpieczeństwa, oferując nie tylko praktyczne wskazówki, ale także studia przypadków, analizy ryzyka i metody ich neutralizacji. I tak już przez dwa lata.

“W SŁUŻBIE BEZPIECZEŃSTWU”

- *W ostatnich miesiącach 2021 roku zaobserwowaliśmy wyraźny wzrost zainteresowania tematyką cyberbezpieczeństwa. Ten trend nie był przypadkowy. Eskalacja napięć między Rosją a Ukrainą, z każdym tygodniem coraz bardziej zaznaczająca się na arenie międzynarodowej, skłoniła wiele podmiotów do poszukiwania informacji na temat ochrony swojej działalności w wirtualnej rzeczywistości. Naturalnym instynktem przedsiębiorców, pragnących zabezpieczyć swoje biznesy przed potencjalnymi zagrożeniami, było zgłębianie wiedzy* w temacie cyberbezpieczeństwa - powiedział **Rafał Stępniewski, redaktor naczelny “Security Magazine”.**

- *Nasze badania rynku ujawniły istotną lukę - w Polsce brakowało łatwo dostępnego, przystępnego źródła wiedzy, dedykowanego kwestiom bezpieczeństwa, z naciskiem na cyberbezpieczeństwo, zarówno w sektorze prywatnym, jak i publicznym. Oczywiście, istnieje wiele serwisów poruszających w sposób profesjonalny tę kwestię, ale dotyczy to głównie zagrożeń skierowanych na osoby indywidualne* - dodał redaktor naczelny “Security Magazine”.

- *Widzieliśmy potrzebę stworzenia platformy, która nie tylko ułatwiłaby firmom pierwsze kroki w zrozumieniu zagrożeń cyfrowych, ale również pomogła w ocenie ryzyka i implementacji skrojonych na miarę rozwiązań bezpieczeństwa, adekwatnych do specyfiki ich działalności. W odpowiedzi na te potrzeby, naszym celem stało się dostarczenie takiego medium, które by służyło jako kompendium wiedzy o cyberbezpieczeństwie - aktualne i praktyczne. Zrozumienie, że bezpieczeństwo informacji jest nie tylko kwestią technologiczną, ale również strategiczną, stało się podstawą naszego podejścia. Poczuliśmy, że edukacja i świadomość w zakresie cyberbezpieczeństwa zarówno małych, jak i dużych przedsiębiorstw, zarówno sektora prywatnego, jak i publicznego, są naszą misją* - zaznaczył Rafał Stępniewski.

Rzetelna Grupa jako wydawca serwisu Polityka Bezpieczeństwa oraz pisma “RODOmagazyn”, mająca zespół ekspertów i praktyków z zakresu bezpieczeństwa, ochrony danych i prawa, podjęła się stworzenia “Security Magazine”, który przez pierwsze dwa lata wydawany był w wersji elektronicznej, w formacie PDF.

- *To był dla nas czas próby, bo z jednej strony*

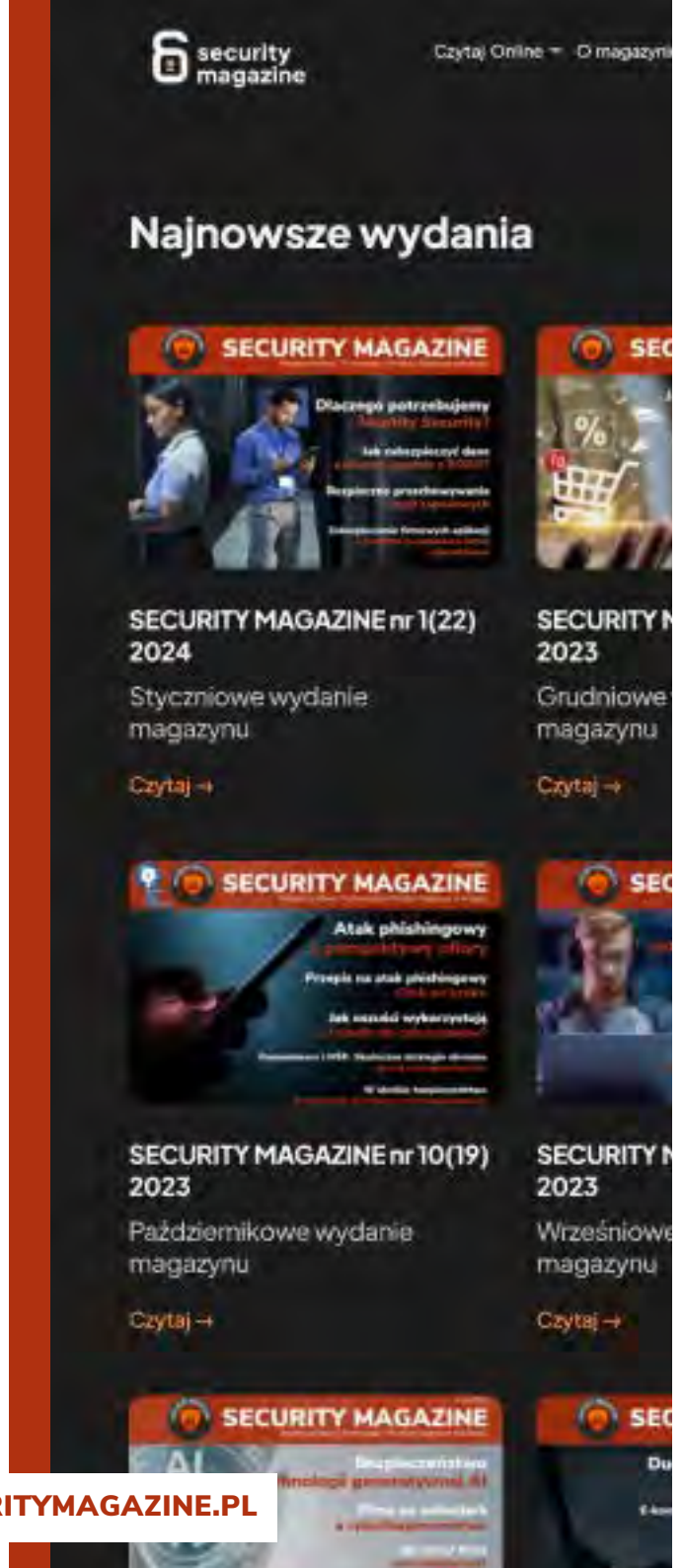
wiedzieliśmy, że jest potrzeba stworzenia podobnego pisma, z drugiej - pomysł zrodził się w czasie, kiedy branża security była jeszcze dość hermetyczna. Mieliśmy obawy co do tego, że nasz koncept może się nie udać, bo firmy związane z szeroko rozumianym bezpieczeństwem sektora prywatnego i publicznego, mogą mieć opory z dzieleniem się case study, rozwiązaniami, czy poradami, które w piśmie miałyby być de facto bezpłatne dla czytelników - wspominał Rafał Stępniewski.

POTENCJAŁ “SECURITY MAGAZINE”

Pierwsze wydanie - planowane początkowo na... 24 lutego 2021 - miało swoją premierę niecały miesiąc później. Wojna i szum medialny wokół niej były kolejnymi czynnikami, które poddały pod wątpliwość nasze plany. Wydanie było jednak gotowe, zarejestrowane, więc daliśmy sobie szansę. W marcu 2021 roku z pierwszymi ekspertami i firmami, które od początku nam zaufały: **Sygnisoft, Grandmetric, Evolution, Come Creations Group, No Fluff Jobs, Marken - Bitdefender w Polsce, Energy Logserver**, ruszyliśmy.

W tym wydaniu redaktor naczelny podkreślił, że "*naszym priorytetem jest przekazanie czytelnikom merytorycznej, profesjonalnej wiedzy bazującej na doświadczeniu praktyków z Polski oraz ze świata. Tematy wokół których będziemy się poruszać dotyczą szeroko pojętego bezpieczeństwa w firmach oraz jednostkach publicznych. Chodzi tu nie tylko o bezpieczeństwo fizyczne, ale i - o coraz istotniejsze - bezpieczeństwo IT. Stawiamy na profesjonalizm, rzetelność i wyczerpujące podejście do opisywanych zagadnień. Nasi autorzy również. Dlatego magazyn, mamy nadzieję, stanie się źródłem i inspiracją dla przedsiębiorców, którym zależy na tak kluczowym aspekcie działalności, jak właśnie bezpieczeństwo.*"

Pierwsze wydanie pobrało 14500 czytelników, co jak na start zupełnie nowego pisma na rynku mediów skierowanego do bardzo konkretnej grupy odbiorców było wielkim sukcesem. Z kolejnymi wydaniami liczba pobrań rosła, osiągając nawet 35000 tysięcy pobrań jednego miesiąca.



Łącznie przez niecałe dwa lata osiągnęliśmy 560 tys pobrań wszystkich dotychczasowych wydań. Średnio na jedno wydanie w formie PDF przypadło niemal 26 tys. pobrań. We wszystkich dotychczasowych wydaniach pojawiło się 291 artykułów eksperckich. Materiały zajęły łącznie 2300 stron. Średnio każde wydanie miało 96 stron. Najwięcej - 117. I średnio 10 profesjonalnych, unikalnych artykułów o długości około 8 tys. znaków. Wiedzą i doświadczeniem podzieliło się łącznie 142 ekspertów, z czego nazwiska 43 pojawiały się w wydaniach minimum dwukrotnie. Średnio w jednym wydaniu pojawiają się nazwiska 10 ekspertów.

Przez ten cały czas objęliśmy 42 patronaty medialne nad najważniejszymi wydarzeniami w Polsce dotyczącymi bezpieczeństwa, w tym najczęściej cyberbezpieczeństwa. Tyle zapowiedzi wydarzeń branżowych w ramach patronatu medialnego pojawiło się w wydaniach. Opublikowaliśmy też 19 obszernych fotorelacji. Na łamach wydań opublikowaliśmy łącznie 140 reklam w różnych formatach. Dodatkowo opublikowaliśmy 13 wizytówek prezentujących firmy.

CZAS NA ZMIANY

Dwa pierwsze lata były czasem próby. Pokazały nam, by iść dalej i rozwijać pismo. Przystępność, na której nam zależało, to nie tylko bezpłatny dostęp do pisma, ale i jego format jako PDF. Wszystko po to, by ułatwić Czytelnikowi lekturę i dopasować się do urządzeń, z których korzysta najczęściej (smartfon, laptop). Każde wydanie można było ściągnąć bez-

pośrednio na swoje urządzenie.

Zdajemy sobie jednak sprawę, że wygodniejszą formą dla czytelników jest strona internetowa, zarówno wersja desktopowa, jak i mobile. Chcąc rozwijać pismo, z okazji jego drugiej rocznicy, zdecydowaliśmy o wprowadzeniu nowej formuły - materiały eksperckie będą co miesiąc dostępne na naszej stronie www.securitymagazine.pl w zupełnie nowej odsłonie (dostępnej od pierwszej połowy marca) dla zarejestrowanych czytelników. Ci, którzy nie zdecydują się na rejestrację zobaczą “Cybernewsy” i zapowiedzi materiałów eksperckich.

Taka formuła zdecydowanie usprawni również komunikację między redakcją a czytelnikami, każdy bowiem otrzyma raz w miesiącu newsletter z zapowiedzią nowego wydania - w ten sposób go nie przeoczy. Konkretne materiały będą dostępne bez potrzeby pobierania całego wydania. Każdy z czytelników po zalogowaniu będzie miał okazję niezobowiązująco ocenić artykuł, ale również oddać swój głos na eksperta.

- *Nowa odsłona “Security Magazine” to też nowe możliwości promocyjne dla firm chcących z nami współpracować. Będą mogły zamieszczać na łamach naszego serwisu nie tylko swoje autorskie artykuły, ale informacje o szkoleniach, webinarach, video, podcasty. A to, oczywiście, nie wszystko. Zainteresowanym współpracą firmom możemy udostępnić zaktualizowaną propozycję współpracy biznesowej* - zaznaczyła Agnieszka Zboralska, kierowniczka ds. sprzedaży w Rzetelnej Grupie.

Kolejną zmianą w “Security Magazine” będzie jego tematyka. - *Statystyki i analizy pokazały nam, że 98% firm chcących publikować na naszych łamach związanych jest z bezpieczeństwem IT. Artykuły dotyczące bezpieczeństwa fizycznego pojawiały się sporadycznie. Stąd też nie zdecydowaliśmy się w naszych PDF-ach na działy tematyczne, o których swego czasu razem z czytelnikami rozmawialiśmy w naszych social mediach. A w kontekście zmian formatu pisma uznaliśmy, że “Security Magazine” poświęcony będzie wyłącznie cyberbezpieczeństwu* - zapowiedział redaktor naczelny, dodając, że jesteśmy w trakcie rozwijania innego naszego serwisu “Polityka Bezpieczeństwa”. - *Ten serwis też zyska nowy wygląd, nowe możliwości i będzie poświęcony bezpieczeństwu organizacji, fizycznemu w firmach* - powiedział Rafał Stępniewski.

Dziękujemy za Państwa obecność od dwóch lat.

Polityka ®
Bezpieczeństwa

SZKOLENIA
Z OCHRONY DANYCH OSOBOWYCH

SPRAWDŹ OFERTĘ

MASZ PYTANIA?

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

SECURITYMAGAZINE.PL

2024 ROK W BRANŻY CYBERSECURITY

Redakcja
SECURITY MAGAZINE

W miarę jak organizacje i indywidualni użytkownicy stają się coraz bardziej zależni od cyfrowych rozwiązań, pojawiają się nowe wyzwania i możliwości dla specjalistów od bezpieczeństwa. Trendy takie jak sztuczna inteligencja, uczenie maszynowe, oraz rozwój kwantowych technologii obiecują rewolucję w sposobach obrony przed cyberatakami. Jakie inne innowacje zdefiniują branżę cybersecurity w 2024 roku? Zapytaliśmy o to naszych ekspertów.

PIOTR BROGOWSKI
Orion Instruments Polska

Rok 2023 w zakresie cyberbezpieczeństwa zapisał się przede wszystkim wyciekami danych (także medycznych i genetycznych) dotykającymi dziesiątki, a nawet setki milionów osób, spektakularnymi i niszczącymi atakami ransomware (liczba ofiar wzrosła rok do roku o 55%), masowymi atakami phishingowymi oraz mającymi globalny zasięg atakami na łańcuchy dostaw. Średni koszt poważnego incydentu cyberbezpieczeństwa wzrósł w 2023 r. w porównaniu do roku poprzedniego o 11%. Jednocześnie zaś budżety na cyberbezpieczeństwo wzrosły tylko o 3%. W 2024 r. nakłady te powinny według przewidywań być wyższe o 8%, co jednak wciąż wydaje się wartością nieadekwatną do poziomu zagrożeń.

Wyzwania

W roku 2024 wyzwaniem będzie nadal jak najwcześniejsze wykrywanie i usuwanie podatności oprogramowania. Dotyczy to szczególnie Internetu Rzeczy (IoT), pojazdów autonomicznych, systemów przemysłowych (OT) oraz aparatury medycznej. Poważnym problemem będzie wciąż poważny deficyt specjalistów z zakresu cyberbezpieczeństwa. Tym większe znaczenie będzie miał dalszy rozwój i coraz powszechniejsze zastosowanie w rozwiązaniach cyberbezpieczeństwa uczenia maszynowego (ML) i sztucznej inteligencji (AI). Przełomowe będzie wprowadzenie generatywnej sztucznej inteligencji (GenAI) do systemów zabezpieczeń takich jak XDR, SIEM, czy SOAR.

Priorytety

Priorytetem dla działów cyberbezpieczeństwa będzie wykrywanie zagrożeń w czasie rzeczywistym i automatyzacja reakcji na incydenty. Motorem wzrostu rynku w najbliższych latach będą inicjatywy mające na celu wykorzystanie jednolitych narzędzi i procedur w całej infrastrukturze, w tym w chmurze, IoT, systemach OT i IT. Rozwijane będzie zarządzanie ryzykiem oparte na sztucznej inteligencji, które dzięki analizie ogromnych zbiorów danych, poprawi ochronę organizacji przed lukami w za-

bezpieczeniach.

Cyberprzestępstwa

Według *Allianz Risk Barometer* incydenty cybernetyczne będą największym globalnym problemem w 2024 r. Istotnym zagrożeniem będą nadal działania grup cyberprzestępczych sponsorowanych przez państwa (Rosja, Chiny, Korea Płn., Iran) i stosujących coraz bardziej wyrafinowane techniki, zwłaszcza spear-phishing, często wspierany przez sztuczną inteligencję.

Szczególnie groźne będą ataki na systemy infrastruktury krytycznej. Coraz częstsze będzie wykorzystywanie RaaS (Ransomware as a Service), co spowoduje zejście cybeprzestępczości „pod strzechy", bowiem umożliwi zaawansowane cyberataki nawet osobom o relatywnie niskim poziomie wiedzy technicznej. Powszechne mogą się stać ataki na przemysłowe systemy sterowania (ICS); mogą też pojawić się realne próby hakowania urządzeń medycznych, pomiarowych, autonomicznych itp.

KRZYSZTOF BRYŁA
2BeAware

Rok 2023 dla świata cyberbezpieczeństwa to kolejny dynamiczny okres. Zmiany w dynamice geopolitycznej, wzrost napięć, wzmogły aktywność haktywizmu, związanego z tymi zmianami jaki i sponsorowanego przez państwa. Kolejną negatywną obserwacją, jest zjawisko rosnącej dysproporcji w implementacji bezpieczeństwa. Powstaje coraz większa dysproporcja pomiędzy organizacjami dojrzałymi, które zdążyły już zainwestować w sferę bezpieczeństwa oraz tymi najbardziej narażonymi, najsłabiej zabezpieczonymi.

Natomiast coraz większą rolę odgrywa cyber-resilience, czyli zdolność organizacji nie tylko do obrony, ale przede wszystkim do utrzymania integralności i funkcjonalności, mimo wystąpienia ataków cybernetycznych.

Wyzwania

Niedobór talentów i specjalistów w dziedzinie cyberbezpieczeństwa, zwłaszcza w sektorze publicznym, stanowi główne wyzwanie. Swego rodzaju antidotum na to, czy raczej uzupełnieniem będzie zastosowanie sztucznej inteligencji. Staje się ona coraz efektywniejszym narzędziem i asystentem działów bezpieczeństwa, zwłaszcza w zadaniach powtarzalnych, uciążliwych.

Niestety, jest też druga, ciemna strona medalu AI. Manipulacja informacją, eskalacje ataków z użyciem socjotechniki, ułatwienie kodowania nowych narzędzia ataku czy wycieki danych i naruszenia prywatności poprzez nieodpowiednie wykorzystanie AI przez użytkowników, to katalog wyzwań na nowy rok.

Optymistycznym akcentem może być dalszy wzrost budżetów na działania w obszarze bezpieczeństwa.

Priorytety

Wspomniana **odporność** cybernetyczna staje się kluczowym priorytetem, tym bardziej że jest ona mocno powiązana z bezpieczeństwem **łańcucha** dostaw.

Oba te aspekty, zwłaszcza w Europie znajdą się w 2024 w obszarze nowych regulacji co sprawi że kolejnym priorytetem stają się działania organizacji w obszarze GRC. Czarny rynek rozwiązań i usług cyberzagrożeń odkrył już wartość, we wzajemnej współpracy. Organizacje, chroniące swoje działania, wytwarzanie dóbr, czy łańcuchy dostaw, powinny rozważyć podobne działania, które dzięki zacieśnieniu współpracy, szybkiej wymianie informacji i wzajemnym wsparciu są w stanie je wzmocnić.

Cyberprzestępstwa

Ransomware, Ataki na łańcuch dostaw, Wykorzystywanie podatności „0-day", Dezinformacja – to rozszerzone „podium" zagrożeń prognozowanych na rok 2024. Ich stopień złożoności będzie stale doskonalony, liczba będzie rosła. I należy się spodziewać, że ich celem coraz częściej będą obiekty infrastruktury krytycznej.

Dlatego firmy powinny być gotowe do dynamicznie zmieniających się warunków i coraz bardziej zaawansowanych form cyberprzestępczości. Będzie to nadal wymagało współpracy, innowacji i strategicznego podejścia zarówno do przeciwdziałania atakom jak i do utrzymania odporności.

JACEK STAROŚCIC

Perceptus

Konflikt zbrojny w Ukrainie trwa, co ma bezpośrednie przełożenie nie tylko na fizyczne bezpieczeństwo polskich obywateli, ale również na sytuację w świecie cyfrowym.

Ilość ataków kierowanych na polskie instytucje, infrastrukturę krytyczną i firmy prywatne w minionym roku znacznie przewyższała ilość, z którą spotykaliśmy się wcześniej. Presja możliwych ataków motywuje wszystkich – zarówno sektor prywatny, jak i publiczny, do podnoszenia nie tylko poziomu zabezpieczeń sprzętowych, ale też poziomu wiedzy pracowników w tej dziedzinie. Rok 2023 w sektorze cyberbezpieczeństwa był wyścigiem zbrojeń.

W Perceptus miniony rok to rozbudowa bardzo ważnego dla naszych klientów elementu uzbrojenia, czyli obszaru SOC-Security Operation Center, który realizuje usługi outsourcingu Centrum Operacji Bezpieczeństwa i zabezpiecza infrastrukturę IT organizacji, którymi się opiekuje. Doświadczenie zdobyte w minionych latach pozwoliło nam idealnie dopasować te usługi do obecnej sytuacji. Dziś, kiedy rynek pracy cierpi na niedobór specjalistów, outsourcing tego typu usług staje się coraz bardziej poszukiwaną opcją.

Wyzwania

Zagrożenia, z którymi zmagaliśmy się w minionym roku nie znikną, ale prawdziwym wyzwaniem dla sektora prywatnego, jak również administracji publicznej i dostawców niektórych usług publicznych będzie dostosowanie się do przepisów wprowadzonych przez NIS2. Przepisy te do polskiego systemu prawnego muszą być zaimplementowane najpóźniej w październiku. Kiedy w obecnej sytuacji politycznej pojawią się konkretne projekty ustaw? Nie wiadomo... A więc sektory gospodarki wskazywane w NIS2 jako kluczowe i ważne, w których utrzymanie cyberbezpieczeństwa jest szczególnie istotne w kontekście bezpieczeństwa kraju, a w związku z tym obwarowane licznymi obowiązkami i karami za brak ich przestrzegania, muszą zacząć dostosowywać się do przepisów, których dzisiaj nadal brak.

Pewne jest, że konieczne będzie holistyczne spojrzenie na kwestie zabezpieczenia organizacji:

- od analizy sytuacji, identyfikacji ryzyk i zagrożeń,
- przez budowę odpornego na ataki systemu zabezpieczania danych i infrastruktury IT, którego elementem jest także edukacja uczestników,
- po stały monitoring sytuacji w sieci.

Model, w którym działy IT pracowały tak, jak reszta organizacji, od 9 do 17 przestał wystarczać. Praca zdalna i hybrydowa, nowoczesne technologie umożliwiające realizację zadań służbowych z drugiego końca globu, a z drugiej strony wieloetapowe ataki, których celem może być sparaliżowanie działania firmy lub uzyskanie dostępu do klu-czowych dla jej istnienia danych... To wszystko wymaga monitoringu realizowanego 24 h, przez 7 dni w tygodniu, 365 dni w roku. Tak właśnie działa Security Operations Center, które poza wykryciem i analizą incydentów zapewnia także odpowiednią reakcję, adek-watną do skali zagrożenia i jego faktycznej wagi. Nie każda anomalia to poważna infekcja i o tym trzeba pamiętać, budując system zabezpieczeń. By odpowiednio analizować dane konieczna jest właściwa interpretacja danych spływających z systemów SIEM czy IDS. To wymaga odpowiednich umiejętności, stąd warto korzystać z doświadczonych zespołów.

Cyberprzestępstwa

Katalog ataków pozostaje od kilku lat mniej więcej taki sam. Poza siłowymi atakami na infrastrukturę kluczową są to głównie działania skierowane na spowodowanie błędu najsłabszego ogniwa, czyli człowieka. Co powinno nas niepokoić, to ich rosnąca skuteczność, która niewątpliwie wynika ze wsparcia przestępców przez sztuczną inteligencję. Tym ważniejsza w prewencji staje się edukacja uczestników organizacji, zarówno ta teoretyczna, jak też symulacje testów, pozwalające każdemu w praktyce sprawdzić swoją czujność, kiedy pojawiają się potencjalne zagrożenia. A jeśli już dojdzie do infekcji – szybkie jej wykrycie.

MIŁOSZ JARZĄB
AON Polska

Trudno nie zauważyć ostatniego wzrostu popularności rozwiązań wykorzystujących sztuczną inteligencję. W 2023 roku powstało wiele narzędzi, które opierają na niej swoje działanie. Dzięki temu wiele branż mogło znacząco usprawnić i zautomatyzować swoje działania, co wiązało się z mniejszym zapotrzebowaniem na nowych pracowników. Przykłady znajdziemy nawet w popularnych branżowych rozwiązaniach SIEM czy oprogramowaniach antymalware. Może to prognozować dalsze prace nad nowymi programami, które ułatwią nam życie, lecz czy na pewno? Jest też spora szansa, że tak jak i w przeszłości, znajdą się wysoko cenione organizacje, które będą przodować wśród tego typu rozwiązań. Czy nadążą za tym pionierzy aktualnych technologii tacy jak Google czy Microsoft?

Wyzwania

Już dzisiaj w większości firm korzysta się z popularnego ChatuGPT, by usprawnić swoją pracę, lecz czy każdy pracownik mający dostęp do tej technologii przeszedł odpowiednie szkolenie lub przeczytał regulamin? I tu powinniśmy się zastanowić nad działaniem tego rozwiązania, ponieważ gromadzi ono wszelkie wprowadzane przez nas dane. Dlatego warto przemyśleć, czy danymi, które tak gorliwie chronimy hasłami i odciskami palców, nie dzielimy się z naszym “internetowym pomocnikiem”.
Każda organizacja, której pracownicy korzystają lub mogą korzystać z rozwiązania ChatGPT, powinni przejść obowiązkowe szkolenie z wykorzystywania tego narzędzia. To może nie tylko uświadomić pracowników w tym, jak przetwarzane są wprowadzane przez nich dane, ale także usprawnić posługiwanie się rozwiązaniami wykorzystującymi AI.

Priorytety

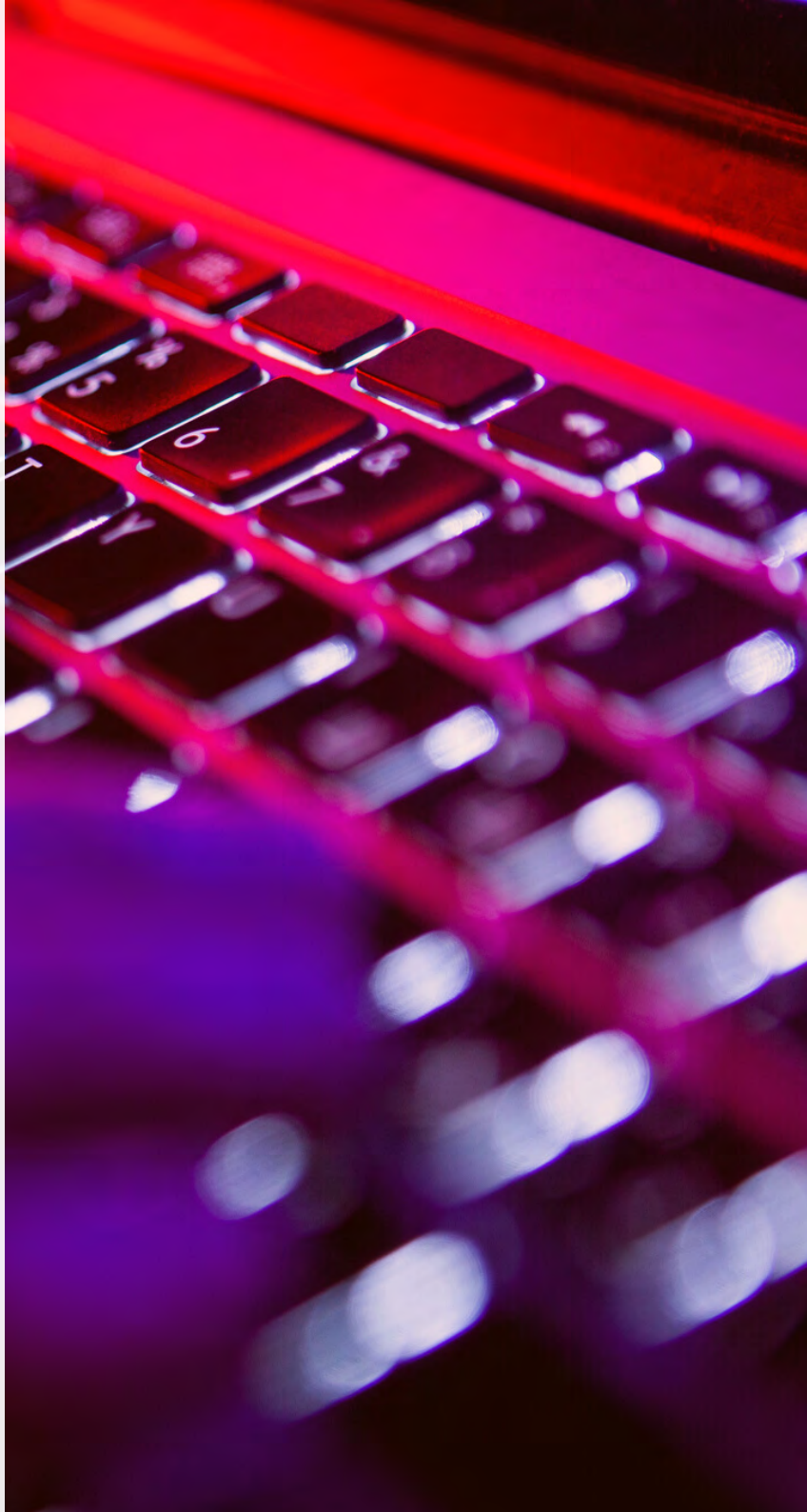
Zanim pracownicy zaczną korzystać ze wspomnianych narzędzi, powinniśmy być pewni, że jesteśmy bezpieczni. Być może dobrym rozwiązaniem jest domyślne blokowanie tego ty-

pu stron i poświęcenie sprawniejszego działania zespołów, na rzecz pewności co do jednego z filarów triady bezpieczeństwa informacji. Zapewnienie poufności danych w organizacji to element, na którym powinniśmy opierać działanie jednostki i nie pozwolić, by żadne usprawnienie czy automatyzacja naruszały jej niepodważalność.

Cyberprzestępstwa

Niestety, rozwiązania, takie jak ChatGPT wykorzystywane są również przez cyberprzestępców. Zaczynając od prostych e-maili phishingowych, po pomoc w tworzeniu kodu złośliwego oprogramowania do zaawansowanych ransomware. Coraz częściej spotykamy również się z tak zwanymi deepfake'ami, czyli fotomontażami wideo wygenerowanymi dzięki sieciom neuronowym. Zdarza się, że takie nagrania wyglądają na tyle realnie, że ucierpieć może nie tylko wizerunek danej osoby, ale także jej zdrowie psychiczne.

Wzrost dostępności takich technologii zwiększa ilość popularnych w branży cyberbezpieczeństwa "script kiddies", którzy mogą wyrządzić szkodę bez świadomości, jakie działania wykonują.



PRZEMYSŁAW KANIA
Cisco w Polsce

W minionym roku nastąpiła popularyzacja narzędzi opartych o AI, które okazały się zagrożeniem dla cyberbezpieczeństwa firm na całym świecie – próg wejścia w cyberprzestępczość stał się jeszcze niższy i tańszy. Z drugiej strony rozwiązania AI napędzają teraz nowe, skuteczniejsze narzędzia obserwowalności sieci i wykrywania anomalii systemowych. Tak więc sztuczna inteligencja jeszcze bardziej zwiększy rywalizację między atakującymi a obrońcami, napędzając „cyfrowy wyścig zbrojeń".

Wyzwania

W związku z coraz większą liczbą ataków, w tym coraz bardziej wiarygodnie wyglądających przynęt phishingowych (m.in. dzięki wspomnianym wyżej narzędziom AI), ważne jest kompleksowe przygotowanie całej firmy na incydenty cyberbezpieczeństwa. Zespoły CyberSec muszą mieć dostęp do odpowiednich narzędzi obserwowalności sieci, wszystkie zasoby powinny być zabezpieczone uwierzytelnianiem dwuskładnikowym, natomiast pracownicy powinni być edukowani z najpopularniejszych form ataków.

Priorytety

W ostatnich latach kluczowego znaczenia nabiera monitorowanie całego ruchu sieciowego w firmie oraz kontrola, czy dostęp do danych i zasobów mają tylko osoby uprawnione.
W związku z tym należy spodziewać się popularyzacji rozwiązań takich, jak Cisco AI Assistant for Security i narzędzi o zbliżonej funkcjonalności, które wesprą zespoły cyberbezpieczeństwa w codziennych zadaniach.

Cyberprzestępstwa

Trzeba zachować szczególną ostrożność – nastąpi popularyzacja nowych metod ataków phishingowych, w tym klonowanie głosu. Z danych Cisco Talos wynika, że należy spodziewać się również ataków z wykorzystaniem popularnych aplikacji internetowych, które stanowiły aż 30 proc. wszystkich incydentów cyberbezpieczeństwa w Q3 2023.

ADRIAN SROKA
Software Security Architect

Trendy na kolejne lata w obszarze bezpieczeństwa aplikacji zazwyczaj jasno wynikają z kilku aspektów. Największe znaczenie ma krajobraz zagrożeń. Z drugiej strony są wszelkiego rodzaju regulacje i standardy bezpieczeństwa, które obligują twórców do konkretnych praktyk. Nawet jeżeli regulacje te początkowo są wymagane tylko względem określonych branż, praktyka pokazuje, że dość szybko stają się obowiązującym standardem.

Wyzwania

Dużym wyzwaniem jest skuteczne wsparcie użytkowników w dbaniu o swoje bezpieczeństwo. Tak by było to dostępne dla każdego.
Na szczęście widać coraz większą adopcję rozwiązania MFA (uwierzytelniania wieloskładnikowego) oraz Passkeys, które wspierają zabezpieczanie dostępów online.
Kolejnym ważnym wyzwaniem, wynikającym z najnowszych regulacji zarówno Unii Europejskiej jak i Stanów Zjednoczonych, jest zapewnienie widoczności tego z czego składa się dany system IT. Tylko dzięki temu jesteśmy w stanie kontrolować bezpieczeństwo złożonych systemów.

Priorytety

Biorąc pod uwagę dużą ilość zagrożeń do zaadresowania na etapie tworzenia oprogramowania, niezwykle istotne są koszty dbania o bezpieczeństwo systemów. Dlatego też tak ważne będzie skupienie się na strategii Shift Left, czyli przeniesieniu myślenia o bezpieczeństwie na początek procesu wytwarzania oraz DevSecOps, czyli automatyzacji kontroli bezpieczeństwa.

Cyberprzestępstwa

W zakresie zagrożeń dla wszelkiego rodzaju aplikacji niezmiennie króluje phishing. Zagrożenie, które niezwykle skutecznie wykorzystuje najtrudniejszy do zabezpieczenia element - użytkownika. Z użyciem szeroko dostępnej AI, łatwo jest przygotować tego typu atak. Stworzyć sztuczną tożsamość, podszyć się pod kogoś lub zbadać słabe punkty danego systemu.

SECURITYMAGAZINE.PL

7. KONFERENCJA „INTELIGENTNA ENERGETYKA” GDZIE JESTEŚMY Z CYBERBEZPIECZEŃSTWEM POLSKIEJ ENERGETYKI?

PATRONAT
SECURITY MAGAZINE

Fot. Inteligentna Energetyka (22)

6 grudnia 2023 r. w Warszawie, odbyła się 7. Konferencja „Inteligentna Energetyka”, nad którą patronat medialny objął Security Magazine. Tematem przewodnim wydarzenia było „Cyber-(NIE)bezpieczeństwo polskiej energetyki – fakty czy mity?”. Spotkanie zgromadziło prawie 100 uczestników zajmujących się cyberbezpieczeństwem w energetyce.

SYTUACJA NA RYNKU CYBERBEZPIECZEŃSTWA W POLSCE

Już tradycyjnie Konferencję „Inteligentna Energetyka” osobiście otworzyła pomysłodawczyni i organizatorka – Izabela Żylińska. Po uroczystym powitaniu obecnych i podziękowaniu partnerom za współpracę rozpoczęła się pierwsza sesja „Teza I: Polska energetyka może czuć się cyberbezpiecznie?”. W ramach tej części Kamil Pszczółkowski, Senior Manager Cyber Security w EY Polska, i dr Magdalena Krawczyk, Adwokat z Kancelarii Adwokackiej dr Magdalena Krawczyk, wygłosili niezwykle ważne dla dalszej dyskusji prezentacje merytoryczne. Przedstawiciel firmy consultingowej opowiedział o trendach i wyzwaniach dotyczących cyberzagrożeń, natomiast Prelegentka przedstawiła ramy prawne dotyczące cyberbezpieczeństwa w sektorze energii.

Sesję zamknął panel dyskusyjny „Obalenie lub potwierdzenie Tezy 1: Polska energetyka może czuć się cyberbezpiecznie”. Do rozmowy przez moderatorkę Izabelę Żylińską zostali zaproszeni: dr inż. Ireneusz Wochlik, Prezes, Aigorithmics sp. z o.o., Maciej Pyznar, Fundacja Bezpieczna Cyberprzestrzeń,

Patronat Security Magazine.

7. Konferencja „Inteligentna Energetyka”

Michał Balwiński, Senior Underwriter, Cyber Practice Leader, Generali T.U. S.A., Kamil Nawrocki, Technical Sales Manager, SMA Solar Technology AG, Mateusz Kopacz, Information Security Officer. W trakcie debaty Uczestnicy wskazali m.in. czy wprowadzane regulacje prawne wspierają polską energetykę we wdrażaniu i prowadzeniu działań związanych z cyberbezpieczeństwem, czy może stwarzają niepotrzebne utrudnienia; czy dostępne technologie z zakresu cyberbezpieczeństwa są wystarczające, aby zabezpieczyć sektor energetyczny; dlaczego ważna jest cyber-higiena; jakie dostępne są formy transferu cyberryzyka, a także czy branża ma odpowiednie fundusze na budowę profesjonalnego cyberbezpieczeństwa?

PRZEDSIĘBIORSTWA POKAZUJĄ JAK JEST!

Kolejne trzy sesje konferencji należały do firm technologicznych. Część „Teza II: Systemy łączności w energetyce do podsłuchania” otworzyło wystąpienie Pawła Zajączkowskiego, Eksperta ds. Bezpieczeństwa Sieci LTE, PGE Systemy SA pt. „Czy systemy łączności w energetyce są do podsłuchania? Wnioski na podstawie budowy sieci łączności specjalnej LTE450 dedykowanej dla polskiej energetyki”. Po nim nastąpiła prezentacja przedstawicieli Nokia Solutions and Networks Sp. z o.o. – Adama P. Grodeckiego, CX CTO, i Pawła Niedzielskiego, Dyrektora ds. Sprzedaży – „Rola sieci prywatnych w bezpieczeństwie infrastruktury krytycznej”. O łączności opowiedział jeszcze Piotr Stępniewicz, Dyrektor Sprzedaży – Telekomunikacja & Cyberbezpieczeństwo w MCX PRO Sp. z o.o. w ramach prelekcji „Security by design w systemach teleinformatycznych w energetyce”.

Część „Teza III: OSD I OSP na granicy cyberodporności” rozpoczęła prelekcja Piotra Szczerka, Kierownika B+R, dział IoT, ANDRA Sp. z o.o. Prelegent opowiedział o „Bezpieczeństwie w systemach bezprzewodowej transmisji

Patronat Security Magazine.

7. Konferencja „Inteligentna Energetyka”

danych Operatorów Systemu Dystrybucyjnego”. W dalszej kolejności wystąpił Piotr Wądołowski, CTO, ESMETRIC GROUP Sp. z o.o., który poruszył zagadnienie „Cyberbezpieczeństwo inteligentnych liczników energii w niepewnych czasach”. Całość zamknął Sławomir Dębski, Senior CyberSecurity Consultant w BlackBerry prezentacją „Sztuczna inteligencja skuteczną odpowiedzią na potrzeby środowiska OT w zakresie cyberbezpieczeństwa”.

W ramach części technologicznej Konferencji „Inteligentna Energetyka” omówiono również „Tezę IV: Wytwórcy energii na celowniku”, w ramach której Kamil Nawrocki, Technical Sales Manager, SMA Solar Technology AG odpowiedział na pytanie „Jak cyberbezpieczeństwo OZE może wypłynąć na stabilność sieci energetycznej w Polsce?”. Jacek Grzechowiak, Właściciel RiskResponse skupił się natomiast na „Bezpieczeństwie fizycznym w cyberbezpieczeństwie – na bazie przykładów praktycznych”.

REKOMENDACJE RYNKOWE

7. Konferencję „Inteligentna Energetyka” zamknął panel dyskusyjny „Rekomendacje

Patronat Security Magazine.

7. Konferencja „Inteligentna Energetyka”

sektorowe z zakresu cyberbezpieczeństwa na podstawie wniosków wynikających z obalenia lub potwierdzenia tez I, II, III i IV”, który poprowadziła ponownie Izabela Żylińska. W rozmowie udział wzięli: Wiesław Paluszyński, Prezes Zarządu, Polskie Towarzystwo Informatyczne, Piotr Golik, Prezes Zarządu ESMETRIC GROUP Sp. z o.o., Mateusz Kopacz, Information Security Officer, Łukasz Górski, Dyrektor, dział IoT, ANDRA Sp. z o.o.

Podczas debaty powiedziano m.in. który z elementów energetyki jest jej najsłabszym ogniwem; czy dyrektywa CER wymusi na branży energetycznej stworzenie czarnych list produktów, oprogramowania i usług; czy w ogóle widać w energetyce chęć do pozyskiwania najnowszej wiedzy o cyberbezpieczeństwie?

Dodatkowo każdy z Prelegentów na bazie swoich doświadczeń i tego, co wynikło z wydarzenia, wskazał po trzy rekomendacje dla branży energetycznej, których wdrożenie wspomoże sektor w zachowaniu najwyższego cyberbezpieczeństwa.

EFEKTYWNY NETWORKING BRANŻOWY

W ramach 7. Konferencji „Inteligentna Energetyka” odbyły się przerwy networkingowe. W tym czasie uczestnicy mieli możliwość porozmawiania ze sobą i nawiązania relacji biznesowych. Wiele osób skorzystało również z okazji odwiedzenia stoisk wystawców, jakimi były firmy Generali T.U., ESMETRIC Group, MCX, Andra, BlackBerry, i bezpośredniego porozmawiania z prelegentami.

Polityka®
Bezpieczeństwa

ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE...

POMOŻEMY

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

SECURITYMAGAZINE.PL

PROCEDURA ZAMÓWIENIA ESET DLA JEDNOSTEK PUBLICZNYCH

Łukasz Zajdel
Perceptus

COAR, czyli Centrum Obsługi Administracji Rządowej uruchomiło elektroniczną platformę, umożliwiającą jednostkom administracji publicznej zamówienia oprogramowania w oparciu o umowy ramowe. Drugim historycznie porozumieniem w ramach tego projektu jest ramowa umowa, dzięki której każda jednostka administracji publicznej może zamówić oprogramowanie ESET Endpoint Protection w ramach uproszczonej procedury.

- 5 grudnia została zawarta umowa ramowa na dostawę oprogramowania antywirusowego ESET, z której już teraz korzystać mogą wszystkie jednostki administracji rządowej i samorządowej. To druga umowa ramowa, po umowie na dostawę pakietu biurowego Office 365, zawarta w ramach programu zamówień centralnych publicznej chmury obliczeniowej realizowanego na zlecenie ***Ministerstwo Cyfryzacji*** *w ramach projektu POPC Wspólna Infrastruktura Informatyczna Państwa przez* ***Centrum Obsługi Administracji Rządowej****. Program umożliwia szybki i sprawny zakup usług chmurowych bez konieczności prowadzenia skomplikowanego postępowania zakupowego wymagającego zaangażowania osób specjalizujących się w zakupach IT oraz pozwala na uzyskanie konkurencyjnych warunków zakupu* – skomentował **Maciej Górski, zastępca dyrektora Centralnego Ośrodka Informatyki na portalu LinkedIn.**

ENDPOINT PROTECTION TO JUŻ OD DAWNA NIE TYLKO ANTYWIRUS

Umowa jest ważna, ponieważ nikogo już dziś nie trzeba przekonywać, że ochrona sprzętu, na którym pracujemy jest konieczna. Skala ataków cybernetycznych sprawiła, że świadomość zagrożeń rośnie nie tylko wśród osób pracujących w IT, ale również w każdym innym obszarze naszego publicznego działania.

Endpoint Protection to oprogramowanie chroniące urządzenia końcowe, takie jak komputery użytkowników. Umowa wspomniana powyżej pozwala na wybór wariantu oprogramowania z pośród 5 wersji oprogramowania antywirusowego ESET PROTECT: Advanced, Complete, Elite, Enterprise oraz Entry.

W najwyższych pakietach to nie tylko ochrona antywirusowa, ale również ochrona serwerów pocztowych, pełne szyfrowanie dysków czy EDR – narzędzia służące do identyfikacji nietypowych zachowań i naruszeń bezpieczeństwa wewnętrznej sieci. Korzystając z tego rozwiązania jednostka publiczna może zamówić licencje, które znacznie podniosą poziom zabezpieczenia nie tylko pojedynczych komputerów, ale także całej sieci.

JAK WYGLĄDA ZAMÓWIENIE W UPROSZCZONEJ PROCEDURZE?

Umowa zawarta została w ramach programu zamówień centralnych Publicznej chmury obliczenio-

wej realizowanego na zlecenie Ministerstwa Cyfryzacji w ramach projektu POPC Wspólna Infrastruktura Informatyczna Państwa.

Jednostka publiczna na platformie zakupowej COAR wskazuje liczbę potrzebnych licencji i wersję oprogramowania, którym jest zainteresowana. Określa ona także swój budżet na realizację zamówienie. W odpowiedzi dostawca oprogramowania składa wiążącą ofertę cenową. Jeżeli mieści się ona w zaplanowanym budżecie jednostki, to zamówienie zostanie udzielone i następuje jego realizacja. Nie ma dodatkowych warunków, jakie musiałaby spełnić którakolwiek ze stron.

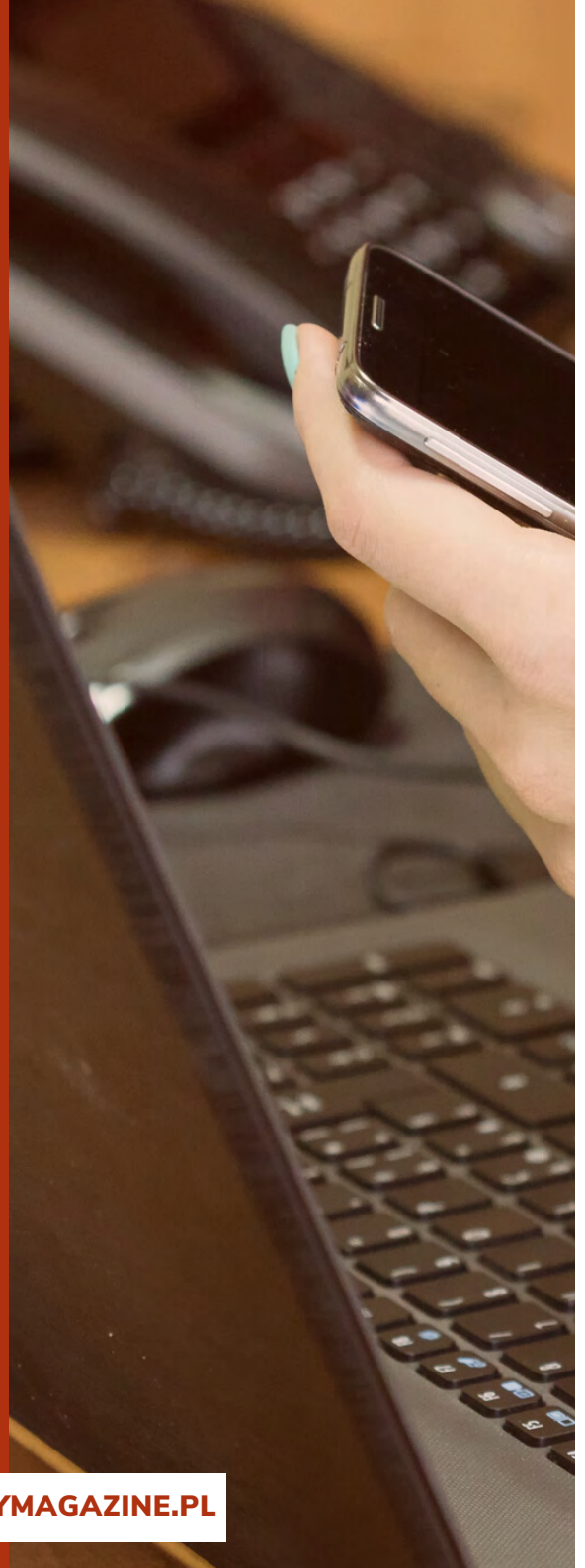
KORZYŚCI Z NOWEJ FORMUŁY DLA JEDNOSTKI ADMINISTRACJI PUBLICZNEJ

Korzyści z takiego trybu zamówienia to przede wszystkim szybki proces, pewna realizacja i zweryfikowany dostawca. Dzięki uproszczonej procedurze na platformie COAR jednostki administracji oszczędzają czas i zmniejszają obciążenie pracowników realizacją tego typu procesów. Finalizacja zamówienia następuje szybko i bez ryzyka niepowodzenia postępowania.

Można zamówić licencje o wartości przekraczającej próg przetargowy, ponieważ zakup jest realizowany przez COAR. Jednostka wszczyna postępowanie, lecz jest ono prowadzone na dedykowanej platformie do zakupów centralnych. Zamawiający ma pewność, że otrzyma system dopasowany do już posiadanych infrastruktury i oprogramowania.

KTO MOŻE ZAMAWIAĆ ESET PRZEZ COAR?

Z uproszczonej procedury mogą skorzystać jednostki sektora finansów



publicznych w tym sądy i trybunały. Szczegóły znajdą Państwo na stronie:

WSPARCIE KROK PO KROKU

Chcesz zamówić oprogramowanie ESET, ale nie potrafisz poruszać się po platformie zamówień COAR? Skontaktuj się z firmą Perceptus, która dostarcza oprogramowanie ESET w ramach umowy i uzyskaj wsparcie w przeprowadzeniu procedury zamówienia krok po kroku.

Rzetelny Regulamin®

POZNAJ SZCZEGÓŁY

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

Kompleksowa obsługa prawna Twojego e-commerce

ROLA SYSTEMÓW KONTROLI DOSTĘPU

Andrzej Mendak
UNICARD SA

Systemy kontroli dostępu (KD) to często integralna część polityki bezpieczeństwa w firmach. Pomagają w jej egzekwowaniu i stanowią istotną składową systemu bezpieczeństwa. Celem SKD jest precyzyjne zarządzanie uprawnieniami użytkowników, aby dostęp do zasobów oraz informacji był ograniczony do odpowiednich osób. Dają możliwość śledzenia i rejestrowania zdarzeń, co jest ważne dla wykrywania nieprawidłowości i przeprowadzania dochodzeń po incydentach.

Aby system realnie wspierał procedury bezpieczeństwa, musi zostać dopasowany do potrzeb firmy. W artykule wyjaśnię, jak wykorzystać kontrolę dostępu, tworząc politykę ochrony dla organizacji.

AUDYT POTRZEB ORGANIZACJI

Nie ma jednego idealnego systemu kontroli dostępu dla wszystkich firm. Każda organizacja ma indywidualne potrzeby, mierzy się z innymi wyzwaniami.
Aby dobrać odpowiednie zabezpieczenia, warto przeprowadzić audyt, który zawiera m.in.:

- analizę obecnych praktyk w kontekście kontroli dostępu;
- identyfikację kluczowych zasobów;
- oceny ryzyka w sytuacji nieautoryzowanego dostępu;
- analizę potrzeb użytkowników;
- identyfikację norm i przepisów, które musi spełniać system KD.

ANALIZA OBECNYCH PRAKTYK I POLITYKI BEZPIECZEŃSTWA

Pierwszym krokiem jest dokładne przeanalizowanie istniejących procedur bezpieczeństwa. W tym celu należy szczegółowo przejrzeć wszystkie procesy, narzędzia i stosowane w firmie praktyki.

W trakcie audytu szczególną uwagę trzeba zwrócić na słabości, luki lub potencjalne zagrożenia w obecnych praktykach. Obejmuje to zarówno zagrożenia zewnętrzne, jak i wewnętrzne, a także możliwości nadużyć lub niezamierzonego naruszenia procedur.

IDENTYFIKACJA KLUCZOWYCH ZASOBÓW I OBSZARÓW DO OCHRONY

Kolejnym krokiem jest stworzenie kompleksowego spisu zasobów organizacji, któ-

re wymagają ochrony. Obejmuje to np. pomieszczenia, w których przechowywane są ważne dokumenty, sprzęt komputerowy, oprogramowanie, także magazyny czy serwerownie.

Po zidentyfikowaniu zasobów, ważne jest ich sklasyfikowanie według poziomu wrażliwości i znaczenia dla działalności organizacji. Niektóre dane, takie jak informacje osobowe klientów czy tajne dokumenty korporacyjne, mogą wymagać wyższego poziomu ochrony. System kontroli dostępu wspomaga ten proces poprzez fizyczne zabezpieczenie pomieszczeń, gdzie znajdują się wrażliwe dane.

Na podstawie oceny ryzyka i znaczenia poszczególnych zasobów należy ustalić priorytety w zakresie ich ochrony. Zasoby o największym znaczeniu i najwyższym ryzyku powinny być chronione w pierwszej kolejności lub wymagać szczególnej kontroli dostępu, np. weryfikacji dwuskładnikowej.

OCENA RYZYKA W RAZIE NIEAUTORYZOWANEGO DOSTĘPU

Aby dobrać odpowiedni system, ważne jest zrozumienie, jakie mogą być konsekwencje nieautoryzowanego dostępu lub innych naruszeń bezpieczeństwa. Należy rozważyć potencjalne straty finansowe, uszczerbek na reputacji, przerwy w działalności firmy, a także konsekwencje prawne.

ANALIZA POTRZEB RÓŻNYCH GRUP UŻYTKOWNIKÓW

Ważna jest też identyfikacja różnych grup użytkowników - pracowników, jak i gości, którzy odwiedzają firmę (kontrahenci, dostawcy czy kandydaci do rekrutacji) oraz zrozumienie ich ról w organizacji.

Konieczne jest zebranie informacji o uprawnieniach ich dostępu i wymaganiach dotyczących bezpieczeństwa. Należy przemyśleć, kiedy i w jaki sposób poszczególne grupy użytkowników będą korzystać z systemów kontroli dostępu.

ZGODNOŚĆ SYSTEMU Z PRZEPISAMI OBOWIĄZUJĄCEGO PRAWA CZY O OCHRONIE DANYCH OSOBOWYCH

Szczególnie dotyczy to instytucji o wysokim stopniu odpowiedzialności za dane osobowe, takich jak szpitale, kancelarie, urzędy czy banki.

Przykładem jest RODO (znane także jako GDPR), które jest rozporządzeniem o ochronie danych w Unii Europejskiej. Każdy system KD wdrażany w firmach działających na terenie UE musi spełniać rygorystyczne wymogi RODO. Obejmuje to odpowiednie mechanizmy bezpieczeństwa, takie jak szyfrowanie oraz umożliwienie użytkownikom dostępu do ich danych i kontrolę nad nimi.

Z kolei lokalne przepisy mogą narzucać instytucjom wymogi dotyczące przejść ewakuacyjnych, odbywania regularnych audytów bezpieczeństwa czy sposobów reagowania na incydenty.

DOBÓR SYSTEMU DLA POTRZEB FIRMY

Dobrze przeprowadzony audyt jest podstawą wyboru systemu KD, który będzie spełniał specyficzne wymogi firmy i odpowiadał na indywidualne wyzwania w kwestii bezpieczeństwa.

SYSTEM LOKALNY CZY OPARTY NA CHMURZE

W sektorze bezpieczeństwa fizycznego obserwujemy istotną ewolucję. Tradycyjne rozwiązania kontroli dostępu oparte o serwery lokalne ustępują miejsca systemom bazującym na technologii chmury (ACaaS, czyli Access Control as a Service), takim jak impero 360 od UNICARD Systems.

Główne korzyści tego systemu chmurowego to:

- wgląd do systemu możliwy jest za pomocą dowolnego urządzenia z dostępem do Internetu i przeglądarki, co umożliwia logowanie się z każdego zakątka świata;
- implementacja rozwiązania chmurowego eliminuje potrzebę inwestycji w serwer, specjalistyczny sprzęt IT czy zatrudniania ekspertów IT, co obniża koszty początkowe;
- zarządzanie bezpieczeństwem i regularne aktualizacje są w pełni obsługiwane przez Data

Center, eliminując potrzebę ciągłej, samodzielnej interwencji wymaganej w przypadku serwerów lokalnych;
- systemy ACaaS wyróżniają się zdolnością do adaptacji oraz łatwej rozbudowy, co pozwala na dopasowanie ich do ewoluujących potrzeb organizacji;
- model płatności abonamentowej pozwala rozłożyć wydatki w czasie (często są to płatności miesięczne lub roczne), dzięki czemu nawet firmy z ograniczonym budżetem mogą korzystać z tej technologii;
- dzięki integracji z Azure Active Directory, z jednego konta możliwe jest zarządzanie tożsamościami użytkowników w systemach KD i IT. To nie tylko ułatwia pracę, ale przede wszystkim pomaga w utrzymaniu bezpieczeństwa.

DOBÓR ZABEZPIECZEŃ

W doborze zabezpieczeń ważne jest zwrócenie uwagi na zaawansowane technologie, takie jak:

- dostęp mobilny, czyli wykorzystanie smartfonów zamiast kart dostępu;
- uwierzytelnianie wielopoziomowe, np. indywidualny identyfikator + PIN dla miejsc szczególnie chronionych;
- biometria, np. autoryzacja za pomocą odcisku palców, skanu twarzy czy tęczówki.

Oprócz tego firmy mogą zastosować dodatkowe środki ochrony: monitoring wizyjny, system SSWiN, kołowroty, czy bramki.

INTEGRACJA Z INNYMI SYSTEMAMI

Aby zoptymalizować zarządzanie i podnieść poziom bezpie-

czeństwa, systemy kontroli dostępu powinny mieć możliwość efektywnej integracji z obecnymi lub planowanymi rozwiązaniami, jak system monitoringu wizyjnego CCTV, system alarmowe SSWiN czy system PPOŻ.

Elastyczny system dostępowy powinien bez trudu współpracować także z:

- systemami parkingowymi, rezerwacją sal konferencyjnych czy awizacją gości (VMS);
- systemami zarządzania budynkiem BMS, w tym kontrolą wind, ogrzewania, oświetlenia, klimatyzacji oraz czujnikami dymu;
- systemami do rejestracji czasu pracy;
- urządzeniami higieny produkcji;
- systemami ERP, takimi jak: SAP, Enova, Sage Symfonia, TETA, Comarch ERP Optima.

USTALENIE ZASAD ZARZĄDZANIA SYSTEMEM KONTROLI DOSTĘPU

Podstawą tego etapu jest opracowanie zasad dostępu do poszczególnych zasobów w firmie i przydzielenie odpowiednich uprawnień. Uprawnienia mogą być nadawane indywidualnie oraz dla grup pracowników, np. różne dla osób zatrudnionych na produkcji, magazynie czy w kadrach.

Uprawnienia można też rozróżniać ze względu na:

- dni tygodnia;
- godziny;
- lokalizacje, gdy system jest rozproszony;
- wykonywane zadania;
- zmiany nocne/dzienne;
- poziomy certyfikacji i kwalifikacji.

Zarządzanie systemem kontroli dostępu wymaga także gotowości na nietypowe i krytyczne sytuacje. Aby SKD realnie wspierał politykę bezpieczeństwa organizacji, należy opracować scenariusze reakcji w przypadku wykrycia nieautoryzowanego dostępu, prób włamania, czy innych naruszeń i zdarzeń w systemie.

W sytuacji zagrożenia bezpieczeństwa niezwykle ważne jest posiadanie jasno określonych procedur, np. ewakuacji.

SZKOLENIA PERSONELU

Głównym zadaniem szkolenia jest upewnienie się, że każdy pracownik zna cel wdrożenia kontroli dostępu oraz rozumie, w jaki sposób system przyczynia się do ochrony pracowników i zasobów firmy.

Pracownicy muszą też wiedzieć, jak postępować w przypadku awarii systemu, zagubienia lub uszkodzenia karty dostępu, a także jak reagować na potencjalne naruszenia bezpieczeństwa. Kluczowa jest też świadomość konsekwencji związanych z niewłaściwym użyciem identyfikatorów lub dzieleniem się nimi z innymi osobami.

Szkolenia można dostosować też do różnych ról i poziomów dostępu w organizacji. Na przykład, personel ochrony może potrzebować bardziej zaawansowanego wdrożenia, podczas gdy pracownicy biurowi zwykle potrzebują podstawowych informacji na temat codziennego użytkowania SKD.

MONITORING I OCENA PRACY SYSTEMU

System kontroli dostępu powinien być regularnie monitorowany i oceniany pod kątem efektywności i skuteczności działania.

Ocena powinna obejmować testowanie niezawodności komponentów systemu, analizę zdarzeń, a także przegląd zgodności z przepisami prawa oraz aktualną polityką bezpieczeństwa. Regularne przeglądy poprawności działania systemu oraz jego konserwacja są zalecane przez producentów SKD, a monitoring zwykle można przeprowadzić we współpracy z dostawcą systemu.

Te działania pozwalają na utrzymanie systemu w prawidłowym stanie technicznym oraz dostosowanie go do ewoluujących potrzeb i wyzwań polityki bezpieczeństwa.

PODSUMOWANIE

Dobrze opracowana – a przede wszystkim skutecznie wdrożona – polityka bezpieczeństwa to nie tylko ochrona przed zagrożeniami cybernetycznymi, ale również efektywne zabezpieczenia fizyczne.

Systemy kontroli dostępu są kluczowym elementem strategii bezpieczeństwa, chroniąc sprzęt, dokumenty oraz dając poczucie bezpieczeństwa pracownikom. Ważne jest nie tylko dobrze dopasowane rozwiązanie, ale też wypracowanie procedur oraz szkolenie osób, które z systemu będą korzystać.

Cały proces – od audytu potrzeb, po monitoring i ocenę pracy SKD – pozwala zadbać, aby ochrona fizyczna w budynku była dostosowana do specyficznych wymagań i ryzyk, które niesie ze sobą działalność danej organizacji.

SECURITYMAGAZINE.PL

OCHRONA URZĄDZEŃ MOBILNYCH I SZYFROWANIE

Redakcja
SECURITY MAGAZINE

#SECURITY
#STARTUP

Świat cyberbezpieczeństwa jest niezwykle rozległy. W sieci czyha na nas coraz więcej zagrożeń i nie sposób im wszystkim sprostać bez pomocy. I to właśnie tę pomoc oferują startupy, które wspierają firmy w najróżniejszych kwestiach. Dowiedz się, jakie spółki technologiczne pomogą ci w poprawieniu swojego cyberbezpieczeństwa.

PROGET – OCHRONA URZĄDZEŃ MOBILNYCH

Urządzenia mobilne, a zwłaszcza smartfony, to nieodzowny element codziennej pracy. Jednak nie ma co ukrywać – zarządzanie całą flotą takich telefonów czy tabletów, może być bardzo problematyczne. I tu na scenie pojawia się startup Proget. Spółka oferuje autorskie rozwiązanie klasy EMM (Enterprise Mobility Management). To ma charakteryzować się nie tylko prostą i intuicyjną konsolą administracyjną, ale także szeregiem zaawansowanych funkcji, umożliwiających pełną kontrolę nad firmowymi urządzeniami mobilnymi.

Proget chwali się, że dzięki nim zyskujesz pełną kontrolę nad aplikacjami na urządzeniach mobilnych w bezpieczny sposób. System umożliwia dostarczanie skonfigurowanych aplikacji zarówno np. z Google Play, jak i z plików. Administrator ma możliwość decydowania o automatycznej instalacji aplikacji lub udostępnieniu ich w służbowym sklepie, gotowych do pobrania przez użytkownika. Elastyczność Proget pozwala również na precyzyjne zarządzanie aktualizacjami apek, co wyklucza potencjalne problemy z ich działaniem.

Co więcej – platforma Proget umożliwia pełne skatalogowanie urządzeń podłączonych do systemu. A to pozwoli ci na uzyskanie szczegółowych danych na ich temat. Zaawansowany moduł raportów umożliwi ci generowanie ich z różnych danych z systemu.

Z kolei funkcja konteneryzacji w Proget pozwala na stworzenie dedykowanej strefy służbowej na urządzeniach. To idealne rozwiązanie dla scenariuszy, w których użytkownicy chcą wykorzystywać swoje prywatne urządzenia do celów biznesowych (tzw. BYOD – Bring Your Own Device). Administracja i monitorowanie danych służbowych stają się prostsze, jednocześnie zachowując prywatność użytkowników.

Ponadto Porget umożliwia integrację z Android Enterprise, Samsung Knox i Apple Business Manager.

Zaletami platformy startupu są niewątpliwie pełna kontrola nad aplikacjami, zaawansowane polityki bezpieczeństwa, czy innowacyjna konte-neryzacja. Dzięki temu – przynajmniej w teorii – zarządzanie flotą urządzeń mobilnych staje się prostsze i bezpieczniejsze.

SPECFILE.PL – SZYFROWANIE PLIKÓW I DANYCH

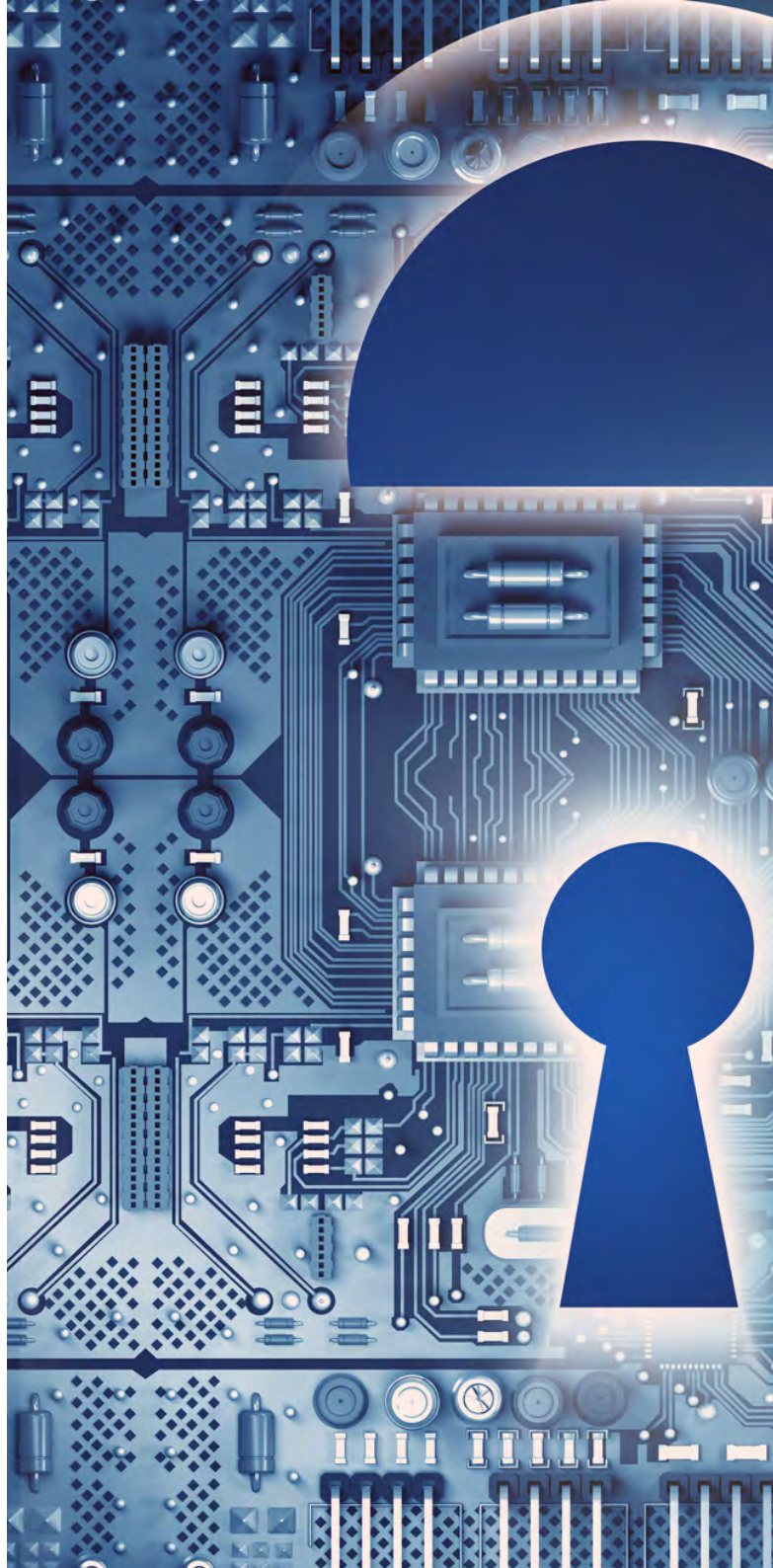
Wymiana informacji odgrywa kluczową rolę w biznesie. Dlatego tak ważne jest odpowiednie zabezpieczenie danych. I tu z pomocą przychodzi startup Specfile.pl. Oferuje on narzędzie, które pozwala na szyfrowanie danych, ale także umożliwia bezpieczną komunikację i przechowywanie informacji.

Specfile.pl to narzędzie, które nie ogranicza się jedynie do standardowego szyfrowania plików. Pozwala zabezpieczać różnorodne rodzaje danych, począwszy od umów i zdjęć, aż po filmy czy projekty. Twórcy narzędzia podkreślają jego potencjał w ochronie patentów, planów biznesowych czy tajemnic firmowych, spełniając jednocześnie wymogi RODO.

Oprogramowanie startupu wyróżniać ma się również prostotą obsługi. Po pobraniu i zainstalowaniu go na komputerze użytkownicy mogą szybko przystąpić do szyfrowania i deszyfrowania plików. A to dlatego, że nie wymaga konkretnej wiedzy technicznej.

Jednym z atutów Specfile.pl jest także możliwość szyfrowania i deszyfrowania plików online, bez konieczności instalacji dodatkowej aplikacji. Proces odbywa się lokalnie i bezpiecznie, co eliminuje ryzyko przechwycenia danych. Rejestracja w systemie umożliwia uzyskanie kluczy szyfrujących, co dodatkowo ułatwia korzystanie z narzędzia.

To jednak nie wszystko, bo Specfile.pl oferuje również funkcje bezpiecznego e-maila. Klienci mogą teraz wysyłać zaszyfrowane maile, zyskując



pewność co do prywatności przesyłanych informacji. Wśród swoich produktów startup posiada także coś, określanego jako Elektroniczny List Polecony. To rozwiązanie dla firm, umożliwiające wysyłkę dokumentów online z potwierdzeniem odbioru – jak tradycyjny list polecony wysyłany przez pocztę. Startup ponadto współpracuje z platformą Sygnanet.pl. Dzięki temu umożliwia anonimowe zgłaszanie nieprawidłowości online. To proste w obsłudze narzędzie, które zachęca do uczciwego raportowania potencjalnych problemów, zapewniając pełną anonimowość dla sygnalistów.

Specfile.pl – jak widać – to kompleksowe narzędzie, które łączy w sobie najwyższe standardy bezpieczeństwa z prostotą obsługi. Startup stawia nie tylko na ochronę danych, ale także na innowacyjne rozwiązania ułatwiające codzienną pracę przedsiębiorstw.

CYBER.DOG – SZYFROWANIE PLIKÓW I WIADOMOŚCI

Cypherdog Encryption – bo tak nazywa się narzędzie oferowane przez startup Cyber.Dog – ma uprościć proces szyfrowania i deszyfrowania wiadomości oraz plików. Jednym kliknięciem chcą zapewnić użytkownikom pełną ochronę danych przesyłanych przez różne kanały komunikacji, od maili po platformy przesyłające pliki.

Rozwiązanie to jest kompatybilne z wieloma systemami operacyjnymi, w tym Windows, macOS i Linux. Dodatkowo Cyber.Dog oferuje możliwość instalacji wtyczek do najpopularniejszych przeglądarek oraz dodatków do klientów pocztowych, takich jak Outlook czy Thunderbird, co ułatwia integrację z istniejącymi narzędziami.

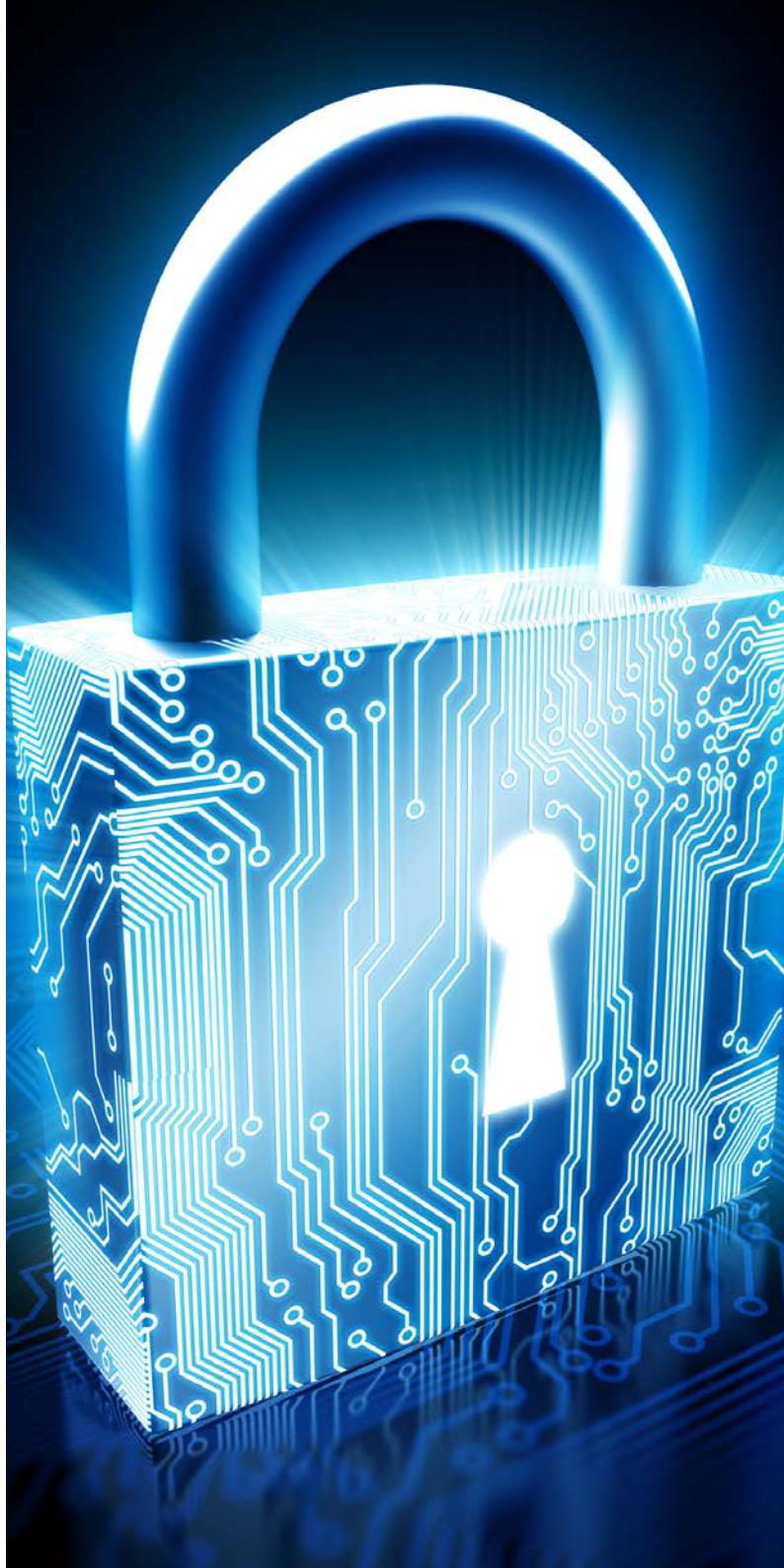
Cypherdog Encryption opiera się na algorytmach kryptograficznych, takich jak 3072-bitowy klucz RSA i funkcja skrótu SHA512. Architektura systemu ma za zadanie umożliwić dostosowywanie się do przyszłych wyzwań, takich jak weryfikacja tożsamości za pomocą technologii blockchain czy rozwój portfeli sprzętowych.

Startup zapewnia, że klucze kryptograficzne pozostają na użytkownika, co wprowadza dodatkową warstwę ochrony. Klucze mogą być przesyłane między urządzeniami, co jest wygodne dla użytkowników korzystających z wielu platform, jednak warto zauważyć, że ich utrata bez kopii zapasowej może stanowić problem.

Cyber.dog kieruje swoje rozwiązanie zarówno do indywidualnych użytkowników, jak i organizacji, oferując możliwość masowego szyfrowania i deszyfrowania plików. Oferując darmową wersję podstawową, starają się uczynić bezpieczeństwo online bardziej dostępnym.

Cypherdog Encryption jawi się jako wielofunkcyjne narzędzie do cyberbezpieczeństwa. Jednak, jak każde, ma swoje ograniczenia i wymaga rozwagi w zakresie utraty kluczy czy kosztów w przypadku potrzeby rozszerzenia funkcji.

To, oczywiście, niejedyne startupy, które mogą usprawnić procesy cyberbezpieczeństwa w twojej firmie. Ostateczny wybór partnera zależy tak naprawdę od ciebie. Jednak pamiętaj, że cyberbezpieczeństwo to ważny aspekt i nie możesz na nim oszczędzać.



Polityka® Bezpieczeństwa

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

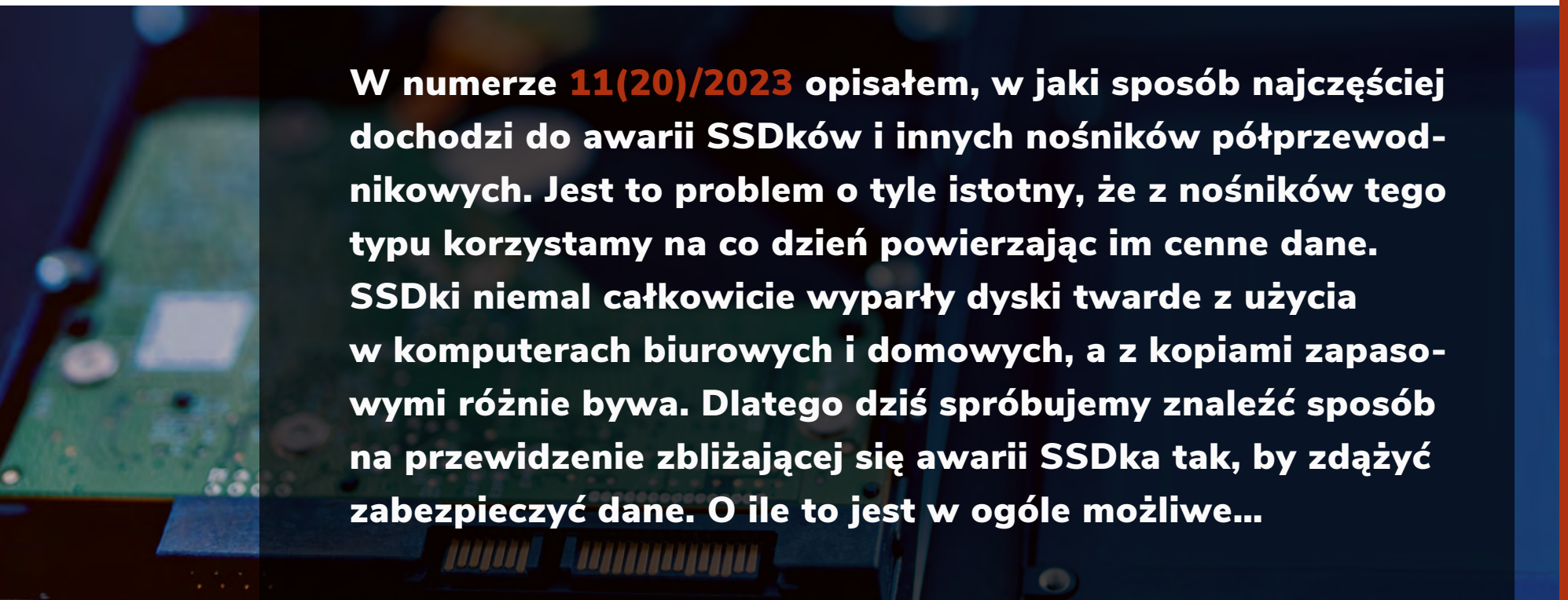
POZNAJ SZCZEGÓŁY

POROZMAWIAJMY

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

JAK PRZEWIDZIEĆ AWARIĘ SSD?

Paweł Kaczmarzyk
Serwis komputerowy Kaleron



W numerze 11(20)/2023 opisałem, w jaki sposób najczęściej dochodzi do awarii SSDków i innych nośników półprzewodnikowych. Jest to problem o tyle istotny, że z nośników tego typu korzystamy na co dzień powierzając im cenne dane. SSDki niemal całkowicie wyparły dyski twarde z użycia w komputerach biurowych i domowych, a z kopiami zapasowymi różnie bywa. Dlatego dziś spróbujemy znaleźć sposób na przewidzenie zbliżającej się awarii SSDka tak, by zdążyć zabezpieczyć dane. O ile to jest w ogóle możliwe...

SMART

Pierwsza rzecz, jaka może nam przyjść na myśl, to SMART, czyli Self-Monitoring, Analysis and Reporting Technology. Technologia ta została wprowadzona przez standard ATA-3 w 1996 r. w celu poprawy bezpieczeństwa danych i ograniczenia ryzyka awarii dysków twardych. Opiera się ona o obserwację i rejestrację różnego rodzaju parametrów i zdarzeń, co w założeniu ma pozwolić na odpowiednio wcześniejsze zauważenie pogarszającego się stanu dysku i jego prewencyjne wycofanie z eksploatacji zanim dojdzie do awarii.

W pewnym stopniu kłopotliwe są pewne niuanse implementacji obsługi SMARTu przez różnych producentów w różnych generacjach modeli dysków, co utrudnia ich interpretację. Jest to związane z pozostawioną producentom dość dużą swobodą w wyborze obsługiwanych parametrów oraz sposobie ich rejestrowania. Z uwagi na zgodność dysków SSD SATA ze standardem ATA, również i w nich zaimplementowano SMART, jednak jego interpretacja jest o wiele trudniejsza, niż w przypadku dysków twardych.

Po pierwsze o wiele bardziej we znaki daje się duża dowolność przy implementacji SMART-u. Jest to problem tym większy, że o ile do pewnej specyfiki kilku producentów dysków twardych można się łatwo przyzwyczaić, to dla licznych marek SSD ukrywających pod swoimi naklejkami produkty różnych rzeczywistych producentów jest to bardzo trudne. Tym bardziej, że każda marka zwykle korzysta z usług kilku podwykonawców, a i podwykonawcy zwykle dostarczają te same nośniki, różniące się wyłącznie wyświetlaną nazwą modelu dla wielu różnych marek i często bez otwarcia obudowy lub użycia odpowiednich programów nie da się stwierdzić, co tak naprawdę kryje się w środku.

Drugim problemem jest niedostosowanie SMART-u do specyfiki fizyki zapisu i przechowywania danych w układach NAND-owych. SMART był rozwijany przede wszystkim z myślą o zastosowaniu w wykorzystujących zapis magnetyczny dyskach twardych. Dlatego wiele parametrów SMART-u dla SSD jest po prostu fikcją zachowaną jedynie ze względu na wymogi zgodności ze standardem ATA.

Oczywiście, z czasem pojawiły się też parametry specyficzne dla SSD. Do najważniejszych z nich należą parametry rejestrujące operacje kasowania oraz programowania. Jeśli pamiętamy o tym, że za zużycie układów NAND-owych odpowiadają właś-

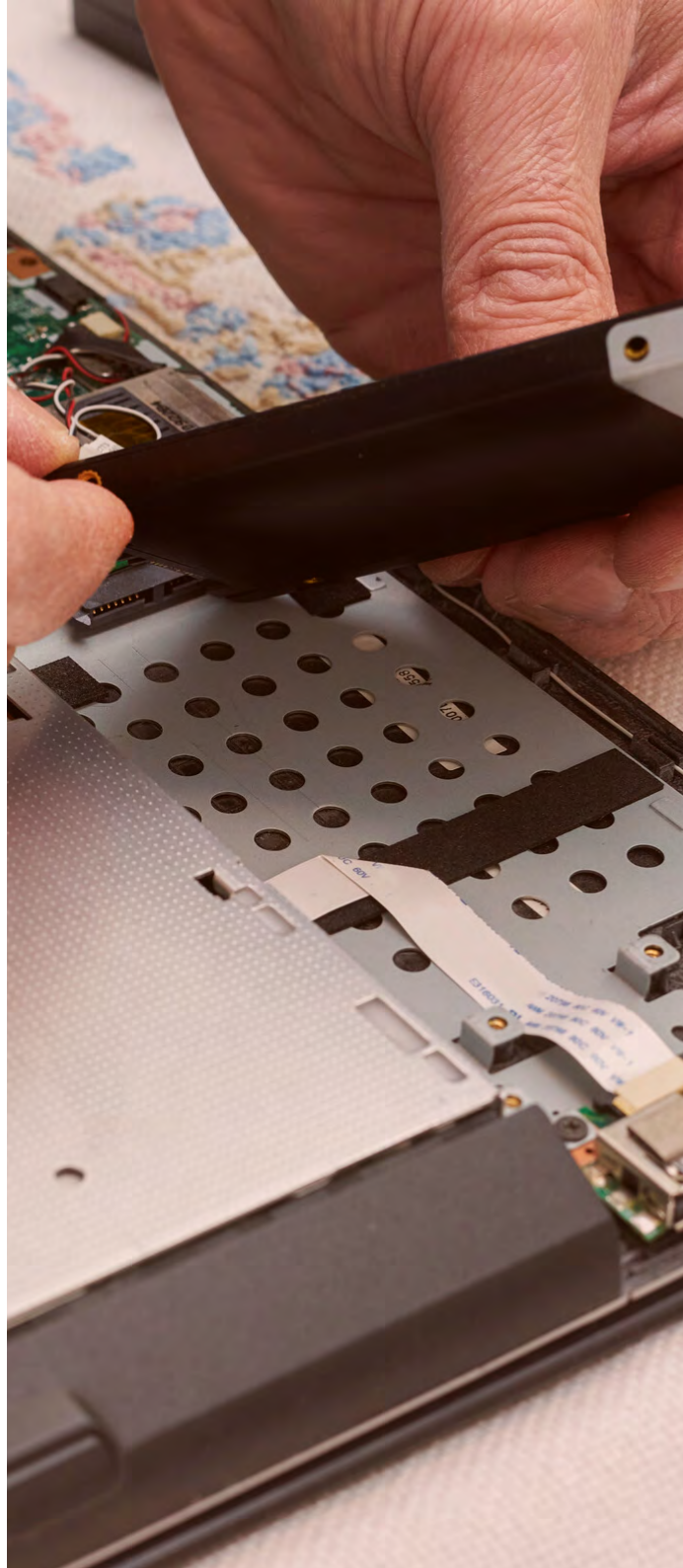
nie te operacje, jasnym stanie się, dlaczego warto zwrócić na nie uwagę i porównać je z deklarowanymi przez producentów resursami operacji kasowania/programowania lub parametrem TBW. Jeśli liczba operacji wykonanych przez nasz nośnik zbliża się do wskazanego przez producenta poziomu granicznego, warto pomyśleć o jego wymianie.

Trzeba przy tym zwracać uwagę na to, w jakich jednostkach nasz SSD podaje zużycie. Najczęściej jest ono podawane w bajtach lub w jednostkach LBA (sektorach liczących 512 B). W razie potrzeby musimy odpowiednio przeliczyć te wartości. Zwracamy także uwagę na parametr 05 – liczbę uszkodzonych (realokowanych) sektorów.

Wprawdzie SSD-ki nie mają fizycznych sektorów i nie prowadzą operacji realokacji, ale mają też wewnętrzną listę defektów, gdzie rejestrują uszkodzone bloki i informację o tych uszkodzonych blokach producenci zwykle umieszczają pod tym parametrem. Rosnąca wartość tego parametru jasno wskazuje na daleko posuniętą degradację układów NAND. Natomiast nieistotne dla nas będą parametry związane z liczbą odczytów, uruchomień, czy czasu pracy SSD-ka, gdyż te czynniki nie mają istotnego wpływu na jego zużycie i awaryjność.

SKAN POWIERZCHNI

SSD wprawdzie to nie dysk twardy i nie ma powierzchni magnetycznej, ale dla zachowania zgodności ze standardami i protokołami komunikacyjnymi zachowuje się tak, jakby ją miał. Skanowanie powierzchni dysku polega na wysyłaniu do niego w odpowiedniej kolejności (zazwyczaj liniowo od 0 do końca) żądania odczytu sektorów LBA i mierzeniu czasów wykonania kolejnych poleceń. W odróżnieniu od dysków twardych (zob. **Security Magazine 1(22)/2024**) w przypadku SSD-ków czas dostępu do poszczególnych fizycznych jednostek alokacji (stron) powinien być identyczny. W praktyce nie zawsze tak jest i to ma dla nas wartość diagnostyczną.



Przy ocenie stanu technicznego SSD-ka najbardziej pomocny będzie wykres szybkości odczytu. Przy jego ocenie musimy pamiętać o funkcji TRIM pozwalającej oszukiwać użytkownika oraz system operacyjny i zwracać wartości 0x00 dla obszarów niezaalokowanych w strukturach logicznych systemu plików (zob. **Security Magazine 5(14)/2023**) bez konieczności ich fizycznego przechowywania i odczytywania. W praktyce taka operacja fikcyjnego odczytu danych jest znacznie szybsza od odczytu realnego i podważy nam wiarygodność wyników testów. Dlatego przed przeprowadzeniem testu najlepiej jest maksymalnie wypełnić SSDka jakimiś plikami, nawet takimi, jakie usuniemy zaraz po zakończeniu testów.

Im szybciej i stabilniej uda się odczytać zawartość SSD-ka, w tym lepszym on jest stanie. Nie musimy się martwić niewielkimi odchyleniami szybkości odczytu, ale jeśli wykres zawiera bardzo duże amplitudy i bardzo wyraźne spadki prędkości odczytu, jest to już powodem do niepokoju.

Takie spadki odczytu oznaczają, że strony zawierające wolno odczytywane sektory czytają się niestabilnie i zawierają dużo błędów bitowych. Dla ich poprawnego odczytu koniecznych jest wiele prób i uruchomienie procedury „read-retry", co zajmuje czas.

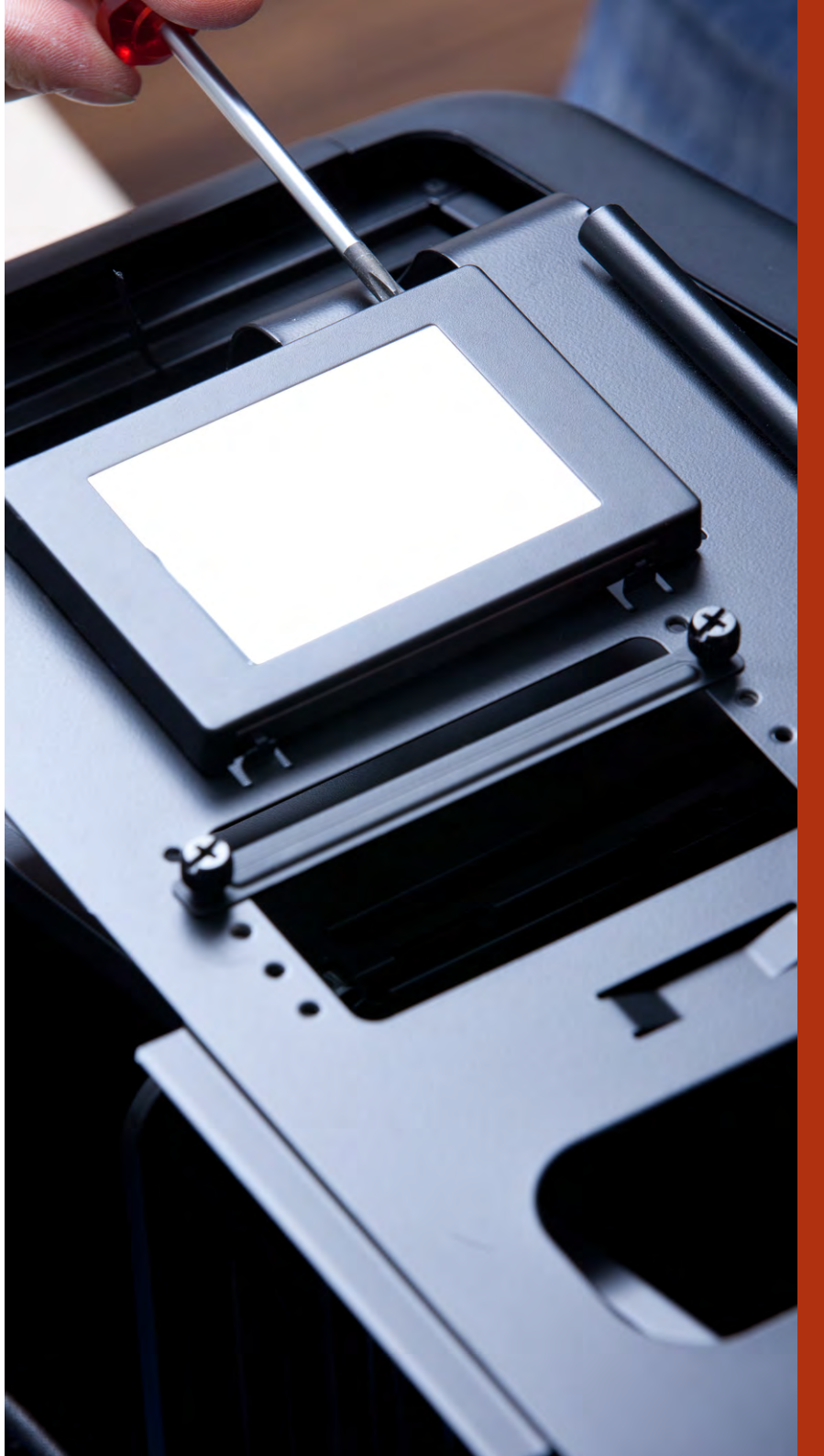
„Read-retry" jest procedurą pozwalającą na uratowanie możliwości odczytania stron zawierających zbyt dużo błędów bitowych, by mogły być skorygowane kodami ECC. Podczas odczytu porównujemy napięcia pomiędzy źródłem, a drenem tranzystorów z pewnymi napięciami odniesienia i w zależności od tego, czy są one wyższe, czy niższe od progu, przypisujemy im określone wartości logiczne. Procedura „read-retry" pozwala nam na delikatne obniżanie lub podnoszenie progowych napięć odniesienia, co w przypadku przeprogramowania (przeładowania bramek pływających nadmierną w stosunku do zakładanej liczbą elektronów) lub niedoporogramowania (umieszczenia w bramkach pływających zbyt małej liczby elektronów) pozwala za

za którymś podejściem odczytać zawartość strony z na tyle małą liczbą błędów bitowych, by była ona możliwa do skorygowania kodami korekcyjnymi.

W czasie testu mogą też wystąpić błędy odczytu. Zazwyczaj są to krótkie sekwencje błędów sumy kontrolnej (UNC) wskazujące na wystąpienie stron, w jakich liczba błędów bitowych przekracza możliwości naprawy zawartości przy pomocy kodu korekcji. Wystąpienie takich błędów jest bezwzględnym powodem dla wycofania SSDka z eksploatacji. W odróżnieniu od nośników magnetycznych, w nośnikach półprzewodnikowych nie ma nadziei na poprawę ich stanu przez nadpisanie zużytych i uszkodzonych jednostek alokacji. Operacje kasowania i programowania jedynie pogłębią degradację układów.

NIESTABILNA PRACA SYSTEMU OPERACYJNEGO

Czasami pierwszym sygnałem wskazującym, że dni naszego SSD-ka są policzone są problemy z systemem operacyjnym. Zawieszanie, resety, niebieskie ekrany, nietypowo długie ładowanie, czy wręcz brak możliwości wystartowania systemu operacyjnego mogą mieć podłoże sprzętowe. W przypadku SSD-ków tym bardziej nie należy tego ryzyka lekceważyć, że w odróżnieniu od dysków twardych,



zazwyczaj umierają one śmiercią gwałtowną, a spóźnienie reakcji może skutkować bolesną utratą danych.

Tak samo sygnałem, że z SSDkiem dzieje się coś złego mogą być problemy z jego detekcją przez BIOS. Jeśli BIOS nie rozpoznaje SSDka lub rozpoznaje go w nieprawidłowy sposób, najprawdopodobniej już doszło do awarii. Dlatego w przypadku, jeśli wystąpią problemy tego typu i zdarzy się, że za którymś razem SSD zostanie rozpoznany poprawnie, w żadnym wypadku nie można uznać, że problem sam się rozwiązał. W takiej sytuacji trzeba jak najszybciej przystąpić do zabezpieczenia danych, bo drugiej szansy może nie być.

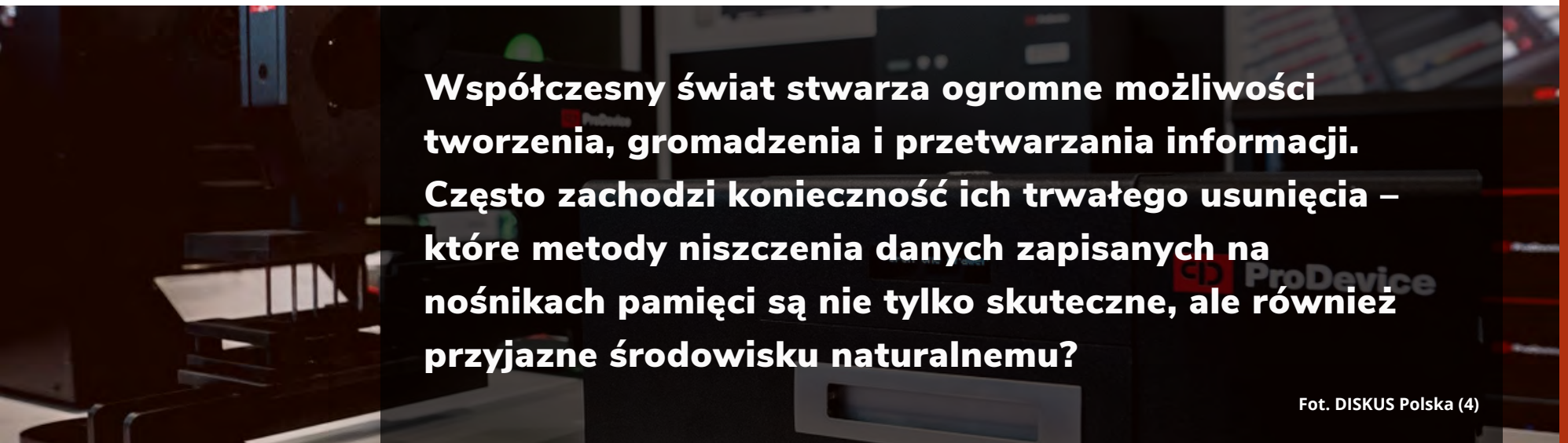
PODSUMOWANIE

Wskazane wyżej sposoby oceny stanu i przewidywania dalszych losów SSDków są obciążone dużą niepewnością i wysoce zawodne. Typowo awarie SSDków występują nagle, kiedy oprogramowanie układowe przestaje sobie radzić z obsługą błędów, zazwyczaj w sytuacjach wykonywania dużej liczby zapisów w krótkim czasie. Często np. w czasie aktualizacji systemu operacyjnego, co stało się podstawą przekonania, że to właśnie aktualizacja Windowsa może uszkodzić SSD. Przy czym w rzeczywistości do uszkodzenia prowadzi nie tyle aktualizacja sama w sobie, co niezbędne dla jej przeprowadzenia zapisy w powiązaniu z wcześniejszym zużyciem układów.

Ze względu na fizykę zapisu i przechowywania danych oraz rozwiązania oprogramowania układowego nigdy nie powstanie naprawdę pewna i skuteczna metoda oceny stanu SSD-ków. Rzadko możemy też liczyć na jakieś sygnały ostrzegawcze związane z niestabilną pracą nośnika. Ponadto rosnąca złożoność kodowania danych w nośnikach półprzewodnikowych powoduje, że zwykle odzyskiwanie z nich danych jest procesem bardziej skomplikowanym, a przez to i kosztowniejszym od odzyskiwania danych z dysków twardych. Dlatego bez względu na bieżącą ocenę stanu SSDka i tak warto mieć kopię przynajmniej najważniejszych danych.

NISZCZENIE DANYCH I OCHRONA ŚRODOWISKA. DEMAGNETYZER CZY NISZCZARKA?

Tomasz Filipów
DISKUS Polska, ProDevice



Współczesny świat stwarza ogromne możliwości tworzenia, gromadzenia i przetwarzania informacji. Często zachodzi konieczność ich trwałego usunięcia – które metody niszczenia danych zapisanych na nośnikach pamięci są nie tylko skuteczne, ale również przyjazne środowisku naturalnemu?

Fot. DISKUS Polska (4)

Niszczenie danych i ochrona środowiska. Demagnetyzer czy niszczarka?

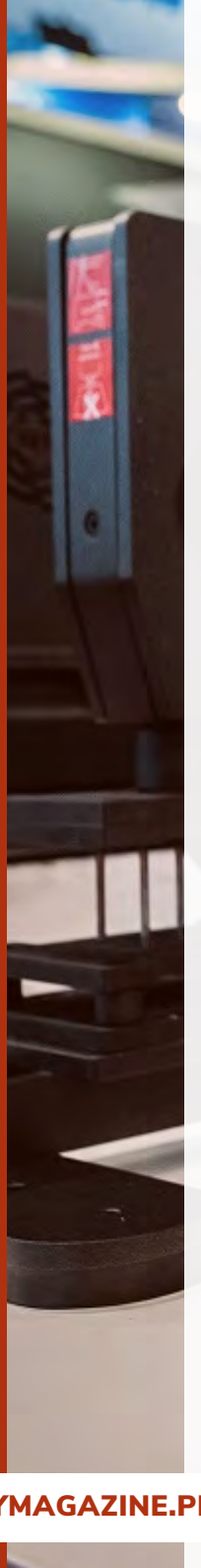
W celach archiwizacji i tworzenia kopii zapasowych dane zapisywane są na różnego rodzaju nośnikach danych, do których zaliczamy nośniki magnetyczne (takie jak np. dyski twarde, taśmy LTO czy dyskietki), nośniki półprzewodnikowe (karty pamięci, dyski SSD itp.) czy nośniki optyczne (np. CD, DVD, Blu-Ray). Często zawierają one nie tylko kluczowe i ważne ze strategicznego dla organizacji punktu widzenia informacje o klientach, kontrahentach, strategie rozwoju biznesu, plany marketingowe, analizy finansowe, ale również prywatne zapisy, typu historie konta bankowego, przebyte choroby itp.

Przepisy i regulacje dotyczące ochrony danych zobowiązują firmy i instytucje do nieodwracalnego, bezpiecznego niszczenia danych z nośników przeznaczonych do sprzedaży, naprawy czy utylizacji – usunięcie informacji musi być przeprowadzone w sposób nieodwracalny, bezpieczny dla ich poufności. Niestety, temat ten często zostaje zlekceważony albo jest słabo rozumianym aspektem bezpieczeństwa organizacji.

NA CZYM POLEGA DEMAGNETYZACJA?

Demagnetyzacja jest powszechnie stosowaną metodą nieodwracalnego niszczenia danych z wszystkich nośników magnetycznych: sprawnych oraz uszkodzonych. Na czym polega?

Wyobraźmy sobie, że powierzchnia dysku twardego pokryta jest niezliczoną liczbą bardzo małych magnesów. Każdy magnes ma dwa bieguny - N (biegun północny) i S (biegun południowy). Kiedy dane zapisywane są na dysku, bieguny te orientowane są

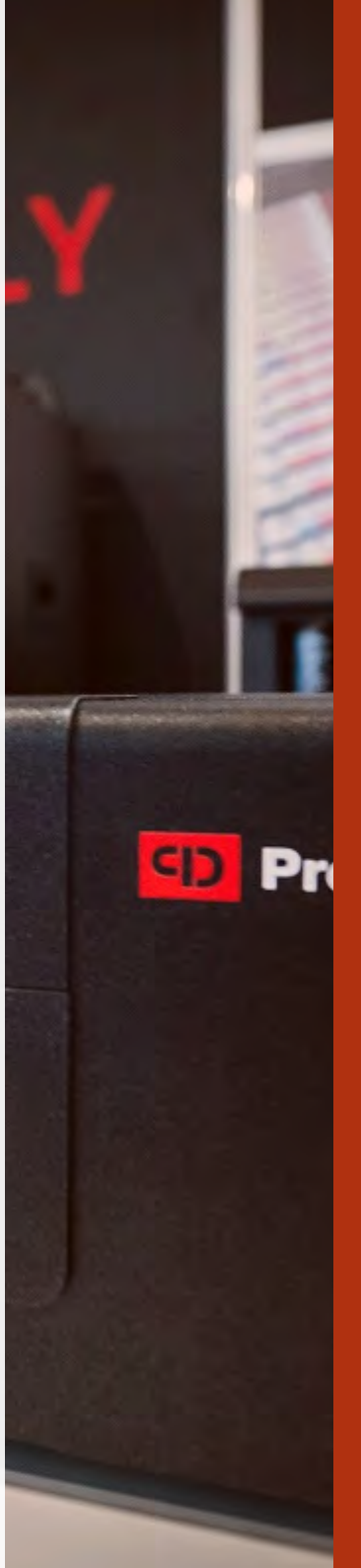


zgodnie z kolejnością bitów (cyfrowych jedynek i zer) tworzących dane (np. plik tekstowy lub zdjęcie). Celem procesu demagnetyzacji jest zmiana namagnesowania wzdłuż powierzchni talerza, aby wspomniane bieguny magnetyczne zorientowane zostały losowo.

Demagnetyzację nośnika przeprowadza się za pomocą urządzenia zwanego demagnetyzerem. Te najnowocześniejsze nie tylko generują silne pole magnetyczne (co zapewnia skuteczne usuwanie danych), ale również współpracują z aplikacją na urządzeniach mobilnych. Cały proces zniszczenia danych zajmuje jedynie kilka sekund. Zgodnie z tym, czego często wymagają wewnętrzne przepisy o ochronie danych, zniszczenie informacji zapisanych na nośniku jest automatycznie dokumentowane w postaci obrazu i wideo przy użyciu zintegrowanych funkcji urządzenia.

FIZYCZNE NISZCZENIE NOŚNIKÓW

Niestety, wśród wielu przedsiębiorców (a niekiedy – o zgrozo – osób odpowiedzialnych w organizacji za bezpieczeństwo danych) wciąż pokutuje przekonanie, że skutecznym sposobem usuwania informacji z dysku czy taśmy jest fizyczne zniszczenie nośnika.
W ruch idą wiertarki, młotki lub niszczarki. Prawda jest jednak taka, że zniszczenie fizyczne nośnika nie powoduje usunięcia danych na nim zapisanych. Fragmenty danych można odzyskać – jest to procedura kosztowna i długotrwała, ale możliwa do przeprowadzenia. Z drugiej strony, wiele firm decyduje się na przeprowadzenie procedury demagnetyzacji, a następnie fizycznego zniszczenia nośników. Czy ma to sens? Jeśli korzystamy z metody skutecznej (jaką jest demagnetyzacja), nie ma konieczności przeprowadzania dodatkowych czynności, aby mieć pewność, że dane zostały zniszczone. Oczywiście często zdarzają się sytuacje, kiedy firmy czy instytucje mają wprowadzone procedury wymagające demagnetyzacji, a następnie fizycznego zniszczenia nośnika.

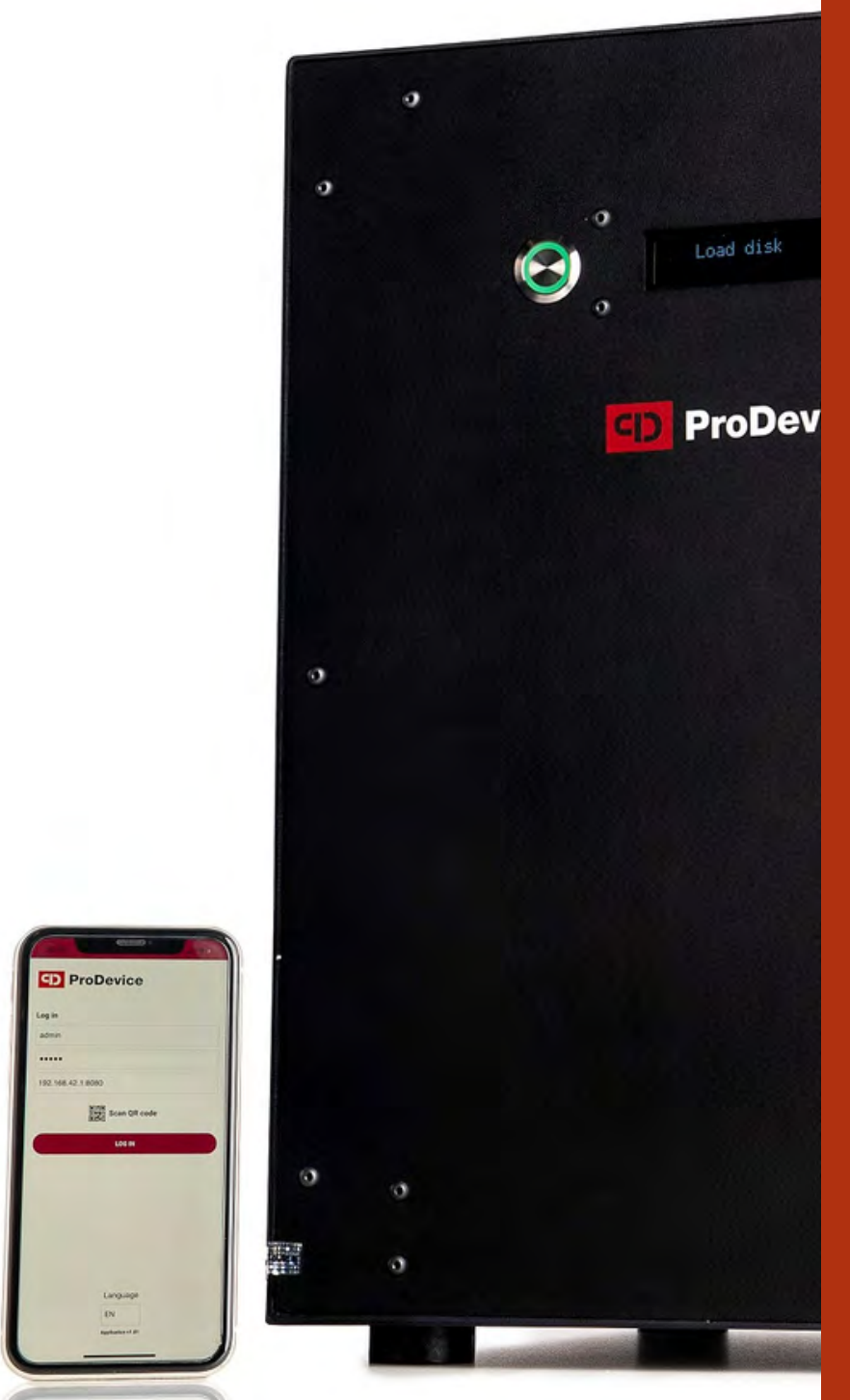


USUWANIE DANYCH PRZY POMOCY OPROGRAMOWANIA

Omawiając sposoby usuwania informacji z nośników, nie można zapomnieć o metodzie programowej, polegającej na nadpisaniu danych. Po przeprowadzonym procesie niszczenia danych, struktura fizyczna nośnika nie jest uszkodzona. Użycie oprogramowania ma jednak swoje ograniczenia: metodę tą można zastosować jedynie w przypadku nośników sprawnych fizycznie, cały proces bywa długotrwały i wymaga większego (niż przypadku demagnetyzacji) zaangażowania oraz wiedzy osoby przeprowadzającej proces. Zaletą tej metody niszczenia danych jest fakt, iż nośnik może być nadal użytkowany.

USUWANIE DANYCH PRZY POMOCY IMPULSU HEI – NOWOŚĆ

Wkrótce na rynek zostanie wprowadzone nowe, innowacyjne urządzenie Deflasher ProDevice T1000 – pierwsze na świecie urządzenie wykorzystujące technologię HEI (High Energy Impulse) do niszczenia danych z nośników wyposażonych w pamięć flash, pozbawionych metalowych obudów. To światowa rewolucja na rynku niszczenia informacji – urządzenie rozwiąże problem wielu przedsiębiorców, którzy usuwają dane z tego typu nośników oprogramowaniem (co często zajmuje dużo czasu) lub poddają nośniki pamięci fizycznemu zniszczeniu (co jest metodą nieskuteczną).



PORÓWNANIE METOD USUWANIA DANYCH

	Demagnetyzacja	Niszczenie fizyczne profesjonalną niszczarką	Niszczenie programowe	Niszczenie impulsem HEI
Możliwość odzyskania danych	Nie	Tak	Tak	Nie
Obsługiwane nośniki elektroniczne	Nośniki magnetyczne: HDD, taśmy, dyskietki, itp.	Wszystkie	Wszystkie nośniki umożliwiające wielokrotne nadpisywanie danych (nośnik musi być sprawny)	Kości pamięci flash, dyski SSD, pendrive, karty pamięci (nośniki pozbawione metalowej obudowy)
Obsługa uszkodzonych nośników	Tak	Tak	Nie	Tak
Czasochłonność procesu	Mniej niż 1 minuta / nośnik	Mniej niż 1 minuta / nośnik	Od kilkunastu minut do wielu godzin na nośnik (w zależności od wybranej metody)	Mniej niż 1 minuta / nośnik

SKUTECZNOŚĆ, WYGODA I KOMFORT UŻYTKOWANIA: DEMAGNETYZER CZY NISZCZARKA?

Demagnetyzacja jest dziś coraz bardziej docenianym, rekomendowanym przez NSA sposobem niszczenia danych, zwłaszcza jeśli mamy do czynienia z nośnikami uszkodzonymi. Warto zaznaczyć, że z tej metody korzystają nie tylko mniejsze czy większe firmy, ale również służby mundurowe czy agencje kosmiczne. Jest to metoda w stu procentach bezpieczna i skuteczna – danych nie da się odzyskać. Poza tym demagnetyzery (w przeciwieństwie do niszczarek) pracują cicho i nie emitują pyłu oraz innych substancji zanieczyszczających. Większość nowoczesnych modeli charakteryzuje się wymiarami typowymi dla sprzętu biurowego; demagnetyzery zwykle są kompaktowe, zajmują mało miejsca i można je łatwo transportować pomiędzy różnymi lokalizacjami. Niszczarki natomiast często osiągają spore rozmiary; modele przemysłowe są duże i ciężkie – bardzo trudno wykorzystać je w kilku lokalizacjach.

KOSZTY UŻYTKOWANIA: DEMAGNETYZER CZY NISZCZARKA?

Niszczarki obsługiwane ręcznie nie są urządzeniami bardzo drogimi; modele przemysłowe to rozwiązanie dla firm/instytucji, które dysponują większymi budżetami. Cena profesjonalnych demagnetyzerów, które – jak wspomniano – skutecznie usuwają dane z nośników magnetycznych, są różne i zależą od siły pola magnetycznego oraz dodatkowych funkcji, w które są wyposażone. Podstawowe demagnetyzery o mocy do 11.000 Gauss kosztują więcej niż ręczne niszczarki, ale mniej niż automatyczne modele niszczarek.

Każda firma czy instytucja musi podjąć własną decyzję dotycząca sposobu niszczenia danych. Dokonując wyboru pomiędzy kupnem demagnetyzera a niszczarki, należy wziąć pod uwagę nie tylko koszty związane z zakupem samego urządzenia. Warto ró-

wnież przeanalizować koszty związane z ewentualną utratą wrażliwych danych, których nie usunięto w sposób skuteczny – w takiej sytuacji w grę wchodzą nie tylko obciążenia finansowe, ale również poważne konsekwencje prawne oraz wizerunkowe. Biorąc pod uwagę te czynniki okazuje się, że cena zakupu demagnetyzera, który nieodwracalnie niszczy dane, jest niewielka w porównaniu z ryzykiem jakie niesie za sobą zakup samej tylko niszczarki, zwłaszcza tej, która nie spełnia surowych norm bezpieczeństwa w zakresie niszczenia danych.

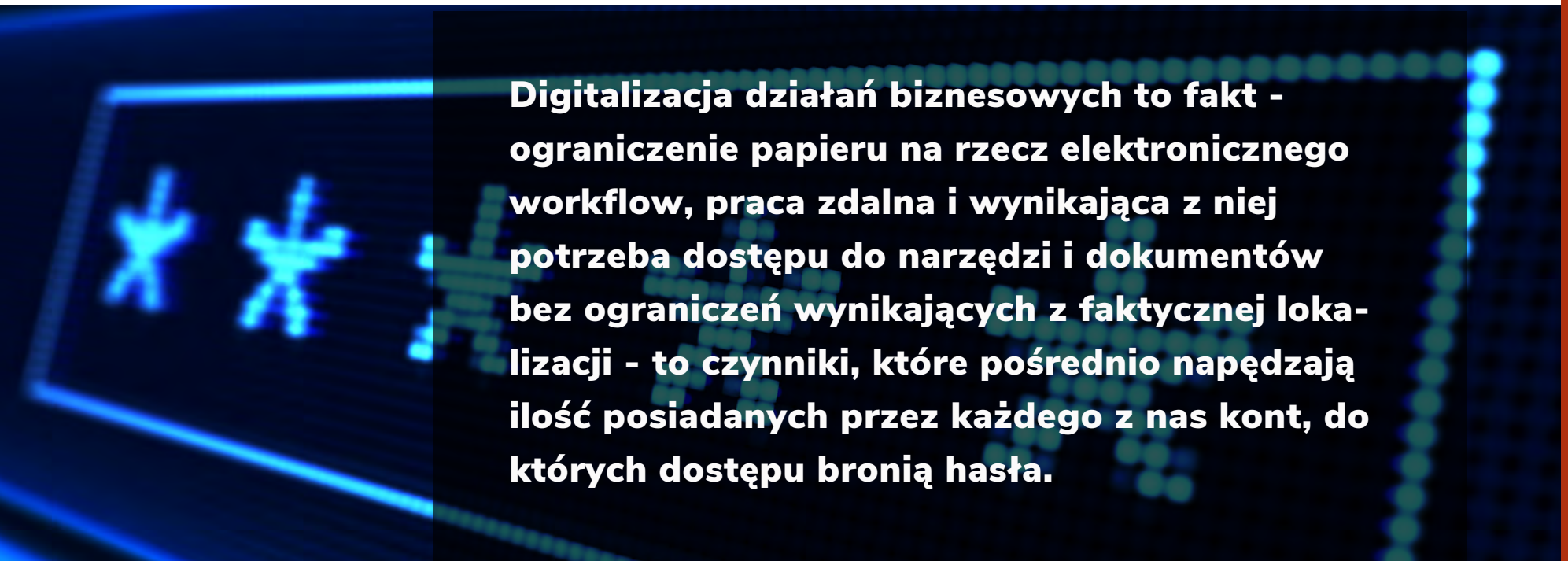
CO Z OCHRONĄ ŚRODOWISKA? DEMAGNETYZER CZY NISZCZARKA?

Zużyty sprzęt elektryczny i elektroniczny (ZSEE/WEEE) to jeden z najszybciej rosnących strumieni odpadów w UE. Mogą one powodować poważne problemy dla środowiska i zdrowia, jeżeli odpowiednio się nimi nie gospodaruje. Produkcja nowoczesnej elektroniki często wymaga również wykorzystania rzadkich i drogich zasobów (pierwiastki ziem rzadkich Rare Earth Elements REE). Recykling tych urządzeń elektronicznych przynosi oczywiste korzyści: to szansa na uniezależnienie się od monopolu krajów trzecich na metale ziem rzadkich i jednocześnie wsparcie idei gospodarki o obiegu zamkniętym, w której cały materiał odpadowy jest ponownie wykorzystywany. Coraz większe znaczenie zaczyna więc nabierać podejście do zasad zrównoważonego rozwoju (sustainability) oraz tzw. urban mining.

Demagnetyzacja nie uszkadza struktury fizycznej nośnika (dysk zostaje w jednym kawałku). To dlatego odzyskanie z niego ważnych pierwiastków czy elektroniki jest dużo łatwiejsze niż w sytuacji, gdy nośnik jest fizycznie zniszczony. Aby wesprzeć rozwój nowoczesnych technologii odzyskiwania REE z dysków twardych (dyski twarde zawierają magnesy neodymowe), konieczne są zmiany regulacyjne na rynku utylizacji danych. Równie istotne jest podejście całej branży IT do kwestii związanych z bezpowrotnym usuwaniem danych. Demagnetyzacja to zdecydowanie bardziej skuteczny sposób kasowania danych niż fizyczne niszczenie nośników (dane można usunąć nawet z uszkodzonych dysków). To również odpowiedzialne i mądre podejście do kwestii ochrony środowiska.

DLACZEGO MANAGER HASEŁ TO DZIŚ NIE LUKSUS, ALE KONIECZNOŚĆ?

Marta Siekacz
Perceptus



Digitalizacja działań biznesowych to fakt - ograniczenie papieru na rzecz elektronicznego workflow, praca zdalna i wynikająca z niej potrzeba dostępu do narzędzi i dokumentów bez ograniczeń wynikających z faktycznej lokalizacji - to czynniki, które pośrednio napędzają ilość posiadanych przez każdego z nas kont, do których dostępu bronią hasła.

Hasła, które teoretycznie tylko my znamy, dzięki czemu zapewniają one określony poziom bezpieczeństwa korzystania z zasobów i narzędzi udostępnianych zdalnie. Hasło powinno być unikalne i silne. Unikalne, by ewentualny wyciek informacji o hasłach z jednego źródła nie zagrażał bezpieczeństwu danych zgromadzonych na innych kontach. Silne, aby nie można go było łatwo złamać.

HASŁA, KTÓRE TRUDNO ZŁAMAĆ

Teoria teorią, ale już na tym etapie pojawiają się problemy. Skoro hasło musi być silne, to powinno być odpowiednio długie i skomplikowane, składać się z różnych elementów: liter, cyfr i znaków specjalnych w przeróżnych kombinacjach lub stanowić kombinację wyrazów trudną do przewidzenia dla osoby chcącej złamać hasło (tzw. passphrase). Efekt końcowy może być trudny do zapamiętania... więc kiedy już opracujemy sobie jedno bardzo silne hasło, często stosujemy je do zabezpieczania kilku kont na różnych platformach. Niestety, nie jest to dobry pomysł.

Rozwiązaniem problemów z tworzeniem i zapamiętywaniem licznych rozbudowanych haseł są aplikacje określane jako menedżery haseł. Nie tylko generują losowe i unikatowe hasła, ale też przechowują je w bezpieczny, szyfrowany sposób.

Dzięki nim użytkownik może zabezpieczać każdą witrynę, z której korzysta, unikatowym hasłem, które generowane jest automatycznie przez aplikację. To nie wszystko - najlepszą funkcją menedżera haseł jest to, że użytkownik nie musi pamiętać haseł, by z nich korzystać. Oczywiście poza hasłem zabezpieczającym dostęp do samego menedżera.

DLACZEGO WARTO KORZYSTAĆ Z MENEDŻERA HASEŁ?

Na ten temat toczyła się w przestrzeni Internetu już niejedna debata... Rozwiązań jest wiele, ale nie ma jednego, które zaspokoiłoby wszystkie potrzeby użytkowników.

Jako menedżery haseł mogą być wykorzystywane narzędzia wbudowane w przeglądarki internetowe, takie jak Chrome czy Firefox. Pozwalają one zarządzać hasłami, adresami lub innymi danymi logowania. Dają również możliwość ustawienia hasła głównego i odblokowania poświadczeń. Ich wadą jest to, że zwykle nie umożliwiają genero-

wania silnych haseł (choć pojawiają się wyjątki), a dodatkowo przeglądarki przechowują hasło w postaci zwykłego tekstu, co ułatwia hakerom kradzież tego typu informacji z komputera.

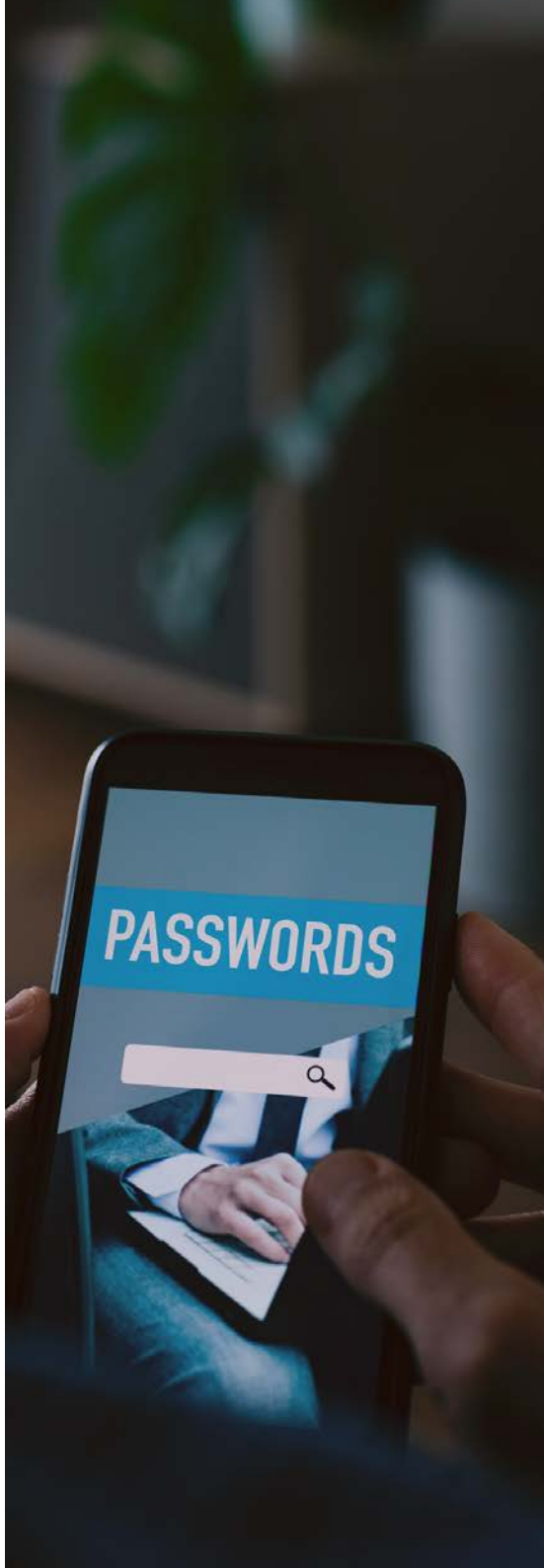
Menedżery haseł przechowują hasła w zaszyfrowanym formacie. Korzystają jedynie z opracowanych specjalnie wtyczek, które ułatwiają przesyłanie danych z aplikacji do przeglądarki, a dokładniej, do strony, do której chcemy się zalogować.

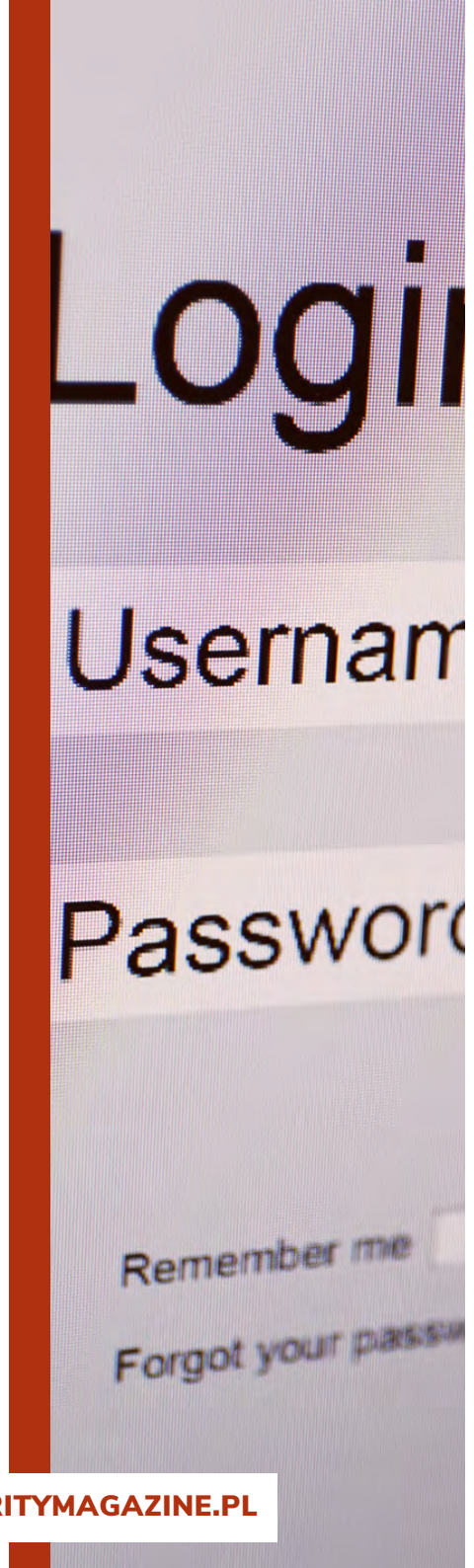
Analizując funkcje, jakie udostępniają użytkownikom autorzy rozwiązań, warto zwrócić uwagę na możliwość udostępniania haseł w elastyczny sposób, który pozwoli na sprawne wykorzystanie tego narzędzia nie tylko do zabezpieczenia prywatnych danych, ale także w zastosowaniach biznesowych.

Wśród najpopularniejszych menedżerów haseł wymienić należy z pewnością aplikacje:

- 1Password
- Bitwarden
- Dashlane
- Enpass
- KeePassXC
- Keeper
- LastPass
- NordPass
- RoboForm
- StickyPassword
- Proton Pass
- PercPass

Ostatnie dwa rozwiązania wymienione na powyższej liście to nowości, które na rynku pojawiły się stosunkowo niedawno.





PercPass to rozwiązanie zaprojektowane przez polską firmę i zasługuje na uwagę ze względu na lokalizację przechowywanych danych. Jako jedyne z powyższych rozwiązań wszystkie informacje przechowuje we własnym data center, w Polsce.

Ta cecha może być istotna w sytuacji, kiedy organizacja kładzie mocny nacisk na zgodność z RODO i wykorzystywanie systemów podlegających europejskiemu prawodawstwu w obszarze ochrony danych osobowych.

DOSTĘP DO DANYCH POD KONTROLĄ

Organizacje korzystające z uporządkowanych procedur tworzenia i udostępniania haseł posiadają większą kontrolę nad dostępem do danych. Normy opisujące procesy zarządzania cyberbezpieczeństwem w organizacjach uwzględniają sposoby tworzenia oraz przechowywania haseł, jako jeden z istotnych obszarów zabezpieczeń (np. NIST, ISO27001).

W aplikacjach typu menedżer haseł, które mogą wymusić określony poziom trudności hasła, dane dostępowe, którymi współpracownicy muszą się ze sobą dzielić, przekazywane są wewnątrz aplikacji. Widoczna jest struktura dostępu do informacji i w sytuacji, kiedy np. któryś z użytkowników zmienia pracę lub zakres działania w obrębie tej samej firmy, łatwo wytypować te dostępy, które powinny być zmienione lub zaktualizowane, oraz dostępy, które powinno się mu odebrać.

To my odgrywamy ważną rolę w zapewnianiu bezpieczeństwa systemów IT, w których pracujemy. W przypadku haseł to od nas zależy zarówno ich siła, sposób przechowywania, jak i sposób dzielenia się informacjami oraz troska o usuwanie uprawnień osobom, które nie powinny ich mieć. W natłoku obowiązków pojawia się pokusa, by iść na skróty i ułatwić sobie działanie. Aplikacje typu Menedżer haseł pozwalają na ułatwienie działania bez konieczności kompromisów w obszarze zabezpieczeń.

SECURITYMAGAZINE.PL

JAK REAGOWAĆ NA INCYDENTY BEZPIECZEŃSTWA WEDŁUG PRAWA?

Mateusz Jakubik
Bonnier Business Polska

Aleksander Wojdyła
Securitum

RODO i ISO 27001 to fundamenty ochrony danych w UE, wymagające od organizacji zastosowania środków technicznych i organizacyjnych. Dodatkowo, testy penetracyjne i działania red team są podstawą dla oceny skuteczności zabezpieczeń i zgodności z przepisami, zabezpieczając przed cyberzagrożeniami.

W Unii Europejskiej istotną rolę odgrywa Rozporządzenie o Ochronie Danych Osobowych (RODO), które nakłada na organizacje obowiązek zastosowania odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia danych osobowych. Audyt ISO 27001, będący międzynarodowym standardem zarządzania bezpieczeństwem informacji, może pomóc w spełnieniu tych wymagań, oferując ramy do efektywnej ochrony danych.

Ponadto, w niektórych branżach istnieją specyficzne regulacje prawne dotyczące cyberbezpieczeństwa. Na przykład, w sektorze finansowym instytucje mogą podlegać dodatkowym wymaganiom związanym z bezpieczeństwem informacji, określonym przez krajowe organy nadzoru finansowego.

Testy penetracyjne i działania red team również wpisują się w wymogi prawne, zwłaszcza w kontekście ciągłego monitorowania i ulepszania środków bezpieczeństwa. Wymogi prawne często zalecają lub wymagają regularnego testowania i oceny skuteczności zabezpieczeń, co jest realizowane przez tego typu działania.

Warto też zwrócić uwagę na wymogi prawne dotyczące reagowania na incydenty bezpieczeństwa. Organizacje są często zobowiązane do raportowania poważnych naruszeń bezpieczeństwa odpowiednim organom regulacyjnym oraz w niektórych przypadkach, osobom, których dane dotyczą.

AUDYT ISO 27001

Audyt ISO 27001 koncentruje się na weryfikacji oraz ocenie zgodności organizacji z normą ISO/IEC 27001, ustanawiającą międzynarodowe standardy zarządzania bezpieczeństwem informacji. W ramach tego audytu przeprowadza się kompleksową analizę systemów zarządzania bezpieczeństwem informacji (ISMS), co obejmuje polityki, procedury oraz praktyki monitorowania.

Celem audytu jest potwierdzenie czy organizacja spełnia wymogi normy oraz efektywnie zarządza bezpieczeństwem informacji. Przyjmując podejście oparte na ocenie zgodności, audyt ISO 27001 skupia się na dostarczeniu dokumentacji oraz dowodów potwierdzających zgodność z normą. Jest to istotne w kontekście spełnienia regulacji i norm branżowych, a także w budowaniu zaufania interesariuszy poprzez udowodnienie skutecznych praktyk zarządzania ryzykiem.

TESTY PENETRACYJNE

Testy penetracyjne, znane również jako pentesty, to bardziej aktywne podejście, które skupia się na identyfikacji i wykorzystaniu potencjalnych słabości w systemach. Zakres tych testów obejmuje skanowanie aplikacji i sieci w poszukiwaniu podatności, a następnie symulację rzeczywistego ataku w celu zidentyfikowania słabych punktów.

Głównym celem testów penetracyjnych jest identyfikacja konkretnych słabości w zabezpieczeniach systemu oraz ocena skuteczności mechanizmów obronnych. W przeciwieństwie do audytu ISO 27001, pentesty angażują ekspertów, którzy używają narzędzi i technik podobnych do tych, które mogą być stosowane przez rzeczywistych atakujących. To podejście pozwala na uzyskanie realistycznego obrazu odporności systemu na różne scenariusze ataków.

TESTY RED TEAM

Testy red team to zaawansowana forma testów penetracyjnych, która podnosi poprzeczkę, symulując ataki w sposób bardziej kompleksowy. Obejmują one nie tylko ocenę aspektów technicznych, ale również biorą pod uwagę czynnik ludzki, skupiając się na ocenie całkowitego poziomu bezpieczeństwa organizacji.

W ramach testów Red Team przeprowadzane są symulacje ataków, które obejmują dostęp do wewnętrznych informacji i zasobów, podobnie jak w przypadku rzeczywistego atakującego. Celem tych testów jest zidentyfikowanie, jak organizacja radzi sobie z zaawansowanymi atakami, a także sprawdzenie efektywności jej procesów reakcji na incydenty. Testy red team angażują zespoły doświadczonych ekspertów, którzy starają się złamać zabezpieczenia w sposób jak najbardziej zbliżony do rzeczywistego ataku, co pozwala na lepszą ocenę całkowitej gotowości organizacji na różne scenariusze zagrożeń.

Integracja tych trzech praktyk może zapewnić kompleksową strategię bezpieczeństwa informacji, obejmującą aspekty zgodności, aktywnego testowania oraz ocenę całkowitej odporności systemu na różne formy ataków.

ASPEKTY PRAWNE

Prawo cyfrowe w kontekście cyberbezpieczeństwa jest rozwijającym się obszarem prawnym, który odpowiada na wyzwania związane z rosnącą cyfryzacją społeczeństwa i gospodarki. Kiedy stale ewoluują zagrożenia w cyberprzestrzeni, zarówno legislatorzy, jak i organizacje działające w przestrzeni cyfrowej muszą dostosowywać się do nowych wymagań. Poniżej przedstawiam najważniejsze aspekty i wymagania związane z prawem cyfrowym w zakresie cyberbezpieczeństwa:

- **Ochrona danych osobowych.** Przepisy takie jak Ogólne Rozporządzenie o Ochronie Danych (RODO) w Unii Europejskiej ustanawiają rygorystyczne wymagania dotyczące ochrony danych osobowych. Organizacje muszą zapewnić bezpieczeństwo danych, w tym przez zastosowanie odpowiednich środków technicznych i organizacyjnych, oraz zgłaszać

naruszenia danych w określonym czasie.

- **Zgodność z lokalnymi i międzynarodowymi przepisami**. W zależności od lokalizacji i zakresu działalności, organizacje mogą być zobowiązane do przestrzegania różnych ustaw i regulacji dotyczących cyberbezpieczeństwa. Przykłady to amerykańska ustawa HIPAA w sektorze zdrowia czy europejskie dyrektywy NIS dotyczące bezpieczeństwa sieci i systemów informatycznych.
- **Zarządzanie ryzykiem cyfrowym**. Prawo cyfrowe coraz częściej wymaga od organizacji stosowania zasad zarządzania ryzykiem cyfrowym. Obejmuje to identyfikację, analizę i minimalizację ryzyk związanych z cyberatakami, wyciekami danych i innymi zagrożeniami cyfrowymi.
- **Obowiązek raportowania i reagowania na incydenty**. Wiele przepisów prawnych nakłada na organizacje obowiązek raportowania poważnych incydentów cyberbezpieczeństwa do odpowiednich organów regulacyjnych. Firmy muszą mieć przygotowane plany reagowania na incydenty oraz procedury komunikacji kryzysowej.
- **Wymogi dotyczące audytu i certyfikacji**. Standardy takie jak ISO 27001 stają się coraz bardziej istotne w kontekście prawnych wymagań dotyczących cyberbezpieczeństwa.

Przeprowadzanie regularnych audytów i uzyskiwanie certyfikacji może być wymagane przez prawo lub zalecane jako najlepsza praktyka.

- **Edukacja i świadomość cyberbezpieczeństwa**. Prawodawstwo coraz częściej podkreśla znaczenie edukacji i podnoszenia świadomości w zakresie cyberbezpieczeństwa. Organizacje są zachęcane do prowadzenia szkoleń dla swoich pracowników oraz implementacji kultur bezpieczeństwa.
- **Wyzwania związane z technologiami nowej generacji**. Rozwój technologii takich jak sztuczna inteligencja, Internet Rzeczy (IoT) czy 5G stwarza nowe wyzwania prawne. Legislacja musi nadążać za szybkimi zmianami technologicznymi, jednocześnie zapewniając odpowiedni poziom bezpieczeństwa i prywatności.

PODSUMOWANIE

Aspekty prawne w zakresie cyberbezpieczeństwa stają się coraz bardziej istotne w kontekście globalnej digitalizacji i rosnących zagrożeń w przestrzeni cyfrowej. Przepisy prawne w wielu krajach i regionach, w tym w Unii Europejskiej z jej Rozporządzeniem o Ochronie Danych Osobowych (RODO), nakładają na organizacje konieczność implementacji skutecznych środków ochrony informacji. Te środki mają na celu nie tylko zabezpieczenie danych osobowych i poufnych, ale także zapewnienie ciągłości działania i odporności na potencjalne cyberataki.

SECURITYMAGAZINE.PL

HAKERZY CZYLI KORSARZE XXI WIEKU?

Redakcja
SECURITY MAGAZINE

Zapewne słyszałeś o piratach – zwłaszcza tych z Karaibów. I siłą rzeczy pewnie obiło ci się o uszy coś o „korsarzach”. A już tym bardziej z pewnością słyszałeś o cyberprzestępcach i jednocześnie o takich grupach powiązanych z rządami różnych państw. Jak się ma zatem współczesna cyberprzestępczość do piractwa i korsarstwa z przełomu XVI–XVIII wieku? Przyjrzyjmy się grupom cyberprzestępczym, które współpracują z organizacjami rządowymi.

KORSARZE I... CYBERKORSARZE?

Piractwo jest praktyką równie starą, co żeglarstwo. W zasadzie nie ma miejsca na świecie, na którym kiedyś w historii ludzkości by ono nie występowało. Starożytni Egipcjanie narzekali na piratów greckich. Chińczycy i Koreańczycy mierzyli się z tymi japońskimi. Średniowieczni Europejczycy zmagali się za to z wikingami czy słowiańskimi chąśnikami i wiciędzami.

W nowożytności we znaki dawali się piraci marokańscy, tureccy, madagaskarscy, indonezyjscy i oczywiście karaibscy (którzy często byli albo byłymi czarnymi niewolnikami, albo po prostu Europejczykami). Ba, nawet dziś słyszymy o piratach jemeńskich czy somalijskich.

Niektórzy morscy bandyci szczególnie upodobali sobie konkretne cele i tak np. angielscy morscy bandyci chętniej napadali na francuskie okręty niż te z Wysp Brytyjskich. A jak mawiają stare porzekadła – wróg mojego wroga jest moim przyjacielem i jeśli nie możesz kogoś pokonać, to zaprzyjaźnij się z nim. Tak narodziło się korsarstwo. Rywalizujące ze sobą potęgi morskie niejednokrotnie płaciły grupom piratów, aby te obierały za cel statki konkurujących z nimi krajów.

Albo (co było znacznie częstsze) w listach kaperskich obiecali im spokój i możliwość zabierania łupów z okrętów wroga. Dzięki temu korsarze mogli „legalnie” uprawiać bandytyzm, korzystając z bander krajów, którym obiecali wierność i korzystać z ich portów.

Władcy z kolei nie musieli wydawać pieniędzy na rozbudowę floty i przy okazji obrywało się im wrogom – układ idealny. Niektórzy korsarze cieszyli się wręcz wyjątkowym szacunkiem władców. Ot, chociażby pochodzący z Lesbos Barbarossa (Hayreddin), służący tureckiemu sułtanowi, czy Sir Francis Drake, o którym Elżbieta I Wielka mawiała „mój pirat", a nawet pasowała go na rycerza.

Jednak jak ma się to wszystko do współczesnych cyberprzestępców? Czasy się zmieniają, tak jak i narzędzia, ale niektóre rzeczy są stałe. Dziś piractwo morskie jest domeną „niszową", ale już przestępczość w rozległym „oceanie sieci" – niekoniecznie. I tak grasujące bo bezkresnym morzu danych grupy cyberprzestępcze nierzadko niczym barokowi korsarze, zawieszają bandery krajom, którym służą i atakują konkretne cele na ich polecenia.

PÓŁNOCNI KOREAŃCZYCY – KRÓLESTWO CYBERPRZESTĘPCÓW

W kontekście grup cyberprzestępczych powiązanych z różnymi krajami czy państwowymi instytucjami, często słyszymy o hakerach rosyjskich lub chińskich. I do nich również wrócimy, ale szczególnie aktywni pod tym względem są też Północni Koreańczycy. Choć zdawałoby się, że kraj ten jest dość mocno zacofany technologicznie, to niekoniecznie tak jest. W internecie znajdziemy liczne informacje o atakach północnokoreańskich grup. Podobnie jak o tym, że często... reżim północnokoreański utrzymuje się z cyberprzestępczego procederu.

Dobrze opisuje to chociażby raport Insikt Group z Record Future, który przeanalizował sukcesy Korei Północnej w kontekście cyberataków wymierzonych w branżę kryptowalutową. KRLD od 2017 r. sukcesywnie zajmuje się kradzieżami kryptowalut i finansuje z tego swoje poczynania. W samym tylko 2022 r. ukradli kryptowaluty o wartości ok. 1,7 mld dolarów, co stanowiło 5% ich PKB oraz 45% budżetu wojskowego. W ten sposób reżim Kim Dzong Una jest w stanie funkcjonować pomimo licznych sankcji państw zachodnich.

Korea Północna za cel obiera sobie najczęściej Koreę Południową, ale od jakiegoś czasu – tamtejsze grupy cyberprzestępcze zaczynają też atakować innych. Zdecydowanie jedną z najpopularniejszych takich organizacji jest Grupa Lazarus, znana także jako APT38, Guardians of Peace czy Whois Team (tak naprawdę ich nazw jest naprawdę mnóstwo). W samym KRLD podobno określa się ich mianem Biura Łącznikowego 414. Lazarusa odkryto w 2009 r., po tzw. operacji Troja, gdzie doszło do licznych ataków DDoS wymierzonych w Koreę Południową.

Lazarus odpowiedzialny jest także m.in. za cyberatak na Sony Pictures w 2014 r., co doprowadziło chociażby do wycieku scenariuszy planowanych filmów japońskiego producenta.

Północnokoreańscy cyberkorsarze ukradli też 12 mln dolarów z Banco del Austro w Ekwadorze oraz milion dolarów z wietnamskiego Tien Phong Bank. Co ciekawe – za cele obierali sobie także banki w Polsce i Meksyku. Do ich niesławnych sukcesów zaliczyć też można wykradzenie 81 mln dolarów narodowemu Bankowi Bangladeszu.

Ponadto czasem Lazarusowi przypisuje się też stworzenie oprogramowania ransomware WannaCry, które w ciągu czterech dni zainfekowało ponad 300 tys. komputerów. Tezę o powiązaniu północnokoreańskich cyberprzestępców z tym wirusem wysnuło Kaspersky Lab, wskazując na podobieństwa pomiędzy kodami. Warto też podkreślić, że jeden z hakerów Grupy Lazarus – Park In Hyok jest ścigany listem gończym przez FBI. Co ciekawe – rząd KRLD zaprzecza w ogóle istnieniu takiej osoby.

EQUATION GROUP – AMERYKANIE TEŻ NIE SĄ ŚWIĘCI?

Choć grupy groźnych hakerów na usługach rządów kojarzą nam się bardziej z reżimowymi i auto-

rytarnymi państwami, to niekoniecznie tylko one korzystają z usług takich organizacji. Istnieje bowiem coś takiego jak Equation Group. Ma być to amerykańska grupa cyberprzestępcza powiązana z NSA. Jej odkrycia dokonano w Meksyku w 2015 r., przez... Kaspersky Lab.

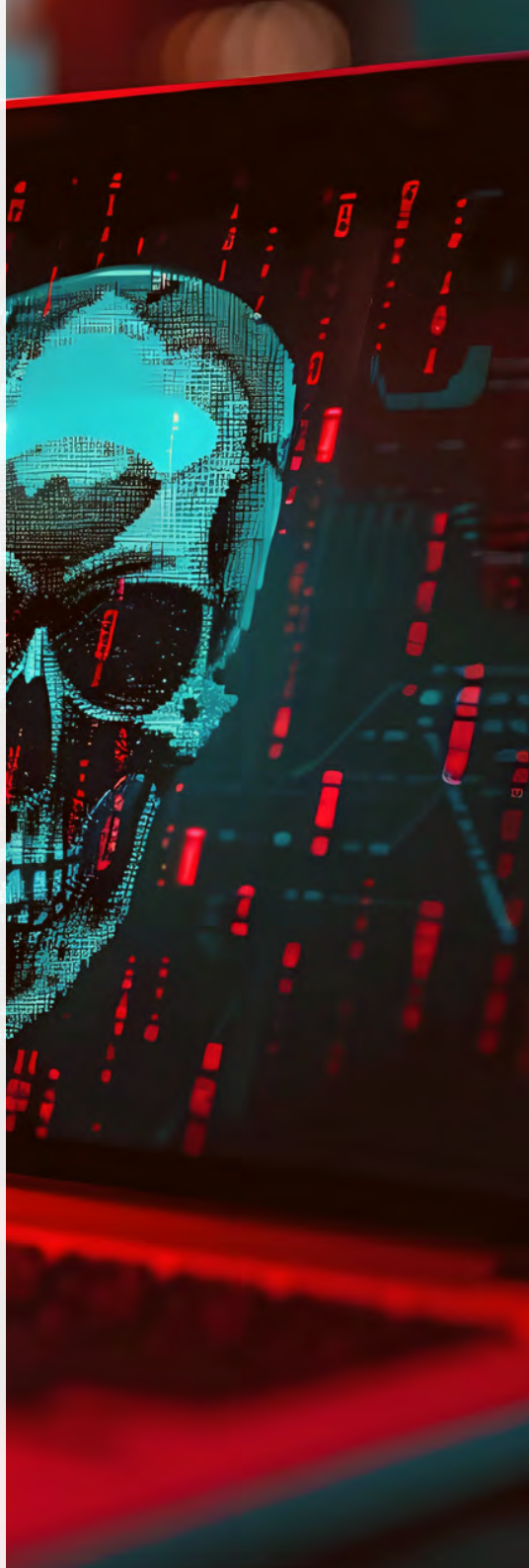
Organizacja ma ponoć działać od 2001 r., liczyć sobie łącznie 60 podmiotów i obierać za cele przede wszystkim organizacje w Iranie, Rosji, Pakistanie, Afganistanie, Indiach, Syrii, Chiny, Mali itd. itp. Co ciekawe – w 2017 r. na WikiLeaks pojawiła się opublikowana rozmowa agenta CIA, który wskazał, jak udało się zidentyfikować Equation Group i podkreślał, że jest to bardziej zbiór narzędzi do hakowania niż konkretna grupa ludzi. Oczywiście – Stany Zjednoczone zaprzeczają, że taka organizacja istnieje, a już tym bardziej że jest przez nie sponsorowana.

Jednak obieranie za cel przede wszystkim państw raczej wrogo nastawionych do Stanów Zjednoczonych i wykorzystywanie przez Equation Group oprogramowań śledzących, których kod przypomina ten używany przez NSA, może nas skłonić do nieco innych wniosków.

Warto też podkreślić, że w 2023 r., kiedy Kaspersky Lab odkryło oprogramowanie szpiegowskie, udające wirusa do kopania kryptowalut i wskazało, że ten jest stworzony niezwykle elegancko oraz skutecznie, to NSA po wypłynięciu sprawy do mediów, odmówiło komentarza. A to – stety lub niestety – coraz mocniej rzuca cień podejrzeń na amerykańskie działania w kontekście Equation Group.

CHIŃCZYCY – CZYLI TRAFIŁ SWÓJ NA SWEGO

Chińscy cyberprzestępcy – tak „indywidualni", jak i sponsorowani przez państwo to zmora współczesnego świata. Oczywiście, choć ChRL zaprzecza sponsorowaniu jakichkolwiek grup cyberprzestępczych, twierdząc, że przecież samo państwo chińskie również często pa-



da ofiarą cyberataków, to chyba nikt nie daje się na to nabrać. Na nic nie zdają się chińskie głosy o nazywaniu Stanów Zjednoczonych „imperium hakerów", kiedy samemu jest się prowodyrem licznych cyberataków.

Cyberkorsarze z Państwa Środka są o tyle groźni, że atakują w zasadzie wszystko – firmy prywatne, instytucje zdrowotne, organizacje rządowe itd. itp. Jedną z najpopularniejszych grup cyberprzestępczych jest STORM-0558.

Organizacja ta odpowiada za włamanie na konta e-mail ok. 25 organizacji, w tym agencji rządowych Stanów Zjednoczonych czy Microsoftu. Wśród wykradzionych przez STORM-0558 danych są m.in. maile sekretarza handlu Stanów Zjednoczonych Giny Raimondo, amerykańskiego wysłannika do Chin Nicholasa Burnsa i zastępcy sekretarza ds. Azji Wschodniej Daniela Kritenbrinka.

To oczywiście nie jedyna organizacja, bo kolejną jest np. Volt Typhoon. Grupa ta odpowiada m.in. za szpiegowanie szeregu infrastruktury krytycznej Stanów Zjednoczonych, organizacji telekomunikacyjnych i węzłów transportowych. W 2023 r. określono to jako jedna z największych kampanii cyberprzestępczych przeciwko amerykańskiej infrastrukturze krytycznej.

Z kolei BackdoorDiplomacy stało za szeregiem cyberataków na ministerstwa i instytucje państwowe Kenii. Według amerykańskich danych – grupa ta ma stanowić część większej organizacji znanej jako APT15. Rzeczone APT15 od 2004 r. atakuje główne organizacje publiczne i prywatne na całym świecie. Grupa ta jest odpowiedzialna za liczne bakcdoory, np. Graphicana.

Warto też podkreślić, że organizacje cyberprzestępcze ChRL nie ograniczają się wyłącznie do Stanów Zjednoczonych, czy Kenii. Jeszcze rok temu mówiło się o szeroko zakrojonej akcji chińskich cyberprzestępców, którzy infiltrowali administracje rządowe, dyplomatów i polityków Europy. Ponadto praktycznie co roku możemy usłyszeć o tym, jak Belgia pada celem ataku chińskich hakerów. Unijne agencje cały czas ostrzegają o tym, że ChRL dąży w ten sposób do destabilizacji naszych państw.

I warto podkreślić, że już w 2021 r. UE wzywała władze chińskie do podjęcia działań, które mają ukrócić złośliwe cyberataki. Jednak ChRL klasycznie – udawała, że tematu nie ma. To, oczywiście, nie wszystkie organizacje sponsorowane przez

ChRL. Zabrakłoby nam czasu, gdybyśmy chcieli je wszystkie wskazać, tak duży jest to proceder.

ROSJA – RAJ HAKERÓW

Zaraz po Chinach najczęściej słyszymy o rosyjskich hakerach i cyberprzestępcach. I podobnie jak z ChRL – Federacja Rosyjska sponsoruje naprawdę wiele organizacji cyberprzestępczych. Grup powiązanych z rządem jest mnóstwo. Jedną z najpopularniejszych jest założona ok. 2008 r. Cozy Bear, która najprawdopodobniej współpracuje z FSB lub SWR.

Głównymi celami Cozy Bear są, oczywiście, sektory rządowy, wojskowy, energetyczny, dyplomatyczny i telekomunikacyjny. Na cele obierali m.in. prywatne i publiczne podmioty w Niemczech, Uzbekistanie, Korei Południowej, czy w Stanach Zjednoczonych, próbując zaatakować nawet Departament Stanu USA czy Biały Dom w 2014 r.

Cozy Bear odpowiada również za atak spearphishingowy na Pentagon w 2015 r. Rosyjscy cyberprzestępcy nie szczędzą też europejskich krajów. W 2017 r. przypuścili atak spearphishingowy na pracowników Ministerstwa Obrony Narodowej i Ministerstwa Spraw Zagranicznych Norwegii. Atakowali też tamtejszą Partię Pracy.

Podobny atak przypuścili również na ministerstwa holenderskie, próbując pozyskać tajną dokumentację Królestwa Niderlan-

dów. W 2019 r. z kolei wypuścili trzy złośliwe oprogramowania: PolyglotDuke, RegDuke i FatDuke. Oprócz tego w 2020 r. próbowali wykraść informacje i dane dotyczące szczepionek oraz metod leczenia koronawirusa opracowywanych w Stanach Zjednoczonych, Kanadzie i Wielkiej Brytanii. Z kolei w 2022 r. przypuścili nieudany atak na Microsoft.

Oczywiście – to nie jedyna sponsorowana przez Rosję grupa cyberprzestępcza, bo tych jest znacznie więcej. Są też nieco mniej „utalentowane" organizacje, ale umiejące również zajść za skórę. Takim przykładem jest Killnet, czyli organizacja, która ujawniła się w 2022 r. po rosyjskiej inwazji na Ukrainę. W Polsce jest ona doskonale znana, bo wielokrotnie groziła naszemu krajowi. W 2023 r. miała włamać się do Grupy Azoty, wykradając dane tamtejszych pracowników, choć organizacja zaprzeczyła, że do takiego ataku w ogóle doszło.

Killnet odpowiedzialny jest też za liczne ataki DDoS na strony publiczne i rządowe w Rumunii, Mołdawii, Czechach, Włoszech, Litwie, Norwegii, Łotwie, Stanach Zjednoczonych, Japonii, Gruzji, Niemczech i oczywiście w Polsce. W 2022 r. próbowali również zablokować stronę WWW Eurowizji podczas występu Ukrainy.

Niesławą cieszy się też grupa Sandworm znana jako Jednostka 74455. Organizacja powstała najprawdopodobniej w latach 2004–2007 i jest odpowiedzialna za cyberszpiegostwo i ataki na infrastrukturę krytyczną. Prawdopodobnie współpracuje z GRU.

Sandworm stoi m.in. za atakami na sieć energetyczną Ukrainy w 2015 r., cyberatakami (ponownie na Ukrainę) w 2017 r., wybory prezydenckie we Francji w 2017 r., czy ceremonię otwarcia Zimowych Igrzysk Olimpijskich w Pjongczangu w 2018 r. Sandworm stoi też za stworzeniem złośliwego oprogramowania Infamous Chisel, które atakuje urządzenia z Androidem – głównie używane przez Ukraińców.

Oczywiście, rosyjskich grup cyberprzestępczych jest znacznie więcej. A część z nich także zajmuje się np. kradzieżą kryptowalut czy środków finansowych jak ich północnokoreańscy odpowiednicy. Rosja jest niestety państwem, które sponsoruje cyfrowy bandytyzm i wykorzystuje go na najróżniejsze sposoby – od dezinformacji, przez infiltrację po działania cyberwojenne.

BLACKJACK, CZYLI UKRAIŃSCY HAKERZY PRZECIW ROSJI

Jeśli mowa o naszych wschodniosłowiańskich sąsiadach, to nie można pominąć również Ukrainy. Państwo to także wspierane jest przez różne organizacje hakerskie, które jednak w dużej mierze walczą z rosyjskim agresorem. Przykładem takiej grupy jest chociażby Blackjack, które to prawdopodobnie powiązane jest z SBU. Jeszcze w styczniu 2024 r. Blackjack wykradł plany 500 rosyjskich baz wojskowych na terenie całej Federacji Rosyjskiej i okupowanych terenów Ukrainy.

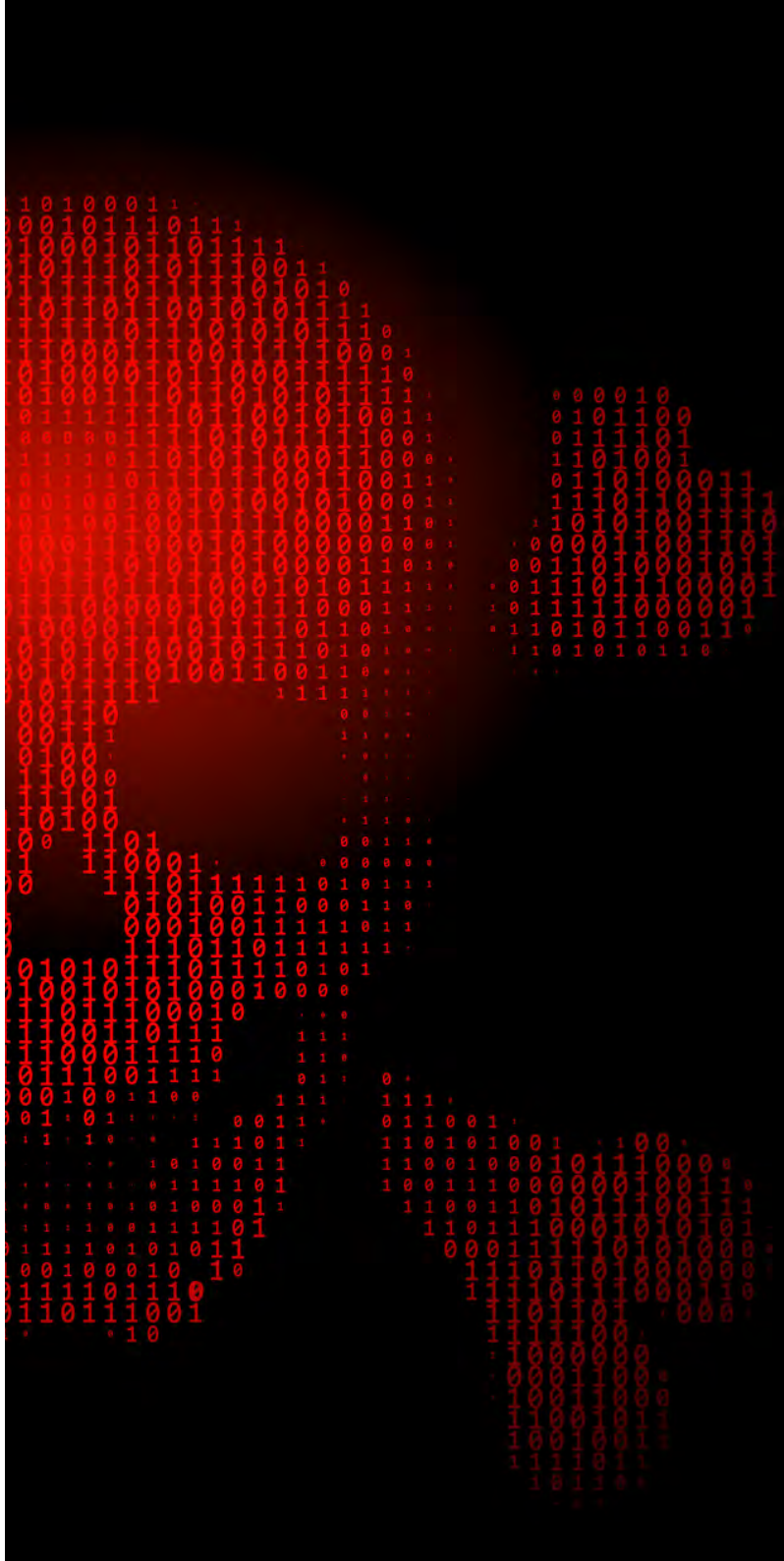
Mowa tutaj o kwaterach rosyjskiego dowództwa, instalacjach obrony przeciwlotniczej czy magazynach broni. Blackjack miało być też odpowiedzialne za usunięcie pozyskanych informacji z rosyjskich serwerów i wyłączenie 150 komputerów Rosjan. Organizacja ta stoi też za atakiem na moskiewską firmę telekomunikacyjną – M9 Telecom.

Warto też wspomnieć o IT Army of Ukraine, czyli grupie ochotników, którzy wspierają ukraińskie działania przeciwko rosyjskiemu agresorowi. Wraz z wybuchem inwazji, ukraiński rząd poprosił lokalnych hakerów, aby ci pomogli odpierać cyberataki na infrastrukturę krytyczną i prowadzić działania cyberszpiegowskie przeciwko rosyjskiej armii. IT Army of Ukraine odpowiada m.in. za cyberatak na Moskiewską Giełdę Papierów Wartościowych, włamanie się na stronę Sbierbanku, czy innych rządowych serwisów Białorusi i Rosji, czy działania przeciwko rosyjskiej sieci energetycznej i kolejowej.

Oprócz tego hakerom udało się zainfekować 800 rosyjskich stron – w tym Roskosmosu – oprogramowaniem, które wyświetlało wiadomość z gratulacjami z okazji święta ukraińskiej konstytucji. IT Army of Ukraine odpowiada także za atak na stronę Yandex Taxi, wykradnięcie danych grupy Wagnera, czy włamanie się na stronę WWW Organizacji Układu o Bezpieczeństwie Zbiorowym („rosyjskiego NATO").

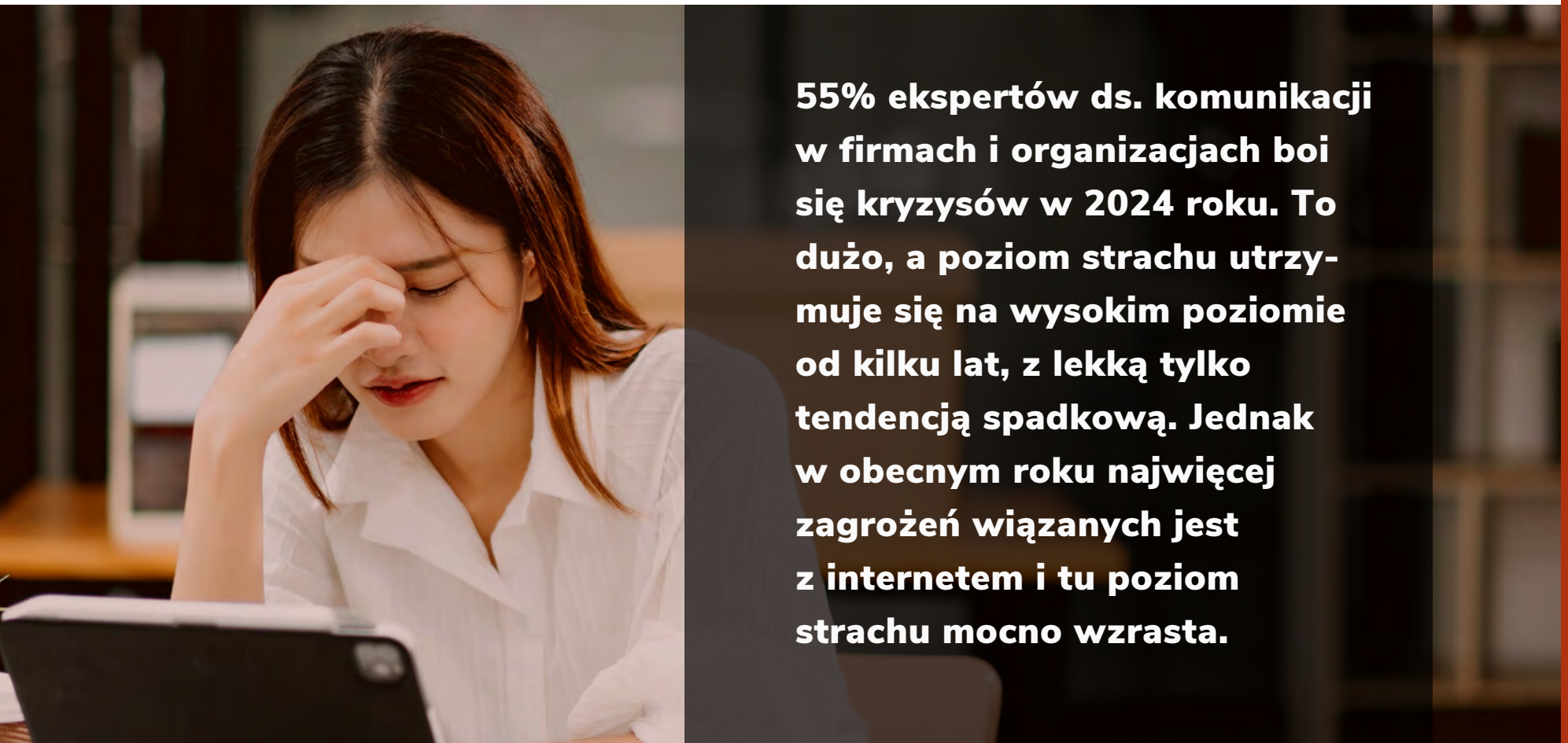
Jak widać – grupy hakerów, czy wręcz cyberprzestępców są sponsorowane przez najróżniejsze państwa i co więcej, mogą prowadzić bardzo różne działania. W tekście, oczywiście, nie wymieniliśmy wszystkich tego typu organizacji. Ba, nie wskazaliśmy nawet wszystkich państw, bo o tym, że tego typu grupy są sponsorowane np. przez Iran czy Białoruś również wiemy. A prawdopodobnie znacznie więcej krajów korzysta z usług „korsarzy XXI wieku".

Co nam to wszystko pokazuje? Że cyberprzestrzeń już od dawna nie jest jedynie miejscem, w którym możemy natknąć się na zwykłych cyberprzestępców, ale wręcz na zorganizowane, sponsorowane przez państwa grupy, które mają świadomy cel w ataku konkretnych podmiotów – w tym firm prywatnych.



E-KRYZYSY ZNOWU STRASZĄ

Beata Łaszyn
Alert Media Communications



55% ekspertów ds. komunikacji w firmach i organizacjach boi się kryzysów w 2024 roku. To dużo, a poziom strachu utrzymuje się na wysokim poziomie od kilku lat, z lekką tylko tendencją spadkową. Jednak w obecnym roku najwięcej zagrożeń wiązanych jest z internetem i tu poziom strachu mocno wzrasta.

Wszystko to mówi Kryzysometr – badanie komunikacji kryzysowej, realizowane od kilku lat przez Alert Media Communications. Obecna 7. edycja pozwala na analizę wyników nie tylko pod kątem zagrożeń przewidywanych w 2024 roku, ale również pokazuje trendy dotyczące poszczególnych obszarów. Po kilku latach widać, że Kryzysometr jak papierek lakmusowy pokazuje zmiany w obszarach wymagających troski i kwestie, jakich obawiają się eksperci, opierając przewi-dywania na swoim doświadczeniu. To pozwala przewidzieć, gdzie mogą pojawić się problemy oraz ostrzec lub wesprzeć w przygotowaniu firmy lub organizacji.

GDZIE CZAJĄ SIĘ ZAGROŻENIA

Jak co roku eksperci wskazali największe zagrożenia, z jakimi przewidują, że będą musieli się zmagać. Obecne wyniki wskazują, że najwięcej obaw wynika z internetu. Aż 44% respondentów wskazało sieć jako źródło największych zagrożeń. 30% spodziewa się, że problemy wizerunkowe będą wynikały z inflacji i trudności gospodarczych, a 27% – z negatywnego wpływu polityki na życie firmy i organizacji. Ponieważ strach przed kryzysami on-line znacząco wzrósł – z 32% w ubiegłym roku i 3. pozycji na 44% i lidera strachu w bieżącym badaniu – skupię się właśnie na nich.

KRYZYSY UKRYTE W SIECI STRASZĄ CORAZ MOCNIEJ

Głębsza analiza wyników wskazuje, że e-kryzysów boi się 38% przedstawicieli biznesu oraz aż 62% przedstawicieli instytucji(!). Różnica w obu środowiskach jest bardzo znacząca. Natomiast, co charakterystyczne, w obu grupach nastąpił spory wzrost obaw w ciągu ostatniego roku, choć wśród instytucji wzrost był dwukrotnie większy. Wzrost w grupie firm prywatnych wyniósł 11 punktów procentowych (p.p.), a w instytucjach – 23 p.p. To znacząca różnica – zarówno między kategoriami, jak i porównując rok do roku.

Kategoria kryzysów on-line bardzo zmieniła się względem ubiegłego roku. Choć to, co niezmienne od wielu lat, to wysoki poziom obaw przed kryzysami wynikającymi z fake newsów. Dziś w Kryzysometrze są najczęściej wymienianą potencjalną przyczyną kryzysów: 44% respondentów wskazała je jako zagrażające wizerunkowi. Natomiast kolejne pozycje zmieniły się znacznie względem roku 2023. W ubiegłym roku (podobnie jak jeszcze poprzednim) drugą najczęstszą przyczyną przewidywanych problemów były fale negatywnych komentarzy lub opinii konsumentów. W tym roku na prowadzenie wyszły obawy przed cyber-

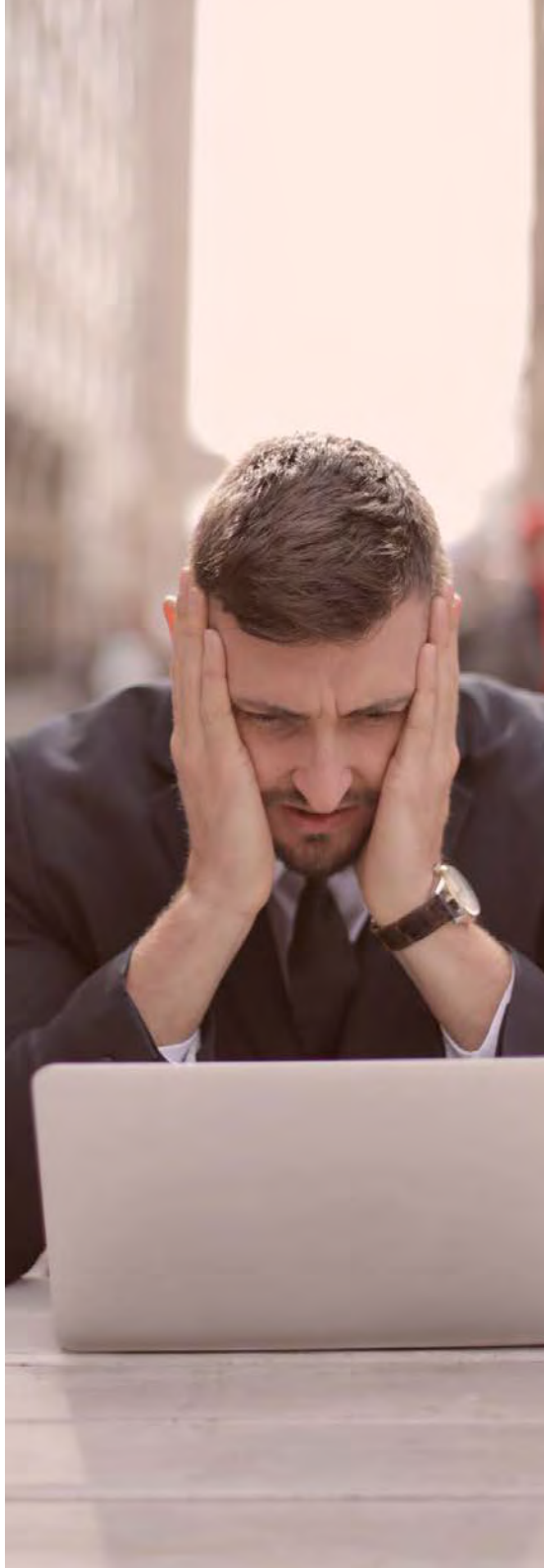
zdarzeniami – wyciekiem danych.

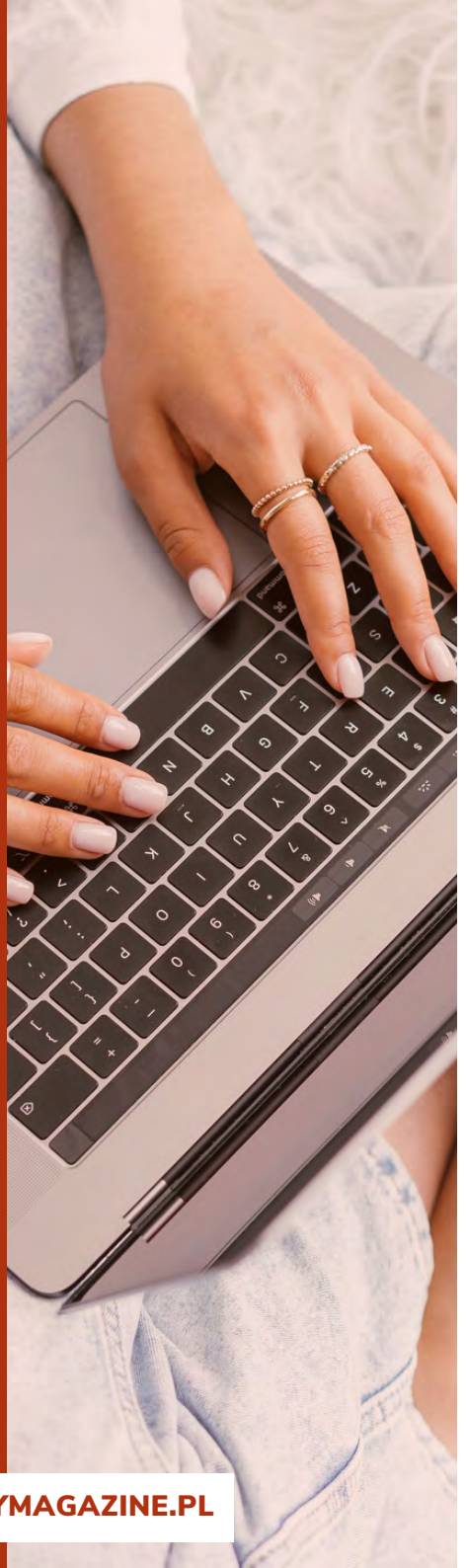
Poniżej przedstawiamy głębszą analizę poszczególnych pozycji wyników Kryzysometru, pokazując zarówno trendy, jak i podział zagrożeń na sektor prywatny oraz publiczny. W wielu przypadkach wskazania są odmienne, a wynikające z nich różnice – bardzo ciekawe.

FAKE NEWSY NADAL NA SZCZYCIE

Od wielu lat z dużym zaciekawieniem przyglądamy się **fake newsom**, szczególnie na tle innych strachów internetowych. O ile wszystkie inne odpowiedzi z roku na rok przesuwają się na skali strachów w zależności od okoliczności lub istotnych zmian w świecie, o tyle fake newsy zawsze i niezmiennie są bardzo wysoko. Każdego roku. Dane z poprzedniego Kryzysometru dopełniają tendencje: strach przed fake newsami był najczęściej wskazaną obawą – około 51% wszystkich specjalistów obawiało się w roku 2023 kryzysów internetowych wynikających z fake newsów. To nie zaskakuje, znając utrzymujący się od paru lat trend, wzmocniony w świetle wydarzeń towarzyszących wojnie w Ukrainie czy kampaniom wyborczym. I to w warunkach infodemii. Informacje o akcjach dezinformacyjnych przede wszystkim Rosji i wielu innych środowisk zwiększyły strach przed nimi, ale i – co dobre – podniosły poziom świadomości w społeczeństwie.

Prawdopodobnie przyczyną takiego stanu rzeczy (nieustannie dużego poziomu strachu) jest fakt, że z fake newsami trudno się walczy. Istnieją narzędzia debunkujące fałszywe przekazy, natomiast problemem jest czas, jaki to zajmuje. Największą wiarygodność mają agencje fact checkingowe, które intensywnie pracują zarówno nad wykrywaniem fake newsów, jak i uświadamianiem społeczeństwa. Jednak nawet jeśli fact checkerzy pracują sprawnie, to ustalenie prawdy zajmuje trochę czasu, a fałszywa teza jest w tym właśnie czasie przyswajana. Siła odkłamania fałszu nie jest tak duża, jak jego samego.





To, na co chciałabym zwrócić uwagę, to że w sytuacji obaw o szkodliwość fake newsów w swojej organizacji warto zorientować się w działaniu i procedurze agencji fact checkingowych: ustalić kontakt, zapoznać z ich pracą i możliwościami, tak by w razie problemów wiedzieć, co można zrobić i z kim się skontaktować. **Jakub Śliż, prezes Stowarzyszenia Pravda**, jednej z organizacji realizującej fact checking, zachęca do tego: - *Dezinformacja w czasach infodemii jest naprawdę groźna i mamy misję, by nie tylko promować prawdziwe informacje, ale i edukować. Uświadamiać. Ważna jest umiejętność pracowników firm i instytucji rozpoznawania dezinformacji i identyfikacji jej źródeł; wiedza, jak właściwie reagować i dlatego zawsze warto kontaktować się, jeśli są obawy w tym obszarze.*

WYCIEKI DANYCH I CYBERATAKI LARUM GRAJĄ

Drugą największą zmorą ekspertów wg Kryzysometru są potencjalne wycieki danych. Zauważyć tu trzeba, że według bezpieczników, tj. ekspertów ds. bezpieczeństwa w sieci, najczęstszą przyczyną wycieków jest błąd ludzki. Niezależnie od przyczyny strach ten w ciągu 2023 roku wzrósł o 10 punktów procentowych (do 37%), co jest dużą różnicą. Natomiast obawy przed cyberatakami wzrosły podobnie (o p.p. względem ubiegłego roku) i wynoszą dziś 32%, zajmując 4. pozycję w zestawieniu.

Co ciekawe, w badaniu z 2021 roku (2 lata temu) w przewidywaniach na 2022 respondenci jeszcze wyżej niż obecnie ocenili prawdopodobieństwo wystąpienia obu problemów: wycieki danych uzyskały wynik 39%, a cyberataki – 38%. Oznacza to, że w ciągu 3 lat obie kategorie najpierw były wysoko, potem w ubiegłym roku spadły, by dziś znowu podskoczyć. Prawdopodobnie przyczyną takiego stanu było to, że wybuch wojny w Ukrainie i wzmożone działania w cyberprzestrzeni szczególnie rosyjskich przestępców spowodowały podniesioną uważność w tej kwestii. W ciągu następnego roku sytuacja ustabilizowała się, choć nie uspokoiła.

Prawdopodobnie przyzwyczailiśmy się do niej. Natomiast obecnie coraz częściej słyszymy o incydentach w firmach i organizacjach, wielu z nas po prostu słyszało o takich przypadkach nie tyle z mediów, co z relacji poszkodowanych. A to wydaje się bliżej niż relacje medialne. Statystyki są nieubłagalne i pokazują systematyczny wzrost zaatakowanych podmiotów w Polsce. Polska należy do najczęściej atakowanego kraju w Europie (wg informacji Wojsk Obrony Cyberprzestrzeni i Polskiego Instytutu Spraw Międzynarodowych).*

Jeszcze ciekawiej się robi, jeśli przeanalizujemy wyniki obu źródeł pod kątem sektora. W obu przypadkach są różnice między podejściem do tych zagrożeń.

38% przedstawicieli firm powiedziało, że wycieki danych stanowią zagrożenie wizerunkowe, podczas gdy sektor publiczny – aż o 9 punktów procentowych mniej (27% przedstawicieli instytucji).

Podobna sytuacja, choć z mniej wyrazista różnicą, jest w podejściu do cyberataków: 32% biznesu obawia się cyberataków i 27% instytucji. Jak widać, zdecydowanie większą uwagę i większe obawy wywołują cyberzdarzenia w biznesie niż w instytucjach

publicznych. Rodzi się oczywiście pytanie, czy instytucje publiczne są lepiej zabezpieczone, mają większy potencjał obronny, czy po prostu ewentualne ataki nie zagrożą ich istnieniu, jak może się zdarzyć w przypadku firm i korporacji. W tym drugim przypadku nadwyrężony wizerunek może zagrozić istnieniu. Niezależnie od powodu różnic – obszar jest wysoce kryzysogenny w obu przypadkach.

*Znaczenie ataków cybernetycznych w strategii Rosji

Wzrost obaw przed wydarzeniami w cyberprzestrzeni – zarówno wyciekiem danych, jak i atakami hakerskimi – wskazuje, że warto się przygotować – zadbać o kontakt ze specjalistami ds. cyberbezpieczeństwa w organizacji, ustalić zasady komunikacji, reagowania i powiadamiania się, ustalić status sytuacji oraz zagrożeń. Dodatkowo obszar komunikacji może wesprzeć obszar bezpieczeństwa sprawnym informowaniem o działaniach systemu i stosowaniu zabezpieczeń, tak by każdy pracownik był skutecznie poinformowany o zasadach i regułach w organizacji.

To jest coraz ważniejszy obszar działania firm i organizacji. Można mieć świetne zabezpieczenia i procedury, ale jeśli są nieprawidłowo wdrożone, źle zakomunikowane, to nie będą skuteczne.

Mateusz Miniewicz, młodszy specjalista ds. cyberbezpieczeństwa podpowiada: - *Wydaje się, że w Polsce lubimy cyberbezpieczeństwo, mamy dobrych ekspertów, sporo osób uczących się, dużo samouków, jednak nadal w organizacjach oraz firmach obszar ten rozwija się niedostatecznie sprawnie. Często pracownicy bagatelizują temat na zasadzie „trzeba przeklikać tę prezentację". Z drugiej strony trzeba uważać, by nie przestraszyć ludzi zasadami czy konsekwencjami przed np. otwarciem niesprawdzonego załącznika, bo będą bali się wykonywać swoje obowiązki. Dlatego znalezienie optymalnego rozwiązania jest tak ważne. Obok technicznych rozwiązań dobrze sprawdza się dodatkowe rozwijanie „miękkiego cyber-*

bezpieczeństwa", tj. bezpieczeństwa organizacji przygotowanego i wprowadzonego w przyjazny sposób, dostosowany do charakterystyki organizacji – bo każda firma jest inna, ma inną specyfikę. Ciekawą metodą jest stworzenie sieci liderów, tzw. cybersecurity chempions.

W każdej jednostce organizacyjnej firmy jedna osoba (np. ta, która interesuje się tematem, ma predyspozycje) jest swoistym łącznikiem z działem bezpieczników, przekazuje cyklicznie przygotowane w „ludzki" sposób informacje, podpowiada, co robić, a czego nie, a w przypadku większych problemów – ułatwia kontakt. Temat cyberbezpieczeństwa w praktyce jest wtedy bliżej ludzi w przyjaznej formie. I, co ważne, system pozwala na szybkie wprowadzenie procedur lub zmian w zasadach, a te z postępem i rozwojem możliwości szybko będą się zmieniać. Taki czy inny system wymaga jednak pracy dwóch stron – bezpieczeństwo musi zadbać o przeszkolone, komunikatywne osoby do kontaktów wewnętrznych – z pracownikami, a pozostałe działy muszą zachować otwartość na obszar cyberbezpieczeństwa. W każdej organizacji można znaleźć odpowiednią metodę, tylko należy jej poszukać, uwzględniając „ludzki" czynnik; stąd określenie „miękkie cyberbezpieczeństwo".

Obawy ekspertów ds. komunikacji oraz bezpieczników potwierdzają twarde dane. Według badania Veeam „Global Report Ransomware Trends 2023" procent firm dotkniętych cyberatakiem w 2023 roku wyniósł 85% (!) i wzrósł o 9% wobec ubiegłego roku. To bardzo wyraźnie pokazuje realną skalę zagrożeń. Co więcej, wg badania 80% firm zapłaciło okup, ale 21% z nich nadal nie było w stanie w pełni odzyskać danych (59% odzyskało) i tylko 16% nie zapłaciło okupu. Jedynie w 4% przypadków nie było żądania okupu. Eksperci przewidują również rozwój darknetu.**

UWAGA: HAKTYWIZM

W związku z omawianym obszarem zwracam przy okazji uwagę na dodatkowy aspekt wynikający z naszej analizy sytuacji w kraju i na świecie. Coraz częściej w różnych sytuacjach uaktywniają się haktywiści – aktywiści wykorzystujący ataki hakerskie, by zwrócić uwagę na problemy i zmiany (np. społeczne, klimatyczne), o jakie walczą.
Często w ten sposób chcą zwrócić uwagę na konkretne problemy lub wymusić na organizacjach określone działanie. Przykład może stanowić grupa Gay Furry Hackers, która w swojej walce zaatakowała sieć NATO.

**Cyberochrona: trendy i zagrożenia w 2024 r.

Atak był na tyle skuteczny, że organizacja wydała oświadczenie, iż eksperci NATO ds. cyberbezpieczeństwa aktywnie zajmują się incydentami, które miały wpływ na niektóre niesklasyfikowane strony internetowe NATO. Zapewniają, że „nie wywarło to żadnego wpływu na misje, operacje i rozmieszczenia wojskowe NATO" – i samo zapewnienie pokazuje poziom spowodowanego niebezpieczeństwa. Ta sama grupa zaatakowała amerykańskie państwowe laboratorium badań nuklearnych. Oba ataki były poważne i miały miejsce w 2023 roku.

POZOSTAŁE ŹRÓDŁA E-KRYZYSÓW

Powracając do Kryzysometru i spodziewanych przyczyn e-kryzysu, warto wspomnieć o falach krytyki i negatywnych komentarzy. To obawa, jaka od wielu lat jest w czołówce strachów. W obecnym badaniu zajęła „dopiero" 3. pozycję, wypchnięta przez wycieki danych, natomiast nadal ma wysoki współczynnik strachu (34% – spadek o 11 p.p. względem ubiegłego roku). Oznacza to, że nie tyle boimy się ich mniej, a pojawiły się kolejne mocne kategorie rodzące zagrożenie. Co ciekawe, przy wielu różnicach między sektorami obecnie wszyscy obawiają się ich w jednakowym stopniu.

Pozycję utrzymał natomiast trolling, rozumiany jako zorganizowane akcje hejtu oraz dezinformacji, który został wskazany przez 30% respondentów. Wynik jest podobny jak w ubiegłym roku i różni się tylko o 1 p.p. Natomiast w tej pozycji istnieje największa różnica w definiowaniu obszaru zagrożenia między sektorami. W biznesie trolling jest szóstym z kolei strachem internetowym, podczas gdy w sektorze publicznym – drugim! Różnice procentowe również są znaczne: biznes – 24%, a publiczne – 41%. 17 punktów procentowych różnicy między sektorami to bardzo dużo. Od razu pojawia się pytanie: dlaczego tak jest? Trolling w badaniu definiujemy jako zorganizowane akcje hejtu i dezinfor-

macji i tu prawdopodobnie kryje się odpowiedź.

Dr Paulina Piasecka (Dyrektor Centrum Badań nad Terroryzmem Collegium Civitas w Warszawie oraz zastępca kierownika Instytutu Analizy Informacji Collegium Civitas) w jednym z odcinków podcastu o dezinformacji stwierdziła, że jesteśmy tak spolaryzowanym społeczeństwem, inicjującym tak wiele różnych wątków podziału społecznego, że rosyjskie działania nie polegają na umieszczaniu nowych przekazów czy narracji w dyskursie politycznym, tylko sterowaniem istniejącymi. - *Polska nie jest trudnym krajem do manipulacji, a polskie społeczeństwo nie jest najtrudniejszym tej manipulacji celem między innymi dlatego, że jesteśmy wewnętrznie skonfliktowani i spolaryzowani, ale także ze względu na to, że jesteśmy społeczeństwem, które jest dość nieufne w stosunku do władz****** – mówi dr Piasecka. To oznacza, że wszyscy raczej spodziewają się trollingu w obszarze właśnie politycznym – stąd wysoki poziom obaw wśród przedstawicieli instytucji publicznych.

Ciekawie się też robi przy kolejnej pozycji: deep fake. Dwa lata temu był na dole skali z wynikiem 6%. Rok później wzrósł do 14% (ponad dwukrotny skok). Tendencja szybkiego wzrostu utrzymała się i dzisiaj, po kolejnym podwójnym wzroście, aż 28% respondentów obawia się problemów wynikających właśnie z deep fake. Różnice między sektorami oczywiście i tu istnieją, choć nie są tak spektakularne jak w przypadku trollingu: biznes w 30% obawia się problemów deep fake'ów, a instytucje nieco mniej – 24%.

***Dezinformacja, czyli dziel i rządź.

****Wniosek z raportu Winning the Information War – Center for European Policy Analysis – za jw.

EPILOG

Poziom obaw na przestrzeni lat zmienia się w zależności od globalnych lub krajowych okoliczności, dlatego warto czytać dane w kontekście – uwzględniając wydarzenia i trendy. Spore różnice z powodów kontekstów krajowych, w tym polaryzacji społecznej, istnieją między ekspertami w firmach a instytucjach publicznych. Różnice te widzimy wyraźnie w naszej działalności, analizowanych kryzysach i sytuacjach trudnych. Na strachy wynikające z internetu z pewnością wpływa nasza specyfika: jesteśmy spolaryzowanym i skłóconym społeczeństwem, mocno walczącym ze sobą, co oznacza, że większość zjawisk internetowych może być mocniejszych niż w innych państwach i mieć większy impakt.

Powyższa analiza wskazuje wyraźnie obszary, jakich eksperci ds. komunikacji obawiają się w 2024 roku. Warto być tego świadomym, by móc się przygotować lub obronić. Bardzo gorąco rekomendujemy analizę sytuacji, obserwację wskazanych obszarów, szczególnie z uwzględnieniem możliwości zabezpieczenia się przed incydentami oraz zoptymalizowania ich występowania lub ewentualnych skutków. Właśnie taki sens ma Kryzysometr – by wiedzieć, gdzie patrzeć, z jakiego kierunku spodziewać się zagrożeń, kiedy czuwać szczególnie.

Z naszych doświadczeń wynika, że większość kryzysów można przewidzieć, a co za tym idzie – przygotować się, by do nich nie dopuścić lub zmniejszyć ich szkodliwość. A statystyki są nieubłagane – Kryzysometr pokazuje, że w ubiegłym roku 36% respondentów miało kryzys, z czego 55% z sektora publicznego i 30% z biznesu. Zważywszy, że to pytanie o zaistniałe kryzysy, to wysoki współczynnik. Z tego powodu zachęcamy do tego, by przygotować się i podpowiadamy, jak to zrobić. Mam nadzieję, że nie będą musieli Państwo z tego korzystać, czego wszystkim serdecznie życzę.

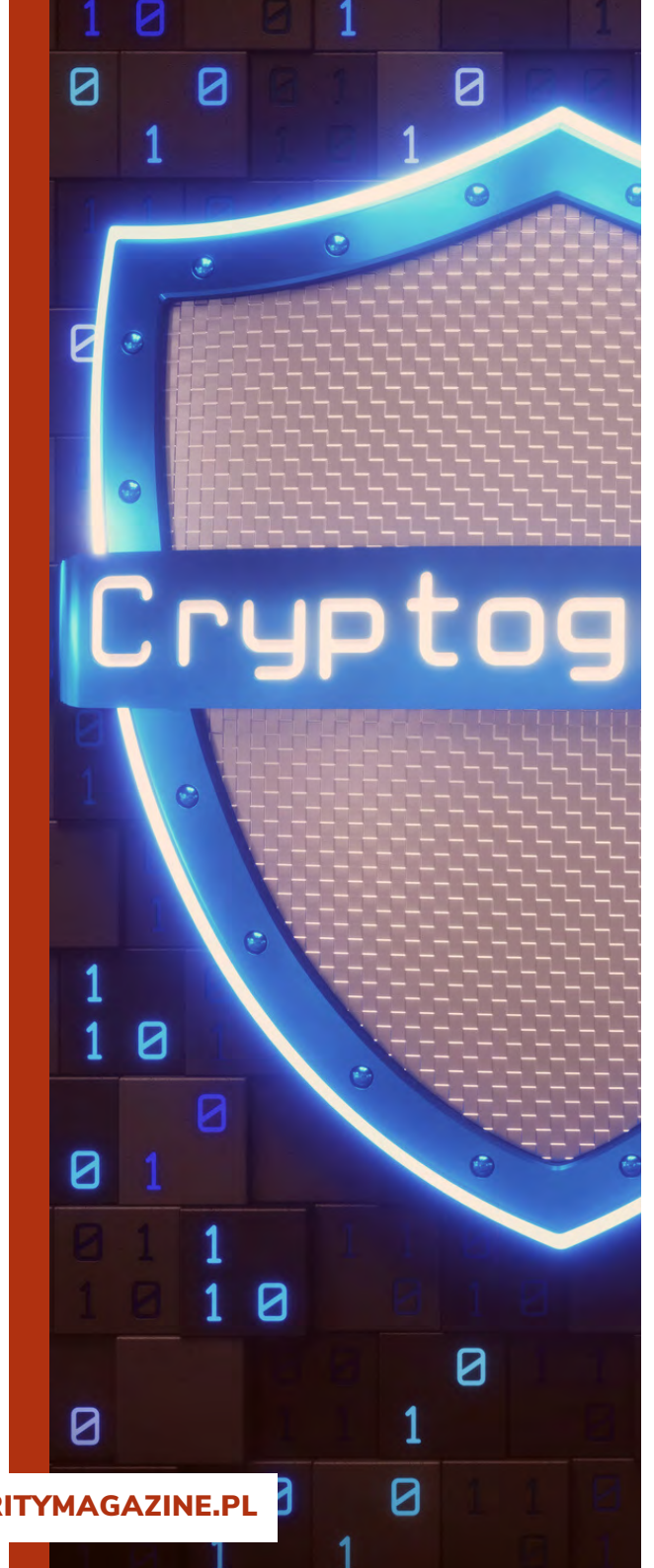
O badaniu

Panel ekspercki badania Kryzysometr 2023/2024 agencja Alert Media Communications przeprowadziła na przełomie listopada i grudnia 2023 r. Wzięło w nim udział 107 rzeczników, dyrektorów i managerów PR z czołowych polskich firm, instytucji państwowych i samorządowych oraz organizacji pozarządowych.

KRYPTOGRAFIA A CODZIENNOŚĆ

Oliver Dedowicz
Cyber Security Lab

Kryptografia może wydawać się przerażająca i zawiła. Szyfrowanie, klucze, złożone procesy matematyczne to pojęcia, o których człowiek niezaznajomiony z informatyką rzadko kiedy ma pojęcie. W coraz bardziej zdominowanym przez technologię świecie kryptografia odgrywa ważną rolę w zapewnianiu bezpieczeństwa danych. Artykuł ten ma na celu przybliżenie roli kryptografii w codziennym życiu oraz przedstawienie jej znaczenia dla ochrony prywatności i bezpieczeństwa informacji.



KRYPTOGRAFIA W KOMUNIKACJI ELEKTRONICZNEJ

Współczesne społeczeństwo coraz bardziej polega na sieci – komunikatory internetowe, bankowość elektroniczna czy zakupy on-line – do tego wszystkiego niezbędna jest odpowiednia ochrona. Kryptografia odgrywa tutaj kluczową rolę, w szczególności w zapewnieniu tzw. bezpiecznego połączenia. Zapewne każdy słyszał kiedyś o protokole HTTPS, zwanym potocznie „zieloną kłódką'' na pasku adresowym. Protokoły SSL/TLS, czyli protokoły szyfrowania chronią nasze transakcje, czyli wszystkie dane, które wymieniane są pomiędzy użytkownikiem, a serwerem, zapewniając warstwę szyfrowania, a co za tym idzie poufność i integralność przesyłanych danych. Jest to standard w dziedzinie komunikacji internetowej.

Użytkownicy, w przypadku korzystania z portali lub aplikacji, które nie stosują tych protokołów, narażeni są na wiele niebezpieczeństw. Przykładów zagrożeń jest wiele, między innymi podatność na podsłuchiwanie transmisji, czyli sniffing czy ataki man-in-the-middle. Ofiara jest w szczególności podatna na powyższe w momencie korzystania z publicznych sieci, gdzie nie mamy pewności kto ma dostęp do pakietów wędrujących po interfejsach. W momencie przechwycenia takich danych przez napastnika, są one całkowicie podatne na odczyt, z uwagi na brak zastosowania szyfrowania (SSL/TLS). Nawet jednorazowe logowanie na portalu bez zaimplementowanego HTTPS może zakończyć się przechwyceniem pakietu zawierającego jawne dane – login oraz hasło. Zastosowanie HTTPS w znaczącym stopniu utrudnia, wręcz uniemożliwia (bez konkretnych kluczy docelowego odbiorcy) odszyfrowanie tych danych, co chroni użytkowników przed omówionymi niebezpieczeństwami.

OCHRONA DANYCH OSOBOWYCH

Dane przechowywane w aplikacjach to bardzo często dane wrażliwe. Wprowadzone w 2018 roku rozporządzenie RODO zdefiniowało kary za niedopatrzenia w zakresie ochrony danych osobowych. W dobie przepływu ogromnych danych wrażliwych przez systemy informatyczne, kryptografia staje się fundamentem ochrony prywatności. Algorytmy szyfrowania muszą zadbać o bezpieczeństwo danych nie tylko w ruchu, ale również w spoczynku.

Do tego celu wykorzystane mogą być specjalistyczne urządzenia kryptograficzne HSM (ang. Hardware Security Module), które umożliwiają zaimplementowanie transparentnego szyfrowania na danych. Proces ten umożliwia natychmiastowe udostępnienie danych tylko osobom upoważnionym (np. programistom) przy zachowaniu pełnego szyfrowania, gdy dane nie są wykorzystywane lub gdy próbuje się do nich dostać osoba trzecia. Co do zabezpieczania danych w ruchu, istotne jest zastosowanie szyfrowania end-to-end w przypadku danych wrażliwych. Odpowiednia kombinacja szyfrowania symetrycznego oraz asymetrycznego wraz z generowaniem materiału kryptograficznego potrzebnego do zabezpieczenia danych po stronie użytkownika umożliwia utworzenie w pełni bezpiecznego i hermetycznego środowiska wymiany informacji.

Na żadnym z elementów procesu transferu danych z punktu A do punktu B niemożliwe jest odszyfrowanie danych. Dopiero upoważniony odbiorca może je zrozumieć. Połączenie tych dwóch technik znacząco może wpłynąć na bezpieczeństwo całego systemu i działać prewencyjnie w przypadku częstych w obecnych czasach ataków hakerskich.

SYSTEMY AUTORYZACJI

W obszarze systemów informatycznych kluczowe są systemy autoryzacji, w któ-

rych niezbędne jest wykorzystanie kryptografii. Odgrywa ona niezwykle istotną rolę w zabezpieczeniu procesów logowania i wymiany danych wykorzystywanych do weryfikacji autentyczności użytkownika. Urządzenia kryptograficzne HSM miały swój historyczny początek w bankomatach.

Zabezpieczały proces wpisywania numeru PIN do karty, co potem przerodziło się w globalny system bankomatowy i znaną dzisiaj bankowość internetową. Dzięki kryptografii w systemach autoryzacji możliwe jest identyfikowanie użytkowników systemów poprzez wykorzystanie kombinacji hasła i loginu oraz ewentualnych weryfikacji dwuetapowych, co jest niezbędne w erze cyfrowej.

PODPISY ELEKTRONICZNE

Kolejnym elementem kryptografii w życiu codziennym i ostatnim omówionym w artykule jest podpis elektroniczny. Ten sposób weryfikacji autentyczności dokumentu jest coraz bardziej popularny w życiu codziennym, między innymi przez rosnące ilości spraw, które są możliwe do zrealizowania przez Profil Zaufany.

Technologia e-podpisów pozwala na objęcie dokumentu cyfrową warstwą ochronną, zweryfikowaną naszą tożsamością, co pozwala na określenie osoby podpisującej dokument z zachowaniem wiązania prawnego. Dzięki wykorzystaniu podpisów elektronicznych użytkownicy takich rozwiązań otrzymują bezpieczny rodzaj dystrybucji dokumentów w sposób integralny, oszczędzając przy tym czas i pieniądze potrzebne na drukowanie i wysyłkę pism czy umów do odbiorców.

PODSUMOWANIE

Kryptografia dziś jest nieodłączną częścią naszego życia. Pełni ona ważną rolę w zabezpieczeniu procesów, zapewnianiu poufności i integralności danych. Jest nieoczywistym strażnikiem, który zapewnia wewnętrzny spokój i uczucie zaufania w trakcie korzystania ze środowisk online.

W firmie Cyber Security Lab doskonale rozumiemy te wyzwania i skutecznie realizujemy zasadę „bezpieczne oprogramowanie – pewne jutro", oferując spersonalizowane rozwiązania kryptograficzne zintegrowane z aplikacjami komputerowymi. Dążąc do doskonałości w dziedzinie bezpieczeństwa danych zapewniamy nie tylko innowacyjność w naszych rozwiązaniach, ale także niezawodność w zakresie ochrony informacji.

SECURITYMAGAZINE.PL

NAJPOWAŻNIEJSZE CYBERATAKI W 2023 ROKU. POLSKA I ŚWIAT

Redakcja
SECURITY MAGAZINE

Eksperci mówią jasno: w 2023 roku doszło do ponad 50 proc. więcej cyberataków niż w roku 2022. Na celowniku przestępców znalazły się zarówno duże firmy, jak i banki, szpitale czy podmioty samorządowe i rządowe. Co jeszcze wydarzyło się w 2023 roku?

2023 ROK REKORDOWY POD WZGLĘDEM CYBERATAKÓW

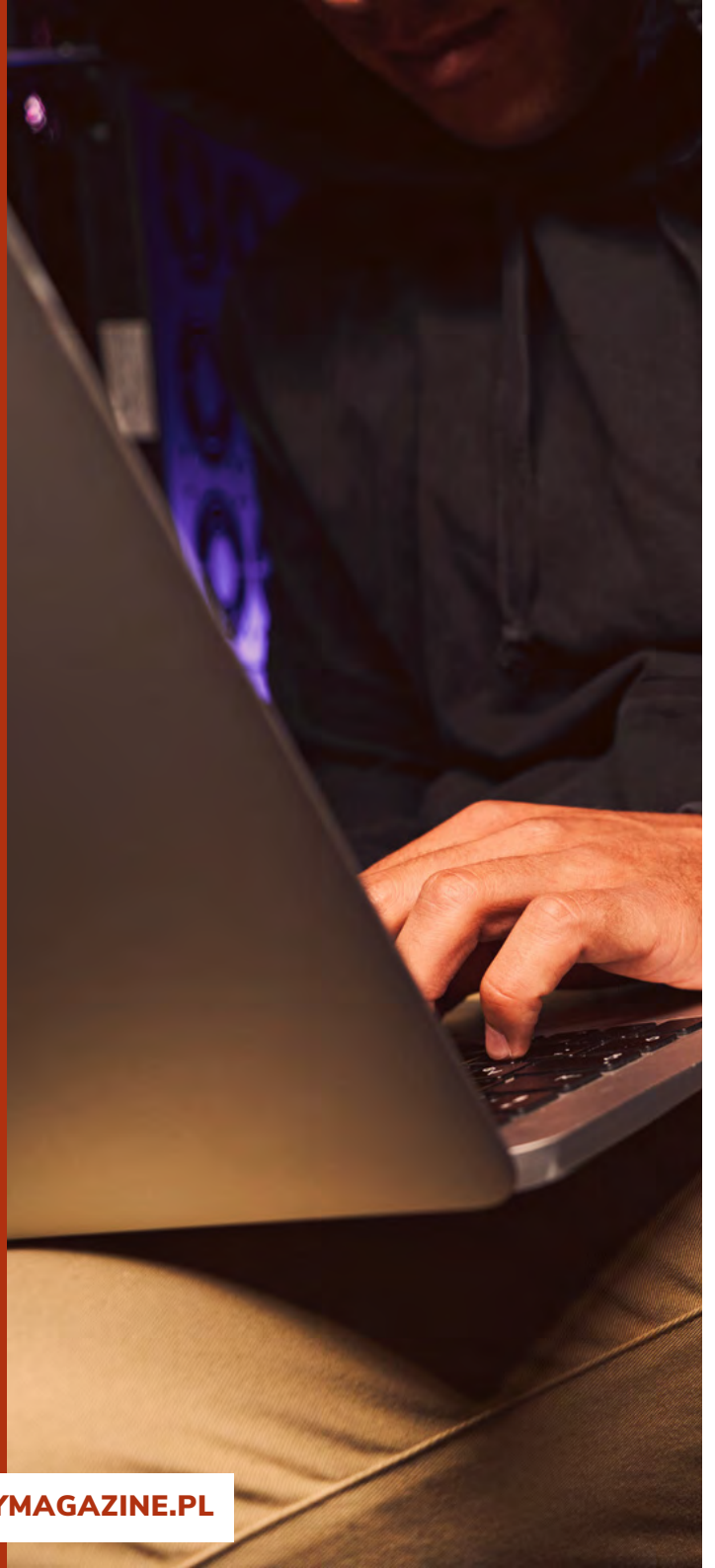
W 2023 o ponad 51 proc. wzrosła liczba ataków typu ransomware. Na celowniku cyberprzestępców, jak twierdzi Crowdstrike, firma zajmująca się cyberbezpieczeństwem, były głównie duże firmy, banki, szpitale czy agencje rządowe. Co więcej, Chainalysis, organizacja analityczna, która śledzi różne branże i finanse, w tym kryptowaluty, wyjawiła, że w 2023 roku mieliśmy do czynienia również z dużym wzrostem płatności na rzecz hakerów i okupów. Cyberprzestępcy otrzymali od firm prawie 500 mln dol. za to, aby przywrócić działanie infrastruktury IT.

O tym, że 2023 rok był dobrym rokiem dla cyberprzestępców świadczy także słowa Nikesha Arory, dyrektora generalnego firmy Palo Alto Networks, zajmującej się m.in. bezpieczeństwem sieciowym. Stwierdził on, że w ubiegłym roku aktywność cyberprzestępców była najwyższa w historii. - *Zwłaszcza jeśli chodzi o oprogramowanie ransomware do cyfrowych okupów. Cyberprzestępcy wyrządzili szkody w znacznie krótszym czasie* - powiedział.

HOT TOPIC I FAŁSZOWANIE DANYCH

Dowodem potwierdzającym te słowa niech będzie nasze zestawienie 10, naszym zdaniem, największych cyberataków na świecie i w Polsce. Nasze zestawienie zacznijmy od portalu Hot Topic. Między lutym a czerwcem serwis mierzył się z falą ataków polegających na fałszowaniu danych uwierzytelniających.

Do wykrycia ataku doszło, ponieważ jeden z użytkowników zgłosił podejrzaną aktywność związaną z logowaniem na jego platformie z nagrodami. 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 płatniczej (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.

NARUSZENIE MOVEIT

W 2023 roku głośno było również o tzw. naruszeniu MOVEit. Rosyjska grupa ransomware o nazwie „CI0p" wykorzystała odkrytą w maju lukę w pakiecie produktów MOVEit firmy Progress Software do kradzieży danych z niezabezpieczonych sieci.

Zaatakowanych zostało ponad 400 organizacji, a do tego opublikowano wrażliwe dane wielu osób. Atak na MOVEit należy do jednych z ciekawszych w ostatnim czasie, ponieważ dotknął wiele organizacji na świecie. Według niemieckiej firmy badawczej KonBriefing zajmującej się cyberbezpieczeństwem na chwilę obecną włamanie do MOVEit dotknęło 421 organizacji (z czego aż 322 w USA) i 22 miliony kont.

NAJWIĘKSZY WYCIEK DANYCH W SEKTORZE FINANSÓW

W minionym roku doszło także chyba do największego wycieku danych w historii sektora finansowego. Mowa tu o Citibanku, który w wyniku naruszenia bezpieczeństwa ujawnił poufne informacje dotyczących milionów klientów.

W wyniku cyberataku zostały ujawnione numery kont, dane osobowe, a nawet historie transakcji. Śledztwo wykazało, że bank stał się ofiarą złożonego ataku hakerskiego, który wykorzystał słabe punkty w infrastrukturze IT banku. Co prawda Citibank starał się ograniczyć szkody, ale sam incydent wywołał globalną i bardzo poważną dyskusję o bezpieczeństwie danych w sektorze bankowym.

W 2023 roku na celowniku cyberprzestępców znaleźli się również dostawcy infrastruktury internetowej Google Cloud, Cloudflare oraz AWS zgłosili 10 października największe w historii ataki DDoS, w którym liczba żądań na sekundę (rps) osiągnęła najwyższą wartość ponad 398 milionów, co stanowi siedem i pół raza więcej niż poprzedni rekordowy Atak DDoS.

CSO Cloudflare Grant Bourzikas napisał w poście na blogu Google, że „kluczowe" jest zrozumienie, że atak mógł być przeprowadzony z użyciem „botnetu skromnej wielkości, składającego się z około 20000 maszyn".

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

JEDEN Z NAJWIĘKSZYCH CYBERATAKÓW W RAMACH WOJNY NA UKRAINIE

W kolei grudniu 2023 r. miał miejsce jeden z największych cyberataków w ramach wojny na Ukrainie. Celem padł telekomunikacyjny gigant Kyivstar. Podano wysokość strat finansowych związanych z incydentem. Ilija Witiuk, szef departamentu cyberbezpieczeństwa SBU, w rozmowie z agencją Reutera przekazał, że hakerzy byli obecni w sieci Kyivstar od co najmniej maja

2023 r.

Dostęp do infrastruktury umożliwiał im kradzież danych. Jakich? Mowa o m.in. przechwytywaniu SMS-ów klientów. Wśród ekspertów i obserwatorów panuje przekonanie, że omawiany cyberatak należy uznać za jeden z najpoważniejszych na Ukrainie od momentu rosyjskiej inwazji z 24 lutego 2022 r.

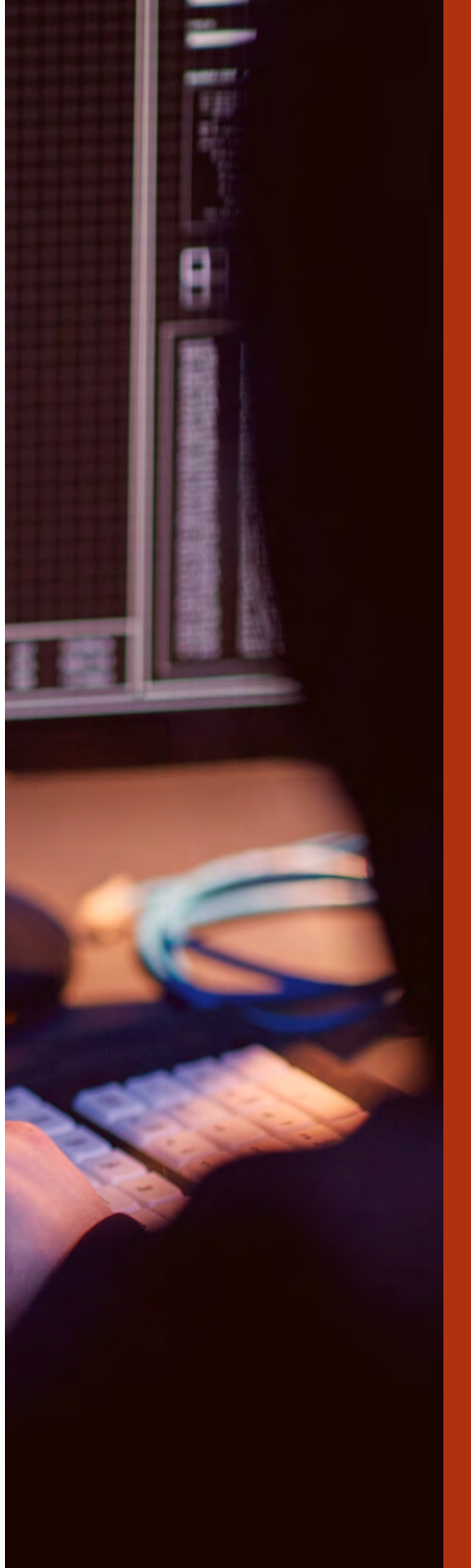
ALAB LABOLATORIA I NARUSZENIE DANYCH MEDYCZNYCH

Jeśli chodzi o Polskę, to zdecydowanie miano najgłośniejszego ataku w 2023 pozyskał ten na ALAB Laboratoria — jedną z największych ogólnopolskich sieci laboratoriów medycznych. Firma padła ofiarą cyberataku skutkującego wyciekiem danych medycznych. W ramach przeprowadzonego ataku wykradzione zostały całe pakiety danych osobowych Polaków z ostatnich sześciu lat. Wśród nich znajdują się imiona, nazwiska, numery PESEL i adresy zamieszkania pacjentów wraz z przypisanymi do nich wynikami badań. Jak podawały media, autorami ataku była grupa ransomware RA World. Opublikowali oni bowiem na swoim blogu nie tylko informację o skutecznym włamaniu, ale także ujawnili próbkę wykradzionych danych.

Ostatecznie okazało się, że wyciek danych dotyczył nie tylko niemal 200 tysięcy numerów PESEL, ale także 190 GB danych firmowych samego ALAB-u.

NA CELOWNIKU CYBERPRZESTĘPCÓW POLSKIE UCZELNIE

Powyższy przykład jest tylko wierzchołkiem góry lodowej. Wiele firm, ze względu na potencjalne straty finansowe i wizerunkowe woli się nie chwalić, że było przedmiotem cyberataku. Tak było, chociażby z Akademią Sztuki Wojennej w Warszawie. Przez półtora miesiąca uczelnia ukrywała, że padła ofiarą największego znanego ataku na wojskową strukturę w Polsce.



Atak był też na tyle poważny, że praktycznie sparaliżował pracę Akademii. Zainfekowane zostały wszystkie komputery znajdujące się w jej sieci. Do ataku doszło, ponieważ uczelnia pozostawiła w użyciu przestarzały sprzęt i niewspierane oprogramowanie systemowe, pozbawione aktualizacji i łatek bezpieczeństwa.

Specjaliści ustalili, że wykorzystane zostało złośliwe oprogramowanie typu wiper. W takim przypadku celem ataku jest sprawienie, aby zaatakowana organizacja na stałe straciła dostęp do danych. Jest to przeciwieństwo ataku ransomware, w którym dane mogą być przywrócone po opłaceniu okupu. Wiper niszczy zainfekowane dane raz na zawsze poprzez zaszyfrowanie lub nadpisanie ich zawartości, a hakerzy, atakując przestarzałe systemy operacyjne mogą uniemożliwić w ten sposób dostanie się do jakichkolwiek danych na komputerze.

W 2023 roku zaatakowano nie tylko Akademię Sztuk Wojennych. Na celowniku cyberprzestępców znalazł się także Uniwersytet Artystyczny im. Magdaleny Abakanowicz w Poznaniu. Po przełamaniu zabezpieczeń hakerzy naruszyli ochronę informacji dotyczących kilkuset pracowników i współpracowników uczelni.

Na wyciek zostały narażone dane osobowe jak nazwiska, adresy czy seria i numer dowodu osobistego. Atak doprowadził do kilkudniowej blokady infrastruktury informatycznej uniwersytetu, a zagrożone środowisko serwerowe obsługujące system kadrowo-płacowy musiało zostać wyeliminowane i postawione na nowo. Było to możliwe dzięki istnieniu kopii zapasowej.

.

CYBERATAK NA SYSTEM ŚLĄSKIEJ KARTY USŁUG PUBLICZNYCH

Cyberprzestępcy zaatakowali system Śląskiej Karty Usług Publicznych, służącej między innymi do płatności za parkowanie czy bilety komunikacji miejskiej w Metropolii Górnośląsko-Zagłębiowskiej. Blokada utrudniała codzienne życie prawie 2 milionów mieszkańców tego obszaru przez niemal dwa tygodnie. System przywrócono do działania przy pomocy tworzonych codziennie kopii zapasowych, a dane osobowe pasażerów nie były zagrożone tylko dzięki temu, że system ich nie gromadził.

W 2023 roku celem ataku cyberprzestępców, a dokładniej rosyjskiej grupy Killnet, stała się Grupa Azoty Police, czyli zakłady chemiczne w Policach należące do kontrolowanej przez Skarb Państwa Grupy Azoty. „Azoty" są największą spółką chemiczną w Polsce i drugim pod względem wielkości producentem nawozów w Unii Europejskiej.

Killnet stwierdził, że wykradł dane pracowników, w tym hasła, dodatkowo sparaliżował sieć korporacyjną dla zatrudnionych w Grupie Azoty Zakłady Chemiczne Police. *„Mamy nadzieję, że w fabryce coś wybuchnie i będzie mniej agresywnej szumowiny na świecie"* – napisali hakerzy na Twitterze. Na szczęście cyberprzestępcom nie poszło tak dobrze, jak utrzymywali. Finalnie, „Azoty" potwierdziły próby włamania do systemu, zapewniając jednocześnie, że atak nie był skuteczny.

NAJLEPSZE PRAKTYKI BEZ ZMIAN

2023 rok pokazał, że trzeba zachować wyjątkową ostrożność w sieci. Jeden mały błąd może skutkować poważnymi konsekwencjami. Co więcej, eksperci zgodnie twierdzą, że w 2024 roku częstotliwość cyberataków wcale się nie zmniejszy, ponieważ ransomware wciąż pozostaje główną działalnością zarobkową dla cyberprzestępców, a to oznacza, że wszystkie porady dotyczące kopii zapasowych systemu, utrzymywania w pełni zaktualizowanego oprogramowania, edukowania pracowników w zakresie rozpoznawania inżynierii społecznej we wszystkich jej formach oraz fundamentalnie zorientowanych na bezpieczeństwo pozostają tak samo ważne, jak w poprzednich latach.

EKSPERCI WYDANIA

PRZEMYSŁAW KANIA
Dyrektor Generalny
Cisco w Polsce

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

JACEK STAROŚCIC
CEO
Perceptus

Zarządza firmą cybersecurity, która zabezpiecza infrastrukturę IT wielu organizacji biznesowych i podmiotów publicznych realizując m.in. usługi SOC certyfikowane zgodnie z normą 27001 i dostarcza mobilne data center, wyróżnione jako rozwiązanie Best in Cloud przez Computerworld.

PIOTR BROGOWSKI
Dyrektor zarządzający
i wiceprezes
Orion Instruments Polska

Dyrektor zarządzający i wiceprezes firmy specjalizującej się w systemach cyberbezpieczeństwa, zwłaszcza SIEM, SOAR i Threat Intelligence. Autor wielu publikacji i wystąpień dotyczących bezpieczeństwa informacji i ochrony danych. Współautor podręcznika ISSA Polska „Bezpieczeństwo IT. Poradnik”.

KRZYSZTOF BRYŁA
GM
2BeAware

Manager i lider, ekspert, trener, mentor w obszarach bezpieczeństwa i IT. Wieloletnim doświadczeniem dzieli się na konferencjach i publikując na LinkedIn. Rozwija programy security awareness, kładąc nacisk na zrozumienie pomiędzy bezpieczeństwem, IT, OT a biznesem. Angażuje się w działania: CISO#Poland, CONLEA, ISSA. Członek rady programowej CyfrowegoSkauta.

EKSPERCI WYDANIA

ANDRZEJ MENDAK
Dyrektor Oddziału
UNICARD SA w Poznaniu

Z firmą UNICARD związany od 2000 roku. Od 2008 kieruje Oddziałem UNICARD SA w Poznaniu. Odpowiedzialny za konsulting i sprzedaż w obszarze systemów Kontroli Dostępu i Rejestracji Czasu Pracy.

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.

BEATA ŁASZYN
Wiceprezeska
Alert Media Communications

Ekspertka komunikacji kryzysowej – od przygotowania do kryzysów, przez wsparcie w komunikacji, po audyty pokryzysowe. Wykonuje analizy, opracowuje strategie komunikacji. Współautorka poradnika „e-Kryzys. Jak Zarządzać Sytuacją Kryzysową w Internecie” Wiceprezeska Alert Media Communications.

ŁUKASZ ZAJDEL
Dyrektor Sprzedaży
Perceptus

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

EKSPERCI WYDANIA

TOMASZ FILIPÓW
CEO
DISKUS Polska, ProDevice

Założyciel firmy DISKUS Polska Sp. z o.o., która dzięki sprawnemu zarządzaniu oraz jasno określonej wizji rozwoju spółki, stała się światowym liderem w produkcji urządzeń ProDevice do usuwania danych (demagnetyzery) oraz fizycznego niszczenia nośników pamięci (niszczarki). W 2018 roku otworzył Centrum R&D zlokalizowane w Wieliczce.

MATEUSZ JAKUBIK
Compliance Officer
Bonnier Business Polska

Doktorant na Wydziale Prawa i Administracji UJ w Krakowie, tam zajmuje się tematyką ODO oraz prywatności. Bierze czynny udział w pracach podgrup ds. ram polityki, ds. badań, innowacyjności i wdrożeń oraz ds. umiejętności cyfrowych w zespole eksperckim Ministerstwa Cyfryzacji ds. programu działań w zakresie AI.

ALEKSANDER WOJDYŁA
IT Security Consultant
Securitum

Doświadczony tester penetracyjny i wykładowca cyberbezpieczeństwa. Posiada umiejętności w identyfikowaniu i łagodzeniu luk w zabezpieczeniach. Jako prelegent na kursach dzieli się wiedzą, pomagając rozwijać umiejętności w walce z cyberprzestępczością. Zainteresowania: hakowanie IoT oraz prawo, co pozwala mu na ciągłe poszerzanie wiedzy i bycie na bieżąco z trendami.

OLIVER DEDOWICZ
CEO
Cyber Security Lab

Specjalista ds. cyberbezpieczeństwa, analityk rozwiązań informatycznych. Ma doświadczenie w realizacji prac B+R+I w ramach projektów informatycznych. M.in.: sporządzał pogłębione analizy oraz badania techniczne, zestawienia funkcjonalne, badania porównawcze, testy i analizy dotyczące cyberbezpieczeństwa, oprogramowania i środowisk teleinformatycznych.

EKSPERCI WYDANIA

MARTA SIEKACZ
Dyrektor Działu Marketingu
Perceptus

Aktywnie działa w obszarze e-commerce i cybersecurity, kreując komunikację marek do klientów biznesowych i testując nowoczesne narzędzia ułatwiające sprawne działanie i wymianę informacji w zdigitalizowanym, często międzynarodowym środowisku.

MIŁOSZ JARZĄB
Cyber Security Analyst
Aon Polska

Magister inżynier cyberbezpieczeństwa. Jako Cyber Security Analyst w Aon Polska specjalizuje się w analizie ryzyka cybernetycznego, opracowując analizy podatności firm na podstawie ich śladu w internecie. Jest aktywnym członkiem (ISC)2 oraz ISSA Polska.

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

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

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.

ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ

Wydanie 2/2022
POBIERZ

Wydanie 3/2022
POBIERZ

Wydanie 4/2022
POBIERZ

Wydanie 5/2022
POBIERZ

Wydanie 6/2022
POBIERZ

Wydanie 7/2022
POBIERZ

Wydanie 8/2022
POBIERZ

Wydanie 9/2022
POBIERZ

Wydanie 1(10)/2023
POBIERZ

Wydanie 2(11)/2023
POBIERZ

Wydanie 3(12)/2023
POBIERZ

Wydanie 4(13)/2023
POBIERZ

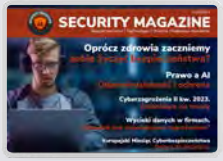
Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

Wydanie 7(16)/2023
POBIERZ

Wydanie 8(17)/2023
POBIERZ

Wydanie 9(18)/2023
POBIERZ



Wydanie 10(19)/2023
POBIERZ

Wydanie 11(20)/2023
POBIERZ

Wydanie 12(21)/2023
POBIERZ

Wydanie 1(22)/2024
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