12(21)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Jak NASK chroni polski internet?
Wywiad z Maciejem Siciarkiem

Jak phishing świąteczny może wpłynąć na reputację Twojego e-biznesu?

Jak szyfrowanie kryptograficzne chroni zasoby firmy?

Secure by Design - bezpieczne oprogramowanie już od samej koncepcji

Architektura SASE jako nowy standard sieciowy

SPIS TREŚCI

Security News	4
Inicjatywa ECSM 2023 dotarła do 1,5 miliona osób. To europejski rekord!	7
Advanced Threat Summit 2023. Jubileuszowe spotkanie ekspertów cyberbezpieczeństwa	14
Jak NASK chroni Polski Internet? Wywiad z Maciejem siciarkiem	26
Efektywność energetyczna w biurze i w serwerowni	39
Jak oszuści wykorzystują karty podarunkowe do wyłudzeń w e-sklepach?	47
Architektura SASE jako nowy standard sieciowy	54
Secure by Design - bezpieczne oprogramowanie już od samej koncepcji	60
AI, zabezpieczenie chmur i ochrona przed hakerami	67
Jak szyfrowanie kryptograficzne chroni zasoby firmy?	73
Wykrywanie CVE przy użyciu nowoczesnych skanerów	78
Jak phishing świąteczny może wpłynąć na reputację Twojego e-biznesu?	97
Eksperci wydania	105

SZANOWNI PAŃSTWO,

w tym roku, jeszcze bardziej niż kiedykolwiek, zrozumieliśmy, jak ważne jest, aby być czujnym i przygotowanym na różnorodne scenariusze, zarówno w świecie wirtualnym, jak i w naszym bezpośrednim otoczeniu.

W wydaniu zamykającym 2023 rok znajdą Państwo nie tylko analizy i porady, ale także inspirujące historie i studia przypadków, które pokazują, jak można zastosować najlepsze praktyki bezpieczeństwa w Waszych firmach i organizacjach. Zachęcam do lektury, która, mam nadzieję, będzie dla Państwa źródłem wiedzy i inspiracji.

Na progu Nowego Roku 2024 pragnę życzyć Państwu, aby był to czas pełen spokoju, bezpieczeństwa i rozwagi. Niech nadchodzące miesiące będą okresem, w którym będziemy razem kontynuować naszą edukację i wzmacnianie świadomości w zakresie bezpieczeństwa. Niech to będzie rok, w którym nasza czujność i świadomość staną się naszym atrybutem.

W imieniu całej redakcji "Security Magazine" życzę Państwu zdrowych, bezpiecznych i radosnych Świąt Bożego Narodzenia oraz pomyślności w roku 2024.

Rafał Stępniewski

SZCZEGÓŁY STR. 109

CYBER COALITION 2023

"Cyber Coalition 2023" to coroczne ćwiczenie cyber wojsk państw NATO, które w tym roku odbywało się od 27 listopada do 1 grudnia. Polska pełniła rolę dowództwa dla państw regionu Europy Środkowej i Wschodniej, od Estonii po Bułgarię. Ćwiczenie, będące największym tego typu na świecie, obejmowało sojuszników z NATO, instytucje UE oraz państwa partnerskie, w tym Szwajcarię, Szwecję, Ukrainę i Japonię.

Scenariusz zakłada atak cybernetyczny na fikcyjne państwo sojusznicze, z działaniami opartymi na realnych zagrożeniach. Ćwiczenie "Cyber Coa-lition" wzmacnia zdolności Sojuszu Północnoatlantyckiego do odstraszania, obrony i przeciwdziałania zagrożeniom w cyberprzestrzeni.

BEZPIECZNA INTEGRACJA PSIE

Polska osiągnęła znaczący postęp w cyberbezpieczeństwie, skutecznie integrując swój Publiczny System Identyfikacji Elektronicznej (PSIE) z systemami jedenastu krajów UE. Ta integracja umożliwia Polakom bezpieczne logowanie do zagranicznych systemów identyfikacji za pomocą e-dowodu lub profilu zaufanego. Dotyczy to Belgii, Czech, Chorwacji, Danii, Estonii, Hiszpanii, Holandii, Luksemburga, Łotwy, Portugalii i Słowenii. Trwają prace nad rozszerzeniem integracji na inne kraje UE. Działania te, prowadzone przez Państwowy Instytut Badawczy NASK, wzmacniają międzynarodową współpracę w zakresie bezpieczeństwa. Notyfikacja PSIE z 2022 roku pozwala obywatelom notyfikowanych krajów UE na bezpieczne korzystanie z polskiego portalu Biznes.gov.pl.

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"

NOWA USTAWA O ZWALCZANIU NADUŻYĆ

Polska podjęła znaczący krok w kierunku wzmocnienia cyberbezpieczeństwa. Niedawno, bo 25 września 2023, przyjęta ustawa o zwalczaniu nadużyć w komunikacji elektronicznej stanowi istotną odpowiedź na potrzeby zwiększenia ochrony cyfrowej obywateli i organizacji. Ta inicjatywa legislacyjna przyczyni się do poprawy bezpieczeństwa w polskiej przestrzeni cyfrowej,

Ustawa wprowadza konkretne środki mające na celu zwiększenie bezpieczeństwa w obszarach takich jak SMS-y, połączenia telefoniczne, poczta elektroniczna i ogólnie dostępny internet. Wśród nich znajduje się nowy, łatwy do zapamiętania numer do zgłaszania podejrzanych wiadomości SMS - 8080, lista wzorców złośliwych wiadomości SMS tworzona przez CSIRT NASK, a także możliwość blokowania złośliwych wiadomości przez operatorów. W zakresie bezpieczeństwa połączeń telefonicznych, ustawa przewiduje listę numerów instytucji publicznych, które są chronione przed nadużyciami. W obszarze poczty elektronicznej, dostawcy usług muszą stosować mechanizmy SPF, DMARC i DKIM oraz zapewniać możliwość uwierzytelniania wieloskładnikowego.

– *Cieszy mnie, że wartość rozwiązań wprowadzonych przez CERT Polska, takich jak Lista ostrzeżeń czy możliwość zgłaszania niebezpiecznych wiadomości SMS, została jednoznacznie potwierdzona poprzez podniesienie ich rangi na mocy obecnej ustawy. Dzięki temu, jak również dzięki nowym narzędziom, takim jak tworzenie wzorców przeciwdziałających rozsyłaniu złośliwych SMS-ów, nasz zespół ma możliwość jeszcze skuteczniejszego blokowania zagrożeń cyfrowych na bardzo wczesnych etapach ich zarejestrowania* – wyjaśnił **Sebastian Kondraszuk, szef zespołu CERT Polska.**

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"

WYRÓŻNIJ SIĘ W BRANŻY
BEZPIECZEŃSTWA

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

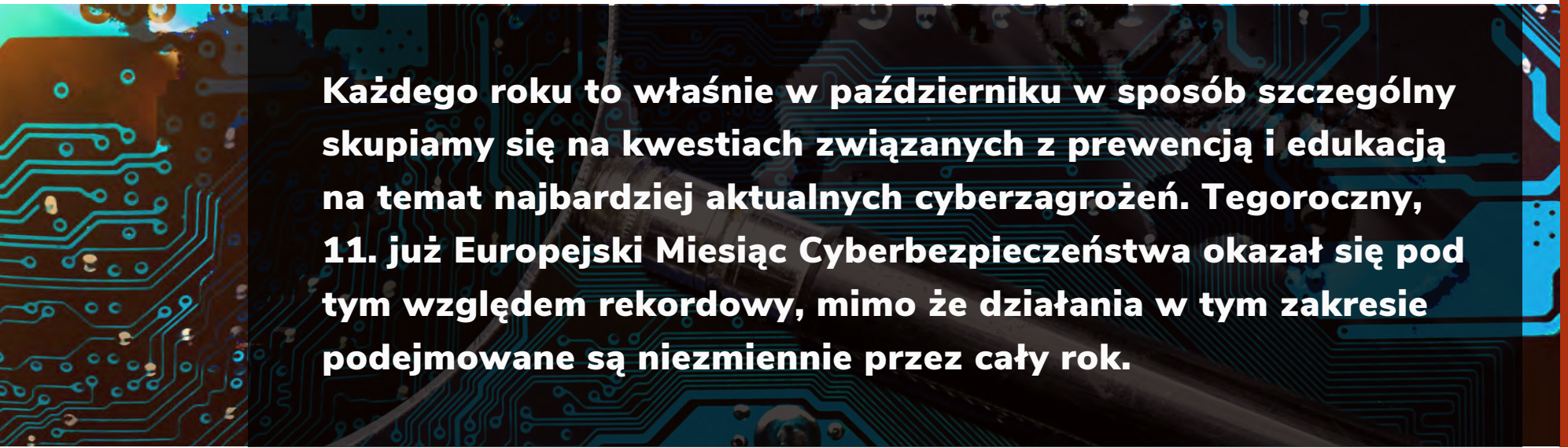
redakcja@securitymagazine.pl
+48 518 609 987

www.securitymagazine.pl

INICJATYWA ECSM 2023 DOTARŁA DO 1,5 MILIONA OSÓB. TO EUROPEJSKI REKORD!

Katarzyna Grabowska
NASK-PIB

Rafał Stępniewski
Security Magazine



Każdego roku to właśnie w październiku w sposób szczególny skupiamy się na kwestiach związanych z prewencją i edukacją na temat najbardziej aktualnych cyberzagrożeń. Tegoroczny, 11. już Europejski Miesiąc Cyberbezpieczeństwa okazał się pod tym względem rekordowy, mimo że działania w tym zakresie podejmowane są niezmiennie przez cały rok.

Inicjatywa ECSM 2023 dotarła do 1,5 miliona osób. To europejski rekord!

Europejski Miesiąc Cyberbezpieczeństwa (ECMS) to ogólnoeuropejska kampania edukacyjna organizowana przez agencję ENISA (European Union Agency for Cybersecurity) z inicjatywy Komisji Europejskiej, mająca na celu budowanie świadomości cyberzagrożeń i promowanie odpowiedzialnego korzystania z internetu wśród wszystkich jego użytkowników, a także dzielenia się dobrymi praktykami w obszarze cyberhigieny. W Polsce projekt koordynowany jest przez Państwowy Instytut Badawczy NASK.

Tegorocznym motywem przewodnim były zagadnienia związane z inżynierią społeczną (socjotechniką), czyli wykorzystaniem przez przestępców różnych technik manipulacji stosowanych w kampaniach phishingowych wycelowanych w użytkowników internetu. Hasło przewodnie ECSM 2023 to „Bądź mądrzejszy niż oszust" – zachęcające do mądrego i rozważnego korzystania z internetu.

REKORDOWY ROK 2023

Tegoroczna kampania Europejskiego Miesiąca Cyberbezpieczeństwa przebiła zeszłoroczny wynik polskich inicjatyw, rekordowy na skalę europejską. W tym roku w trakcie trwania polskiej edycji kampanii zgłoszonych zostało 81 inicjatyw edukacyjnych, które dotarły – według szacunków ich organizatorów – do ponad 1,5 miliona osób. Dla porównania – w zeszłym roku zgłoszono 73 projekty edukacyjne, a jeszcze rok wcześniej – 71.

Wśród zgłoszonych inicjatyw znalazły się:

- **publikacje materiałów edukacyjnych** (np. artykuły w „Security Magazine" czy na blogu KwestiaBezpieczenstwa.pl), część z nich odnaleźć można przez **bezpiecznymiesiac.pl**
- **webinary i lekcje** (np. Cyberprofilaktyka 3.0 czy Inteligentne Miasto i ScottieGO! z #kodujzUKE)
- **konferencje** (np. 5. edycja „Digital Festival", „Fortinet Security Day 2023" czy „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online")
- **wyzwania, które można podejmować** (np. misja PEGI udostępniona przez Stowarzyszenie Producentów i Dystrybutorów Gier Video, Awareness Game AR-IN-A BOX przeprowadzona przez NASK),
- a także **kampanie edukacyjne** (np. **kampania na temat bezpiecznych płatności** realizowana przez NASK we współpracy z CSIRT KNF i CBZC czy „Bądź cyberbezpieczny z Bankiem

Spółdzielczym").

ECSM 2023 – PATRONATY

Patronat nad ECSM 2023 objęły najważniejsze instytucje podejmujące odpowiedzialność za kwestie cyberbezpieczeństwa i edukacji w tym obszarze:

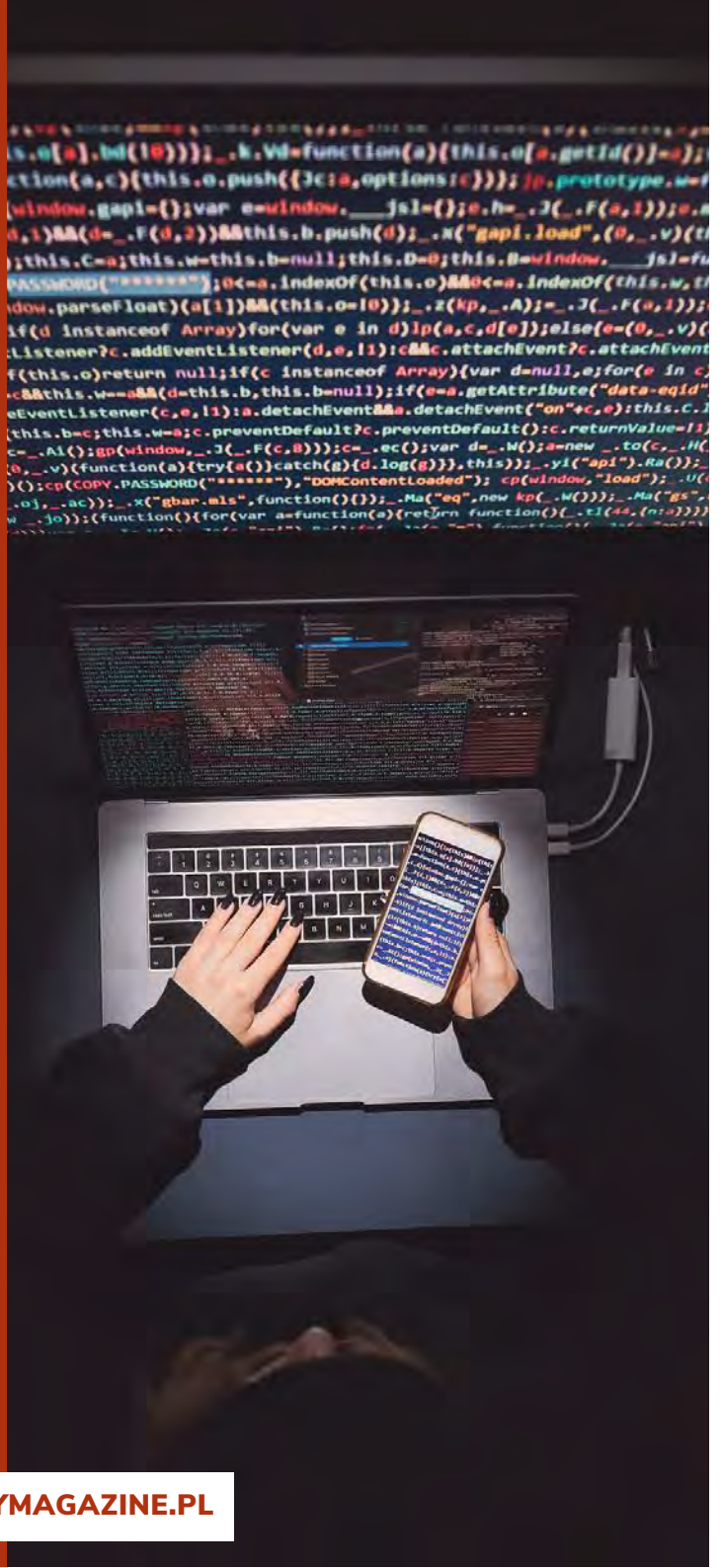
- Ministerstwo Cyfryzacji
- Ministerstwo Edukacji i Nauki
- Komisja Nadzoru Finansowego
- Fundacja Bezpieczna Cyberprzestrzeń
- Komendant Główny Policji
- Polskie Towarzystwo Informatyczne
- Związek Pracodawców Branży Internetowej IAB Polska
- Krajowy Związek Banków Spółdzielczych
- Warszawski Instytut Bankowości

PAMIĘTAJ, MIESIĄC BEZPIECZEŃSTWA TRWA CAŁY ROK

Dziękujemy wszystkim za aktywne włączenie się w 11. edycję kampanii Europejskiego Miesiąca Cyberbezpieczeństwa, a równocześnie zachęcamy do odwiedzania strony polskiej edycji ECSM.

– *Zakończenie obchodów Europejskiego Miesiąca Cyberbezpieczeństwa (ECSM) 2023 nie oznacza końca naszych działań. W świecie, w którym zagrożenia cyfrowe ewoluują szybciej niż kiedykolwiek, okres skupienia się na edukacji i prewencji w obszarze cyberzagrożeń trwa w rzeczywistości cały rok. W tym roku ECSM ugruntował zrozumienie, że cyberbezpieczeństwo to wspólna odpowiedzialność każdego z nas, od indywidualnych użytkowników po największe korporacje. Dlatego tak ważna jest współpraca z partnerami reprezentującymi różne sektory, tworzącymi treści dla wielu odrębnych grup odbiorców* – podkreśliła **Zuzanna Polak, kierowniczka Działu Budowania Świadomości Cyberbezpieczeństwa w NASK.**

Inicjatywa ECSM 2023 dotarła do 1,5 miliona osób. To europejski rekord!



Z myślą o wszystkich użytkownikach usług cyfrowych, którzy poszukują informacji na temat bezpieczeństwa, na polskiej stronie ECSM utworzona została **zakładka Baza Wiedzy** oferująca bogaty zbiór darmowych materiałów, które mają na celu podniesienie świadomości w zakresie cyberbezpieczeństwa każdego z nas.

Wśród ostatnio opublikowanych wymienić można:

- poradnik **„Internetowe love. Jak zadbać o swoje cyberbezpieczeństwo w relacjach online”**,
- poradnik **„Cyberbezpieczne wakacje 2023”**

Warto korzystać z tych materiałów i troszczyć się o swoje cyberbezpieczeństwo – i to przez cały rok!

“SECURITY MAGAZINE” PO RAZ KOLEJNY DOŁĄCZYŁO DO ECSM

Po raz drugi nasza redakcja dołączyła do inicjatywy Europejski Miesiąc Cyberbezpieczeństwa, która w Polsce koordynowana jest przez NASK. W ubiegłym roku zgłosiliśmy wydanie październikowe jako nasz wkład w popularyzację wiedzy w temacie cyberzagożeń i jak się przed nimi bronić.

W tym roku zaprosiliśmy do współpracy firmy, z którymi realizowaliśmy już wiele innych projektów. Nasi partnerzy przygotowali inspirujące artykuły i materiały multimedialne dotyczące cyberbezpieczeństwa.

Artykuły z cennymi wskazówkami, poradami i wartościowymi informacjami znalazły się **w październikowym wydaniu,**

materiały multimedialne – w naszych mediach społecznościowych, naszych partnerów i patronów. Przez cały miesiąc prezentowaliśmy materiały z poradami dotyczącymi socjotechnik, w szczególności na jakie zagrożenia zwracać uwagę.

Współpracowaliśmy z firmami i ekspertami:

- Grandmetric,
- Perceptus,
- Marken Systemy Antywirusowe - Bitdefender Polska,
- Adrian Sroka,
- Sygnisoft SA,
- Barracuda,
- Secfense,
- Concept Data
- i Nomios Group.

I w tym miejscu chcę podziękować każdej firmie oraz każdej osobie za jej wkład i chęć dzielenia się wiedzą z naszymi czytelnikami. Współpraca przebiegła znakomicie. Ich determinacja we wspólny projekt to dowód na to, że branża cyberbezpieczeństwa jest otwarta na współpracę. Każdy z naszych partnerów wnosił unikalne doświadczenie oraz swoją perspektywę, co wzbogaciło nasze treści i pozwoliło na głębsze zrozumienie zagadnień związanych z cyberbezpieczeństwem.

Jesteśmy wdzięczni za ich profesjonalizm, gotowość do dzielenia się wiedzą i zaangażowanie w edukowanie społeczności. To dzięki nim nasze wydanie stało się kompendium wiedzy, które nie tylko informowało, ale i inspirowało do dalszego zgłębiania tematu cyberbezpieczeństwa.

Nasza współpraca pokazała, że razem możemy osiągnąć więcej i lepiej służyć naszym czytelnikom, dostarczając im wartościowych i aktualnych informacji. To właśnie dzięki takim partnerstwom możemy stale podnosić poziom świadomości na temat cyberzagrożeń i sposobów ich przeciwdziałania.

Efekty, jakie udało nam się osiągnąć, nie byłyby możliwe, gdyby nie wsparcie NASK-PIB oraz Centralnego Biura Zwalczania Cyberprzestępczości. To właśnie te organizacje objęły patronatem nasz projekt, co znacznie podniosło jego prestiż i zasięg.

Ich doświadczenie i autorytet w dziedzinie cyberbezpieczeństwa były dla nas nieocenione, a zaangażowanie pozwoliło dotrzeć do jeszcze szerszego grona odbiorców. Dzięki temu nasza inicjatywa zyskała dodatkowy wymiar i stała się jeszcze bardziej skuteczna w promowaniu bezpie-

czeństwa w cyberprzestrzeni.

Z JAKIM EFEKTEM?

9 - tyle firm dołączyło do naszego projektu wsparcia ECSM 2023

2 - to liczba patronów, którzy wspierali nasze działania w ramach ECSM 2023

12 - tylu ekspertów podzieliło się wiedzą i doświadczeniem w wydaniu październikowym

17 - tyle osób (oprócz ekspertów i łącznie z zespołem redakcyjnym) zaangażowało się w tworzenie tego wydania

117 - tyle stron liczyło wydanie październikowe

34 - tyle materiałów multimedialnych do social mediów dotyczących inżynierii społecznej przygotowaliśmy razem z naszymi partnerami

62025 - do tylu osób dotarliśmy naszymi kanałami w social mediach (LinkedIn, Facebook)

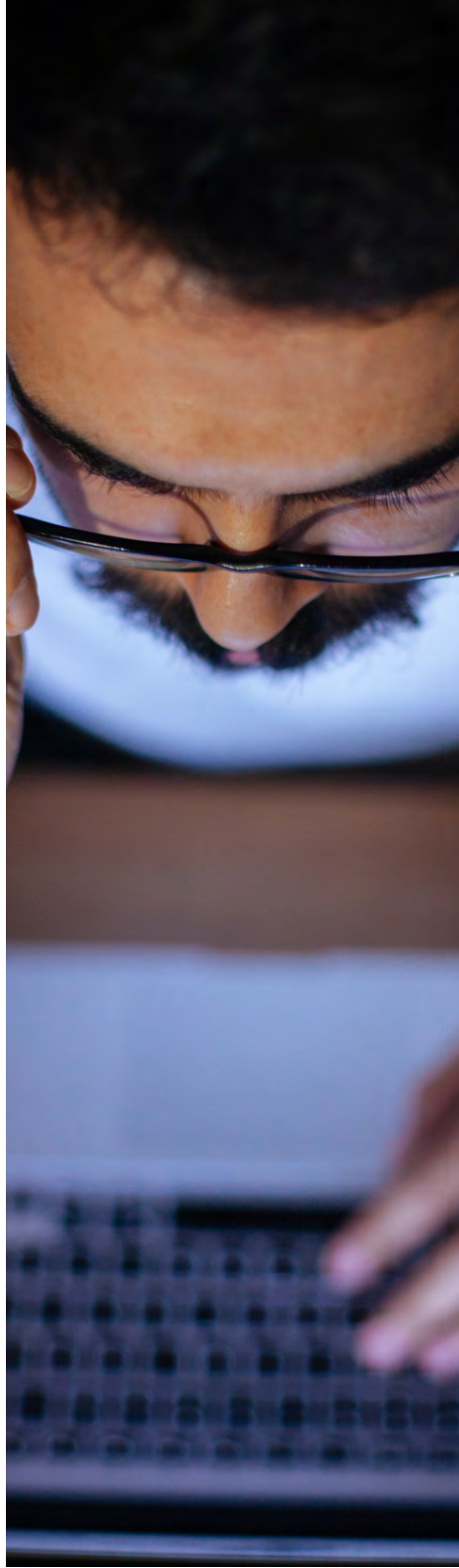
1002 - tyle osób otrzymało wiadomość e-mail z wydaniem październikowym

359072 - tyle osób dowiedziało się o wydaniu październikowym za pośrednictwem serwisów Polityka Bezpieczeństwa i Dziennik Prawny

30004 - tyle pobrań wydania zanotowaliśmy między 6 października a 1 listopada.

W ramach Europejskiego Miesiąca Cyberbezpieczeństwa 2023, "Security Magazine" po raz drugi z rzędu aktywnie włączyło się w promowanie świadomości na temat cyberzagrożeń. Nasze październikowe wydanie, wsparte przez NASK oraz Centralne Biuro Zwalczania Cyberprzestępczości, stało się platformą edukacyjną, dzięki której udało się dotrzeć do szerokiej publiczności. Nasza współpraca z renomowanymi firmami i ekspertami w dziedzinie cyberbezpieczeństwa zaowocowała stworzeniem wartościowych materiałów.

Dzięki ich profesjonalizmowi, udało się stworzyć kompendium wiedzy, które nie tylko informowało i nadal informuje (bo wydanie można przecież nadal pobrać), ale również inspirowało do dalszego zgłębiania tematu cyberbezpieczeństwa. To doświadczenie utwierdziło nas w przekonaniu, że współpraca i dzielenie się wiedzą są ogromną wartością dla budowania bezpieczniejszej przestrzeni online.



SECURITYMAGAZINE.PL

ADVANCED THREAT SUMMIT 2023. JUBILEUSZOWE SPOTKANIE EKSPERTÓW CYBER-BEZPIECZEŃSTWA

PATRONAT
SECURITY MAGAZINE

Fot. Evention (28)

22 i 23 listopada oraz 24 listopada - online, odbyła się 10. Jubileuszowa Edycja konferencji „Advanced Threat Summit”, uznawana za najważniejsze wydarzenie w dziedzinie cyberbezpieczeństwa w Polsce. Wydarzenie zgromadziło kilkuset osobowe grono ekspertów i profesjonalistów z zakresu bezpieczeństwa IT, reprezentujących przedsiębiorstwa, banki oraz instytucje finansowe i publiczne z całego świata.


CYBERBEZPIECZEŃSTWO
WSZECHOBECNE
22-24 LISTOPADA, 2023
WARSZAWA ONSITE-ONLINE
ADVANCED
THREAT
SUMMIT
II PANEL DYSKUSYJNY CSO COUNCIL - 2 PERSPEKTYWY
REGULACYJNA ŁAMIGŁÓWKA


OpenText Aviator
OpenText Content Aviator
Embrace a new way to interact with content and extract knowledge
Text Business Network Aviator
Revolutionize the internet of clouds via connectivity
enText IT Operations Aviator
Redefine all Level 1 business support (IT, HR, Sales)
OpenText DevOps Aviator
Elevate 30 million developers
enText Cybersecurity Aviator
Respond to threats in real time and ensure data is private and secure
penText Experience Aviator
Transform customer communications
JUBILEUSZOWA 10. EDYCJA
ADVANCED

Jubileuszowa edycja AT Summit, obchodząca swoje dziesięciolecie, wyróżniała się nie tylko ze względu na swój okrągły jubileusz, ale przede wszystkim dzięki bogactwu poruszanych tematów, dogłębnie opracowanych case studies oraz najlepszych praktyk w dziedzinie bezpieczeństwa IT. To wydarzenie stało się znaczącym punktem na mapie międzynarodowych konferencji, skupiającym uwagę profesjonalistów z całego świata.

Znaczącym aspektem tej edycji była obecność 100 ekspertów z największych firm działających na polskich oraz światowych rynkach. Taka reprezentacja świadczy o międzynarodowym znaczeniu i prestiżu konferencji.

W skład Rady Programowej konferencji AT Summit 2023 weszli: dr Magda Chelly - Responsible Cyber, Dariusz Czerniawski - Eurofins, Przemysław Dęba - Orange Polska, Karolina Doran - IBM Polska, Kraje Bałtyckie i Ukraina, Patryk Gęborys - EY, Przemysław Jaroszewski - Standard Chartered Global Business Services, Dariusz Jurewicz -

Patronat: Advanced Threat Summit 2023

HSBC Bank Polska, Paweł Kaczmarek - ING Bank Śląski, Marcin Kobyliński - Manpo-werGroup / ISSA Polska, Lech Lachowicz - PepsiCo, Barbara Nerć-Szymańska - ISACA Warsaw Chapter, Krzysztof Słotwiński - BNP Paribas, prof. Jerzy Surma - SGH, dr Jakub Syta - Akademia Marynarki Wojennej W Gdyni / ISSA Polska, Marcin Szydłowski - Booksy International oraz Jakub Teska - EY.

Wśród gości specjalnych znaleźli się: Gynvael Coldwind - HexArcana Cybersecurity GmbH, Tamara Hendriksen - Orange Cyberdefense, Jake Norwood - Booz Allen Hamilton, Mark Snel - Signify, Richard Stiennon - IT-Harvest i Liviu Vâlsan - CERN.

A wśród ponad 100 prelegentów konferencji, których nie sposób wymienić z osobna, znaleźli się reprezentanci między innymi firm i organizacji: European Union Agency for Cybersecurity, DPD, Evention, Urząd Komisji Nadzoru Finansowego, IBM, QuoIntelligence, Mastercard, Fortinet, Sandoz, Avon, ISSA Polska, ING Bank Śląski, Labyrinth, Linux Polska, EY Polska, ISACA Board of Directors, PepsiCo, TAURON Polska Energia, #CyberMadeInPoland, Akamai Technolgies, Orange Polska, (ISC)2 Chapter Poland, Huawei Technologies, ERGO Hestia, Paytel, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Safesqr, ESET, Netskope, SentinelOne, Uniwersytet Śląski, DAGMA Bezpieczeństwo IT, G2A.COM, Santander Bank Polska, CISCO, Volvo.

Eksperci ci dzielili się swoją wiedzą i doświadczeniem, oferując uczestnikom unikalne spojrzenie na aktualne i przyszłe wyzwania w dziedzinie cyberbezpieczeństwa. Wśród poruszanych tematów znalazły się takie

Patronat: Advanced Threat Summit 2023

kwestie jak rozwój technologii, cyberzagrożenia, ochrona danych oraz innowacyjne podejścia do zarządzania bezpieczeństwem informacji.

Case studies prezentowane podczas konferencji pozwoliły uczestnikom zrozumieć realne scenariusze i wyzwania, z jakimi borykają się organizacje na całym świecie. Analiza konkretnych przypadków dała możliwość zgłębienia wiedzy na temat skutecznych strategii i rozwiązań w dziedzinie cyberbezpieczeństwa. To praktyczne podejście było nieocenione dla profesjonalistów, którzy mogli zastosować zdobytą wiedzę w swoich codziennych działaniach.

Jubileuszowa edycja AT Summit była również platformą do wymiany najlepszych praktyk. Uczestnicy dyskutowali i dzielili się doświadczeniami. Networking i możliwość nawiązania nowych kontaktów biznesowych dodatkowo podkreślały wartość tego wydarzenia.

Podczas AT Summit uczestnicy mieli okazję wziąć udział w ponad 20 tematach dyskusji, 10 warsztatach oraz 12 spotkaniach w ra-


JUBILEUSZOWA 10. EDYCJA
ADVANCED
THREAT
SUMMIT


JUBILEUSZOWA 10. EDYCJA
ADVANCED
THREAT
SUMMIT
ATS


JUBILEUSZOWA 10. EDYCJA
ADVANCED
THREAT
SUMMIT

mach forum dobrych praktyk. Dodatkowo, wieczór specjalny z rozstrzygnięciem Jubileuszowego Konkursu AT Summit z rozdaniem nagród w kategoriach Ludzie, Projekty, Organizacje był jednym z najbardziej oczekiwanych punktów programu.

W tym roku szczególny nacisk położono na konsekwencje ekspansji cyberbezpieczeństwa poza tradycyjne obszary jego zastosowań. Eksperci podkreślali, jak cyberbezpieczeństwo staje się nieodłączną częścią działalności biznesowej, a także jak ogromna jest skala wyzwań w tym obszarze, zwłaszcza w kontekście narastającego kryzysu kadrowego oraz rosnącej liczby regulacji istotnych dla branży.

Przed rozpoczęciem konferencji, 21 listopada, odbyło się spotkanie i kolacja dla wszystkich prelegentów i panelistów w Hotelu Marriott Warszawa Centrum. Było to doskonałe miejsce do nawiązywania kontaktów i wymiany doświadczeń przed oficjalnym rozpoczęciem konferencji.

Organizatorem wydarzenia była firma Evention wraz ze stowarzyszeniem ISSA Polska, która zadbała o każdy szczegół, aby uczestnicy mogli w pełni skupić się na merytorycznej stronie konferencji. Uczestnicy mieli również możliwość uzyskania do 19 punktów CPE, co jest dodatkowym atutem dla profesjonalistów z branży.

10. Jubileuszowa Edycja Advanced Threat Summit 2023 była wydarzeniem pełnym wiedzy, inspiracji i możliwości nawiązania cennych kontaktów. Stanowiła platformę do dyskusji o aktualnych oraz przyszłych wyzwaniach w dziedzinie cyberbezpieczeństwa, a jej międzynarodowy charakter potwierdził znaczenie Polski na globalnej mapie cyberbezpieczeństwa.


CYBERBEZPIECZEŃSTWO


YPLOM
ATS


CYBERBEZPIECZEŃSTWO
WSZECHOBECNE
ATS


ADVANCED
THREAT

- Konferencja Advanced Threat Summit to nasze najważniejsze wydarzenie w temacie cybersecurity - można powiedzieć, że nasz okręt flagowy. Pozycjonujemy je na wydarzenie adresowane przede wszystkim w stronę czynnych menedżerów cybersecurity, którzy pracują w sektorze enterprise. Wiedzą, że to co robią, ma rolę służebną wobec biznesu, rozumieją ograniczenia czasu, zasobów ludzkich i budżetu. Dlatego agenda konferencji jest budowana (wspólnie z Radą Programową) wokół triady tworzonej przez 1. technologie, 2. procesy, procedury i regulacje (organizację) i 3. ludzi. Co roku mamy wielu świetnych prelegentów z zagranicy, ale trzon konferencji to przedstawiciele polskiego środowiska cybersec - szczególnie liczną grupą są członkowie społeczności CSO Council. Prace nad konferencją trwają przez 9-10 miesięcy - jest to wielki złożony projekt, angażujący cały team Evention. Cieszę się, że zrobiliśmy już 10 edycji konferencji, z rekordową dużą niedawną jubileuszową edycją. To wydarzenie od początku robimy wspólnie z ISSA Polska, której to organizacji zawsze jesteśmy wdzięczni za zaangażowanie i obecność. Natomiast sama konferencja jest też wspierana przez inne liczące się organizacje branżowe oraz praktycznie wszystkich liczących się dostawców technologii i usług cyberbezpieczeństwa - jest więc miejscem spotkania się całego rynku cybersecurity w Polsce - podsumował wydarzenie **Przemysław Gamdzyk, Meeting Designer & CEO Evention, organizator Advanced Threat Summit.**

Polityka® Bezpieczeństwa

ANALIZA FORMALNA WYCIEKU DANYCH

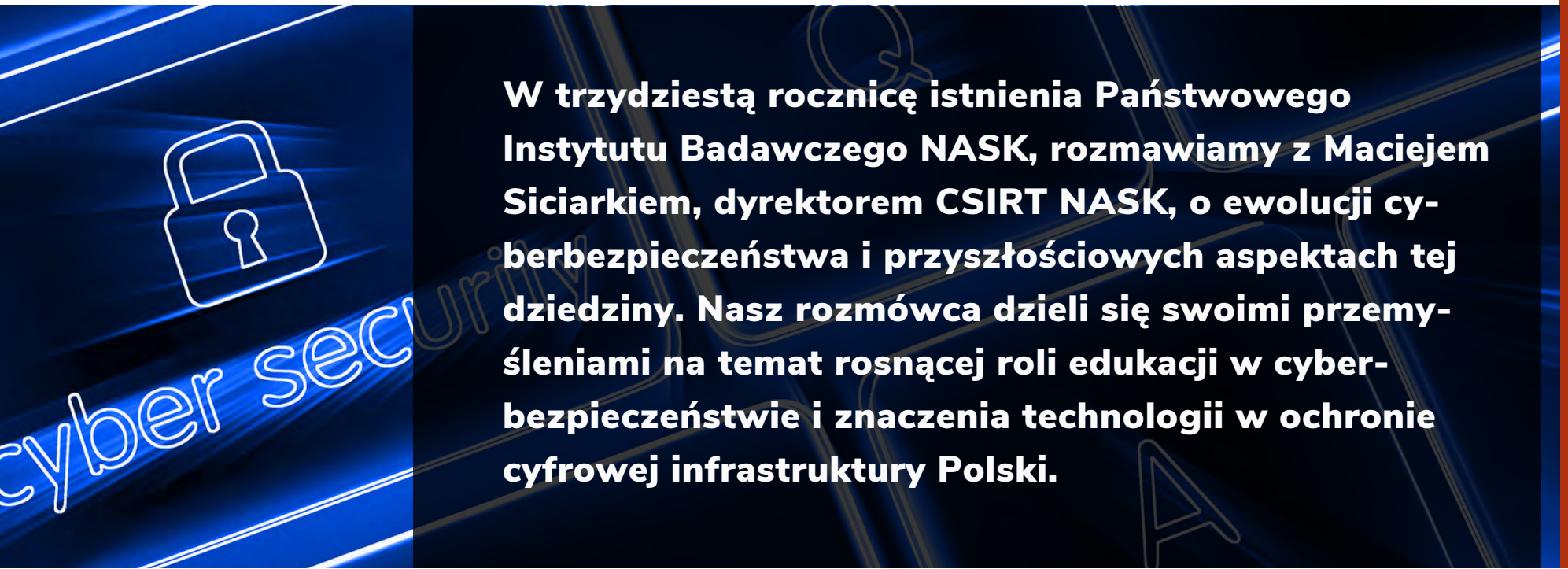
MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE...

POMOŻEMY

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

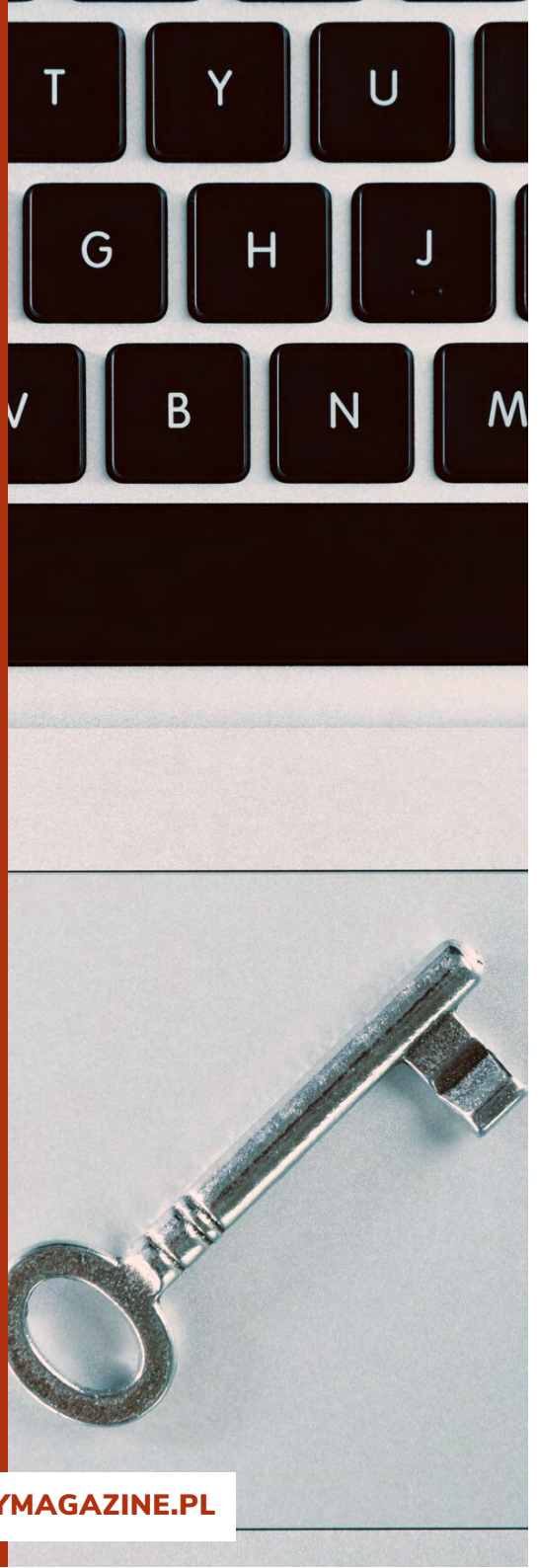
JAK NASK CHRONI POLSKI INTERNET? WYWIAD Z MACIEJEM SICIARKIEM

Maciej Siciarek
CSIRT NASK



W trzydziestą rocznicę istnienia Państwowego Instytutu Badawczego NASK, rozmawiamy z Maciejem Siciarkiem, dyrektorem CSIRT NASK, o ewolucji cyberbezpieczeństwa i przyszłościowych aspektach tej dziedziny. Nasz rozmówca dzieli się swoimi przemyśleniami na temat rosnącej roli edukacji w cyberbezpieczeństwie i znaczenia technologii w ochronie cyfrowej infrastruktury Polski.

Jak NASK chroni polski internet? Wywiad z Maciejem Siciarkiem



Państwowy Instytut Badawczy NASK to instytucja silnie utożsamiana z wiedzą ekspercką w zakresie cyberbezpieczeństwa. Od jak dawna zajmujecie się Państwo tą dziedziną?

Maciej Siciarek, dyrektor CSIRT NASK: NASK powstał dokładnie trzydzieści lat temu. Przeżywaliśmy wtedy w Polsce głębokie zmiany społeczne, polityczne i gospodarcze. Zlikwidowana została również bariera blokująca dostęp do nowych technologii, którymi kraje zachodnie żyły już od jakiegoś czasu. Polska podejmowała zatem nowe wyzwania i ktoś musiał zająć się również internetem, choć używano wtedy różnych innych określeń. Mało kto, oprócz wąskiego grona naukowców komunikujących się ze swoimi kolegami zza świeżo pękniętej żelaznej kurtyny, wiedział wtedy, co to jest, a już na pewno trudno było przewidzieć, że w ciągu kolejnych dekad przeżyjemy tak ogromną rewolucję cyfrową.

Grono zapaleńców związanych właśnie ze środowiskiem naukowym, skupionym m.in. wokół Uniwersytetu Warszawskiego, podjęło wyzwanie i tak stopniowo powstał NASK, który najpierw siebie, a potem innych w Polsce uczył, czym jest internet. Zajęcie się bezpieczeństwem teleinformatycznym, powstanie zespołu CERT Polska, czyli pierwszego w kraju zespołu reagowania na incydenty w sieci, oraz zdobywanie kompetencji w dziedzinie, którą dzisiaj określamy cyberbezpieczeństwem – wszystko to było konsekwencją właśnie tego wcześniejszego zaangażowania się w temat internetu.

Do dzisiaj w strukturach NASK działa założony w tamtym czasie zespół CERT Polska, który jest głównym elementem wypełniania roli CSIRT NASK, jednego z trzech CSIRT-ów poziomu krajowego, powołanych w mo-

mencie wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa. W praktyce oznacza to, że to właśnie do NASK, do CERT Polska, trafiają zgłoszenia o incydentach, czyli niebezpiecznych i potencjalnie szkodliwych dla użytkownika zdarzeniach w sieci. Informacje takie przekazują do CSIRT NASK zgodnie ze wspomnianą ustawą m.in. osoby prywatne oraz podmioty gospodarcze, ale też jednostki samorządowe, szkoły i uczelnie.

Jakie wyzwania związane z cyberbezpieczeństwem uważa Pan za najważniejsze w kontekście szybko rozwijającego się świata wirtualnego?

M.S.: Od ponad trzydziestu lat jesteśmy świadkami i uczestnikami rewolucji cyfrowej, a otaczająca nas rzeczywistość każdego roku staje się w jeszcze większym stopniu oparta o technologie cyfrowe. Wiąże się z tym wiele korzyści – zarówno dla firm i organizacji, jak i dla prywatnych użytkowników usług online. Natomiast misja Państwowego Instytutu Badawczego NASK pozostaje niezmienna. Od początku ambitne wyzwania, jakie sobie stawia NASK, to właśnie udział w cyfryzacji kraju, budowa wartościowych inicjatyw pokazujących pozytywne strony wykorzystania internetu oraz to, co niestety idzie w parze z tym postępem, czyli ochrona użytkowników przed niebezpieczeństwami, które niesie ze sobą świat sieci. Najważniejsze obecnie wyzwania to właśnie budowanie świadomości użytkowników internetu, nie tylko o korzyściach z używania cyfrowego świata, ale również o zagrożeniach w cyberprzestrzeni.

Docieramy do wszystkich grup wiekowych, od najmłodszych użytkowników sieci oraz ich rodziców i opiekunów, aż po seniorów. Oprócz tego istotne jest dla nas zdobywanie aktualnej wiedzy, ale też czynny udział w rozwoju najnowszych technologii. Cele te realizujemy poprzez badania naukowe, wdrożenia innowacyjnych produktów, działania społeczne oraz akcje edukacyjne.

Jakie są główne zagrożenia w zakresie cyberbezpieczeństwa, na które Polacy powinni obecnie zwracać uwagę?

M.S.: Tak jak wspomniałem, otrzymujemy zgłoszenia o niebezpiecznych zdarzeniach, czyli tak zwanych incydentach, zachęcamy też użytkowników sieci, by – traktując nas jako podmiot zaufany – nie obawiali się przychodzić do nas z tego typu informacjami. Dzięki temu, oprócz oferowania poszkodowanym pomocy czy porad, możemy na podstawie zgłoszeń budować wiarygodny obraz zagrożeń w cyberprzestrzeni i ostrzegać innych.

Z obecnych statystyk CSIRT NASK, zawartych m.in. w raportach i informacjach dostępnych na stronie zespołu CERT Polska, wynika, że w dalszym ciągu dominują ataki bazujące na socjotechnice, zwłaszcza działania phishingowe. W tym roku obsłużyliśmy już ponad trzy tysiące incydentów zaklasyfikowanych jako phishing. To zła wiadomość, ponieważ wszyscy jesteśmy narażeni na tego typu ataki, niezależnie od wieku, płci czy poziomu wykształcenia. I wszyscy możemy paść ich ofiarą.

Każdy z nas zapewne otrzymał w ostatnich miesiącach wyglądające w pierwszej chwili dość wiarygodnie wiadomości e-mail lub SMS, nakłaniające np. do zapłaty za prąd, przesyłkę czy inną usługę, które po wnikliwym przeanalizowaniu okazywały się oszustwem. Dlatego musimy dziś bardzo uważnie i krytycznie odnosić się do informacji, które otrzymujemy w przestrzeni cyfrowej.

Dobrą natomiast wiadomością jest to, że walka z oszustwami socjotechnicznymi nie wymaga stosowania bardzo wyrafinowanych technologii czy wydajnych urządzeń. Bazuje przede wszystkim na wiedzy i świadomości zagrożeń, a zatem możemy skutecznie im przeciwdziałać poprzez szeroko prowadzoną edukację i profilaktykę. To właśnie jeden z podstawowych elementów misji NASK, o których już wspomniałem. Działamy, edukujemy, ostrzegamy, uczymy – to wszystko na wiele różnych sposobów, począwszy od telewizyjnych reklam społecznych, artykułów w prasie, poprzez szkolenia i webinary, a skończywszy na licznych publikacjach.

Jesteśmy dość ostrożni w wyrażaniu optymizmu co do pełnej skuteczności podejmowanych akcji, bo przeciwnik szybko zmienia metody działania, do których my musimy się adaptować, ale zdecydowanie widzimy pozytywne rezultaty naszych starań.

Dodatkowo angażujemy się też w działania legislacyjne, których wymiernym efektem jest np. ustawa o nadużyciach w komunikacji elektronicznej, która weszła w życie we wrześniu tego roku. Nowe, lepsze prawo będzie zdecydowanie wspierać skuteczniejszą walkę z tego rodzaju oszustwami.

W przypadku firm i instytucji główne zagrożenia, takie jak malware, ransomware i ataki DDoS, pozostają niezmienne. Częściej niż kiedyś obserwujemy jednak działania typu spear phishing, wycelowane w konkretne osoby czy zespoły. Nowym zjawiskiem, wycelowanym zarówno w pojedyncze osoby, jak i organizacje, jest coraz częstsze wykorzystywanie przez przestępców sztucznej inteligencji oraz szersza dostępność różnorodnych form ataków, oferowanych na zasadzie usług realizowanych przez podwykonawców, czyli specjalizowane grupy przestępcze, np. Ransomware as a Service czy DDoS as a Service.

Jak Pan ocenia obecny poziom świadomości Polaków, a także polskiego biznesu na temat cyberbezpieczeństwa?

M.S.: Bazując na statystkach z otrzymywanych przez nas zgłoszeń, mogę powiedzieć, że ta świadomość rośnie. Trzeba tu wspomnieć, że zgłoszenia to nie tylko informacja od osoby czy podmiotu już bezpośrednio poszkodowanego przez cyberprzestępców, ale coraz częściej świadome przekazanie informacji o samodzielnie zidentyfikowanych zagrożeniach.

W 2021 roku zespół CERT Polska otrzymał 116 071 zgłoszeń, co przełożyło się na zarejestrowanie 29 483 incydentów. Oznacza to, że na jedno unikalne zidentyfikowane zagrożenie lub też incydent bezpieczeństwa z nim związany przekładają się niecałe cztery zgłoszenia.

W 2022 roku tych zgłoszeń było już 322 479. Wynikało to zarówno z faktu, że do 39 683 wzrosła liczba samych incydentów, jak też właśnie z rosnącej świadomości Polaków w tym obszarze. Średnio każdy notowany przez nas incydent lub zagrożenie były bowiem zgłaszane przez ponad osiem różnych osób.

W tym roku w dalszym ciągu obserwujemy dużą liczbę zgłoszeń – w ciągu trzech kwartałów otrzymaliśmy ich ponad 200 000, co potwierdza, że świadomość Polaków, m.in. dzięki działaniom edukacyjnym NASK oraz Ministerstwa Cyfryzacji, nadal rośnie.

Z drugiej strony główny nacisk kładziemy obecnie na usuwanie zagrożeń, zanim zetkną się z nimi użytkownicy usług cyfrowych. Wiele narzędzi technologicznych, takich jak tworzona przez CERT Polska i udostępniana m.in. operatorom telekomunikacyjnym lista ostrzeżeń, czy też rozwiązań prawnych, takich jak wspomniana już ustawa o zwalczaniu nadużyć w komunikacji elektronicznej, a także bezpośrednia, bardzo konkretna codzienna praca ekspertów zespołu CERT Polska, pozwalają nam jeszcze skuteczniej odcinać wiele zagrożeń i ataków, mimo że ich liczba również się zwiększa.

W jaki sposób NASK promuje bezpieczne praktyki wśród młodszych użytkowników internetu?

M.S.: Młodzi użytkownicy internetu są dla NASK szczególnie ważni i otaczamy ich wyjątkową troską. Liczny zespół spośród pracowników zatrudnionych w Instytucie zajmuje się właśnie działaniami mającymi poprawiać bezpieczeństwo cyfrowe najmłodszych – i to na wiele różnych sposobów.

Po pierwsze, edukujemy. Zarówno bezpośrednio, budując nasz przekaz do dzieci i młodzieży, jak i pośrednio – poprzez nauczycieli i rodziców. Stworzyliśmy wiele publikacji na temat cyberhigieny, które są dostępne bezpłatnie. To bogate i zróżnicowane materiały. Wśród propozycji NASK znajdziemy kursy dotyczące cyberbezpieczeństwa dla najmłodszych i nieco starszych dzieci tworzone w ramach OSE IT Szkoła, jak również Cyberlekcje 3.0 dla młodzieży, czyli zestawy gotowych materiałów dla nauczycieli do prowadzenia lekcji na wszystkich etapach nauki w szkole podstawowej i ponadpodstawowej. Wydajemy również poradniki dla rodziców i nauczycieli, okresowe raporty pomagające lepiej rozumieć tę rzeczywistość, czy też na bieżąco publikujemy w naszych mediach społecznościowych informacje i ostrzeżenia odnoszące się do bieżących problemów w sieci. Oprócz tego nasi eksperci prowadzą warsztaty z młodzieżą, aby przybliżać jej m.in. zasady cyberhigieny, pokazać metody przeciwdziałania przemocy w internecie czy pomóc w identyfikacji fałszywych informacji w mediach cyfrowych.

Po drugie, NASK, we współpracy z Ministerstwem Cyfryzacji, prowadzi też program Ogólnopolskiej Sieci Edukacyjnej (OSE), który dostarcza do polskich szkół bezpieczny, szerokopasmowy dostęp do internetu. Korzysta już z niego zdecydowana większość placówek edukacyjnych w Polsce. Z punktu widzenia szkoły jest to usługa darmowa.

Warto na koniec przypomnieć o trudnej, ale niezwykle ważnej misji zespołu Dyżurnet.pl, również działającego w strukturach CSIRT NASK. To bardzo ważny obszar naszej aktywności, łączący istotny obszar naszej działalności misyjnej i społecznej ze stosowaniem i rozwojem najnowszych technologii i narzędzi. Dzięki pracy Dyżurnet.pl identyfikujemy i zwalczamy naganne zjawisko wytwarzania i dystrybucji nielegalnych materiałów z udziałem osób nieletnich zazwyczaj związanych z ich seksualnym wykorzystywaniem. Dzięki pracy zespołu w 2022 roku udało się usunąć z sieci 100% zgłoszonych do niego materiałów tego typu, co nie oznacza oczywiście, że „posprzątaliśmy" już cały internet. Jest to nadal duże wyzwanie, ale prężnie rozwijamy ten obszar naszej działalności, budując nie tylko nowe narzędzia, ale też rozwijając współpracę z instytucjami krajowymi i zagranicznymi. Mając wysokie kompetencje w tej dziedzinie, pomagamy innym, mniej doświadczonym krajom budować tego typu zespoły.

Jakie działania podejmuje NASK, by zwiększyć świadomość społeczną na temat zagrożeń związanych z dezinformacją w sieci?

M.S.: Dezinformacja nie jest zjawiskiem nowym, jednak w dobie internetu, zwłaszcza popularności mediów społecznościowych nabrała zupełnie nowego znaczenia. Stała się jeszcze bardziej niebezpieczna za sprawą szybkiego rozprzestrzeniania się szkodliwych, zwłaszcza budzących silne emocje, treści w internecie, jak również poprzez ogromną elastyczność i szybkość powstawania nowych źródeł takiej infor-

macji.

W NASK identyfikujemy to zjawisko i tam, gdzie jest możliwe, zwalczamy je. Dział Przeciwdziałania Dezinformacji monitoruje treści w mediach społecznościowych i informuje podmioty publiczne o zagrożeniach dezinformacyjnych. Opracowujemy także analizy jakościowe i ilościowe dla administracji publicznej, wspierające identyfikację i reakcję na treści o charakterze dezinformacyjnym.

Niezwykle istotnym elementem naszych działań jest edukacja. Realizujemy dziesiątki szkoleń i warsztatów, które kierujemy do wszystkich grup społecznych narażonych na działanie dezinformacji, m.in. seniorów, dzieci i młodzieży, ale także samorządowców czy osób zajmujących się komunikacją w administracji centralnej. Zwiększamy także świadomość społeczną w kontekście zagrożeń dezinformacyjnych, tworząc i biorąc udział w różnorodnych kampaniach oraz za pośrednictwem mediów społecznościowych. Na profilach „Włącz Weryfikację" w mediach społecznościowych regularnie zamieszczamy wpisy ostrzegające przed zmanipulowanymi lub fałszywymi treściami oraz informacje o charakterze edukacyjnym.

W ramach przeciwdziałania dezinformacji koncentrujemy się również na wydarzeniach aktualnie szczególnie istotnych dla społeczeństwa, np. takich jak ostatnie wybory. Aby zadbać o bezpieczeństwo informacyjne i cyberbezpieczeństwo tego procesu, zainicjowaliśmy projekt widoczny jako portal informacyjny BezpieczneWybory.pl. Portal oferuje użytkownikom internetu m.in. intuicyjny i wygodny formularz zgłoszeń do NASK w sprawie incydentów cyberbezpieczeństwa i niepokojących treści w infosferze oraz szybką ścieżkę kontaktu do platform społecznościowych w sprawach wszelkich naruszeń polityk i praw.

Jakie są plany NASK w zakresie badań nad technologiami sztucznej inteligencji i ich zastosowaniem w cyberbezpieczeństwie?

M.S.: NASK już od dłuższego czasu prowadzi prace badawcze w dziedzinach cyberbezpieczeństwa oraz zastosowań sztucznej inteligencji, działając jako NASK SCIENCE. Opracowaliśmy podstawy generycznej metodyki określenia stopnia podatności modeli predykcyjnych na wybrane typy ataków, wykorzystujące m.in. adversarial machine learning, występujących w obszarze systemów „cyberfizycznych", czyli m.in. robotyki i automatyki przemysło-

wej oraz systemów cyberbezpieczeństwa.

Warto wymienić także przygotowane w NASK nowe algorytmy uczenia maszynowego do oceny złośliwości aplikacji mobilnych, detektor aplikacji złośliwych dla systemu Android czy nowy detektor anomalii w ruchu sieciowym – IoT. W gruncie rzeczy lista dokonań naszych naukowców w tym obszarze jest na tyle długa, że trudno je wszystkie nawet skrótowo wymienić. Dodam tylko, że NASK współpracuje również przy wytwarzaniu polskiego rozwiązania do bezpiecznej komunikacji z wykorzystaniem szyfrów wymienianych kanałem kwantowym oraz współtworzy szkielet polskiej sieci do kwantowej wymiany kluczy w ramach inicjatywy Komisji Europejskiej – EuroQCI.

Czy rozważają Państwo wprowadzenie nowych narzędzi i rozwiązań dla przedsiębiorstw w zakresie cyberbezpieczeństwa?

M.S.: NASK już od lat pełni rolę ważnego partnera przedsiębiorstw w obszarze cyberbezpieczeństwa. Współpracujemy z nimi zarówno przez działania edukacyjne i profilaktyczne, jak i poprzez dostarczanie wielu konkretnych, specjalnie utworzonych narzędzi i rozwiązań. Warto tu wymienić chociażby projekty prowadzone przez zespół CERT Polska, takie jak system N6, dzięki któremu, zwłaszcza większe przedsiębiorstwa i operatorzy sieci telekomunikacyjnych otrzymują bezpłatnie informacje o zdarzeniach dotyczących bezpieczeństwa, związanych z przestrzenią adresów sieciowych lub nazw domenowych konkretnego użytkownika, ale dostarczane przez społeczność wszy-

stkich użytkowników systemu. Kolejny ważny projekt to Artemis, czyli automatyczny i bezpłatny system skanujący udostępnione w internecie systemy teleinformatyczne – serwisy informacyjne, systemy poczty e-mail, systemy brzegowe sieci lokalnych itp.

Celem jest identyfikacja najbardziej widocznych podatności bezpieczeństwa i błędów konfiguracyjnych, o których informujemy skanowany podmiot. W ten sposób ostrzegamy właścicieli infrastruktury o zagrożeniach i zachęcamy do bardziej poważnego potraktowania obszaru zabezpieczeń, w tym np.: skorzystania z pogłębionych badań i skanów oferowanych przez wiele podmiotów na rynku.

Inne projekty rozwijane od lat w NASK, to narzędzie BotSense, już dziś wzmacniające bezpieczeństwo transakcji w 12 dużych polskich bankach czy ARAKIS Enterprise, system wczesnego wykrywania i analizy zagrożeń bezpieczeństwa.

W kontekście krajowego systemu cyberbezpieczeństwa jesteśmy także w trakcie wdrożenia Systemu S46, który wybranym grupom przedsiębiorstw i instytucji objętych ustawą o krajowym systemie cyberbezpieczeństwa zapewnia możliwość przekazywania danych o zagrożeniach, a także integruje ostrzeżenia i dane przekazywane tym podmiotom. Istotną wartością tego systemu może być w przyszłości możliwość łączenia informacji o podobnych incydentach oraz propagacji

skutków zagrożeń z nich wynikających pomiędzy podmiotami korzystającymi wzajemnie ze swoich usług.

Z nowych rozwiązań przeznaczonych dla polskiego biznesu proponujemy program Firma Bezpieczna Cyfrowo, który jest przeznaczony przede wszystkim dla sektora małych i średnich przedsiębiorstw. Dzięki niemu w łatwy sposób można samodzielnie przeprowadzić ocenę stanu cyberbezpieczeństwa własnej firmy, otrzymać bezpłatne porady dotyczące obrony przed zagrożeniami, a na końcu uzyskać certyfikat, który świadczyć będzie o odpowiednim poziomie cyfrowych kompetencji, będących w dzisiejszym świecie elementem budowania wiarygodności i zaufania między przedsiębiorcami, ich partnerami i klientami. Kolejną ważną inicjatywą, są spotkania i szkolenia w społeczności Partnerstwa dla Cyberbezpieczeństwa, skierowane szczególnie do polskich przedsiębiorców i jednostek samorządowych.

Dziękuję za rozmowę.

Polityka ®
Bezpieczeństwa

SZKOLENIA
Z OCHRONY DANYCH OSOBOWYCH

SPRAWDŹ OFERTĘ

MASZ PYTANIA?

michal.wolinski@rzetelnagrupa.pl

+48 508 554 285

EFEKTYWNOŚĆ ENERGETYCZNA W BIURZE I W SERWEROWNI

Kamil Jóźwiak
Dell Technologies

Rafał Szczypiorski
Dell Technologies

Rafał Brudnicki
Servers24.pl

Dziś rozwijająca się technologia informatyczna stanowi krytyczny element funkcjonowania gospodarki, rośnie więc znaczenie efektywności energetycznej. Działy informatyki mają bowiem znaczący wpływ na zużycie energii w firmach, zwłaszcza jeśli chodzi o zasilanie serwerowni czy codzienną pracę pracowników biurowych. Na jakie rozwiązania dziś postawić by mieć bardziej przyjazną dla środowiska organizację, a jednocześnie obniżyć rachunki za prąd?

Jak pokazuje badanie Skaner MŚP (marzec 2023 r.), prawie 50% przedsiębiorców w Polsce obawia się wzrostu kosztów funkcjonowania biznesu, a 7 na 10 firm z branży przetwórstwa przemysłowego wskazuje drogi prąd i gaz jako duży problem. Co więcej – według prognoz – ilość zużywanej energii na świecie podwoi się do 2050 roku. Statystyki te nie zaskakują, gdyż w minionych dekadach rewolucja cyfrowa przyczyniła się do ogromnego wzrostu ilości danych i gwałtownego zapotrzebowania na moc obliczeniową, a tym samym na energię elektryczną. Na szczęście równolegle rozwijają się technologie związane z ochroną środowiska i efektywnością energetyczną, dzięki czemu działy IT mogą dziś podejmować świadome decyzje biznesowe, chociażby poprzez wybór bardziej ekologicznego sprzętu przeznaczonego do pracy biurowej czy centrów danych.

ENERGOOSZCZĘDNE TRIKI

- *Kwestia poboru prądu przez sprzęt technologiczny, taki jak laptopy pracowników, oraz jego wpływ na ślad węglowy, stanowi istotny aspekt zrównoważonego rozwoju i odpowiedzialności środowiskowej organizacji. Warto wiedzieć, że optymalizacja działania sprzętu ma bezpośredni wpływ na zwiększenie jego efektywności i wydajności, jak również powoduje zmniejszenie poboru prądu i ponoszonych kosztów operacyjnych. Wystarczy wprowadzić kilka usprawnień w sposobie użytkowania laptopów* - wytłumaczył **Kamil Jóźwiak, ekspert Dell Technologies.** Co należy więc zrobić, aby laptopy pracowników były na co dzień bardziej efektywne energetycznie?

Monitory zewnętrzne stanowią jedno z największych wyzwań dla efektywności energetycznej w dzisiejszych biurach i domach. Choć są nieodłącznym elementem wielu miejsc pracy i centrum rozrywki w domu, ich wpływ na zużycie energii jest znaczący ze względu m.in. na technologie podświetlenia ekranu, ich wielkość czy rozdzielczość. Warto wiedzieć, że siedmioletni monitor 24-calowy pobierze 2 razy więcej prądu od nowego monitora – przy 30 sztukach w biurze roczne zużycie prądu może osiągnąć nawet 1500 kWh, podczas gdy pięcioletnie 24-calowe monitory pobiorą około 1200 kWh, a najnowsze modele zaledwie 770 kWh. Jak to możliwe? Najnowsze propozycje monitorów Dell (premiera w 2. połowie tego roku) wyposażone są w czujniki jasności otoczenia, dzięki czemu mogą automatycznie dostosować poziom jasności obrazu zmniejszając zużycie prądu, co daje najbardziej wymierne rezultaty w okresie jesienno-zimowym.

Więcej uruchomionych procesów to większe obciążenie komputera. Laptop najwięcej prądu pobiera w chwili uruchamiania się, później zużycie spada w momencie wystartowania systemu operacyjnego i wzrasta ponownie podczas włączania dodatkowych procesów.

Warto więc sprawdzić i usunąć niepotrzebne obciążenia. *-Zdarza się, że klienci pytają nas jak zoptymalizować sprzęt pracowników. Dell Technologies posiada usługę, która pozwala na przywrócenie ustawień fabrycznych, a w tym wgranie najbardziej optymalnych sterowników. Skorzystanie z tej opcji obniża ilość obciążeń, a tym samym wpływa na zmniejszenie ilości poboru energii* – wyjaśnił **Rafał Brudnicki z firmy Servers24.pl**, która zajmuje się doradztwem i dostawami sprzętu IT, w tym również od Dell Technologies.

Indywidualny tryb oszczędzania energii powinien być dopasowany do trybu pracy i możliwości organizacji. - *W laptopach Latitude i Precision pomocna będzie aplikacja Dell Power Manager, dostępna w oprogramowaniu Dell Optimizer 4.0. Pozwala ona na wybór ustawienia akumulatora, które będzie optymalne dla danego sposobu użytkowania systemu. Niektóre funkcje są skupione na przedłużeniu czasu pracy baterii, podczas gdy inne oferują szybszy czas jej ładowania* – radził **Kamil Jóźwiak.**

-Aplikacja to pozwala wymusić także, aby wszystkie komputery w określonych godzinach pracowały wyłącznie na baterii, bez pobierania prądu z sie-

ci, co sprawia, że system operacyjny lepiej zarządza oszczędzaniem energii. A jeżeli laptopy podłączone są na stałe do prądu można ustawić, aby ładowanie ich baterii do pełna odbywało się w nocy, kiedy to obciążenie sieci energetycznych, a czasem także stawka w cenniku, są niższe – dodał.

Starsze technologie to większy pobór prądu – jeżeli komputery pracowników lata świetności mają za sobą, warto rozważyć zmianę na nowsze, bardziej ekologiczne modele. Dlaczego? Bo im wyższa wydajność sprzętu, tym niższy pobór energii. Najnowsze laptopy posiadają większą moc obliczeniową, dzięki czemu są w stanie wykonać określone procesy nawet 2 razy szybciej i przy około 40% obciążeniu.

- Idealnym przykładem będą najnowsze modele z serii Dell Latitude i Dell Precision, wyposażone w procesory Intel Core 13. generacji i najnowsze funkcje Dell Optimizer, które zapewniają nawet 18% oszczędności prądu – powiedział Rafał Brudnicki.:

- Wśród naszych klientów dużym zainteresowaniem cieszy się zwłaszcza linia Latitude 7000 i 9000. Modele te posiadają m.in. nową baterię, pozwalającą pracować nawet do 2h dłużej bez ładowania oraz opcjonalny system kamer z funkcją Inteligentnej Prywatności, który potrafi automatycznie wygasić ekran, jeśli użytkownik nie patrzy na laptopa.

SERCE OPERACJI INFORMATYCZNYCH: SERWEROWNIA

Jednak głównym źródłem kosztów energetycznych są obecnie centra danych. Okazuje się bowiem, że emitują one tyle samo CO2 co globalny ruch lotniczy. - *Nadal bardzo duża grupa klientów w swojej serwerowni posiada sprzęt, który charakteryzuje się wysokim wskaźnikiem PUE* – wytłumaczył **Rafał Szczypiorski, ekspert Dell Technologies.** - *Dla przykładu, PUE 3 zapewnia organizacji trzykrotnie wyższe rachunki za prąd, porównując do samego zasilania infrastruktury IT. Czyli mamy tu dużo większe koszty operacyjne, ale także większy ślad węglowy* – dodał. Jak zatem przygotować serwerownię, która będzie nie tylko wydajna, ale i efektywna energetycznie?

Analiza sytuacji – bardzo ważne na początku jest sprawdzenie, co dokładnie posiada organizacja w swoim data center. Według statystyk, klienci używają średnio tylko 17% mocy procesora, 48% pamięci RAM i 49% przestrzeni dyskowej (wyniki badania przeprowadzonego przez Dell Technologies na 2.7 mln serwerów przy użyciu oprogramowania LiveOptics), co pokazuje, jak wiele zasobów i energii elektrycznej jest każdego dnia marnowanych w organizacji.

Konsolidacja zasobów do nowych platform – na rynku dostępna jest już 16. generacja serwerów Dell Technologies, które pozwalają na zmniejszenie ilości używanych serwerów, bez utraty wydajności. Potencjalne scenariusze oszczędności pokazują, że dziś przy większej mocy obliczeniowej, można zaoszczędzić na zużyciu energii. Przykładem niech będzie migracja z serwerów Dell PowerEdge R730 (z 2014 roku) do Dell PowerEdge R760.

Według danych zmiana ta pozwala m.in. na:

- redukcję ilości serwerów aż o 67% (przejście z 21 maszyn do 7),
- zmniejszenie zużycia energii o 95,181 kW/h rocznie,
- zaoszczędzenie 72,301 kg CO2 rocznie,
- zmniejszenie wpływu termicznego.

Wybór chłodzenia – w serwerach za zużycie prądu odpowiada przede wszystkim procesor (60%), a drugim „prądożernym” zespołem są wentylatory (20% zużycia prądu). - *Oczywistym jest, iż organizacje nie mogą pozwolić sobie na utratę wydajności, a tym samym użycie mniejszych procesorów w serwerowni, dlatego warto*

rozważyć sprzęt posiadający zaawansowane rozwiązania w kontekście efektywnego chłodzenia – radził **Rafał Brudnicki z Servers24.pl.**

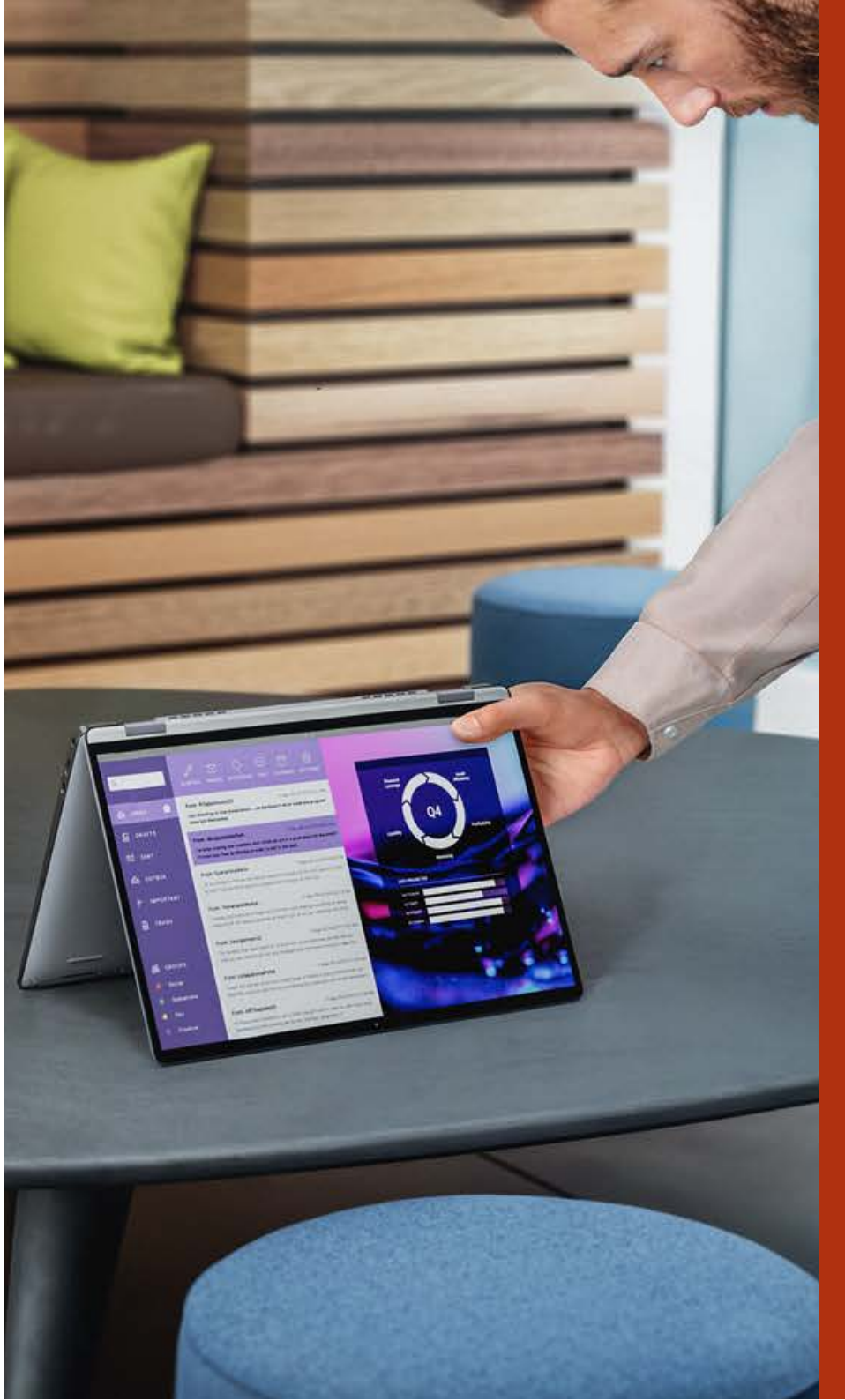
Szczególną uwagę warto zwrócić m.in. na technologię PowerEdge Multi-Vector Cooling, dostępną w serwerach typu RACK od Dell Technologies, która to kieruje przepływ powietrza do najgorętszych części serwera i zarządza wykorzystaniem wentylatorów w sposób inteligentny – bazując na parametrach termicznych komponentów zainstalowanych i działających w slotach PCI-E, czy opcjonalną funkcjonalność chłodzenia serwerów cieczą - Direct Liquid Cooling, wykorzystującą opatentowaną technologię wykrywania wycieków cieczy chłodzącej. „*Konstrukcja obudowy nowych serwerów wykorzystująca specjalnie zaprojektowane wentylatory oraz chłodzenie adaptacyjne, zapewniają bardziej efektywne zużycie energii, zwiększając tym samym wydajność energetyczną nawet o 60% w porównaniu z poprzednimi generacjami*" – mówił **Rafał Szczypiorski z Dell Technologies.**

Zmiana ustawień – warto również sprawdzić ustawienia serwerów w systemie BIOS i iDRAC (karty zdalnego zarządzania serwerami Dell PowerEdge), które pozwalają na zmniejszenie zużycia energii poprzez zaimplementowanie profilu DAPC (Dell Advanced Power Control), dla dowolnego obciążenia roboczego, który to profil dynamicznie dostosowuje parametry zasilania w zależności od aktualnych potrzeb systemu, tak aby w okresie bezczynności aplikacji redukować pobór prądu serwera.

Czy warto?

Temat efektywności energetycznej organizacji to nie tylko kwestia odpowiedzialności środowiskowej, ale także strategii biznesowej.

Wprowadzanie nawet drobnych usprawnień, optymalizacja procesów i świadome zarządzanie zasobami energetycznymi stanowią klucz do osiągnięcia równowagi między efektywnością operacyjną a zrównoważonym rozwojem. Warto już teraz rozpocząć proces dążenia do większej efektywności energetycznej zarówno w serwerowni, jak również na laptopach pracowników.



Rzetelny Regulamin®

POZNAJ SZCZEGÓŁY

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

Kompleksowa obsługa prawna Twojego e-commerce

SECURITYMAGAZINE.PL

JAK OSZUŚCI WYKORZYSTUJĄ KARTY PODARUNKOWE DO WYŁUDZEŃ W E-SKLEPACH?

Redakcja
SECURITY MAGAZINE

Przestępcy z coraz większym sprytem stosują różne metody zdobycia numerów kart podarunkowych, co w praktyce równa się kradzieży gotówki, bez możliwości odzyskania środków przez ofiarę. Karty podarunkowe często wybierane są jako prezent przez przedsiębiorstwa, z przeznaczeniem dla pracowników czy w ramach podziękowania dla klientów. Do czego i jak wykorzystują je cyberprzestępcy?

OSZUSTWA Z KARTAMI PODARUNKOWYMI

Zjawisko oszustw związanych z kartami podarunkowymi nabiera na sile ze wzrastającą popularnością zakupów online, zwłaszcza w okresie świątecznym. Jednak jak podejść do tego problemu oraz jakie strategie wdrożyć, aby ochronić się przed cyberprzestępcami?

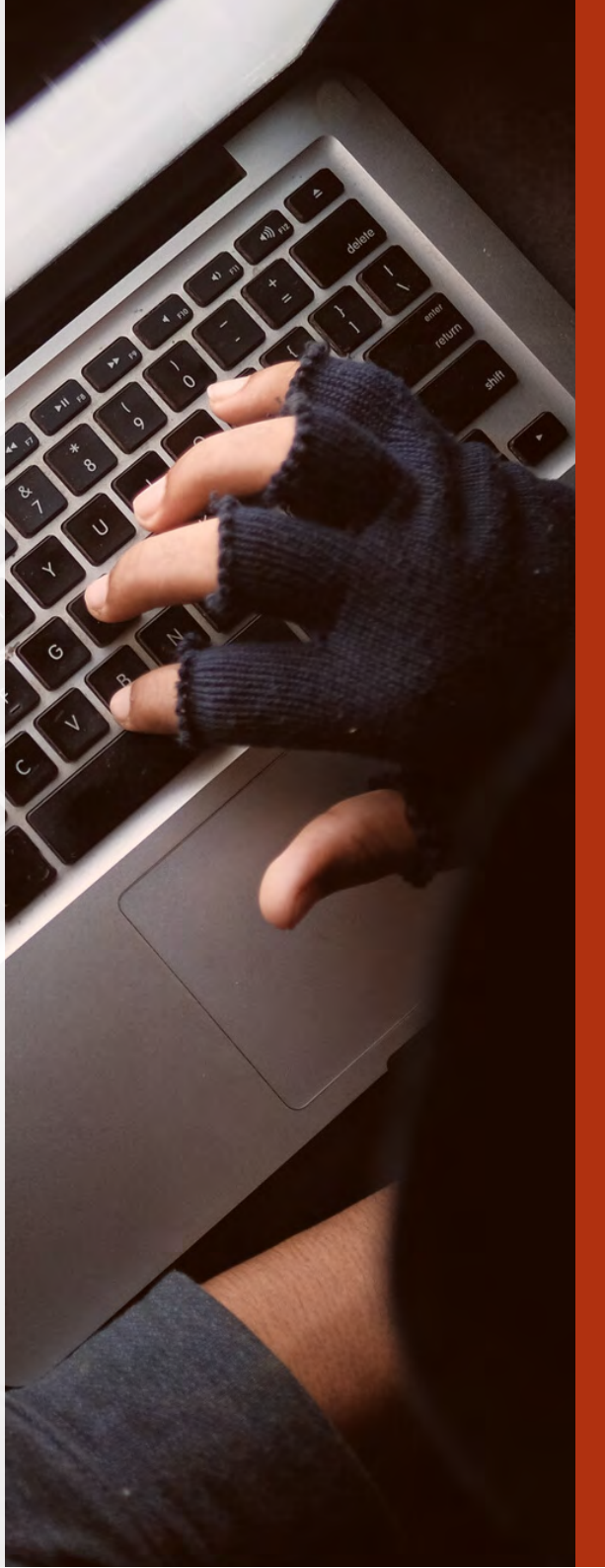
Przestępcy zaczęli wykorzystywać nowe metody oszustw związanych z cyfrowymi kartami podarunkowymi. Jedną z nich jest wykorzystanie botów do testowania różnych kombinacji numerów kart, sprawdzając ich salda. To stosunkowo tanie narzędzie, a walka z nim wymaga zaawansowanych technologii do przeglądania adresów IP i blokowania prób przełamania zabezpieczeń.

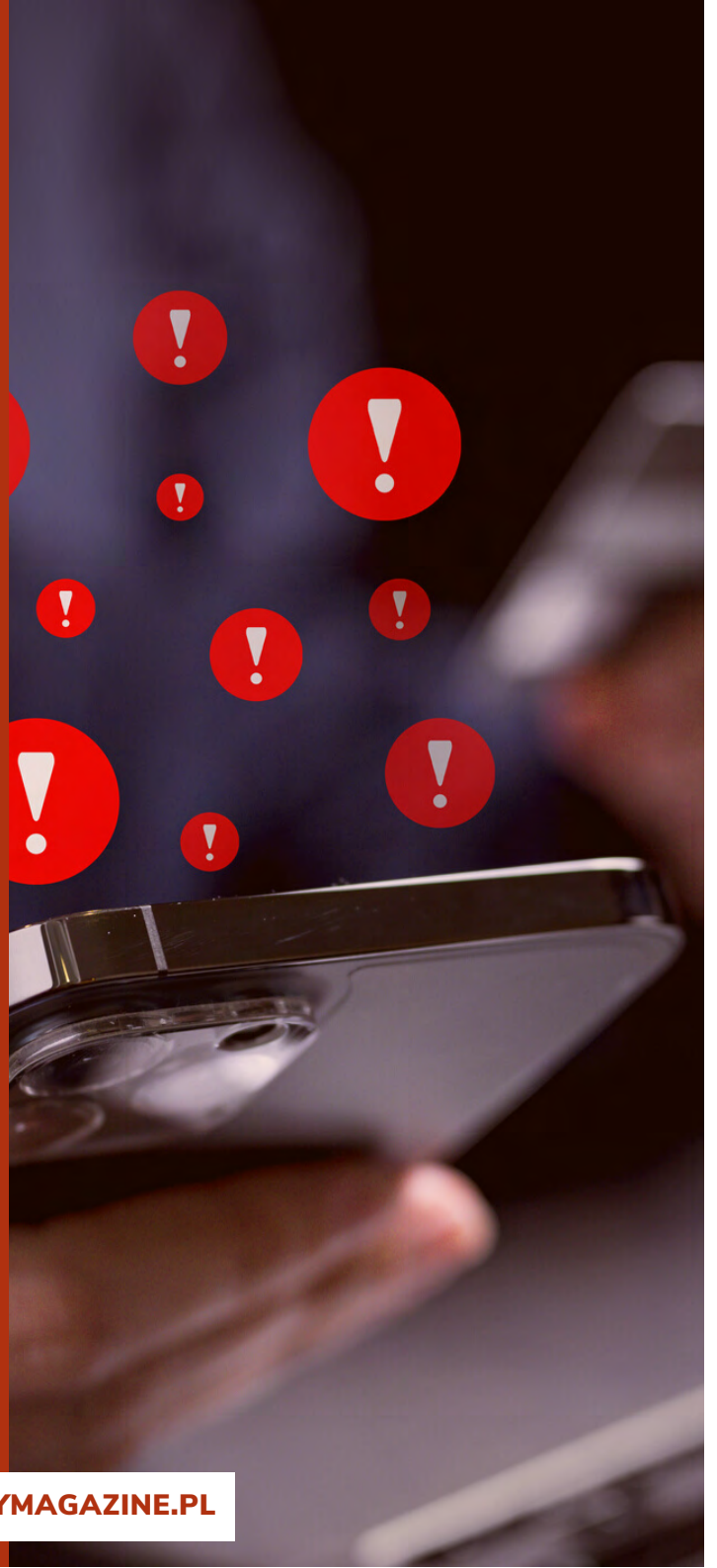
Inną praktyką jest używanie skradzionych kart kredytowych do zakupu cyfrowych kart podarunkowych, co czyni transakcje trudniejszymi do wykrycia. Detaliści, zwłaszcza ci działający globalnie, opracowują zaawansowane systemy analizy transakcji, korzystając z analizy danych, aby skutecznie zwalczać te nowoczesne formy oszustw.

PERSPEKTYWA ONLINE I OFFLINE

W kontekście zakupów online, przedsiębiorcy stają muszą utrzymać równowagę między zapewnieniem bezpieczeństwa a ochroną prywatności konsumentów, szczególnie w przypadku transakcji kartami podarunkowymi.

W środowisku cyfrowym, gdzie transakcje są mniej widoczne i często anonimowe, wykrywanie podejrzanych działań bez naruszania prywatności klientów jest niezwykle istotne. Firmy muszą stosować zaawansowane technologie, takie jak inteligentne systemy monitorowania i analizy zachowań zakupowych,





aby skutecznie identyfikować oszustwa, jednocześnie minimalizując ingerencję w prywatność klientów. Przestępcy stosują różne taktyki, takie jak ataki botów, używanie skradzionych kart kredytowych do zakupu cyfrowych kart podarunkowych, czy wykorzystywanie opóźnień w synchronizacji danych między systemami.

W przypadku zakupów offline, wyzwaniem jest adaptacja tradycyjnych metod ochrony kart płatniczych i kredytowych do specyfiki kart podarunkowych. Ich anonimowy charakter i brak rejestracji utrudniają śledzenie transakcji. Stąd detaliści powinni dostosować swoje strategie bezpieczeństwa, być może przez współpracę z zewnętrznymi dostawcami usług bezpieczeństwa, by lepiej chronić swoje interesy i prywatność klientów.

Oszustwa związane z kartami podarunkowymi ewoluują, wykorzystując nowoczesne technologie i luki w systemach bezpieczeństwa. Przedsiębiorcy muszą być świadomi tych zagrożeń oraz stosować zróżnicowane metody ochrony, które są skuteczne zarówno w środowisku online, jak i offline.

SPOSOBY ZAPEWNIENIA BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Przede wszystkim, istotna jest edukacja pracowników na temat typowych schematów oszustw, przy jednoczesnym zachowaniu ich prywatności. Firmy powinny również monitorować transakcje związane z kartami podarunkowymi, ale z zachowaniem zgodności z przepisami o ochronie danych.

Wprowadzenie jasnych zasad i procedur dotyczących użycia kart podarunkowych może pomóc w zapobieganiu nadużyciom, pod warunkiem, że nie naruszają one prywatności. Ważne jest także wykorzystanie technologii zabezpieczających, które szanują prywatność użytkowników, oraz współpraca z dostawcami kart podarunkowych w celu wzmocnienia bezpieczeństwa. Wszystkie działania powinny być zgodne z obowiązującymi przepisami o ochronie danych, co zapewnia legalne i transparentne przetwarzanie informacji. Podstawą jest odpowiednie połączenie edukacji, procedur, technologii i przestrzegania prawa, aby skutecznie chronić przed oszustwami, nie naruszając przy tym prywatności.

W walce z tymi zagrożeniami, przedsiębiorcy oraz sklepy detaliczne muszą inwestować w nowoczesne technologie ochronne, które obejmują analizę dużych zbiorów danych przy wykorzystaniu sztucznej inteligencji. Jednakże, trzeba pamiętać, że technologie te są skuteczne tylko w połączeniu z zaawansowanymi systemami CRM i POS, umożliwiającymi analizę w czasie rzeczywistym i minimalizację luk w zabezpieczeniach.

W miarę jak cyberataki stają się bardziej zaawansowane, sklepy detaliczne muszą kontynuować inwestowanie w nowoczesne narzędzia bezpieczeństwa.

Jednak równie ważne jest utrzymanie równowagi między ochroną a prywatnością klientów. Świadomość i przestrzeganie najlepszych praktyk bezpieczeństwa online są podstawą ochrony przed rosnącym zagrożeniem oszustw związanych z kartami podarunkowymi, zwłaszcza w okresie wzmożonych zakupów świątecznych online.

JAK ZABEZPIECZYĆ SIĘ PRZED TYMI OSZUSTWAMI?

1. Silne hasła

Silne hasła są pierwszą linią obrony w ochronie przed nieautoryzowanym dostępem do kont online. Hasło uważane jest za silne, gdy jest wystarczająco długie (zalecane jest minimum 12 znaków) i zawiera kombinację wielkich i małych liter, cyfr oraz symboli. Takie hasła są trudniejsze do odgadnięcia lub złamania przez narzędzia stosowane przez cyberprzestępców.

Ważne jest, aby dla każdej platformy czy serwisu internetowego stosować inne hasło.

Powtarzanie tego samego hasła na różnych stronach znacznie zwiększa ryzyko, że w przypadku wycieku danych z jednej strony, inne konta również staną się podatne na ataki.

Oprócz silnych haseł, warto również rozważyć użycie losowych identyfikatorów użytkownika (loginów). Chociaż nie jest to tak powszechna praktyka jak stosowanie silnych haseł, może dodatkowo zwiększyć bezpieczeństwo. Unikalny identyfikator użytkownika, który nie jest łatwo powiązany z daną osobą, utrudnia potencjalnym atakującym skojarzenie konta z konkretnym użytkownikiem.

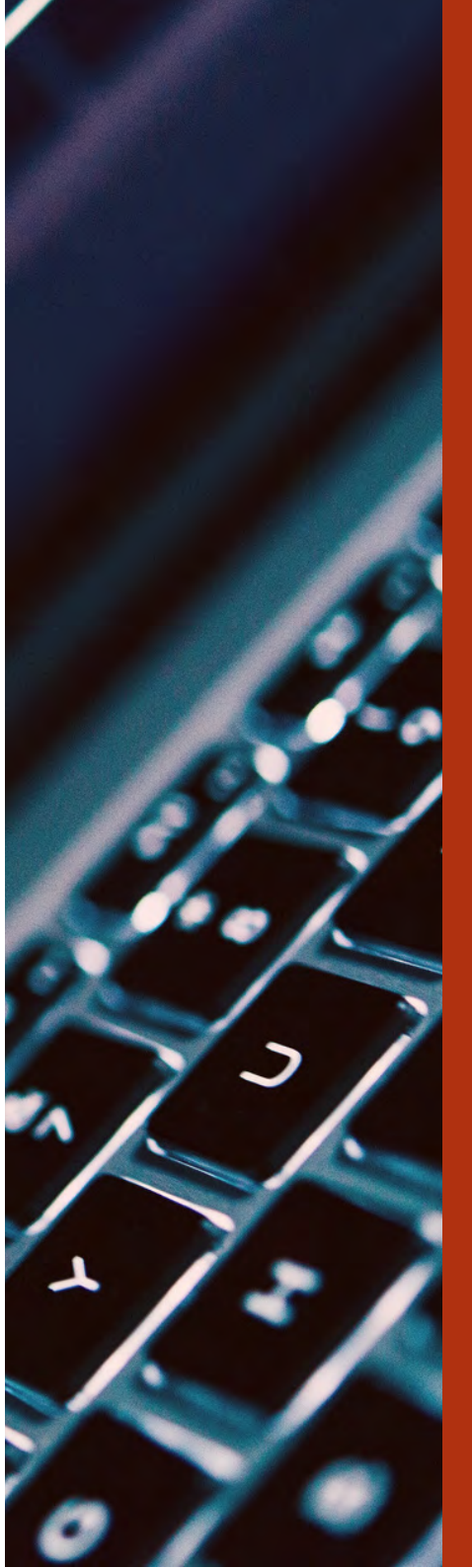
2. Ostrożność przy zakupach kart podarunkowych

Przy zakupach kart podarunkowych w sklepach fizycznych, warto dokładnie sprawdzić je pod kątem ewentualnych śladów manipulacji. Bezpieczniej jest również nabywać je w miejscach, gdzie są przechowywane za ladą. Jednym z działań przestępców jest manipulacja fizyczną kartą, poprzez zdrapywanie warstwy ochronnej, na której zapisane są numery PIN, a następnie zastąpienie jej naklejką. Oszuści w ten sposób starają się uzyskać pełen dostęp do środków zgromadzonych na karcie.

3. Ostrożność w zakupach online

Bardzo ważne jest, aby być szczególnie ostrożnym w przypadku próśb o płatność za zakupy online za pomocą kart podarunkowych, które otrzymuje się drogą mailową. Takie e-maile mogą pochodzić od oszustów, którzy próbują wykorzystać karty podarunkowe jako sposób na anonimowe uzyskanie pieniędzy. W przeciwieństwie do transakcji kartą kredytową, płatności kartą podarunkową są trudniejsze do śledzenia i często niemożliwe do odzyskania, co czyni je atrakcyjnym celem dla oszustów.

Płatności kartą kredytową zazwyczaj oferują wyższy poziom ochrony. Większość firm wydających karty kredytowe ma wdrożone zaawansowane systemy monitorowania



oszustw i oferuje ochronę konsumenta w przypadku nieautoryzowanych transakcji. Ponadto, w przypadku stwierdzenia oszustwa, konsument ma większe szanse na odzyskanie utraconych środków.

Przed dokonaniem zakupu online, zawsze warto sprawdzić wiarygodność sklepu lub sprzedawcy. Czytanie opinii, sprawdzanie adresu strony internetowej oraz unikanie podejrzanie niskich cen może pomóc w uniknięciu oszustw.

– *Płatności bezgotówkowe, zwłaszcza te internetowe, na stałe weszły do naszego życia. Przede wszystkim są szybkie, wygodne, a przy zachowaniu rozsądku i zasady ograniczonego zaufania, również bezpieczne. Zanim zdecydujemy się na innowacyjne metody płatności sprawdźmy, czy usługodawca jest rzetelny i czy możemy mu powierzyć nasze dane i finanse* – powiedziała **ekspertka NASK, Anna Kwaśnik.**

Cyberprzestępcy mogą wykorzystać karty podarunkowe do ataków na konta sklepów internetowych. Posługują się skradzionymi danymi logowania (taktyka znana jako credential stuffing) lub używają różnych kombinacji haseł w połączeniu z adresem e-mail ofiary (taktyka password spraying), aby przejąć kontrolę nad kontem i dokonywać nieautoryzowanych transakcji.

-20%

SECURITY MAGAZINE

ŚWIĄTECZNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

WAŻNY DO

10.01.2024

KONTAKT I SZCZEGÓŁY:

redakcja@securitymagazine.pl

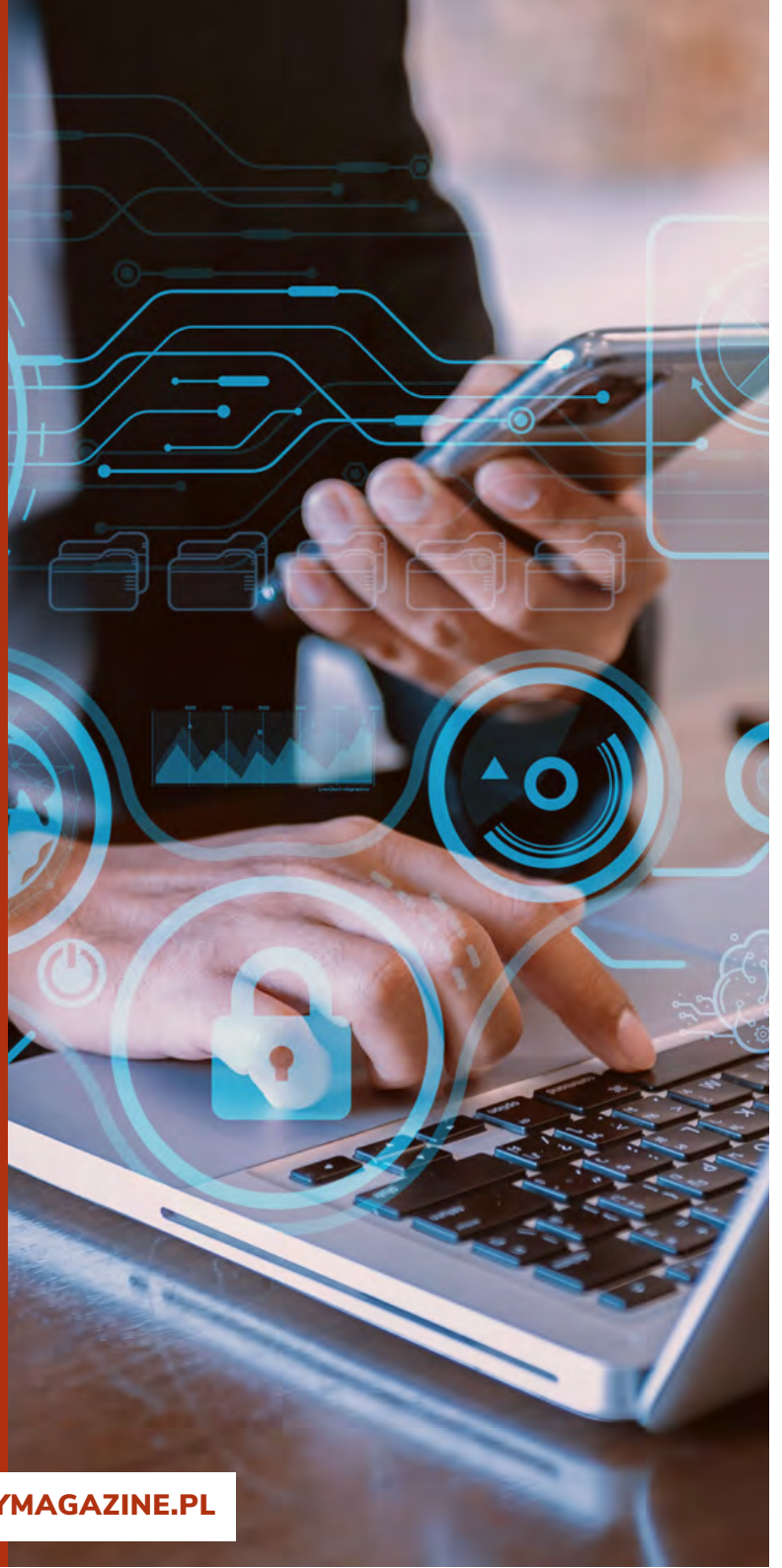
+48 518 609 987

SECURITYMAGAZINE.PL

ARCHITEKTURA SASE JAKO NOWY STANDARD SIECIOWY

Sebastian Strzelak
NetFormers

Ostatnie lata okazały się rekordowe pod względem liczby przeprowadzonych na świecie cyberataków, co podkreślają eksperci cyberbezpieczeństwa w swoich raportach badawczych.

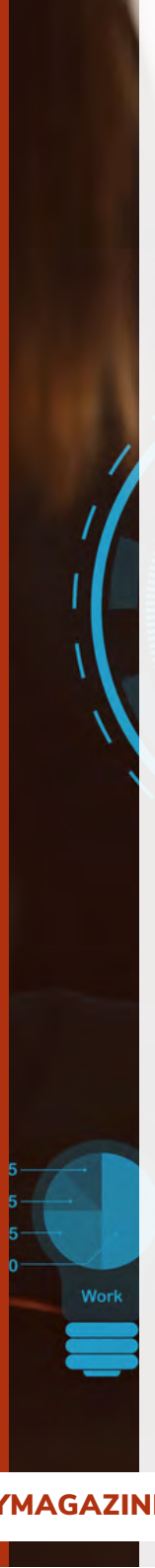


Nasi Klienci, polscy przedsiębiorcy, a szczególnie operatorzy usług kluczowych, widzą potrzebę inwestycji w cyberbezpieczeństwo i dostosowania bieżących systemów zabezpieczeń do nowych, zaawansowanych zagrożeń.

Okres pandemii przyśpieszył proces uelastycznienia rynku pracy. Skuteczne i bezpieczne zarządzanie zespołem osób, w którego skład wchodzą zarówno wewnętrzni pracownicy, jak zewnętrzni kontrahenci jest w dzisiejszym świecie biznesu kluczowy.

Aby jednak w pełni korzystać ze zwiększonej mobilności i efektywności pracowników czy niższych kosztów infrastruktury, trzeba wiedzieć, jak odpowiednio zabezpieczyć dostęp do usług w chmurze i eliminować zagrożenia związane z cyfrową transformacją. Konieczne są rozwiązania, które sprostają nowym wyzwaniom bezpieczeństwa, jakie zrodziły się w wyniku olbrzymiego wzrostu popularności pracy zdalnej oraz masowej adopcji chmury.

Jedną z takich innowacji jest SASE (ang. Secure Access Service Edge), koncepcja architektury sieciowej łącząca w sobie elastyczną, rozległą i wysokoprzepustową sieć SD-WAN oraz szereg zaawansowanych funkcji zabezpieczeń dostępnych w chmurze dla łatwego, jednolitego dostępu. Warto rozważyć wdrożenie tego rozwiązania jeśli firma działa w modelu pracy zdalnej lub hybrydowej. Starsze rozwiązania mogą wówczas okazać się niewystarczające, aby sprostać wymaganiom chmury i urządzeń przenośnych.



Architektura SASE łączy sieciowe funkcje bezpieczeństwa (takie jak SWG, CASB, FWaaS and ZTNA), z możliwościami oferowanymi przez sieć WAN (np. SDWAN) aby zapewnić dynamiczny, bezpieczny dostęp do aplikacji w oparciu o identyfikację osób, urządzeń oraz kontekstu dostępu do danych.

Prześledźmy, jak konkretne rozwiązania SASE wpływają na poprawę bezpieczeństwa oraz efektywności sieciowej.

1. Bezpieczne punkty dostępowe (Secure Access Points)

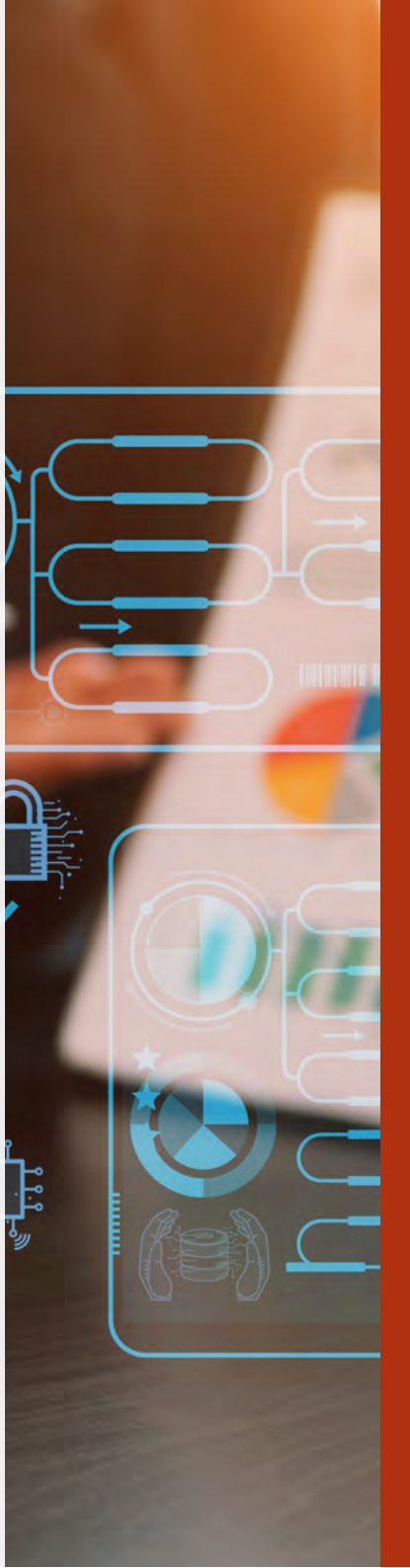
Centralnym elementem architektury SASE są bezpieczne punkty dostępowe. Te zaawansowane rozwiązania umożliwiają organizacjom zapewnienie bezpiecznego dostępu do zasobów sieciowych z dowolnego miejsca na świecie. Dzięki technologii mikrosegmentacji, bezpieczne punkty dostępowe tworzą warstwę obronną na poziomie każdego punktu dostępu, eliminując potencjalny atak. Rozwiązania te, często oparte na technologiach zerowego zaufania (Zero Trust), gwarantują, że każde połączenie jest odpowiednio autoryzowane i monitorowane.

2. Integracja funkcji bezpieczeństwa w chmurze

SASE wykorzystuje potencjał chmur obliczeniowych do dostarczania funkcji bezpieczeństwa. Rozwiązania te obejmują zaawansowane narzędzia do detekcji zagrożeń, analizy ruchu sieciowego oraz kontroli dostępu. Dzięki integracji z chmurą, organizacje mogą skorzystać z ciągłych aktualizacji i elastycznego skalowania, co jest kluczowe w obliczu dynamicznie zmieniającego się krajobrazu cybernetycznego.

3. Wirtualne prywatne sieci (VPN) w kontekście SASE

W ramach architektury SASE, VPN staje się bardziej niż tylko narzędziem umożliwiającym zdalny dostęp do zasobów. SASE wykorzystuje technologię VPN do



stworzenia bezpiecznych, szyfrowanych połączeń między użytkownikami a zasobami sieciowymi. Jednak kluczową innowacją jest adaptacja VPN do architektury SASE, co oznacza, że dostęp jest dynamicznie dostosowywany w zależności od kontekstu użytkownika, lokalizacji czy urządzenia, co znacząco zwiększa elastyczność i bezpieczeństwo dostępu.

4. Bezpieczne dostępy do aplikacji (Secure Access to Applications)

W kontekście pracy zdalnej i korzystania z różnorodnych urządzeń, bezpieczny dostęp do aplikacji biznesowych staje się priorytetem. SASE oferuje rozwiązania, które łączą technologie jednorazowych haseł (OTP), wielopoziomowego uwierzytelniania (MFA) oraz kontroli dostępu opartej na politykach. Dzięki temu pracownicy mogą swobodnie korzystać z aplikacji, a jednocześnie organizacja utrzymuje wysoki poziom bezpieczeństwa.

5. Optymalizacja wydajności przy użyciu sztucznej inteligencji (AI)

SASE, wykorzystując potencjał sztucznej inteligencji, może dostosować się do zmiennych warunków sieciowych w czasie rzeczywistym. Algorytmy uczenia maszynowego analizują ruch sieciowy, prognozują obciążenie i dostosowują trasowanie danych w celu optymalizacji wydajności. To podejście pozwala na minimalizację opóźnień i maksymalizację przepustowości, co jest kluczowe dla organizacji, które wymagają szybkiego i niezawodnego dostępu do zasobów.

6. Szkolenie pracowników i cyberedukacja

Wprowadzenie architektury SASE wymaga zaangażowania pracowników i odpowiedniego przeszkolenia. Bezpieczeństwo sieci oparte na SASE często opiera się na ścisłych politykach dostępu oraz rygorystycznych procedurach uwierzytelniania. Edukacja cybernetyczna staje się więc kluczowym elementem skutecznej implementacji SASE, gwarantując, że pracownicy są świadomi i przestrzegają wymogów bezpieczeństwa.

7. Wyzwania implementacji SASE

Choć SASE niesie ze sobą wiele korzyści, implementacja tego modelu może napotkać pewne wyzwania. Migracja z istniejących rozwiązań sieciowych, dostosowanie polityk bezpieczeństwa czy skuteczne zarządzanie ruchem sieciowym to tylko kilka z potencjalnych wyzwań. Jednak staranne planowanie, współpraca z dostawcami technologii SASE i edukacja personelu mogą zminimalizować te trudności.

8. Przyszłość SASE: Integracja z IoT i Rozwój Technologii

Patrząc w przyszłość, można przewidzieć, że SASE będzie rozwijane w kierunku integracji z Internetem Rzeczy (IoT) oraz dalszego wykorzystania sztucznej inteligencji. Integracja z IoT pozwoli na bardziej kompleksową ochronę urządzeń i danych w środowisku rozproszonym. Ponadto, rozwój technologii bezpieczeństwa, takich jak biometryka czy blockchain, może dodatkowo wzbogacić funkcje SASE.

PODSUMOWANIE

Architektura SASE reprezentuje ewolucję standardów sieciowych w erze chmurowej. Bezpieczeństwo i wydajność, łączone w ramach jednej architektury, stają się bardziej dostępne i skuteczne dzięki konkretnym rozwiązaniom, takim jak bezpieczne punkty dostępu, integracja z chmurą, zaawansowane technologie VPN, bezpieczny dostęp do aplikacji oraz optymalizacja przy użyciu sztucznej inteligencji. Wdrożenie SASE wymaga jednak starannego planowania i adaptacji do indywidualnych potrzeb organizacji. W miarę rozwoju technologii, SASE zapowiada nową erę w zarządzaniu sieciami, gdzie bezpieczeństwo i wydajność idą ramię w ramię, spełniając oczekiwania dynamicznego świata biznesu.

Pora na nasz ruch. Cyberprzestępcy nie będą na nas czekać. Decydując się na wdrożenie technologii przyszłości, mamy szansę wyprzedzić ich o krok i zapewnić bezpieczeństwo swojej firmie.

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

SECURE BY DESIGN - BEZPIECZNE OPROGRAMOWANIE JUŻ OD SAMEJ KONCEPCJI

Oliver Dedowicz
Cyber Security Lab

Secure by Design to oprogramowanie bezpieczne z założenia. W procesie deweloperskim, jest to technika wytwarzania software'u bezpiecznego już od samych fundamentów. Można ją porównać do budowy domu - lepiej jest postawić go na solidnych fundamentach aniżeli musieć dobudowywać podpory, aby się nie zawalił.

ISTOTA CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo jest dziś jednym z najważniejszych i największych obszarów informatyki, co spowodowane jest rozwojem technologii i rosnącym zagrożeniem, które „czyha" na użytkownika na każdym kroku w cyberprzestrzeni. Zalew informacji online, transformacja wielu procesów, takich jak bankowość, załatwianie spraw urzędowych oraz innych, w wirtualne czy dynamiczny rozwój mediów społecznościowych, zmuszają firmy do projektowania i tworzenia oprogramowania bezpiecznego, które uchroni użytkowników i ich dane przed niepożądanym dostępem osób trzecich.

W erze, gdy dane i prywatność są jednym z najważniejszych i najcenniejszych aktywów, kluczowe staje się zagwarantowanie bezpieczeństwa i potencjalne zapobieganie atakom na użytkowników, takim jak np. kradzież tożsamości. Uchronienie użytkowników narzędzi cyfrowych przed atakami to dziś konieczność, ponieważ uchybienia w tym zakresie są coraz częściej eksponowane przez media i prowadzą do utraty renomy przez firmę. Przykład: zeszłoroczny wyciek danych z menedżera haseł LastPass, który zaowocował licznymi negatywnymi komentarzami w prasie. Jego efektem był m.in. artykuł zatytułowany „Why You Should Stop Using LastPass (...)" opublikowany w Forbes, którego twórcy oprogramowania z pewnością woleliby uniknąć... Jeden incydent naruszenia bezpieczeństwa może całkowicie zrujnować reputację produktu lub firmy, co pociąga za sobą realne straty finansowe i wizerunkowe.

EWOLUCJA BEZPIECZEŃSTWA W PROGRAMOWANIU

Secure by Design opiera się na ważnej zasadzie – bezpieczeństwo użytkownika jest czymś, o czym trzeba myśleć od samego początku procesu tworzenia oprogramowania. Teraz może się to wydawać oczywiste, lecz nie zawsze tak było. W latach 60. i 70. bezpieczeństwo było kwestią drugorzędną. Budowano zamknięte, lokalne programy (pierwsze systemy operacyjne), które głównie skupiały się na funkcjonalności.

W kolejnych latach, wraz ze wzrostem popularności i powszechności Internetu, zaczęły pojawiać się pierwsze ataki hakerskie oraz ryzyka z tym związane. Twórcy oprogramowania zaczęli dostrzegać istotę cyberbezpieczeństwa na etapie samego projektowania. W późnych latach 90. rozpoczęto stosowanie sformułowania „bezpiecznego

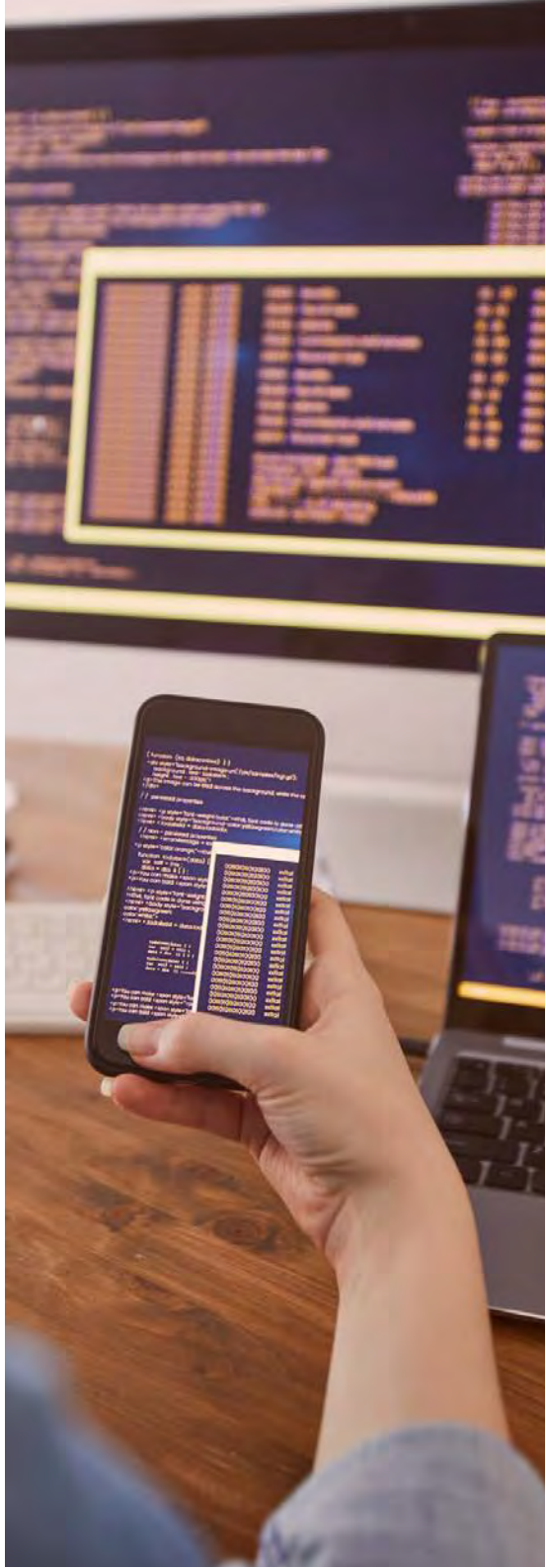
kodowania", jednakże większość tych praktyk polegała na łataniu błędów i zabezpieczaniu luk po wdrożeniu programu na środowiska produkcyjne. Wraz z XXI wiekiem koncepcja Secure by Design weszła do informatycznego słownika i zaczęła po-woli zastępować reakcję na ataki skuteczną prewencją.

JAK ZACZĄĆ?

Pierwszym krokiem do wdrożenia *Secure by Design* jest zrozumienie koncepcji i środowiska projektowanego oprogramowania. Analityk powinien postawić się w pozycji potencjalnego napastnika i pomyśleć o przypadkach w jakim celu i w jaki sposób chciałby i mógłby zaatakować program. Proces ten nazywa się modelowaniem zagrożeń i w dużym stopniu pozwala na zidentyfikowanie podatności i tzw. słabych punktów oprogramowania.

Dobrą praktyką jest kreowanie aktorów, czyli wymyślonych przez nas postaci z własną motywacją, konkretnymi umiejętnościami i celem, który chcą osiągnąć. Przykład: projektując system społecznościowy, możemy wymyśleć aktora – wyłudzacza pieniędzy, który chciałby przejąć konto użytkownika, aby pod jego tożsamością prosić jego znajomych na tym portalu o szybki przelew z obietnicą zwrotu. W tym celu wykonał fałszywą stronę logowania łudząco podobną do prawdziwej i próbuje za jej pomocą przejąć dane do logowania do konta nieświadomego użytkownika. Po wymyśleniu takiej historii, analityk powinien znaleźć rozwiązanie, które uniemożliwi aktorowi-napastnikowi pomyślnego wykonania opisanego ataku. W tym przypadku może to być, na przykład, zastosowanie weryfikacji dwuetapowej.

Kolejną dobrą praktyką przy projektowaniu jest tzw. minimalizacja powierzchni ataku, którą można zastosować, poprzez ograniczenie funkcjonalności oprogramowania do niezbędnego minimum. Eliminuje to potencjalne wektory ataku i ułatwia testowanie na etapie dalszego procesu deweloperskiego. Można to też osiągnąć przez zastosowanie dobrze przemyślanego systemu kontroli dostępu do funkcjonalności, do których dostęp mają jedynie osoby uprawnione.



Istotne również jest zaangażowanie testera penetracyjnego na wczesnym etapie projektu, co potrafi przynieść bardzo istotne wnioski i wyniki, które wdrożyć można bez potrzeby przerabiania większości zrealizowanych funkcjonalności – zaoszczędzone zostają wtedy potencjalnie czas i pieniądze. Istnieją również narzędzia pozwalające na automatyczne skanowanie bezpieczeństwa kodu, które potrafią wykryć lukę bezpieczeństwa bez ingerencji człowieka – aczkolwiek nie będą tak skuteczne jak doświadczony tester penetracyjny.

INTEGRACJA CYBERBEZPIECZEŃSTWA W CYKL ŻYCIA OPROGRAMOWANIA

Programiści przyzwyczajeni są do standardowego cyklu życia oprogramowania, opierającego się na dowolnej metodyce i składającego się z elementów takich jak analiza, wykonanie, testy, wdrożenie i utrzymanie. Secure by Design jest czymś więcej niż dodatkowym etapem w cyklu życia, ponieważ zastępuje ten wzorowy własnymi elementami (zaznaczam, iż jest to skondensowany i przykładowy schemat, który nie jest wzorem sprawdzającym się w każdym przypadku):

- **Definicja założeń projektu i polityki bezpieczeństwa** – definicja wszystkich założeń projektu, istotne jest pamiętanie o polityce bezpieczeństwa i identyfikacji zagrożeń.
- **Analiza zagrożeń i ryzyka** – ocena ryzyka i priorytetyzacja.
- **Projektowanie bezpiecznej architektury** – wdrożenie zasady Secure by Design na poziomie architektury oprogramowania.

- **Programowanie w oparciu o bezpieczne praktyki** – wytworzenie kodu przez wyszkolonych programistów z zakresu cyberbezpieczeństwa, świadomych o aktualnych zagrożeniach cybernetycznych.
- **Testowanie** – nie tylko manualne i automatyczne, istotne są testy penetracyjne, które zbadają bezpieczeństwo na każdym etapie życia projektu.
- **Zabezpieczenie procesów CI/CD** – zapewnienie bezpiecznego kanału ciągłej integracji i dostarczania, uniemożliwienie potencjalnego ataku związanego z podmianą kodu źródłowego do kompilacji.
- **Monitorowanie i reagowanie na incydenty** – wykorzystanie osobnego zespołu do monitorowania i natychmiastowa reakcja na incydenty związane z cyberbezpieczeństwem. Istotne jest przygotowanie planów na ewentualne ataki.
- **Edukacja użytkowników** – funkcje edukacyjne dotyczące cyberbezpieczeństwa, np. porady przy logowaniu, na co zwrócić uwagę – zielona kłódka, ważny certyfikat, adres URL itp.
- **Audyty bezpieczeństwa –** wykonywane przez firmy zewnętrzne, potwierdzające bezpieczeństwo systemu lub wskazujące na miejsca wymagające poprawy.

Powyższe punkty składają się na cykl – po dotarciu do ostatniego punktu, z zasady oprogramowanie będzie musiało być rozwijane, aby wciąż być bezpieczne i funkcjonalne. Z tego też powodu należy wrócić do pierwszego kroku i każdą nową funkcjonalność rozpocząć od analizy bezpieczeństwa, idąc przez każdy z punktów, docierając aż do audytu.

SECURE BY DESIGN OD CYBER SECURITY LAB

W Cyber Security Lab nie tylko implementujemy program Secure by Design, ale także stale analizujemy i reagujemy na zmieniające się zagrożenia w środowisku cybernetycznym. Realizując oprogramowanie w oparciu o trzy filary – funkcjonalność, doświadczenie użytkownika i bezpieczeństwo – nie tylko spełniamy oczekiwania użytkowników pod względem wydajności i łatwości użytkowania, ale również utrzymujemy najwyższe standardy bezpieczeństwa. Bezpieczeństwo nie jest u nas tylko dodatkiem, ale integralną częścią procesu tworzenia oprogramowania od analizy i koncepcji do jego dostarczenia.

Jako profesjonaliści z obszaru cyberbezpieczeństwa, zdajemy sobie sprawę, że zagrożenia nie śpią,

dlatego ciągła edukacja, monitorowanie, oraz aktualizacje są nieodłączną częścią naszego podejścia.

Dążymy do tego, aby nasze systemy były nie tylko odporne na obecne zagrożenia, ale również elastyczne i gotowe na wyzwania przyszłości.

W połączeniu z programem *Secure by Design*, nasz plan na bezpieczeństwo obejmuje również regularne przeglądy, testy penetracyjne oraz ścisłą współpracę z ekspertami ds. bezpieczeństwa. Dzięki temu nie tylko reagujemy na bieżące zagrożenia, ale także antycypujemy przyszłe wyzwania, aby nasze oprogramowanie nadal pozostawało w czołówce, jeśli chodzi o bezpieczeństwo i niezawodność. Wierzymy, że tylko poprzez holistyczne podejście i ciągłe doskonalenie możemy sprostać dynamicznemu środowisku cybernetycznemu i chronić naszych klientów przed ewoluującymi zagrożeniami.

PUBLIKUJ OGŁOSZENIA OFERT PRACY

SZUKASZ SPECJALISTY Z BRANŻY SECURITY?

ZACZNIJ REKRUTOWAĆ Z NAMI

Znajdź najlepszych w branży z "Security Magazine"!

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

Celuj w specjalistów z branży

Wysoka widoczność wśród kandydatów

Skróć czas rekrutacji

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

SECURITYMAGAZINE.PL

AI, ZABEZPIECZENIE CHMUR I OCHRONA PRZED HAKERAMI

Redakcja
SECURITY MAGAZINE

#SECURITY
#STARTUP

W świecie cyfrowym czyha na nas wiele zagrożeń. Zwłaszcza jeśli prowadzimy firmę – wówczas stajemy się łakomym kąskiem dla cyberprzestępców. Na szczęście istnieje wiele startupów, które dostarczają rozwiązań tak potrzebnych dla cyberbezpieczeństwa.

BLACKPOINT – OCHRONA PRZED RANSOMWARE

Cyberprzestępcy stali się wyjątkowo aktywni i coraz śmielej atakują firmy – nierzadko za pomocą złośliwych oprogramowań typu ransomware. Na szczęście w takich sytuacjach z pomocą przychodzi startup BlackPoint, który dostarcza specjalny ekosystem cyberbezpieczeństwa.

Technologia zarządzanego wykrywania i reagowania (MDR) firmy BlackPoint działa bezustannie, monitorując sieć i reagując na pierwsze oznaki zagrożenia. To właśnie szybka reakcja na incydent ma kluczowe znaczenie. BlackPoint chwali się, że działa szybciej od potencjalnych przeciwników, zapewniając natychmiastową odpowiedź na atak.

Startup podkreśla, że ich platforma działa 24/7, reagując w zaledwie kilka minut od wykrycia incydentu, co pozwala szybko zneutralizować zagrożenie. Mowa tutaj o monitorowaniu wskaźników naruszeń bezpieczeństwa, identyfikując podejrzane działania i eliminując je, zanim spowodują większe szkody.

Kiedy takowe zagrożenie zostanie wykryte, BlackPoint izoluje i zatrzymuje złośliwe procesy, neutralizują je w czasie rzeczywistym. Organizacja wskazuje, że ich rozwiązanie jest pod każdym względem skuteczniejsze od starszych form ochrony przed cyberzagrożeniami, takimi jak zapory ogniowe, ochrony punktów końcowych czy antywirusy.

Startup dzięki swojej platformie zapewnia bezpieczeństwo w chmurze dla Microsoft 365 i Google Workspace, wykrywa zagrożenia dla komputerów PC i Mac, a także automatyzuje funkcje ochronne przed ransomware.

CADO SECURITY – BEZPIECZEŃSTWO W CHMURZE

Dziś rozwiązania chmurowe stanowią kluczową część technologicznego ekosystemu, stąd istnieje coraz większa potrzeba skutecznych narzędzi do ich zabezpieczania.

Pomimo inwestycji w zapobieganie oraz wykrywanie zagrożeń w chmurze, wiele organizacji boryka się z brakiem właściwych rozwiązań do analizy i reakcji na zaistniałe sytuacje. Tutaj na scenę wkracza Cado Security, czyli startup oferujący pierwszą platformę umożliwiającą skuteczne prowadzenie analiz i reagowanie na incydenty w śro-

dowiskach chmurowych.

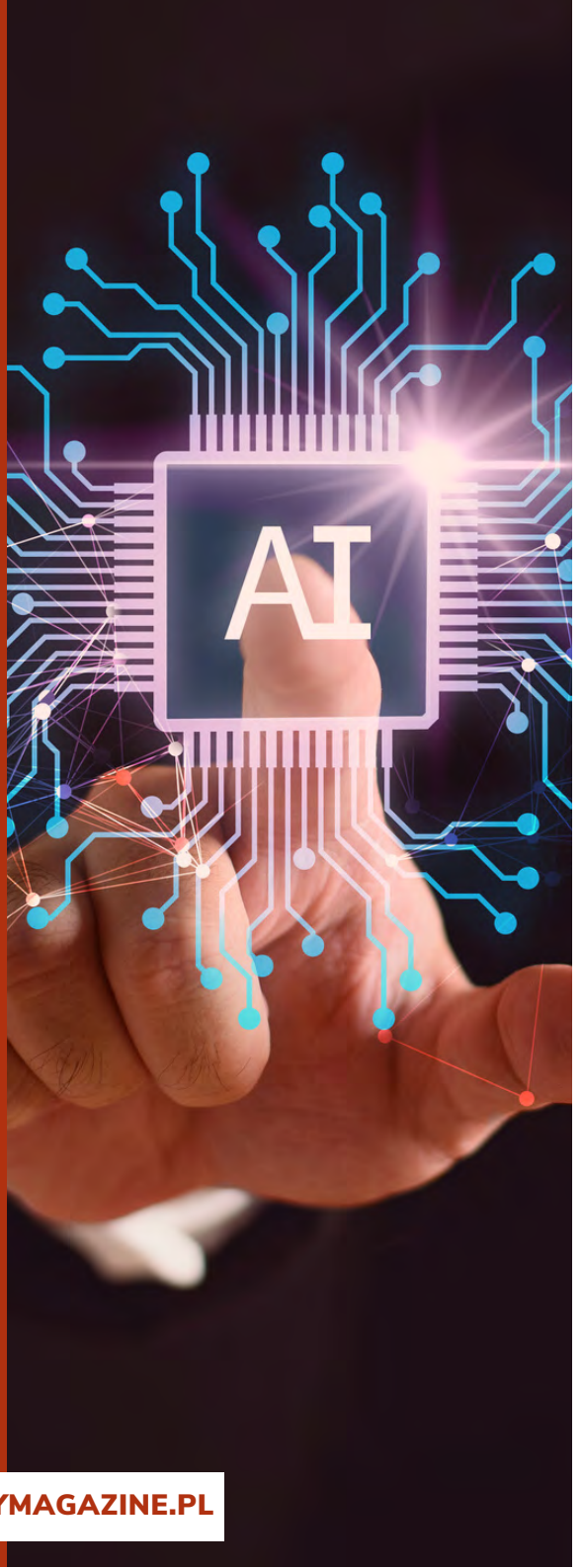
Cado Security dostarcza platformę, umożliwiającą zespołom ds. cyberbezpieczeństwa dokładną analizę cyberincydentów. To, co kiedyś zajmowało analitykom całe dni, teraz ma być możliwe do rozwiązania w zaledwie kilka minut. Automatyzacja procesu gromadzenia danych, a także szybkość ich przetwarzania to kluczowe elementy platformy Cado.

Rozwiązanie oferowane przez startup charakteryzuje:

- **Szeroki zasięg** – analiza setek źródeł danych włącznie z dziennikami dostawców usług w chmurze, na dysku, w pamięci i nie tylko;
- **Przetwarzanie równoległe** – opatentowana technologia Cado ma pozwalać na przetwarzanie dużych zbiorów danych w kilka minut;
- **Wspólne analizy** – możliwość pracy nad jednym lub wieloma analizami jednocześnie z dowolnego miejsca;
- **Automatyzacja** – automatyczne ujawnianie kluczowych szczegółów incydentów, w tym pierwotnej przyczyny, zagrożonych ról i zasobów, oraz kompleksowej oś czasu zdarzeń;
- **Konfigurowalność** – możliwość dostosowania platformy przez konfigurowalne zestawy reguł i raportów.

IMMERSIVE LABS – AI W SŁUŻBIE CYBERBEZPIECZEŃSTWA

Sztuczna inteligencja – zwłaszcza ta generatywna – stała się ważnym elementem pracy wielu stanowisk technologicznych. Jednak trzeba mieć świadomość, że cyberprzestępcy też zaciągnęli ją do swojej pracy i niecnych celów. Mimo to – AI pomaga nam w kontekście cyberbezpieczeń-



stwa, czego przykładem jest rozwiązanie od Immersive Labs.

Startup wykorzystuje sztuczną inteligencję w celu tworzenia realistycznych scenariuszy. Dzięki nim zespoły mogą zdobyć umiejętności wykorzystania AI do zwiększania odporności organizacji na cyberzagrożenia.

Dane dotyczące wydajności poszczególnych osób i zespołów są kluczowe dla potwierdzenia możliwości całej organizacji. Immersive Labs umożliwia korzystanie z nich w ramach cyberbezpieczeństwa, co pozwala na ciągłe dostosowywanie się do zmieniających się warunków i zagrożeń.

Dzięki wiarygodnym wskaźnikom oraz odpowiedniej ocenie postępów, zespoły ds. cyberbezpieczeństwa mogą lepiej zrozumieć działanie cyberprzestępców. Co więcej – dzięki rozwiązaniu od Immersive Labs możliwe jest skrócenie czasu reakcji na incydenty oraz umiejętne zarządzanie cyberkryzysami. Ponadto platforma ma wspierać proces rekrutacji, pomagając w identyfikacji i zatrudnianiu wysokiej jakości talentów w obszarze cyberbezpieczeństwa.

Immersive Labs umożliwia także kodowanie bezpiecznie oraz identyfikację luk w aplikacjach i środowiskach chmurowych. Skupia się na redukcji luk w zabezpieczeniach na wczesnym etapie oraz w całym cyklu życia oprogramowania (SDLC), co przyczynia się do zwiększenia bezpieczeństwa systemów.

To jednak nie koniec, bo platforma pomaga w optymalizacji kosztów związanych z cyberbezpieczeństwem poprzez skonsolidowanie szkoleń, redukcję zależności od zewnętrznych konsultantów oraz podejmowanie świado-

mych decyzji inwestycyjnych opartych na ryzyku, co zmniejsza ryzyko kar finansowych.

Świat cyberbezpieczeństwa jest niezwykle zróżnicowany. Niektóre działania rozwiązania startupów skupiają się na nowych technologiach, takich jak AI, inne pomagają się zabezpieczyć przed znanymi już od dawna zagrożeniami takimi jak ransomware. Niezależnie od tego na jakim aspekcie się skupimy – o cyberbezpieczeństwo zwyczajnie trzeba dbać.

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

Skontaktuj się z nami

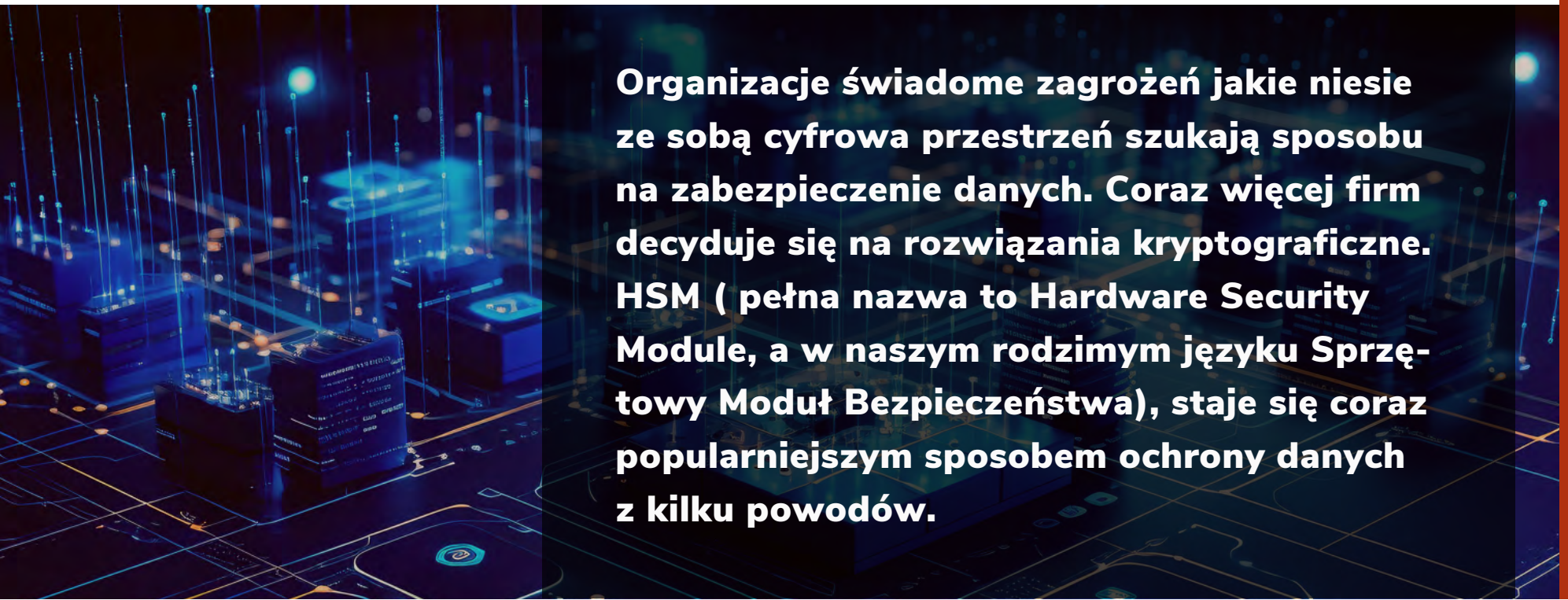
redakcja@securitymagazine.pl

+48 22 390 91 05
+48 518 609 987

Deadline:
wydanie styczniowe: do 10.12
wydanie lutowe: do 22.01

JAK SZYFROWANIE KRYPTOGRAFICZNE CHRONI ZASOBY FIRMY?

Przemysław Sobczyk
Perceptus Sp z o. o.



Organizacje świadome zagrożeń jakie niesie ze sobą cyfrowa przestrzeń szukają sposobu na zabezpieczenie danych. Coraz więcej firm decyduje się na rozwiązania kryptograficzne. HSM (pełna nazwa to Hardware Security Module, a w naszym rodzimym języku Sprzętowy Moduł Bezpieczeństwa), staje się coraz popularniejszym sposobem ochrony danych z kilku powodów.

CZYM JEST HSM?

HSM to sprzętowy moduł bezpieczeństwa do zabezpieczenia najważniejszych danych serwerów oraz aplikacji. Umożliwia generowanie i przechowywanie kluczy kryptograficznych w chronionym, odizolowanym środowisku. Obejmuje on oprogramowanie integracyjne, które obsługuje standardy branżowe (np. PKCS#11, Microsoft CSP/CNG, JCE, OpenSSL). Dzięki temu urządzenia te charakteryzują się:

- najwyższym poziomem bezpieczeństwa – zapewniają niezawodną ochronę fizyczną i logiczną materiału kryptograficznego,
- najwyższą wydajnością działania,
- prostotą wdrożenia – zarówno w nowej, jak i w istniejącej infrastrukturze.

JAKIE PLATFORMY SPRZĘTOWE MOŻNA “UZBROIĆ” W HSM?

Dzięki modułowej budowie systemu, urządzenia te działają na wszystkich platformach sprzętowych – od kart PCIe po dedykowane urządzenia typu appliance. Istnieje szereg możliwości w kwestii wyboru odpowiedniego urządzenia.

Urządzenia PCIe są przewidziane do wykorzystania w autonomicznych serwerach i urządzeniach w istniejącej już infrastrukturze IT bez potrzeby jej modyfikacji. Oferują najlepszy stosunek ceny do efektywności i zapewniają mniejsze wykorzystanie zasobów serwerów. Umożliwiają zdalną administrację i oprócz bezpiecznego zarządzania kluczami są w stanie wykryć sabotaż.

Serwer LAN HSM znajdzie zastosowanie tam, gdzie zalecane jest fizyczne odseparowanie modułu szyfrującego od reszty infrastruktury sprzętowej. Urządzenia te są w pełni skalowalne i dają możliwość klastrowania i równoległego dostępu z wielu urządzeń w sieci. Poza tym charakteryzują się rozbudowaną zdalną konfiguracją i zdolnością do wykrycia sabotażu.

Hardware Security Module wykorzystywany jest wszędzie tam, gdzie trzeba:

- **Podnieść bezpieczeństwo cyfrowych informacji:** funkcje jakie zapewnia, to m. in. ochrona zasobów, podwojona kontrola, bezpieczeństwo pierwszego kontaktu i szyfrowanie baz danych,
- **Usprawnić procesy:** tu niezwykle przydatne są funkcje takie jak: weryfikacja zgodności kluczy, szybki czas wdrożenia, szyfrowanie i deszyfrowanie danych kluczami kryptograficznymi,

- **Zarządzać operacjami kryptograficznymi:** HSM pozwala na tworzenie struktury uprawnień, tworzenie kluczy prywatnych/publicznych, stosownie do algorytmu, współpracę z aplikacjami poprzez ustandaryzowane interfejsy, generowanie cyfrowych certyfikatów, wydawanie i akceptowanie wniosków o kluczowe dane, posiada miejsce na kilkaset kluczy.

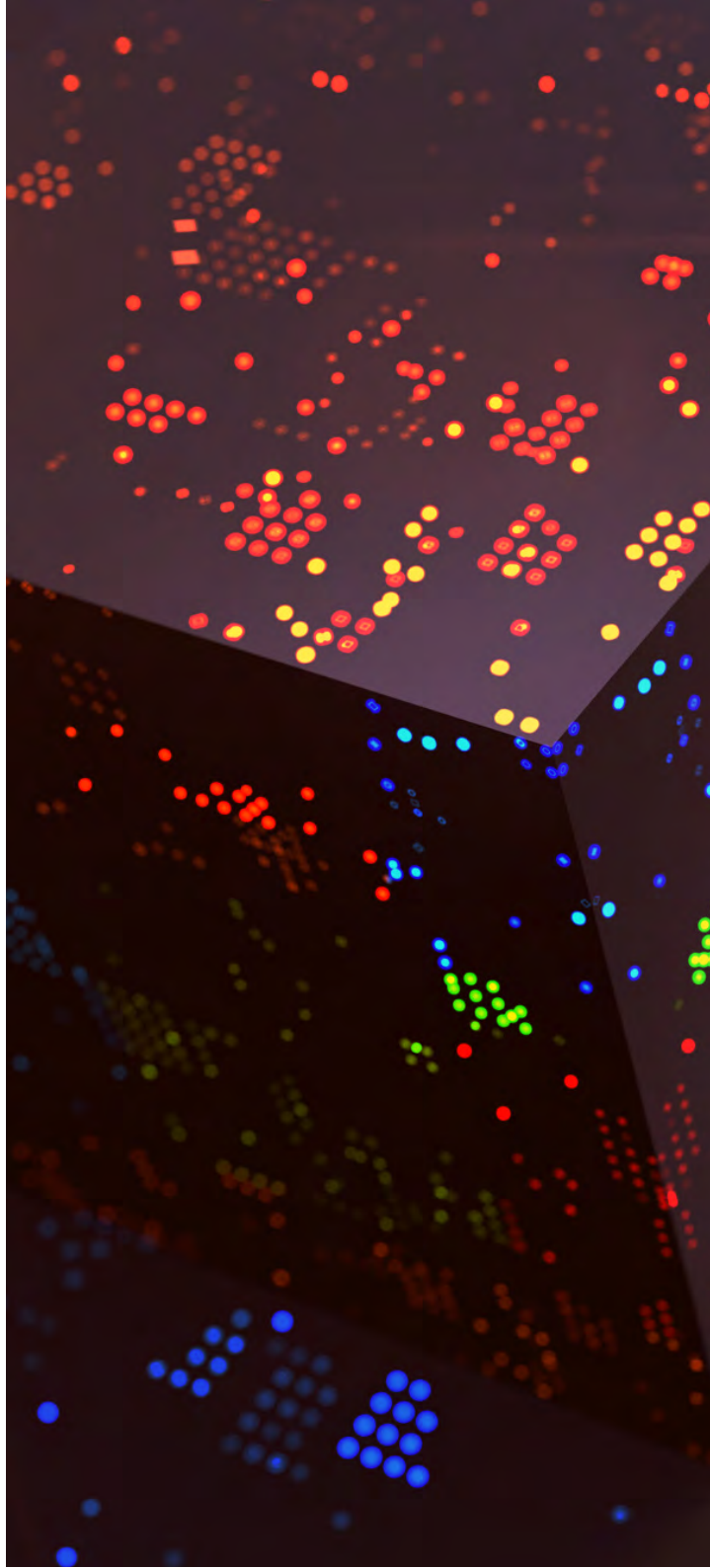
KIEDY WARTO SKORZYSTAĆ Z KRYPTOGRAFII?

HSM nie jest rozwiązaniem niezbędnym w każdej organizacji. Wybór sprzętowego modułu bezpieczeństwa powinien być podyktowany ilością i istotnością danych, do których dostęp należy ograniczać.

Analiza zasobów informacyjnych organizacji jest jednym z filarów cyberbezpieczeństwa. Jeśli organizacja dysponuje dużą ilością danych wrażliwych lub danymi o kluczowym znaczeniu, dostęp do nich powinien być ograniczony. Nie mam tu na myśli jedynie zewnętrznego dostępu. Ograniczenia dostępu do danych kluczowych warto wprowadzić również wewnątrz organizacji. Zabezpieczenia sprzętowe znacząco przy tym pomagają i są bardziej odporne na złamanie niż systemowe ograniczenia, choć te z pewnością też rozwiązują problem powszechnej dostępności informacji.

Hardware Security Module często stosuje się do przechowywania materiału kryptograficznego (kluczy), które wykorzystywane są do szyfrowania danych cyfrowych w procesach i transakcjach biznesowych. Kluczy szyfrujących używa się m. in. do:

- zabezpieczenia cyfrowego dokumentów elektronicznych w urzędach i instytucjach,
- zarządzania kluczami dostępu i bezpieczeństwem w ramach wymiany danych,
- bezpiecznego generowania kluczy do szyfrowania transakcji w Internecie,
- przechowania tych kluczy w sposób uniemożliwiający ich kopiowanie i przenoszenie,
- umożliwienie kontroli nad poufnymi danymi kryptograficznymi.



WYDAJNOŚĆ I SKALOWALNOŚĆ HSM

HSM to wydajne rozwiązanie, które zapewnia sprawną pracę i możliwość skalowania infrastruktury, co z kolei pozwala organizacjom obsługiwać duże ilości danych i transakcji kryptograficznych. Ma to szczególne znaczenie np. przy zabezpieczaniu danych płatniczych w handlu elektronicznym.

Coraz więcej standardów nakłada na organizacje obowiązek ochrony danych, np. PCI DSS, HIPAA czy GDPR. Szyfrowanie danych przy pomocy HSM pomaga organizacjom spełniać te wymagania. Rozwiązania, które w Perceptus oferujemy naszym klientom gwarantują najwyższy poziom zabezpieczenia danych wrażliwych w chronionym, odizolowanym środowisku.

Dowodem tego są certyfikaty z USA FIPS 140-2 Level 3 oraz Level 4 i europejski certyfikat eIDAS Common Criteria EAL4+.

JAK DOKŁADNIE DZIAŁA SZYFROWANIE PRZY UŻYCIU HSM?

Szyfrowanie z wykorzystaniem HSM opiera się na następujących czynnościach:

Generowanie kluczy kryptograficznych

HSM generuje klucze o wysokiej entropii, co oznacza, że są one trudne do odgadnięcia przez potencjalnego atakującego. Klucze te są przechowywane wewnątrz HSM i są dostępne tylko dla upoważnionych użytkowników, posiadających odpowiednie uprawnienia zapisane na dedykowanej karcie inteligentnej.

Przechowywanie kluczy

Dostęp do kluczy jest ściśle kontrolowany i wymaga autoryzacji, za pomocą jednego bądź dwóch składników autoryzacji

Szyfrowanie danych

Aby zaszyfrować dane, użytkownik lub aplikacja musi zwrócić się do HSM z prośbą o wykorzystanie odpowiedniego klucza kryptograficznego do szyfro-

wania danych. HSM wykonuje operację szyfrowania, używając klucza, który jest przechowywany wewnątrz urządzenia.

Deszyfracja danych

Aby odczytać zaszyfrowane dane, użytkownik lub aplikacja musi również zwrócić się do HSM z prośbą o wykorzystanie odpowiedniego klucza kryptograficznego do deszyfrowania danych.

Kontrola dostępu do kluczy kryptograficznych

HSM zapewnia również kontrolę dostępu do kluczy kryptograficznych i operacji szyfrowania/deszyfrowania. Tylko upoważnieni użytkownicy lub aplikacje mają dostęp do kluczy i mogą wykonywać operacje kryptograficzne.

Monitorowanie

HSM natywnie rejestruje operacje związane z kluczami i kryptografią, co umożliwia identyfikowanie prób nieautoryzowanego dostępu,ataków lub nadmiernego użycia.

Chcesz wdrożyć HSM w swojej infrastrukturze? Porozmawiajmy!

SECURITYMAGAZINE.PL

WYKRYWANIE CVE PRZY UŻYCIU NOWOCZESNYCH SKANERÓW

Bogdan Barchuk
Intellias

W tym artykule omówione zostaną wyzwania stojące przed nowoczesnymi programami skanującymi w zakresie wykrywania podatności oprogramowania przy użyciu systemu Common Vulnerabilities and Exposures (CVE). Formatowi NIST University, który jest używany do opisywania podatności i zagrożeń, brakuje standaryzacji i szczegółowości, co utrudnia nowoczesnym programom skanującym powiązanie podatności i zagrożeń z oprogramowaniem, którego one dotyczą.

W rezultacie nowoczesne programy skanujące bazują na niekompletnych lub niedokładnych danych, co prowadzi do uzyskiwania fałszywych wyników pozytywnych i negatywnych. Aby sprostać tym wyzwaniom, NIST musi podjąć działania w kierunku standaryzacji formatu, natomiast dostawcy powinni dostarczać dokładnych i szczegółowych informacji o swoich produktach i wersjach. W poniższym artykule analizie poddane zostanę różne narzędzia oceny podatności wraz z podkreśleniem różnic w ich definicjach. Ponadto przedstawione zostaną różne metody wykrywania nowych podatności i zagrożeń w czasie rzeczywistym, takie jak oficjalne repozytorium CVE w serwisie GitHub, Twitter i kanał RSS.

GLOBALNE PROBLEMY DOTYCZĄCE CVE

System Common Vulnerabilities and Exposures (CVE) jest kluczowym aspektem cyberbezpieczeństwa, który pomaga identyfikować i śledzić podatności w różnych rodzajach oprogramowania. Skuteczność systemu CVE zależy jednak w dużej mierze od ich dokładnego wykrywania i powiązania z oprogramowaniem, którego dane zagrożenia dotyczą. Nowoczesne programy skanujące odgrywają kluczową rolę w wykrywaniu podatności i zagrożeń, jednak napotykają znaczne trudności związane z formatem NIST University, który jest używany do opisywania podatności. W artykule omówione zostaną wyzwania stojące przed nowoczesnymi programami skanującymi w zakresie wykrywania podatności i zagrożeń. Zaproponowano w nim również rozwiązania, które pozwolą sprostać tym wyzwaniom.

Podatności i zagrożenia w systemie CVE często nie zawierają szczegółowych informacji na temat wersji oprogramowania, których dotyczą, co utrudnia określenie zakresu konkretnych podatności. Ponadto niekompletne lub niedokładne dane oraz brak ścisłych standardów dotyczących podatności i zagrożeń spowodowały, że baza National Vulnerability Database (NVD) stosuje podejście oparte na najlepszych możliwych rozwiązaniach.

Dane CPE zawarte w systemie CVE mogą dostarczać cennych informacji, ale w przypadku braku prawidłowego raportowania mogą one prowadzić do wystąpienia fałszywych wyników pozytywnych lub fałszywych wyników negatywnych. Rozwiązanie tych kwestii ma kluczowe znaczenie dla poprawy dokładności i praktycznego zastosowania podatności i zagrożeń.

Ponadto istnieją inne bazy danych, takie jak baza podatności WordPress oraz chińska baza podatności, w których znajdują się podatności nieuwzględnione w bazie danych NIST, a także lista luk w zabezpieczeniach niemających przypisanego numeru CVE, ponieważ nie zostały zgłoszone ani zaakceptowane, mimo iż są autentyczne.

Niektóre podatności mogą być również oznaczone jako podatności MS (Microsoft), ale nie mają przypisanego numeru CVE, co utrudnia ich znalezienie i powiązanie z konkretnymi produktami, których dotyczą.

CVE to uznany na całym świecie system służący do identyfikowa-

nia i śledzenia publicznie znanych podatności w różnym oprogramowaniu. System ten przypisuje każdej podatności unikatowy identyfikator, który ułatwia specjalistom ds. cyberbezpieczeństwa śledzenie tych podatności oraz ograniczanie ich wpływu na bezpieczeństwo. System CVE jest zarządzany przez National Institute of Standards and Technology (NIST), który prowadzi również bazę danych wszystkich podatności i zagrożeń. System CVE przyczynił się w kluczowy sposób do zapobiegania cyberatakom i poprawy ogólnego bezpieczeństwa różnego oprogramowania.

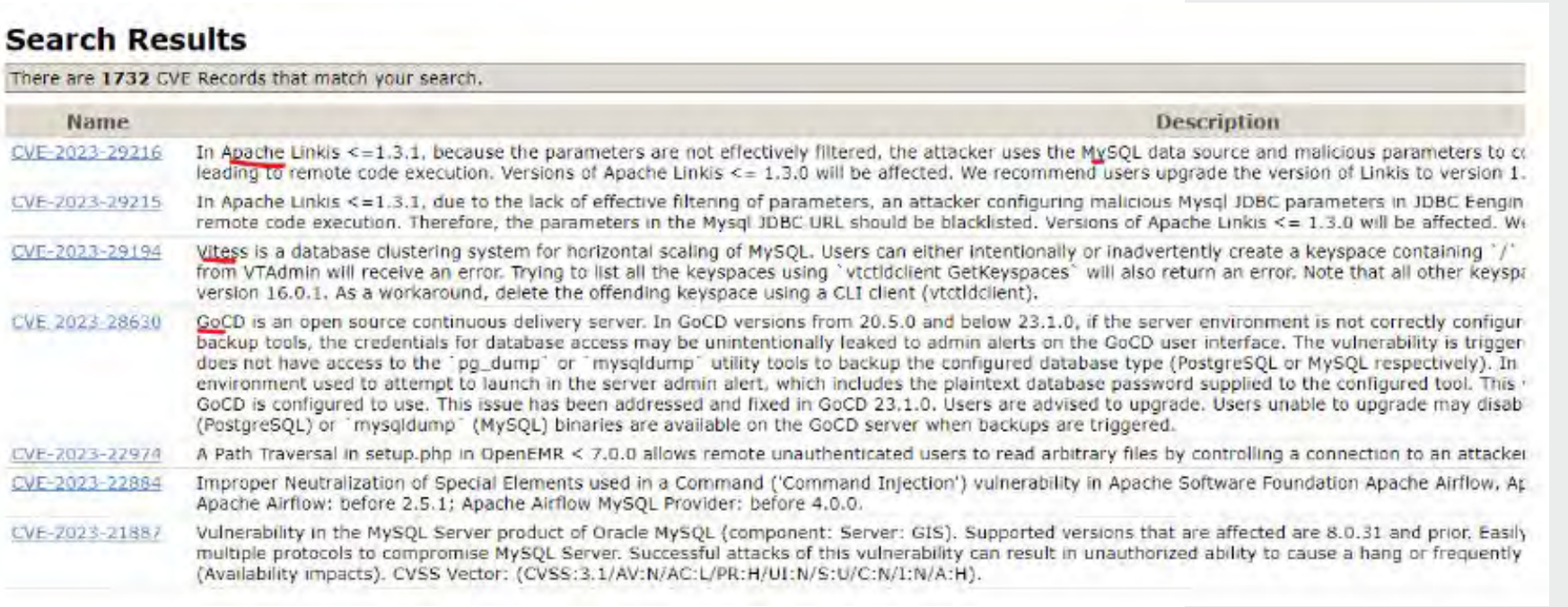
Skuteczność systemu CVE zależy jednak w dużej mierze od możliwości nowoczesnych programów skanujących w zakresie wykrywania podatności i zagrożeń oraz powiązania ich z oprogramowaniem, którego dotyczą. Nowoczesne programy skanujące wykorzystują różne metody wykrywania podatności, takie jak sygnatury podatności oraz programy skanujące podatności. Borykają się one jednak z problemami wykrywania podatności i zagrożeń z powodu problemów z formatem NIST University.

PROBLEM Z WYSZUKIWANIEM PODATNOŚCI I ZAGROŻEŃ

Do tej pory z programem CVE współpracowały 284 organizacje z 36 krajów. CNA (CVE Numbering Authority) to organizacje z całego świata, które mają upoważnienie do przypisywania identyfikatorów CVE (CVE ID) i publikowania rekordów CVE dotyczących podatności w określonych produktach w ramach odrębnego zakresu, który został dla nich uzgodniony, do uwzględniania w pierwszych podatności. Może to prowadzić do problemów w zależności od jakości moderacji konkretnych podatności i zagrożeń.

Wyszukiwanie według dostawcy lub technologii na stronie CVE jest problematyczne z powodu braku odpowiednich filtrów.

CPE (Common Platform Enumeration) istnieje, jednak nie jest możliwe wyszukiwanie według CPE, dopóki nie jest zaktualizowane o aktywne dane systemu CVE, co sprawia, że jest bezużyteczne.



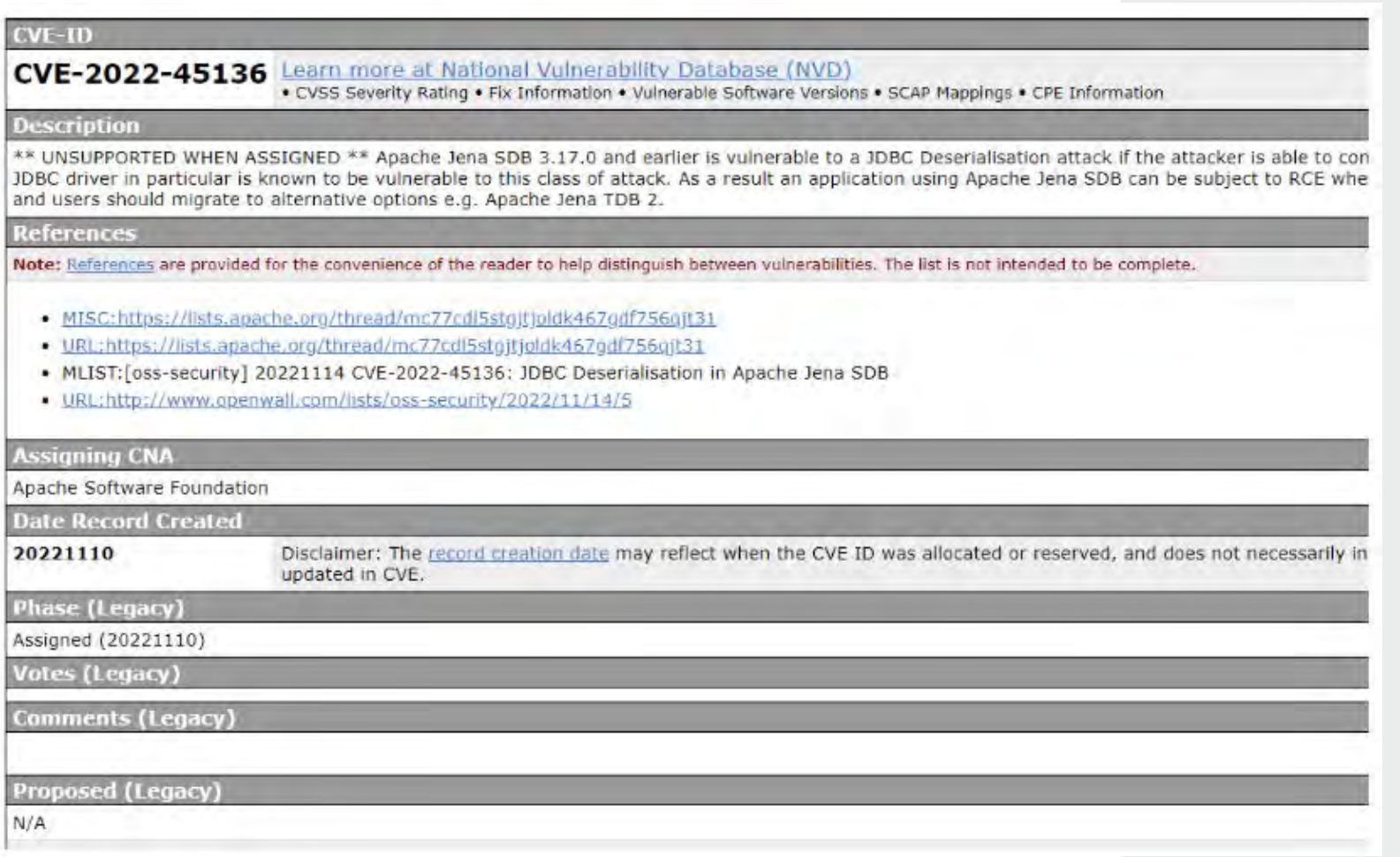
Search Results

There are **1732** CVE Records that match your search.

Name	Description
CVE-2023-29216	In Apache Linkis <=1.3.1, because the parameters are not effectively filtered, the attacker uses the MySQL data source and malicious parameters to c leading to remote code execution. Versions of Apache Linkis <= 1.3.0 will be affected. We recommend users upgrade the version of Linkis to version 1.
CVE-2023-29215	In Apache Linkis <=1.3.1, due to the lack of effective filtering of parameters, an attacker configuring malicious Mysql JDBC parameters in JDBC Engin remote code execution. Therefore, the parameters in the Mysql JDBC URL should be blacklisted. Versions of Apache Linkis <= 1.3.0 will be affected. W
CVE-2023-29194	Vitess is a database clustering system for horizontal scaling of MySQL. Users can either intentionally or inadvertently create a keyspace containing `/` from VTAdmin will receive an error. Trying to list all the keyspaces using `vtctldclient GetKeyspaces` will also return an error. Note that all other keysp version 16.0.1. As a workaround, delete the offending keyspace using a CLI client (vtctldclient).
CVE-2023-28630	GoCD is an open source continuous delivery server. In GoCD versions from 20.5.0 and below 23.1.0, if the server environment is not correctly configur backup tools, the credentials for database access may be unintentionally leaked to admin alerts on the GoCD user interface. The vulnerability is trigger does not have access to the `pg_dump` or `mysqldump` utility tools to backup the configured database type (PostgreSQL or MySQL respectively). In environment used to attempt to launch in the server admin alert, which includes the plaintext database password supplied to the configured tool. This GoCD is configured to use. This issue has been addressed and fixed in GoCD 23.1.0. Users are advised to upgrade. Users unable to upgrade may disab (PostgreSQL) or `mysqldump` (MySQL) binaries are available on the GoCD server when backups are triggered.
CVE-2023-22974	A Path Traversal in setup.php in OpenEMR < 7.0.0 allows remote unauthenticated users to read arbitrary files by controlling a connection to an attacke
CVE-2023-22884	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Ap Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0.
CVE-2023-21887	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.31 and prior. Easily multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Rysunek 1. Przykład wyszukiwania dla MySQL pokazuje kilka losowych podatności i zagrożeń

Rysunek 2. Przykład podatności i zagrożeń, w którym wyraźnie brakuje następujących elementów: dostawca, zagrożona wersja, CPE, dotkliwość, poprawka itp



CVE-ID

CVE-2022-45136 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** UNSUPPORTED WHEN ASSIGNED ** Apache Jena SDB 3.17.0 and earlier is vulnerable to a JDBC Deserialisation attack if the attacker is able to con JDBC driver in particular is known to be vulnerable to this class of attack. As a result an application using Apache Jena SDB can be subject to RCE whe and users should migrate to alternative options e.g. Apache Jena TDB 2.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://lists.apache.org/thread/mc77cdl5stgjtjpldk467gdf756qjt31
- URL:https://lists.apache.org/thread/mc77cdl5stgjtjpldk467gdf756qjt31
- MLIST:[oss-security] 20221114 CVE-2022-45136: JDBC Deserialisation in Apache Jena SDB
- URL:http://www.openwall.com/lists/oss-security/2022/11/14/5

Assigning CNA

Apache Software Foundation

Date Record Created

20221110 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily in updated in CVE.

Phase (Legacy)

Assigned (20221110)

Votes (Legacy)

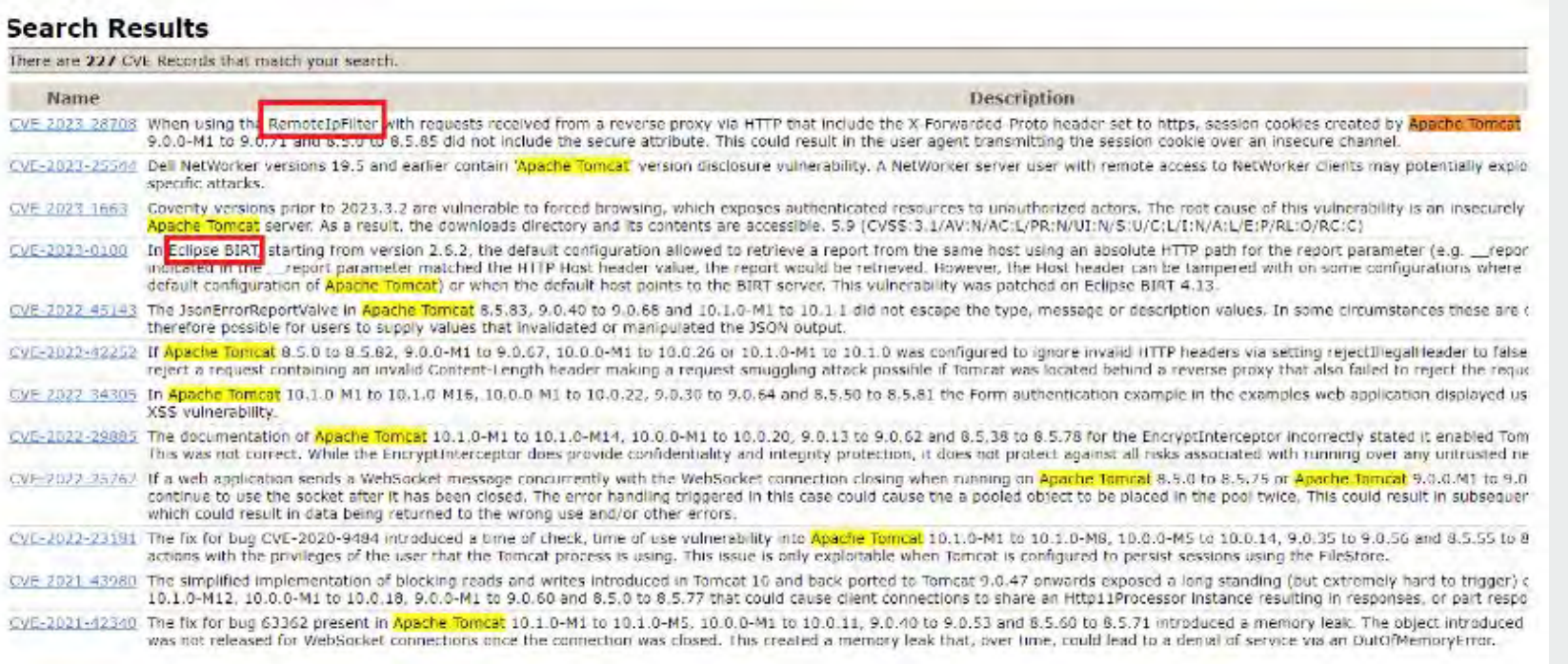
Comments (Legacy)

Proposed (Legacy)

N/A

Dodatkowo nie widzimy informacji o statusie możliwości wykorzystania luki w zabezpieczeniach, powiązanych linkach do luki w zabezpieczeniach i i powiązanych podatności i zagrożeń, co sprawia, że od początku jest bardzo źle sformatowany do pracy i wyszukiwania błędów.

Rysunek 3. Przykład kolejnego wyszukiwania



Search Results

There are 227 CVE Records that match your search.

Name	Description
CVE-2023-28708	When using the RemoteIpFilter with requests received from a reverse proxy via HTTP that include the X-Forwarded-Proto header set to https, session cookies created by Apache Tomcat 9.0.0-M1 to 9.0.71 and 8.5.0 to 8.5.85 did not include the secure attribute. This could result in the user agent transmitting the session cookie over an insecure channel.
CVE-2023-25504	Dell NetWorker versions 19.5 and earlier contain 'Apache Tomcat' version disclosure vulnerability. A NetWorker server user with remote access to NetWorker clients may potentially explo specific attacks.
CVE-2023-1663	Coverity versions prior to 2023.3.2 are vulnerable to forced browsing, which exposes authenticated resources to unauthorized actors. The root cause of this vulnerability is an insecurely Apache Tomcat server. As a result, the downloads directory and its contents are accessible. 5.9 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/E:P/RL:O/RC:C)
CVE-2023-0100	In Eclipse BIRT starting from version 2.6.2, the default configuration allowed to retrieve a report from the same host using an absolute HTTP path for the report parameter (e.g. __repor indicated in the __report parameter matched the HTTP Host header value, the report would be retrieved. However, the Host header can be tampered with on some configurations where default configuration of Apache Tomcat) or when the default host points to the BIRT server. This vulnerability was patched on Eclipse BIRT 4.13.
CVE-2022-45143	The JsonErrorReportValve in Apache Tomcat 8.5.83, 9.0.40 to 9.0.68 and 10.1.0-M1 to 10.1.1 did not escape the type, message or description values. In some circumstances these are therefore possible for users to supply values that invalidated or manipulated the JSON output.
CVE-2022-42252	If Apache Tomcat 8.5.0 to 8.5.82, 9.0.0-M1 to 9.0.67, 10.0.0-M1 to 10.0.26 or 10.1.0-M1 to 10.1.0 was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the requ
CVE-2022-34305	In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed us XSS vulnerability.
CVE-2022-29885	The documentation of Apache Tomcat 10.1.0-M1 to 10.1.0-M14, 10.0.0-M1 to 10.0.20, 9.0.13 to 9.0.62 and 8.5.38 to 8.5.78 for the EncryptInterceptor incorrectly stated it enabled Tom This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted ne
CVE-2022-25762	If a web application sends a WebSocket message concurrently with the WebSocket connection closing when running on Apache Tomcat 8.5.0 to 8.5.75 or Apache Tomcat 9.0.0-M1 to 9.0 continue to use the socket after it has been closed. The error handling triggered in this case could cause the a pooled object to be placed in the pool twice. This could result in subsequer which could result in data being returned to the wrong use and/or other errors.
CVE-2022-23181	The fix for bug CVE-2020-9484 introduced a time of check, time of use vulnerability into Apache Tomcat 10.1.0-M1 to 10.1.0-M8, 10.0.0-M5 to 10.0.14, 9.0.35 to 9.0.56 and 8.5.55 to 8 actions with the privileges of the user that the Tomcat process is using. This issue is only exploitable when Tomcat is configured to persist sessions using the FileStore.
CVE-2021-43980	The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) c 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part respo
CVE-2021-42340	The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError.

Na powyższym zrzucie ekranu (Rysunek 3) wyraźnie widać, że wyszukujemy podatności dotyczące systemu Ttomcat i otrzymujemy losowe dane wyjściowe z produktami, które nie były wyszukiwane. Oznacza to, że wyszukiwanie jest nieścisłe i nie ma możliwości sprawienia, by było one w pełni precyzyjne w przypadku braku podania CPE.

MITREMITRE PONOWNIE UDERZA Z SZALONYMI CVE: WIDEO RHYTHM NATION I ALGORYTM REKOMENDACJI TWITTERA

Firma Microsoft ujawniła nową podatność, która może wydawać się niedorzeczna, jednak w rzeczywistości nadano jej faktyczny numer podatności i zagrożeń CVE-2022-38392. Podatność ta występuje podczas odtwarzania teledysku Janet Jackson pt. „Rhythm Nation” (1989), powodując nieprawidłowe działanie i awarię niektórych dys-

ków twardych w laptopach wyprodukowanych około 2005 roku. Dziwnym zjawiskiem jest to, że częstotliwości występujące w teledysku powodują występowanie rezonansu w dyskach twardych, nie tylko na urządzeniu odtwarzającym teledysk, ale także na innych urządzeniach znajdujących się w pobliżu. Numer CVE został przypisany na podstawie wpisu na blogu firmy Microsoft, a podatność została wyeliminowana przez niestandardowy filtr audio.

Fakt, że numer CVE został przypisany do tak nietypowej podatności, pokazuje brak jakiejkolwiek realnej bariery wejścia dotyczącej rejestracji numerów CVE. Instytucje nadające numery CVE mogą przypisać numery CVE prawie do wszystkiego, bez względu na to, jak absurdalne lub niepotwierdzone jest dane uzasadnienie. Przykładem tego jest inny numer podatności i zagrożenia CVE-2023-29218, który został przypisany do algorytmu rekomendacji serwisu Twitter. Algorytm ten pozwala użytkownikom na negatywne ocenianie użytkowników, powodując obniżenie ich wyniku reputacji. Obecnie ten numer CVE jest podany na stronie internetowej National Vulnerability Database jako „W TRAKCIE ANALIZY”.

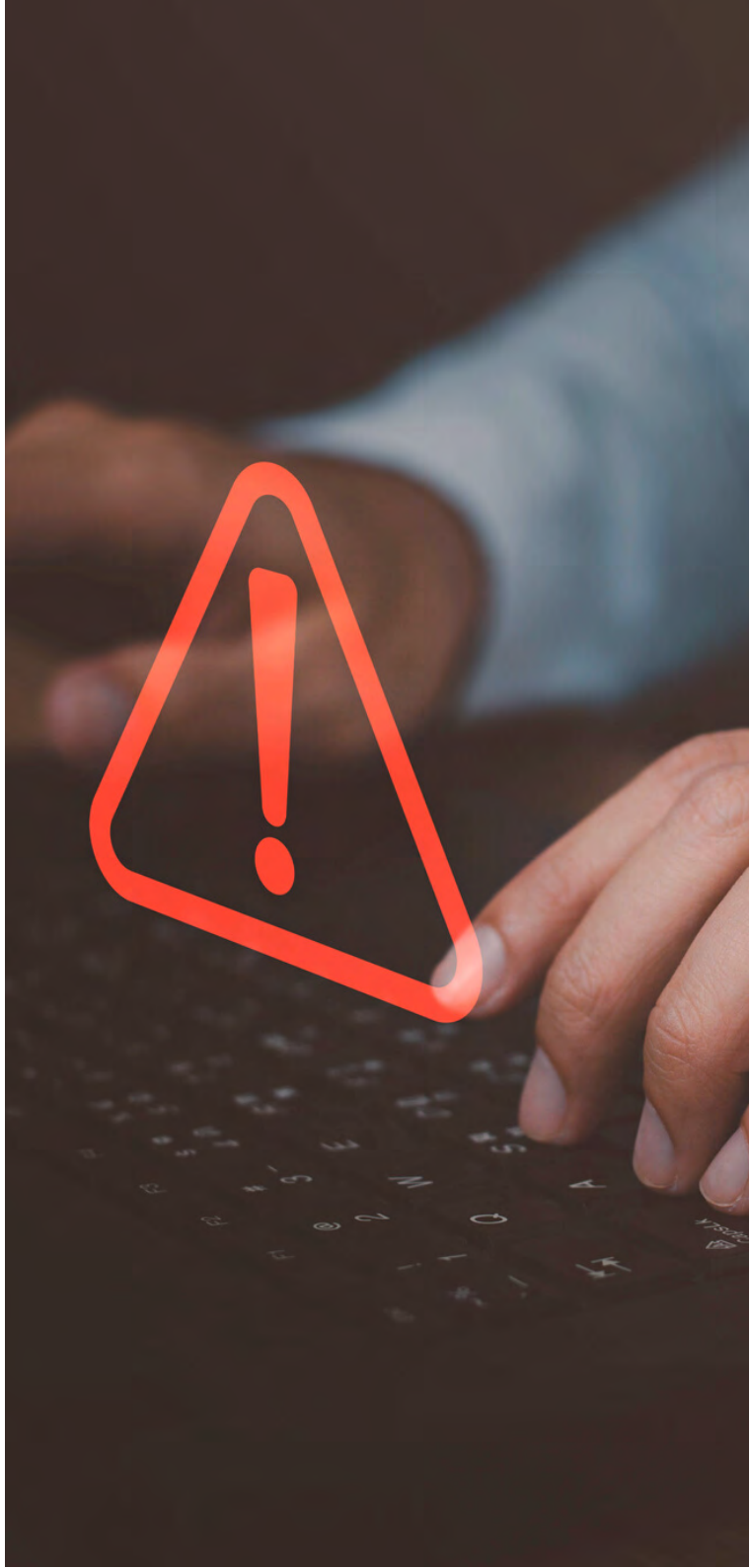
Badacze mają trudności ze zgłaszaniem i naprawianiem krytycznych podatności, podczas gdy takie niedorzeczne przypadku CVE są przypisywane do mało poważnych błędów. Sytuacja ta budzi obawy dotyczące procesu rejestracji

CVE i znaczenia priorytetowego traktowania faktycznych podatności w zabezpieczeniach w stosunku do tych o trywialnym charakterze.

WYZWANIA ZWIĄZANE Z FORMATEM NIST UNIVERSITY

Format NIST University jest używany do szczegółowego opisu podatności i zagrożeń, z uwzględnieniem oprogramowania, wersji i innych istotnych informacji. Jednak format ten nie zawsze jest spójny, co utrudnia nowoczesnym programom skanującym powiązanie podatności i zagrożeń z oprogramowaniem, którego one dotyczą. Jednym z głównych problemów związanych z formatem NIST University jest brak standaryzacji. Różni dostawcy stosują odmienne konwencje nazewnictwa, co utrudnia identyfikację i śledzenie podatności i zagrożeń. Inną kwestią związaną z formatem NIST University jest brak szczegółowości w identyfikacji oprogramowania i jego wersji. Format często wykorzystuje ogólne terminy, które nie dostarczają nowoczesnym programom skanującym wystarczających informacji, które pozwalałyby dokładnie zidentyfikować zagrożone oprogramowanie. Ten brak szczegółowości utrudnia dostawcom powiązanie podatności i zagrożeń z ich produktami i wersjami (CPE).

Załóżmy na przykład, że chcemy wyszukać podatności w systemie MySQL. Można wyszukać je na stronie NIST lub w bazie danych luk w zabezpieczeniach, lecz w wynikach mogłoby pojawić się wiele nieistotnych rezultatów, które nie są bezpośrednio związane z MySQL. Wynika to z faktu, że nie ma normalnego sposobu wyszukiwania dostawcy i wersji bądź zakresu wersji, co prowadzi do dużej ilości niepożądanych i mało istotnych wyników.



Ponadto nowoczesne programy skanujące mają trudności związane z wyszukiwaniem i powiązaniem luk w zabezpieczeniach z określonymi podatnościami. Searchsploit to narzędzie, które pozwala użytkownikom wyszukiwać luki w zabezpieczeniach w lokalnej bazie danych. Baza danych opiera się jednak na dokładności bazy danych CVE, co może prowadzić do wystąpienia fałszywych wyników pozytywnych i fałszywych wyników negatywnych.

Witryna vulners.com jest kolejnym narzędziem, które agreguje dane z wielu źródeł, aby zapewnić kompleksowy wgląd w podatności i luki w zabezpieczeniach. Jednak narzędzie to również napotyka trudności związane z wyszukiwaniem luk w zabezpieczeniach oraz podatności i zagrożeń według wersji. Wynika to z braku standaryzacji w konwencjach nazewnictwa stosowanych przez dostawców i braku szczegółowości w formacie NIST University.

Ponadto niektórzy dostawcy, jak np. SentinelOne, wykorzystują oprogramowanie do tworzenia własnych podatności i zagrożeń w oparciu o oprogramowanie, ufając interfejsowi API NIST, co może powodować występowanie fałszywie wyników pozytywnych u klientów. Może to prowadzić do braku zaufania do systemu CVE i podważać skuteczność nowoczesnych programów skanujących w wykrywaniu podatności i zagrożeń.

PROPONOWANE ROZWIĄZANIA

Istnieje kilka rozwiązań, których wdrożenie pozwoliłoby rozwiązać problemy związane z formatem NIST University i powiązanymi kwestiami. Po pierwsze, NIST powinien dążyć do standaryzacji formatu, aby zapewnić spójność wszystkich podatności i zagrożeń. Taka standaryzacja ułatwi nowoczesnym programom skanującym identyfikację oraz śledzenie podatności i zagrożeń.

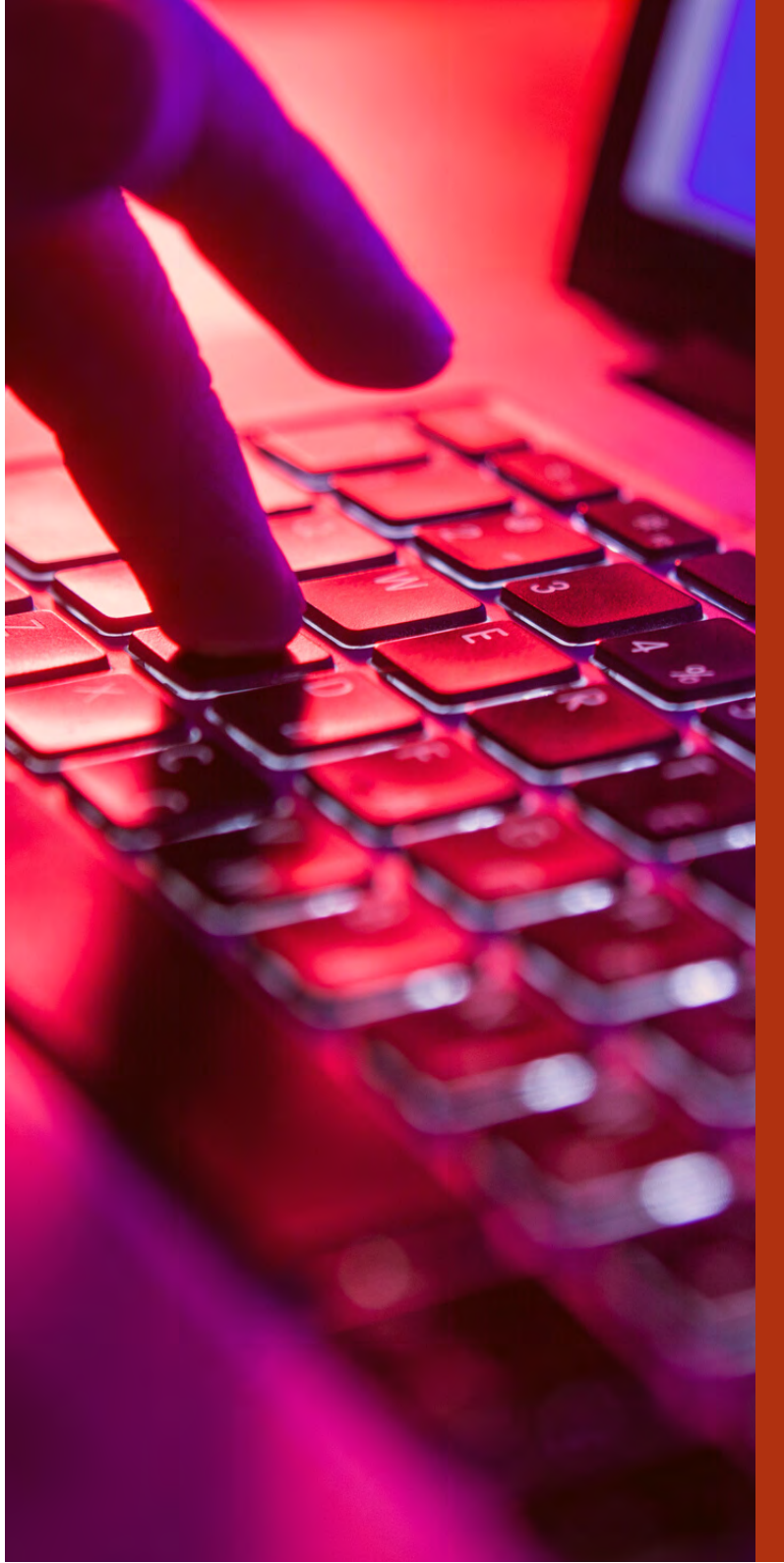
poważne konsekwencje dla cyberbezpieczeństwa z uwagi na problemy z formatem NIST University. Fałszywie pozytywne i fałszywie negatywne wyniki mogą prowadzić do braku zaufania do systemu CVE i podważać skuteczność nowoczesnych programów skanujących w wykrywaniu podatności.

Poprzez standaryzację formatu i zwiększając szczegółowość formatu NIST University, można poprawić dokładność i skuteczność nowoczesnych programów skanujących w zakresie wykrywania podatności oraz łagodzenia ich skutków. Dostawcy odgrywają również kluczową rolę w dostarczaniu dokładnych i szczegółowych informacji o swoich produktach i wersjach, co ułatwia nowoczesnym programom skanującym dokładne powiązanie podatności i zagrożeń z produktami, których one dotyczą.

INICJATYWA OVAL FIRMY MITRE

Oval (Open Vulnerability and Assessment Language) to międzynarodowy standardowy język używany do oceny i zgłaszania podatności w oprogramowaniu i systemach sprzętowych. Został on opracowany przez firmę MITRE w 2002 roku i od tego czasu jest utrzymywany przez społeczność programistów oraz ekspertów ds. zabezpieczeń.

Język Oval zapewnia ustrukturyzowany format możliwy do odczytu maszynowego służący do opisywania podatności, konfiguracji oraz poprawek.



Umożliwia to administratorom bezpieczeństwa oraz twórcom systemów szybką ocenę poziomu bezpieczeństwa ich systemów i ustalenie priorytetów w zakresie działań naprawczych.

Mimo że język Oval zyskał pewną popularność w społeczności cyberbezpieczeństwa, w rzeczywistości nie jest szeroko stosowany przez wszystkich specjalistów ds. zabezpieczeń. Może to wynikać z braku świadomości lub zrozumienia języka – jak również z faktu, że inne narzędzia do oceny podatności są bardziej popularne lub preferowane przez użytkowników.

Ponadto skuteczność języka Oval może się różnić w zależności od konkretnych potrzeb i wymagań organizacji w zakresie bezpieczeństwa. Mimo że język Oval jest skutecznym narzędziem, może nie być najlepszym rozwiązaniem dla każdego programu lub środowiska zabezpieczeń.

Należy jednak zauważyć, że określenie języka Oval jako „bezużytecznego" może nie być zgodne z prawdą. Być może nie jest on tak szeroko stosowany jak inne narzędzia do oceny podatności, jednak w dalszym ciągu służy wartościowym celom w społeczności cyberbezpieczeństwa i może pomóc organizacjom w poprawie ich stanu bezpieczeństwa. Obecnie Oval zawiera około 20270 definicji w serwisie GitHub, co sprawia, że jest około 10-krotnie mniejszym niż powinien być oficjalnie, jednak trudno jest przeanalizować te statystyki, gdyż w niektórych definicjach niektóre podatności i zagrożeń są uwzględnione wielokrotnie.

ANALIZA I PORÓWNANIE DEFINICJI PODATNOŚCI

Przeanalizowano jedno z najpopularniejszych źródeł do definiowania i wykrywania podatności w zabezpieczeniach. Wyniki pokazują dużą różnicę i niezbyt stabilną sytuację u wielu dostawców, co jest oczywistym dowodem na występowanie luki.

Na początku chcemy wskazać popularne miejsca przechowywania informacji dotyczących luk w zabezpieczeniach oraz podatności:

Są to oczywiście exploit-db i CVE firmy MITRE:
Nazwa: strona internetowa MITRE CVE
Liczba: 200 857 na stronie w porównaniu do 213 267 z repozytorium GitHub
Dodatkowe informacje:
Łączna liczba podatności miesięcznie w 2023 roku wyniesie średnio 270 w przypadku podatności o

Łatwy w użyciu format może obejmować następujące informacje: wersja lub zakres wersji, status „naprawione” lub „nienaprawione” oraz wersja, w której zagrożenie zostało naprawione, CPE, dokładna nazwa oprogramowania i możliwości z nim związane, powiązane oprogramowanie, powiązane luki w zabezpieczeniach, szczegółowy opis, status: luka możliwa do wykorzystania lub nie itp.

Po drugie, NIST powinien współpracować z dostawcami w celu zwiększenia szczegółowości formatu NIST University. Można to osiągnąć poprzez uwzględnienie w formacie bardziej szczegółowych informacji o produktach i wersjach oprogramowania, których dany problem dotyczy. Ułatwiłoby to nowoczesnym programom skanującym dokładne powiązanie podatności i zagrożeń z oprogramowaniem, którego dotyczą, a także ustalenie odpowiednich priorytetów dotyczących wprowadzania poprawek.

Po trzecie, dostawcy powinni dążyć do zapewnienia dokładnych i szczegółowych informacji o swoich produktach i wersjach (CPE). Powinni również dążyć do przyjęcia standardowego formatu opisu podatności, aby ułatwić nowoczesnym programom skanującym łączenie się z bazą danych podatności i zagrożeń.

Wyzwania stojące przed nowoczesnymi programami skanującymi w zakresie wykrywania podatności i zagrożeń mogą nieść

wysokim stopniu zagrożenia oraz 155 podatności krytycznych, które często dają atakującym możliwość zdalnego przejęcia kontroli nad systemami komputerowymi. W samym 2023 roku dodano już: 8488 podatności i zagrożeń o różnych poziomach krytyczności.
Adres URL: https://cve.mitre.org/

Nazwa: Exploit-db
Liczba: 45 423
Adres URL: https://www.exploit-db.com/
Nazwa programu skanującego: Nuclei
Liczba: 6318 szablonów podatności i zagrożeń
url:https://github.com/projectdiscovery/nuclei-templates
Dodatkowo: istnieje wiele alternatywnych rozwiązań do sondowania podatności i weryfikacji koncepcji wykrywania podatności, w większości opracowanych w Chinach.

Nazwa programu skanującego: Nessus Scanner
Liczba: 185 639 wtyczek
url:https://www.tenable.com/plugins/newest

Nazwa programu skanującego: OpenVAS
Liczba: Ponad 50 000 NVT
Adres URL: https://www.openvas.org/

Nazwa programu skanującego: Nmap
Liczba: Ponad 1250 modułów, które nie są oficjalnie aktualizowane, ostatnia aktualizacja sprzed 9 miesięcy
https://github.com/nmap/nmap/tree/master/scripts

Ponadto:
istnieje również kilka nieoficjalnych skryptów nmap, które można znaleźć w serwisie **GitHub** oraz jasne jest, że skrypty nse nie wyglądają na zbyt popularne

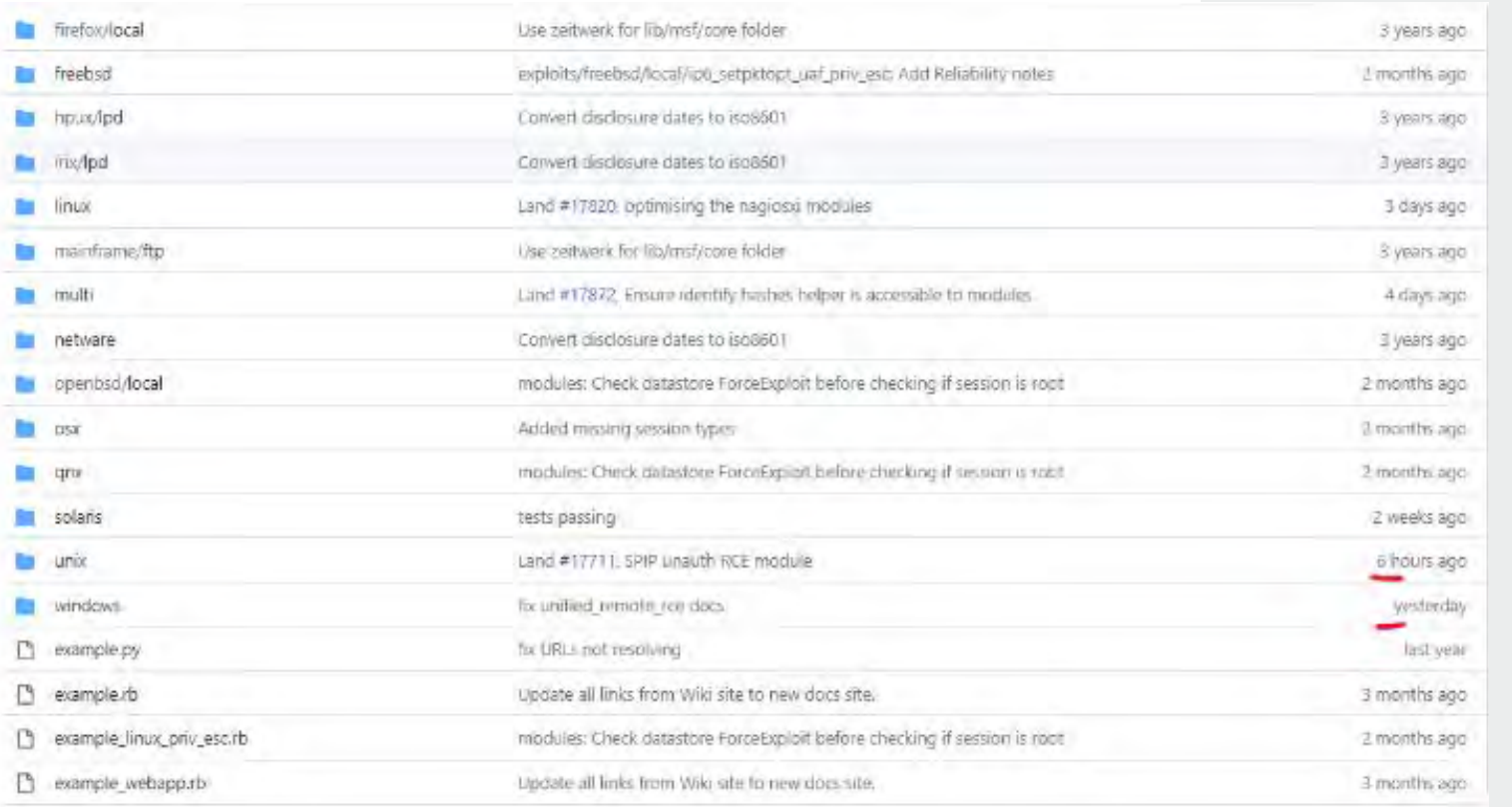
Tabela 1. Programy skanujące i informacje o nich (na str. 92)

Nazwa programu skanującego	Liczba	Dodatkowe informacje
Strona internetowa mitre CVE	200 857	Łączna liczba podatności miesięcznie w 2023 roku wyniesie średnio 270 w przypadku podatności o wysokim stopniu zagrożenia oraz 155 podatności krytycznych, które często dają atakującym możliwość zdalnego przejęcia kontroli nad systemami komputerowymi. W samym 2023 roku dodano już 8488 podatności i zagrożeń o różnych poziomach krytyczności. Adres URL: https://www.cvedetails.com/vulnerability-list/
OVAL CVE, konwersja	20 270	Konwersja OVAL CVE do określonego formatu Adres URL: https://github.com/CISecurity/OVALRepo/tree/master/repository/definitions/vulnerability
Exploit-db	45 423	Dobrze znana i ciesząca się największą popularnością witryna przechowująca informacje o podatnościach Adres URL: https://www.exploit-db.com/
Nuclei	6318	Istnieje wiele alternatywnych rozwiązań do sondowania podatności i weryfikacji koncepcji wykrywania podatności, w większości opracowanych w Chinach. Adres URL: https://github.com/projectdiscovery/nuclei-templates
Nessus Scanner	185 639	Adres URL: https://www.tenable.com/plugins/newest
OpenVAS/Greenbone	Ponad 50 000	Szablony NASM
Nmap	Ponad 1250	Ostatnia oficjalna aktualizacja miała miejsce 9 miesięcy temu. Istnieją również nieoficjalne skrypty Nmap, które można znaleźć w serwisie GitHub. Adres URL: https://github.com/nmap/nmap/tree/master/scripts, https://github.com/takeshixx/nmap-scripts

OpenVAS używa szablonów NASM, Nmap używa szablonów nse, Metasploit ma moduły pomocnicze w języku Ruby, Nexpose i Nessus mają swój własny zastrzeżony format, natomiast Nuclei ma otwarty format źródłowy do wykrywania podatności i zagrożeń.

Oczywistym wnioskiem jest więc, że programy skanujące nie zapewniają stabilności w kwestii posiadania określonego formatu do wykrywania podatności.

Moduły Metasploit są regularnie aktualizowane przez społeczność, a ponadto istnieje też komercyjna wersja Metasploit pro o większej liczbie aktualizacji oraz skuteczności działania, co sprawia, że jest to dobrze zaktualizowany mechanizm.



Rysunek 4. Przykładowe moduły Metasploit

Tabela 2. Podstawowe porównanie programów skanujących

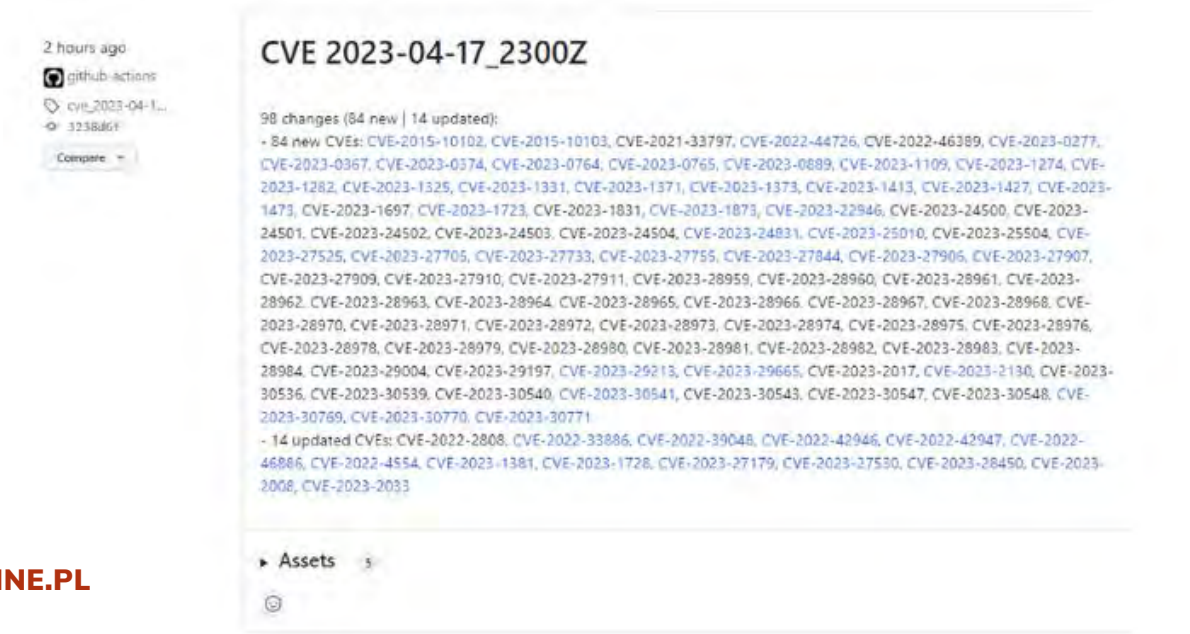
Program skanujący	Profil skanowania	Krytyczne	Wysokie	Średnie	Niskie	Info
Nessus 5	Profil sieci zewnętrznej	3	6	22	8	137
OpenVAS 5	Pełny profil skanowania kontrolnego	0	38	24	36	44
Nexpose	Pełny profil skanowania kontrolnego	49	103	18	0	0

W oparciu o ostatnie testy programów skanujących podatności Metasploitable2 oczywiste jest, że istnieje duża liczba problemów na rynku wykrywania podatności STANDART.

WYKRYWANIE NOWYCH PODATNOŚCI I ZAGROŻEŃ W CZASIE RZECZYWISTYM

Jest wiele sposobów otrzymywania bieżących informacji o oficjalnie publikowanych podatnościach.

Aktualizacje podatności i zagrożeń w serwisie GitHub i oficjalnej stronie są bardzo częste:



Jednak bardzo łatwo jest zauważyć nowe CVE za pomocą oficjalnego repozytorium GitHub, serwisu Twitter lub kanałów RSS.

Baza danych NVD, która jest w pełni zsynchronizowana z **listą CVE,** więc wszelkie aktualizacje systemu CVE pojawiają się natychmiast w bazie NVD, oferując następujące kanały treści CVE:

- Kanał JSON dotyczący podatności.
- Kanał RSS dotyczący podatności.
- Kanały tłumaczeń dotyczących podatności.
- Oświadczenia dostawców podatności.

Rysunek 5. Zrzut ekranu z Twittera CVE

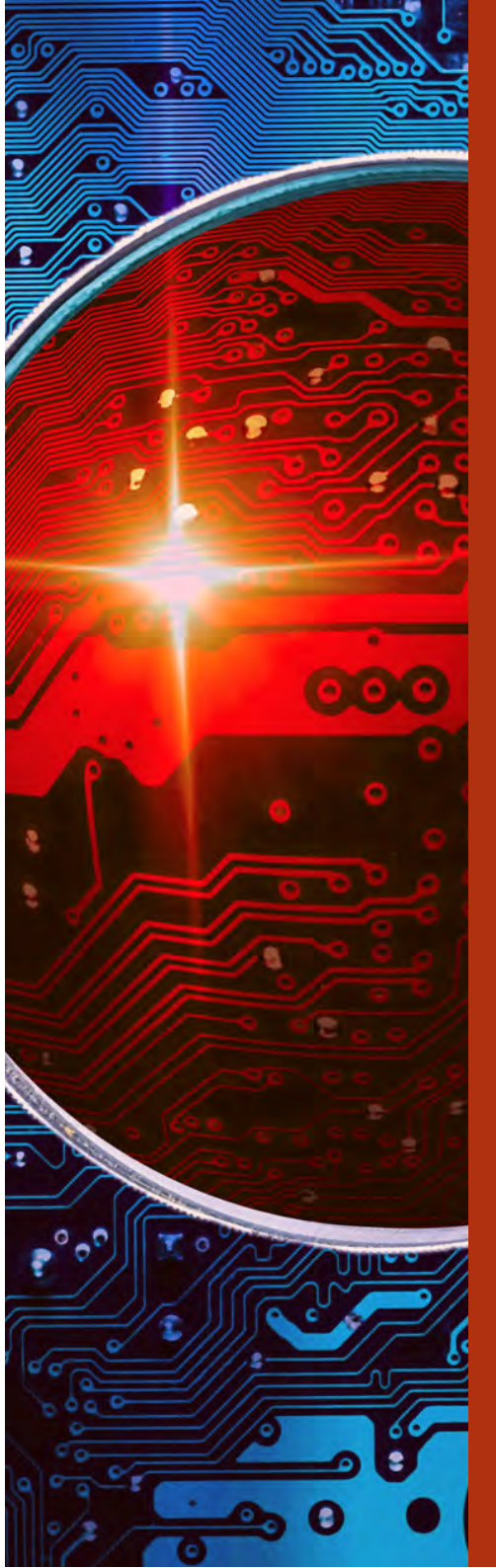
Twitter lub oficjalne kanały, które są bardzo często aktualizowane, mogą pomóc w terminowym zapobieganiu podatnościom i zagrożeniom.

PODSUMOWANIE

Wykrywanie i śledzenie przy użyciu systemu Common Vulnerabilities and Exposures (CVE) odgrywa kluczową rolę w dziedzinie cyberbezpieczeństwa. Nowoczesne programy skanujące borykają się jednak z wieloma problemami dotyczącymi wykrywania podatności i zagrożeń ze względu na problemy z formatem NIST University, gdyż jest on pozbawiony szczegółowości w zakresie identyfikowania produktów i wersji oprogramowania, których dotyczą dane problemy. Ponadto niekompletne lub niedokładne dane oraz brak ścisłych standardów dotyczących podatności i zagrożeń powodują, że baza National Vulnerability Database (NVD) stosuje podejście oparte na najlepszych możliwych rozwiązaniach.

Standaryzacja formatu i poprawa specyfiki formatu NIST University ma kluczowe znaczenie dla poprawy dokładności i użyteczności systemu CVE. Dostawcy muszą również zaopatrywać w dokładne i szczegółowe informacji o swoich produktach i wersjach. Ponadto istnieje potrzeba stworzenia lepszych formatów i narzędzi do oceny podatności, ponieważ te obecnie istniejące nie są spójne ani szczegółowe.

Należy dążyć do stworzenia formatu zawierającego wersję lub zakres wersji, status „naprawione” lub „nienaprawione”, CPE, dokładną nazwę oprogramowania, powiązane oprogramowanie lub podatności i zagrożenia, powiązane luki w zabezpieczeniach, szczegółowy opis, status i inne dane. Sprostanie tym wyzwaniom i wdrożenie lepszych formatów i narzędzi do oceny podatności pozwala nam poprawić dokładność i skuteczność nowoczesnych programów skanujących w zakresie wykrywania podatności i łagodzenia ich skutków, zwiększając ogólny poziom cyberbezpieczeństwa oprogramowania.



JAK PHISHING ŚWIĄTECZNY MOŻE WPŁYNĄĆ NA REPUTACJĘ TWOJEGO E-BIZNESU?

Redakcja
SECURITY MAGAZINE

Okres świąteczny to nie tylko wzrost sprzedaży i wpływów w e-commerce, ale też czas, w którym wzmożone są cyberzagrożenia. Niestety, phishing może negatywnie wpłynąć na reputację Twojego e-commerce. Dowiedz się, jak mu przeciwdziałać.

PHISHING ŚWIĄTECZNY – CZY TO FAKTYCZNIE PROBLEM?

W okresach wzmożonej aktywności zakupowej, rośnie też liczba oszustw. To, niestety, fakt. Pokazują to m.in. dane firmy Zscaler, która obliczyła, że w ciągu różnego rodzaju świąt odnotowuje się nawet 400% wzrost aktywności phishingowej.

Dlaczego tak się dzieje? Aktywność phishingowa zwykle wzrasta z rozpoczęciem sezonu zakupowego, ponieważ osoby atakujące wiedzą, że kupujący mogą chętniej reagować na „oferty specjalne" lub powiadomienia dotyczące wysyłki i podobnych kwestii.

Phishing świąteczny często przybiera formę fałszywych ofert promocyjnych, maili z pozornie atrakcyjnymi rabatami, czy też stron internetowych, które imitują popularne serwisy e-commerce. Najczęstszym celem przestępców jest oczywiście uzyskanie haseł, numerów kart czy dane osobowe.

JAK DZIAŁA PHISHING ŚWIĄTECZNY?

W sezonie świątecznym cyberprzestępcy, aby z powodzeniem oszukać swoje ofiary, niejednokrotnie podszywają się pod znane marki czy sklepy lub marketplace'y. W Stanach Zjednoczonych bardzo chętnie w okresie świątecznym próbują zwieźć swoje ofiary, podając się np. za Amazon. Do niczego nieświadomych użytkowników trafiają maile czy SMS-y o rabatach, kartach podarunkowych, przesyłkach itd.

W internecie pojawiają się też wówczas fałszywe strony internetowe, które do złudzenia przypominają oryginalne. Nierzadko pojawiają się one w wy-

szukiwarkach czy social mediach jako złośliwe reklamy stosowane przez cyberprzestępców, by uwiarygodnić swoje działanie. Dość powiedzieć, że zgodnie z danymi Business of Apps w 2022 r. rynek fałszywych reklam wyceniano nawet na 81 miliardów dolarów. Innym sposobem zetknięcia się ofiary z tego typu fałszywymi stronami jest kliknięcie linku w mailu czy SMS-ie, który rzekomy „sklep" wysyła do nich.

Co się dzieje, jeśli ofiara nabierze się na taką reklamę lub wiadomość i kliknie link? Zostanie przekierowana na fałszywą stronę, która będzie prawie nie do odróżnienia od tej oryginalnej. Zazwyczaj na rzeczonej stronie użytkownik zostanie poproszony o podanie jakichś danych lub zalogowanie się np. za pomocą konta facebookowego, Gmaila itp. Jeśli to zrobi – prawdopodobnie rzeczone konta utraci, a dane zostaną wykorzystane dalej.

Nierzadko też, jeśli w konkretnej fałszywej stronie występuje mechanizm zakupowy, nieświadoma ofiara po np. dostarczeniu danych karty płatniczej, może stracić wszystkie swoje pieniądze.

PHISHING ŚWIĄTECZNY – PODSZYWANIE SIĘ POD APLIKACJE

Jednak cyberprzestępcy nie tylko wykorzystują fałszywe reklamy, strony czy wiadomości. Oszuści – zwłaszcza ci bardziej zaawansowani – czasem tworzą nawet fałszywe aplikacje. Zgodnie z danymi Interceptd 31% aplikacji na iOS i 25% aplikacji na Androida to oszustwa. Co więcej – firmy TrafficGurad i Juniper Networks szacują, że jedna na 13 instalowanych przez nas aplikacji jest... fałszywa.

Dlaczego to robią? Jednym z głównych celów tworzenia fałszywych aplikacji jest kradzież poufnych danych, takich jak hasła, numery kart, informacje osobowe itp. Cyberprzestępcy mogą wykorzystywać je dalej do kradzieży tożsamości, oszustw finansowych czy wreszcie odsprzedać je na czarnym rynku. Nierzadko też w ten sposób rozpowszechniają złośliwe oprogramowanie typu malware.

I niestety – choć bigtechy starają się zapobiegać tego typu działaniom, to nie od dziś wiadomo, że fałszywe aplikacje nierzadko i tak trafiają do oficjalnych sklepów, jak Google Play czy App Store.

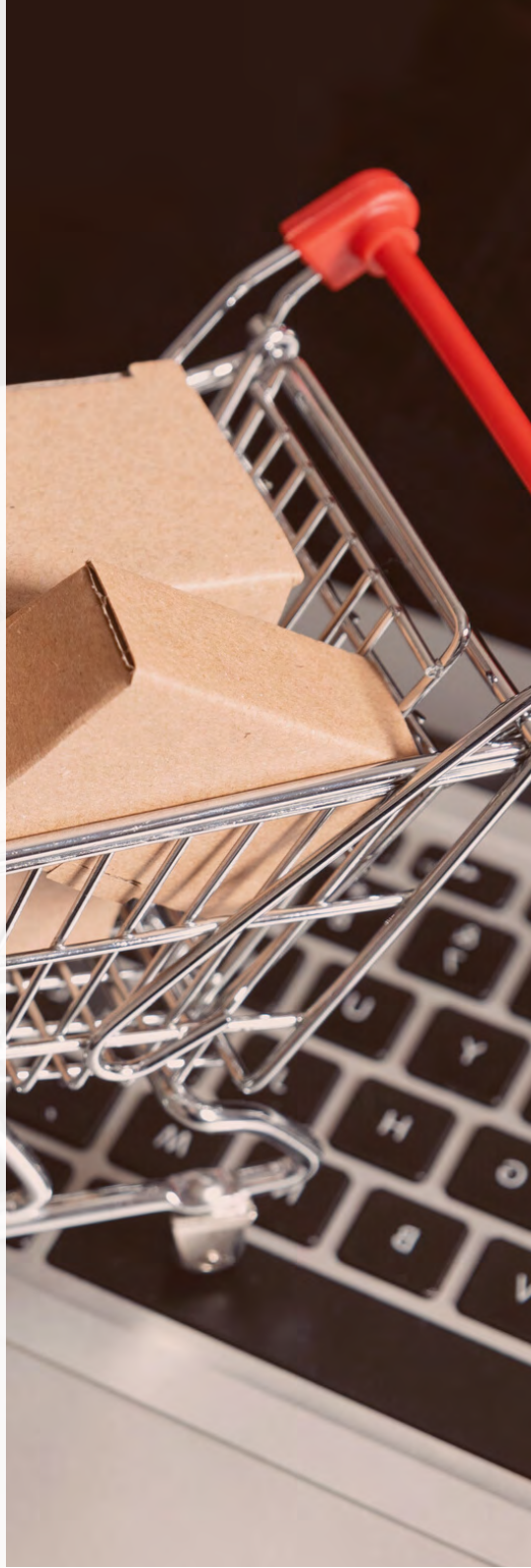
PHISHING ŚWIĄTECZNY – ZAGROŻENIE DLA REPUTACJI

Teoretycznie na razie wymieniamy wyłącznie zagrożenia, które dotykają Twoich dotychczasowych lub potencjalnych klientów. Jednak działania cyberprzestępców w tym obszarze są także ze szkodą dla ciebie, a zwłaszcza twojej reputacji.

Jeśli cyberprzestępcy podszywają się pod twoją markę skutecznie ich ofiary mogą obwiniać... ciebie, przekonani, że przecież zapłacili za produkt, a go nie otrzymali. Albo np. że z powodu zalogowania się na stronę twojego e-sklepu, utracili swoje konta społecznościowe. Mowa tutaj zatem o tradycyjnym kryzysie PR-owym.

Jednak co w sytuacji, w której to... twój sklep internetowy padł ofiarą phishingu? Nie jest przecież powiedziane, że wyłącznie klienci muszą mieć się na baczność w okresie świątecznym. Ty również możesz w trakcie tego sezonu otrzymywać wzmożone wiadomości phishingowe. I w tym przypadku akurat masz znacznie większy wpływ na to, czy tak się stanie, czy nie. W kontekście podszywania się pod twoją markę czy nieuważność twoich klientów – nie jesteś w stanie wiele zdziałać.

Najczęściej, kiedy mówimy o phishingu skierowanym przeciwko e-sklepom będą to wiadomości podszywające się właśnie pod twoich klientów. A czasem znane marketplace'y, jak Allegro, OLX lub Amazon, jeśli prowadzisz tam sprzedaż albo np. firmy kurierskie. W tym przypadku mówimy bardziej o oszustwie typu BEC (Business E-mail Compromise), którego celem nierzadko jest nie tylko przejęcie twoich środków finansowych, ale czasem też dostępów do np. oficjalnych kont społecznościowych sklepu czy samej strony e-commerce'u.



TWÓJ E-SKLEP PRZEJĘTY – KONSEKWENCJE

Załóżmy przez chwilę, że atak phishingowy cyberprzestępców się powiódł i w jego wyniku niefortunnie udostępniłeś np. swoje dane dostępowe do CMS-a, na którym stoi twój e-sklep.

Co wtedy? Prawdopodobnie cyberprzestępcy będą próbowali zainfekować twoją witrynę lub przekształcić ją w jeden wielki phishingowy scam. Po co? Aby pozyskiwać dane lub pieniądze od niczego nieświadomych klientów.

W tym przypadku mamy do czynienia nie tylko z kryzysem wizerunkowym, bo trudno będzie wytłumaczyć klientom, że to nie ty ich oszukałeś, ale też może to doprowadzić np. do problemów z Googlem.

Jeśli Google zauważy podejrzaną aktywność twojej strony, to może ją oznaczyć jako niebezpieczną. Co to oznacza? Obok nazwy twojej witryny w wyszukiwarce pojawi się informacja dotycząca np. tego, że twoja strona jest niebezpieczna lub mogła zostać zhakowana. To ostrzeżenie dla użytkowników.

Czasem Google może podejść do sprawy bardziej radykalnie i ukryć twoją stronę w wynikach wyszukiwania. Jeśli jednak gigant technologiczny zauważy podejrzaną aktywność twojej strony, to wyśle do ciebie maila z ostrzeżeniem. Oczywiście, jeśli korzystasz Google Search Console.

Unormowanie tej sytuacji może potrwać – zwłaszcza jeśli utraciłeś dostęp do swojego e-sklepu. A to oznacza nie tylko straty wizerunkowe, ale też finansowe, co może okazać się prawdziwym ciosem, zwłaszcza w takim okresie. Tym bardziej jeśli w ogóle np. prowadzisz sprzedaż sezonową.

JAK ROZPOZNAĆ ŚWIĄTECZNY PHISHING?

Skupmy się na oszustwie skierowanym do e-sklepów. Phishing w okresie świątecznym będzie w jakiś sposób odnosić się do zarówno twoich specjalnych ofert, jak i ofert twoich partnerów. Jeśli otrzymasz wiadomości od klientów, którzy „zapłacili za produkt, ale go nie dostali”, a jako dowód załączają np. potwierdzenia przelewów w pdf-ach, to bardzo możliwe, że będzie to oszustwo.

Jest to o tyle trudne do rozpoznania, że możesz otrzymać sporo takich wiadomości od prawdziwych

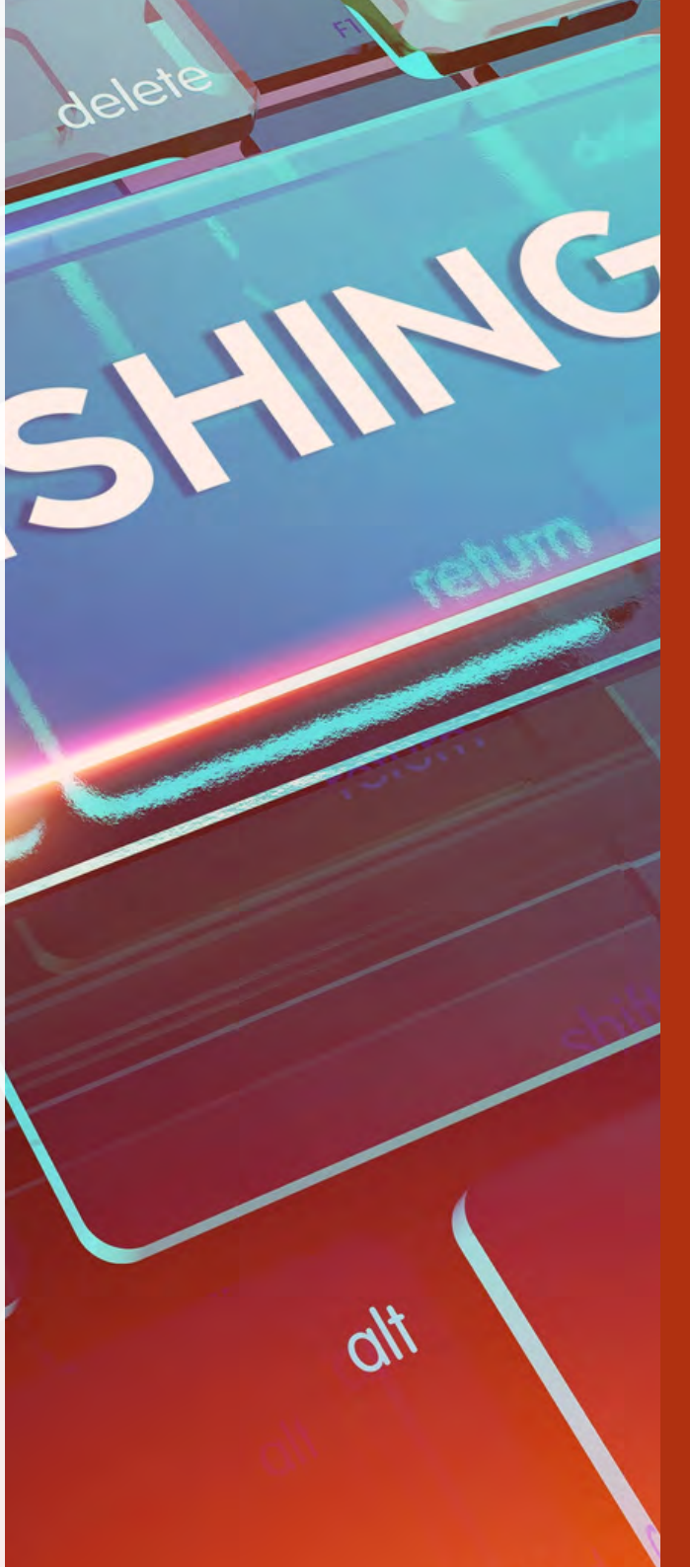
klientów. W końcu w okresie świątecznym czasem przesyłki się opóźniają, osoby, które zapłaciły za produkty, są zniecierpliwione, a cyberprzestępcy doskonale to wiedzą i wykorzystują. Dlatego uważaj na tego typu wiadomości, nie klikaj podejrzanych linków i nie otwieraj załączników, a już tym bardziej nie klikaj odnośników, które się w nich znajdują.

Możesz w tym okresie także otrzymywać wiadomości od dużych marketplace'ów czy firm kurierskich. Jeśli otrzymasz maila np. o specjalnych ofertach zniżkowych ze względu na okres świąteczny, lepiej napisz samemu maila do rzeczonych platform czy firm, aby to potwierdzić. Sprawdzaj też, jak wyglądają adresy mailowe, z których otrzymujesz tego typu wiadomości. Pamiętaj jednak, że i tutaj cyberprzestępcy mogą się podszyć, tworząc podobnie brzmiące domeny, np. Allegro zamiast Allegro czy wykorzystując różnego rodzaju bramki.

JAK BRONIĆ SIĘ PRZED PHISHINGIEM?

Skuteczna obrona przed phishingiem obejmuje szereg działań. Kluczowe jest regularne szkolenie pracowników w zakresie rozpoznawania i reagowania na phishing. Warto to zrobić zwłaszcza przed okresami sezonowymi, w których pojawia się większa sprzedaż i ogólnie wzmożona aktywność.

Ważne jest również wdrożenie zaawansowanych narzędzi bezpieczeństwa, które są w stanie wykrywać i blokować podejrzane wiadomości oraz monitorować ruch sieciowy – dostawcy poczt elektronicznych, co prawda dość skutecznie filtrują spam, ale zawsze coś jest w stanie się „prześlizgnąć".



Zwłaszcza teraz, kiedy cyberprzestępcy wykorzystują generatywne AI, do tworzenia wiarygodniejszych informacji. Warto też weryfikować wiadomości przez inne kanały komunikacji – zwłaszcza, jeśli nie jesteśmy pewni, czy to phishing, czy nie.

Koniecznie musisz też wykonywać regularne audyty czy testy penetracyjne w swojej firmie, żeby odkryć jej słabe punkty. Dość powiedzieć, że najczęstszym powodem, dla którego cyberatak się udaje jest czynnik ludzki. A w przypadku takich zagrożeń jak phishing, czy inne ataki socjotechniczne, to wręcz oczywiste. Dlatego musisz wiedzieć, jak dobrze pracownicy znają zasady cyberbezpieczeństwa i czy ich przestrzegają.

Co więcej – zawsze warto mieć przygotowany plan zarządzania kryzysowego i ciągłości działania. Jeśli jakimś sposobem cyberprzestępcy podszyją się pod twoją markę lub przejmą dostęp nad twoją stroną, pocztą mailową czy kontami w social mediach, musisz wiedzieć, co robić, kto będzie odpowiedzialny za kontakt z klientami, partnerami itd. itp. a także jak postępować, aby jak najszybciej odzyskać dostępy i nie stracić na reputacji.

Reasumując, phishing świąteczny to poważny problem. W każdym okresie sezonowym, gdzie sprzedaż znacząco wzrasta, musisz być przygotowany na cyberprzestępców wykorzystujących ataki socjotechniczne. W przeciwnym wypadku twój e-sklep może stracić nie tylko wizerunkowo, ale również finansowo.

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

MACIEJ SICIAREK
Dyrektor
CSIRT NASK

Menedżer i specjalista ds. bezpieczeństwa IT. Od ponad 20 lat zaangażowany w projekty ICT związane z bezpieczeństwem teleinformatycznym. Aktywnie uczestniczy w budowie Krajowego Systemu Cyberbezpieczeństwa oraz współpracuje z instytucjami krajowymi i zagranicznymi. Kieruje Pionem CSIRT w NASK PIB, w tym CERT Polska i Dyżurnet.pl.

KAMIL JÓŹWIAK
Client Solutions Specialist
Dell Technologies Poland

Entuzjasta nowych technologii cyfrowych, łączący pasję z pracą. Specjalizuje się w rozwiązaniach klienckich zwiększających produktywność: komputerach, monitorach, peryferiach, oprogramowaniu i narzędziach do zarządzania. Absolwent dwóch Uniwersytetów: Warszawskiego (Zarządzanie) oraz Łódzkiego (Informatyka Stosowana).

RAFAŁ SZCZYPIORSKI
Business Development Manager
w organizacji Data Center Sales
Dell Technologies

Z branżą IT i obecnym pracodawcą związany od przeszło 19 lat. Przez większą część tego czasu odpowiadał za projektowanie rozwiązań do centrów danych klientów głównie sektora teleko-munikacyjnego i finansowego. Pełnił również role regionalne dla krajów CEE. Od ponad 5 lat odpowiedzialny za rozwój dla Dell Technologies polskiego rynku serwerów x86.

RAFAŁ BRUDNICKI
Właściciel
Servers24.pl

Od 12 lat prowadzi firmę Servers24.pl, która zapewnia kompleksową obsługę i wsparcie działów IT. We współpracy z zespołem specjalistów pomaga klientom dopasować sprzęt i rozwiązania technologiczne do bieżących i przyszłych potrzeb ich firmy. Prywatnie pasjonat sportu i motoryzacji.

EKSPERCI WYDANIA

KATARZYNA GRABOWSKA
Specjalista ds. budowania świadomości cyberbezpieczeństwa
NASK-PIB

Specjalista ds. budowania świadomości cyberbezpieczeństwa w Państwowym Instytucie Badawczym NASK. Autorka materiałów popularyzacyjno-edukacyjnych z zakresu cyberbezpieczeństwa, trenerka z zakresu profilaktyki niebezpiecznych zachowań w internecie oraz zagadnień związanych z cyberhigieną.

SEBASTIAN STRZELAK
Prezes Zarządu
NetFormers

Od 20 lat zajmuje się projektowaniem, sprzedażą i wdrażaniem bezpiecznych, globalnych, ujednoliconych rozwiązań komunikacyjnych, początkowo u czołowych integratorów w Polsce, a od 10 lat w NetFormers. Posiada certyfikaty CCIE Security, CISSP, PMP, co pozwoliło mu pracować nad zaawansowanymi projektami dla głównych graczy na rynku.

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.

RAFAŁ STĘPNIEWSKI
Redaktor naczelny
Security Magazine

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.

EKSPERCI WYDANIA

OLIVER DEDOWICZ
CEO
Cyber Security Lab

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

PRZEMYSŁAW SOBCZYK
Dyrektor Działu Technicznego
Perceptus

Dyrektor Działu Technicznego w Perceptus Sp. z o.o. od 8 lat zajmuje się bezpieczeństwem danych firmy i ich klientów. Jest certyfikowanym inżynierem rozwiązań HSM marki Utimaco. Odpowiada za największe wdrożenia rozwiązań Endpoint Protection w Polsce. Wdraża urządzenia HSM w jednostkach Ministerialnych.

BOGDAN BARCHUK
Senior Application
Security Engineer
Intellias

Ekspert ds. cyberbezpieczeństwa z ponad 15-letnim doświadczeniem. Pasjonuje się odkrywaniem luk w systemach komputerowych i opracowywaniem narzędzi zwiększających bezpieczeństwo. Posiada ponad 20 różnych certyfikatów z zakresu cyberbezpieczeństwa. Jedną z jego specjalności jest identyfikowanie słabych punktów w usłudze Active Directory.

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

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