6(15)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Due diligence w cybersecurity
Dlaczego jest ważny?

E-kompetencje dzieci a przyszłość Twojej firmy
Powiązanie, które musisz zrozumieć

Płeć i wiek nie mogą
wykluczać z branży cybersecurity

Wi-Fi 6 i Wi-Fi 6E
bezpieczniejsze sieci bezprzewodowe

Przewagi i problemy
zapisu SMR

SPIS TREŚCI

SZANOWNI PAŃSTWO,

wydanie czerwcowe zdominowały relacje z wydarzeń związanych z szeroko rozumianym bezpieczeństwem, głównie - cyberbezpieczeństwem. Kwiecień, maj oraz czerwiec są miesiącami, które obfitują w konferencje, warsztaty z tej dziedziny. A nas niezmiernie cieszy, że tylu organizatorów obdarzyło nas zaufaniem i zdecydowało się na podjęcie współpracy patronackiej.

W tym wydaniu poświęcamy sporo miejsca cyberbezpieczeństwu jednostek publicznych. Nie sposób nie wspomnieć tu o ogromnym sukcesie Wojsk Obrony Cyberprzestrzeni czy spotkaniu w jednym miejscu 600 urzędników z całej Polski odpowiedzialnych za cyberbezpieczeństwo sektora publicznego.

Szczególnej uwadze polecam także nasze dwa redakcyjne materiały. Pierwszy odpowiada na pytanie, dlaczego due diligence, czyli staranne badanie i analiza w zakresie cyberbezpieczeństwa, odgrywa kluczową rolę w ochronie firm? Drugi - dlaczego firmy nie mogą udawać, że powiązanie: kompetencje cyfrowe dzieci a przyszłość tych firm, ich nie dotyczy? Co mogą i co powinny robić, by dbać o edukację w zakresie cyberbezpieczeństwa swoich przyszłych pracowników?

Serdecznie polecam lekturę tego wydania i zachęcam do współpracy!

Rafał Stępniewski


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

CYFRYZACJA POLA WALKI

Wojskowe Biuro Zarządzania Częstotliwościami dołączyło do Wojsk Obrony Cyberprzestrzeni. Decyzją Ministra Obrony Narodowej Biuro przeszło w podporządkowanie Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. Działania WBZC wpisują się w zadania realizowane przez DKWOC jakim jest m.in. zapewnienie bezpiecznej komunikacji w Siłach Zbrojnych RP i resorcie Obrony Narodowej.

STOP KRADZIEŻY TOŻSAMOŚCI

Od czerwca 2024 roku każdy będzie mógł zastrzec swój PESEL. Instytucje finansowe, notariusze i operatorzy telekomunikacyjni będą zobowiązani do sprawdzenia statusu PESEL-u przed podpisaniem umowy skutkującej zobowiązaniami finansowymi. Dzięki temu ofiary kradzieży tożsamości nie będą ponosić konsekwencji działań oszustów. Dane będą gromadzone w nowo utworzonym systemie, a zastrzeżenie i rezygnacja z niego będą odbywały się w czasie rzeczywistym.

KONIEC ASA 5500-X

Cisco wycofuje z eksploatacji popularną serię firewalli. End of Life obejmie lata 2023-2026. Oznacza to, że po tym czasie urządzenia nie będą rozwijane ani serwisowane. Dla użytkowników to czas wymiany urządzeń na nowe serie rekomendowane przez producenta, czyli firewalle Firepower 1000, 2100 i 4100. Jeśli ASA w Twojej sieci nie może zostać wymieniona, alternatywą jest uzyskanie zewnętrznego wsparcia, np. przez integratora IT.

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"

SECURITYMAGAZINE.PL

BARDZO UDANA EDYCJA TARGÓW POLSECURE 2023

PATRONAT
SECURITY MAGAZINE

Targi POLSECURE pojawiły się w kalendarzu Targów Kielce zaledwie w zeszłym roku, a biorąc pod uwagę dane liczbowe zostały zauważone. W ubiegłym roku powierzchnia wystawy zajmowała nieco ponad 3 000 metrów kwadratowych, w tym roku wystawa urosła ponad 100% - powierzchnia wystawiennicza zajęła blisko 6 500 metrów kwadratowych. Wystawę odwiedziło przeszło 5000 zwiedzających.

Targi POLSECURE zostały także docenione poza granicami naszego kraju, o ile w 2022 roku uczestniczyli wystawcy tylko z Polski i Niemiec, o tyle podczas tegorocznej edycji swoją ofertę zaprezentowały firmy z siedmiu krajów: Belgii, Czech, Francji, Izraela, Niemiec, Wielkiej Brytanii oraz, oczywiście, Polski.

Wystawę odwiedziło 36 delegacji z 27 krajów takich jak: Bułgaria, Chorwacja, Czechy, Estonia, Gruzja, Hiszpania, Izrael, Korea Południowa, Litwa, Łotwa, Malta, Mołdawia, Niemcy, Norwegia, Portugalia, Rumunia, Rwanda, Słowacja, Słowenia, Ukraina, USA, Węgry, Wielka Brytania, Włochy oraz przedstawiciele Europolu i FRONTEX-u. Wydarzenie było doskonałą okazją do zapoznania się z ofertą firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania służącego łączności, dowodzeniu czy kontroli – czyli od racji żywnościowych dla funkcjonariuszy po całe laboratoria kryminalistyczne.

MERYTORYCZNA STRONA TARGÓW POLSECURE – KONFERENCJE , SEMINARIA, DEBATY

O działalności zespołów DVI w różnych krajach i metodach identyfikacji w miejscu katastrof rozmawiali eksperci międzynarodowej konferencji organizowanej przez Komendę Główną Policji podczas pierwszego dnia Targów Polsecure.

Nie zabrakło też ekspertów z Centralnego Laboratorium Kryminalistycznego Policji. Międzynarodową konferencję pn. „Pewność w identyfikacji ofiar – rola zespołu DVI na miejscu katastrof masowych” rozpoczęto od odpowiedzi na pytania: czym są zespoły DVI, dlaczego identyfikacja ofiar jest bardzo ważna oraz jak wygląda działalność zespołów do identyfikacji ofiar w różnych krajach m.in. w Ukrainie, na Malcie i w Wielkiej Brytanii.

Bardzo udana edycja Targów POLSECURE 2023

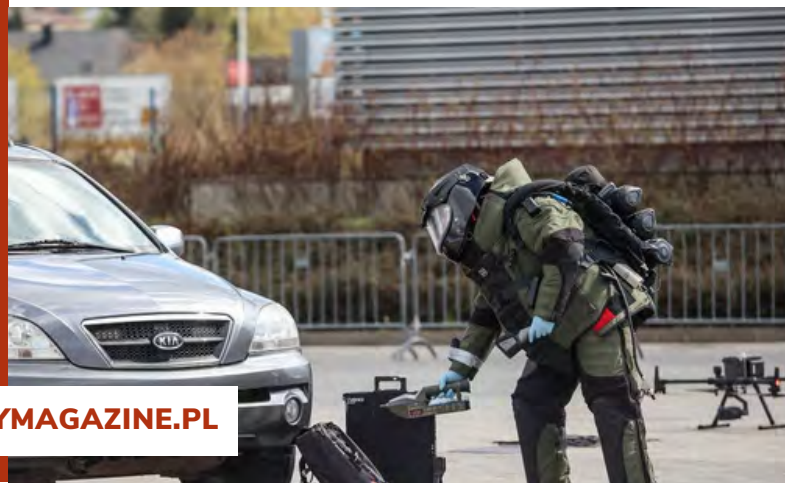
Drugi dzień konferencji poświęcony był między innymi tematowi „Innowacyjność oraz budowanie kapitału ludzkiego na rzecz walki z cyberprzestępczością". W trakcie panelu poruszono istotne zagadnienie, jakim jest rozwój innowacji oraz budowanie kapitału ludzkiego, w kontekście zwalczania cyberprzestępczości. Skuteczne zapobieganie temu zagrożeniu, wymaga od organów ścigania ciągłej kreatywności i innowacyjności w stosowanych narzędziach i procedurach. Osiągnięcie tych celów uzależnione jest jednakże od zbudowania efektywnej strategii budowania wysoce kompetentnych kadr, zdolnych do podejmowania najtrudniejszych wyzwań.

W ramach Międzynarodowych Targów Polsecure odbyła się również konferencja poświęcona działaniom Straży Granicznej na granicy z Białorusią i z Ukrainą. Było to pierwsze takie wydarzenie organizowane przez Straż Graniczną.

W konferencji uczestniczył m.in. zastępca dyrektora wykonawczego Frontexu, Uku Sarekanno który mówił, że choć migracja była już wykorzystywana jako broń, to jednak nie w tak oczywisty i niepokojący sposób, jak robił to reżim Aleksandra Łukaszenki. W ocenie wiceszefa Frontexu z podobnymi zagrożeniami Europa może mieć do czynienia także w przyszłości.

POKAZY DYNAMICZNE – WAŻNY ELEMENT TARGÓW DLA BEZPIECZEŃSTWA

Pokazy dynamiczne zawsze wzbudzają zainteresowanie gości, którzy na żywo, w warunkach kontrolowanych mogą zobaczyć przedstawicieli różnych służb mundurowych w akcji. Nie inaczej było w tym roku, gdzie w specjalnym bloku zaprezentowano najnowocześniejszy sprzęt oraz umiejętności pracowników Straży Granicznej i Policji oraz ekspertów od zabezpieczeń. Nie zabrakło muzy-



cznych akcentów.

Występ Orkiestry Reprezentacyjnej Straży Granicznej oraz Policji rozpoczął blok pokazów pierwszego dnia targów POLSECURE. Na terenie zewnętrznym Targów Kielce Komenda Główna Policji zaprezentowała pokaz Motocyklowej Asysty Honorowej. Widowiskowa eskorta w wykonaniu policjantów na jednośladach, pokazała nie tylko ich umiejętności jazdy na motorze, ale i sposób zabezpieczenia najgwarniejszych osób w państwie. Wydział Zabezpieczeń Działań Straży Granicznej przeprowadził z kolei akcję pokazową z użyciem psa bojowego. Czworonogi od lat stanowią o sile jednostek Straży Granicznej i wykorzystywane są zarówno w patrolach, jak i w akcjach specjalnych.

Ważnym elementem pokazów dynamicznych jest prezentacja najnowocześniejszego sprzętu i systemów bezpieczeństwa. Jeden z nich zaprezentowała firma KRD, zajmująca się m.in. produkcją szyb bezpiecznych. W przeprowadzonym teście wytrzymałości szyb KasiGlas, producenci przekonywali o ich wyższości nad takim środkami zabezpieczenia, jak chociażby kraty. Firma Transactor Security pokazała system do detekcji oraz neutralizacji dronów. Bogata oferta wyspecjalizowanego sprzętu objęła m.in. innowacyjne systemy do neutralizacji zagrożeń IED/EOD, sprzęt detekcyjny do wykrywania zagrożeń bombowych, biologiczno-chemicznych i radiologicznych.

Bardzo ciekawe warsztaty gotowości COMBAT DEFENCE przeprowadzili specjaliści Fundacji Gotowi. Skupia ona doświadczonych specjalistów w wielu dziedzinach, będących jednocześnie pasjonatami przygotowywania się na trudne czasy. W trakcie spotkania eksperci dzielili się swoimi umiejętnościami, wiedzą i doświadczeniami potrzebnymi do przetrwania zagrożeń. Kampania GOTOWI.ORG przekazuje informacje o tym, w jaki sposób można się przygotować na sytuacje kryzysowe i pomimo trudności przetrwać je.

Bardzo udana edycja Targów POLSECURE 2023

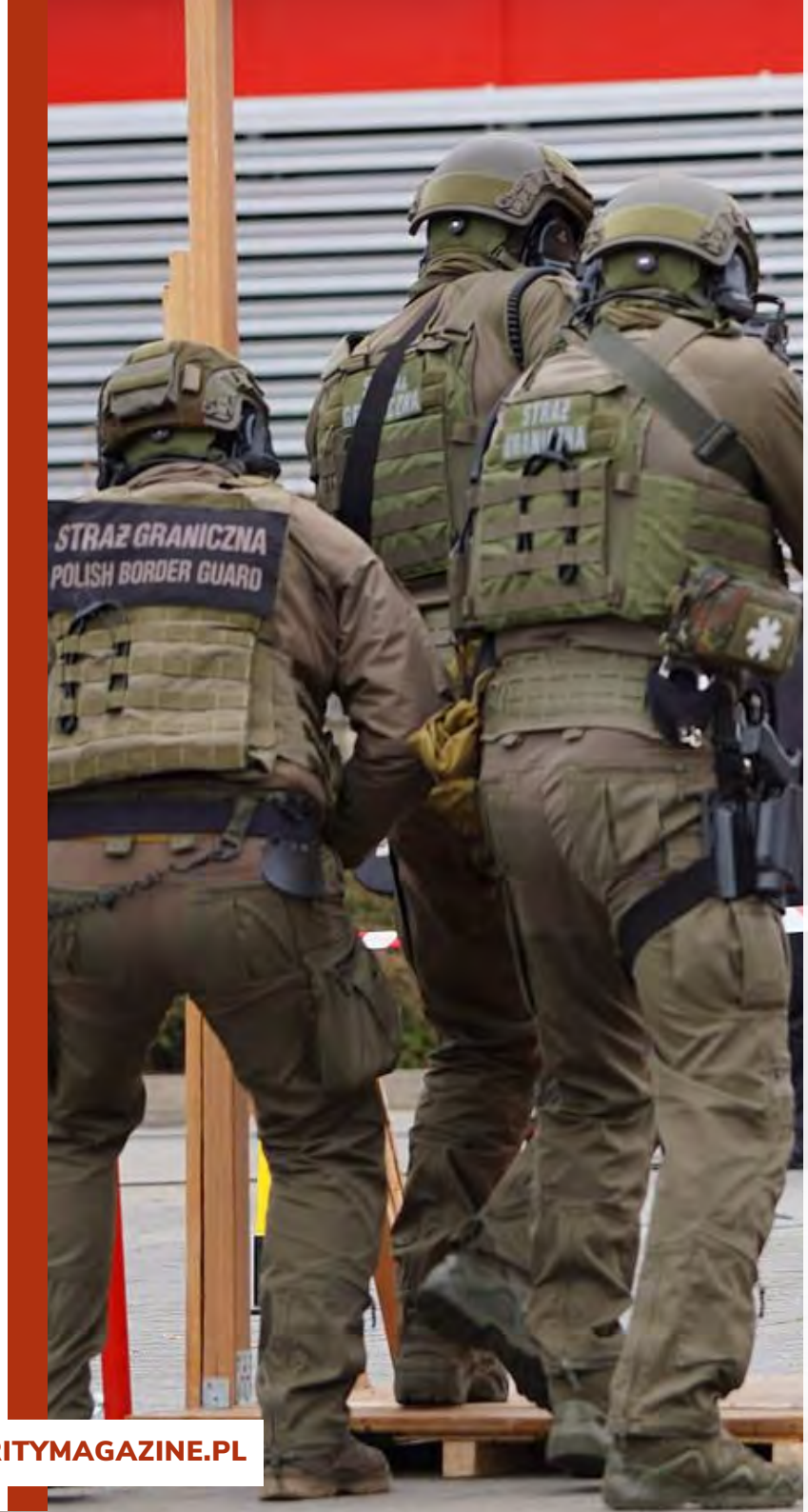
WAŻNE POROZUMIENIA PODCZAS TARGÓW POLSECURE

Targi POLSECURE to nie tylko ciekawa ekspozycja skierowana do funkcjonariuszy służb, ale także miejsce podpisywania ważnych dla bezpieczeństwa umów i porozumień.

Komendant Główny Policji gen. insp. Jarosław Szymczyk podpisał porozumienia o współpracy z instytucjami zajmującymi się bezpieczeństwem. Pierwsze z nich zostało zawarte z gen. bryg. Karolem Molendą – Dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni z siedzibą w Legionowie jako organizatorem Wojskowego Systemu Telekomunikacyjnego. Porozumienie reguluje współpracę pomiędzy jednostkami polskiej Policji w zakresie m.in. ochrony granicy, zabezpieczenia zdarzeń masowych, wspólnych ćwiczeń oraz współdziałania na wypadek kryzysu lub konfliktu zbrojnego. Szef polskiej Policji podpisał również umowę z Przedsiębiorstwem Sprzętu Ochronnego MASKPOL S.A.

Podpisany dokument reguluje procedury zmierzające do zakupu kamizelek kuloodpornych kwalifikowanych stanowiących indywidualną ochronę każdego policjanta. Ułatwienie prac Centralnemu Laboratorium Kryminalistycznemu ma na celu natomiast podpisanie porozumienie w zakresie rekonstrukcji antroposkopijnych z Instytutem Chemii Bioorganicznej Polskiej Akademii Nauk z ramienia policji dokument podpisał nadinsp. Paweł Dobrodziej. Polska policja było podpisała także list intencyjny z Grupą WB Electronics S.A. Podpisana została również umowa ramowa z Lubawą S.A.

Fabryka Broni „Łucznik” – Radom i Straż Graniczna podpisały umowę na dostawę 240 karabinków MSBS GROT C16 FB-A2 kal. 5.56×45 mm. Pograniczni-



cy kolejny raz kupują karabinki MSBS GROT. Dotychczas trafiło do nich ok. 1300 szt.

Funkcjonariusze Straży Granicznej podkreślają, że broń z Radomia doskonale sprawdza się w ich służbie i można ją łatwo przystosować do konkretnych działań, dlatego zdecydowano się na zakup następnej partii broni. Umowę w Kielcach podpisali reprezentujący Fabryką Broni „Łucznik" – Radom sp. z o.o. dr Wojciech Arndt, prezes zarządu oraz Seweryn Figurski, członek zarządu i Komendant Główny Straży Granicznej gen. dyw. SG Tomasz Praga.

GALA WRĘCZENIA NAGRÓD NA ZAKOŃCZENIE POLSECURE

Międzynarodowe Targi Policji i Bezpieczeństwa Publicznego zostały zakończone uroczystym wręczeniem nagród dla najlepszych produktów. Komisja konkursowa po przeanalizowaniu zgłoszeń nagrodziła trzy produkty.

- Konsorcjum, w którego skład wchodzą: Lider - Politechnika Warszawska oraz VORTEX, Wyższa Szkoła Policji, Longevity za Mobilny Punkt Dystrybucji Infrastruktury Teleinformacyjnej (MPDiT)
- ChangePro, producent HackingDept za HackingDept Offensive Training
- Megmar Logistics & Consulting za Mobilne Bariery Antyterrorystyczne MVB-3X do ochrony przed pojazdami taranującymi.

Wyróżnienie specjalne Komendanta Głównego Policji trafiło do firmy Flytronic, GRUPA WB, WB Electronics za wielozadaniowy bezzałogowy system latający Fly-Eye. Nagroda Komendanta Głównego Straży Granicznej „Laur Graniczny" otrzymała firma PCO z Warszawy za ręczną kamerę termowizyjną NPL-1T.

Wyróżnienie specjalne Dyrektora Generalnego Służby Więziennej za zastosowane rozwiązania technologiczne i projektowe trafiło do firmy PPO Przedsiębiorstwo Państwowe ze Strzelców Opolskich za obuwie taktyczne PPO MILITA-RY- MODEL 941.

PATRONAT
SECURITY MAGAZINE

10 powodów, dla których warto wziąć udział w CYBERSEC FORUM/EXPO 2023!

Już 21-22 czerwca w Katowicach odbędzie się 17. edycja European Cybersecurity Forum – CYBERSEC. Tegoroczne wydarzenie to wyjątkowe połączenie klasycznego FORUM i unikalnych targów EXPO. W dyskusjach udział wezmą cenieni specjaliści, a wystawcy z Polski i ze świata zaprezentują swoje najnowsze produkty i usługi.
Poznaj 10 powodów, dla których warto pojawić się na CYBERSEC FORUM/EXPO 2023:

1) **Nawiąż wartościowe kontakty biznesowe z branżą IT pozyskaj nowych partnerów, klientów i inwestorów.** CYBERSEC to miejsce spotkań czołowych firm, mediów i specjalistów związanych z IT. W strefie EXPO zawrzesz umowę z nowym dostawcą usług IT lub uzyskasz wsparcie finansowe na rozwój swojego projektu.

2) **Poznaj trendy cyberbezpieczeństwa. Wykorzystaj wskazówki topowych ekspertów, aby skutecznie zaadaptować najnowsze standardy branżowe.** Uzyskaj rekomendacje, które rozwiązania są najefektywniejsze i jakie są możliwości ich implementacji w środowisku twojej firmy.

3) **Przygotuj swoją firmę na cyberataki. Reaguj na zagrożenia.** FORUM/EXPO daje przestrzeń do indywidualnych konsultacji, w której poznasz usługi i ofertę najlepszych firm, które pomogą Ci zadbać o bezpieczeństwo twojej firmy.

4) **Znajdź skuteczne narzędzia walki z cyberatakami. Stwórz skuteczny plan reakcji na incydenty w cyberprzestrzeni.** 2 dni konferencji to formaty szkoleniowe, w tym warsztaty i wykłady techniczne, oraz prezentacja startupów oraz scaleupów z pionierskimi rozwiązaniami.

5) **Wzmocnij swój dział IT. Rozwijaj kompetencje zespołu.** Zapewnij pracownikom możliwość dyskusji ze specjalistami z branży.

6) **Otwórz się na międzynarodową współpracę.** Na CYBERSEC poznasz przedstawicieli biznesu z całego świata. Wykorzystaj szansę na poznanie międzynarodowych rynków i nawiąż strategiczną współpracę, która pozwoli Ci na opracowanie przełomowej usługi.

7) **Zwiększ konkurencyjność swojej firmy.** Wiedza zdobyta na CYBERSEC pozwoli Ci na lepsze zrozumienie rynku i wdrożenie strategii cyfrowej, zwiększającej efektywność biznesu.

8) **Wyróżnij się na tle konkurencji. Buduj swoją markę.** Dzięki CYBERSEC zdobędziesz cenne leady, poszerzysz sieć kontaktów i zbudujesz pozycję lidera w branży.

9) **Postaw na rozwój. Zainwestuj w sztuczną inteligencję.** Innowacyjne technologie i usługi przyciągną uwagę klientów, a nowatorskie rozwiązania prezentowane na CYBERSEC pomogą w zwiększeniu sprzedaży.

10) **Zbuduj sieć kontaktów ze specjalistami.** Podczas FORUM/EXPO uczysz się od najlepszych w swojej dziedzinie. Czerp inspiracje od innych uczestników i wymieniaj doświadczenie związane z cyberbezpieczeństwem.

ZAREJESTRUJ SIĘ

Bilet standard 20% taniej z kodem SecMag20ST

OBRONA CYBER-PRZESTRZENI: TRIUMF POLSKI PODCZAS ĆWICZEŃ LOCKED SHIELDS

Redakcja
SECURITY MAGAZINE

Polska, pod przewodnictwem drużyny DKWOC (Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni), zdobyła trzecie miejsce na międzynarodowych ćwiczeniach z cyberbezpieczeństwa zorganizowanych przez NATO, znanych jako Locked Shields. Ćwiczenia te, przeprowadzane od 2010 roku, są uważane za największe i najbardziej złożone na świecie.

ĆWICZENIA NA POLU BITWY

Locked Shields jest corocznym ćwiczeniem, organizowanym przez CCDCOE od 2010 roku. Jak powiedział dyrektor NATO CCDCOE, Mart Noorm, żadne inne ćwiczenie cyberobrony nie oferuje tak specjalistycznego i szczegółowego doświadczenia, jak Locked Shields.

Ćwiczenie to umożliwia ekspertom ds. bezpieczeństwa cybernetycznego doskonalenie umiejętności w zakresie obrony krajowych systemów informatycznych i infrastruktury krytycznej przed atakami w czasie rzeczywistym. Nacisk kładziony jest na realistyczne scenariusze, najnowocześniejsze technologie i symulacje masowego incydentu cybernetycznego, w tym podejmowania strategicznych decyzji, aspektów prawnych i komunikacyjnych.

To okazja dla cyberobrońców do przećwiczenia ochrony krajowych systemów informatycznych i infrastruktury krytycznej pod presją poważnego cyberataku. Locked Shields to też obrona systemów, zgłaszanie incydentów, podejmowanie strategicznych decyzji i rozwiązywanie problemów kryminalistycznych, prawnych i medialnych – wszystko to stanowiło część ćwiczeń.

Jednak aspekty techniczne to tylko część wyzwania. W tych ćwiczeniach równie ważna była strategia i współpraca między uczestnikami. W świecie, w którym duży cyberatak może szybko przerodzić się w kryzys bezpieczeństwa na dużą skalę, tego rodzaju ćwiczenia są kluczowe dla lepszego przygotowania.

- Scenariusz ćwiczeń przewidywał konieczność obrony fikcyjnego państwa, które padło ofiarą cyberataków na dużą skalę. Zadaniem drużyn była ochrona systemów informatycznych i infrastruktury krytycznej – systemów bankowych, elektrowni czy sieci przemysłowych przed tysiącami ataków - przekazał naszej redakcji **płk Grzegorz Wielosz, szef Oddziału Współpracy Międzynarodowej, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni.**

POLSKA NA PODIUM

Polska drużyna, pod przewodnictwem oficera DKWOC, zdobyła trzecie miejsce, tuż za drużynami szwecko-islandzką i estońsko-amerykańską. Jak zauważył gen. bryg. Karol Molenda, Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni, sukces drużyny pokazuje, że siła tkwi we współpracy, a dobrze prowadzony

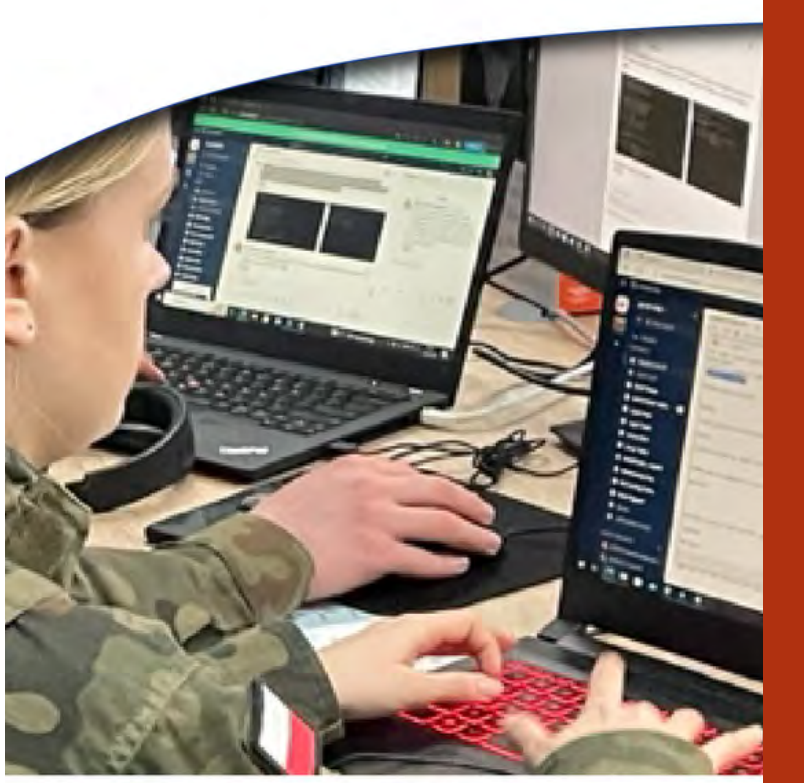
zespół może osiągnąć spektakularne wyniki.

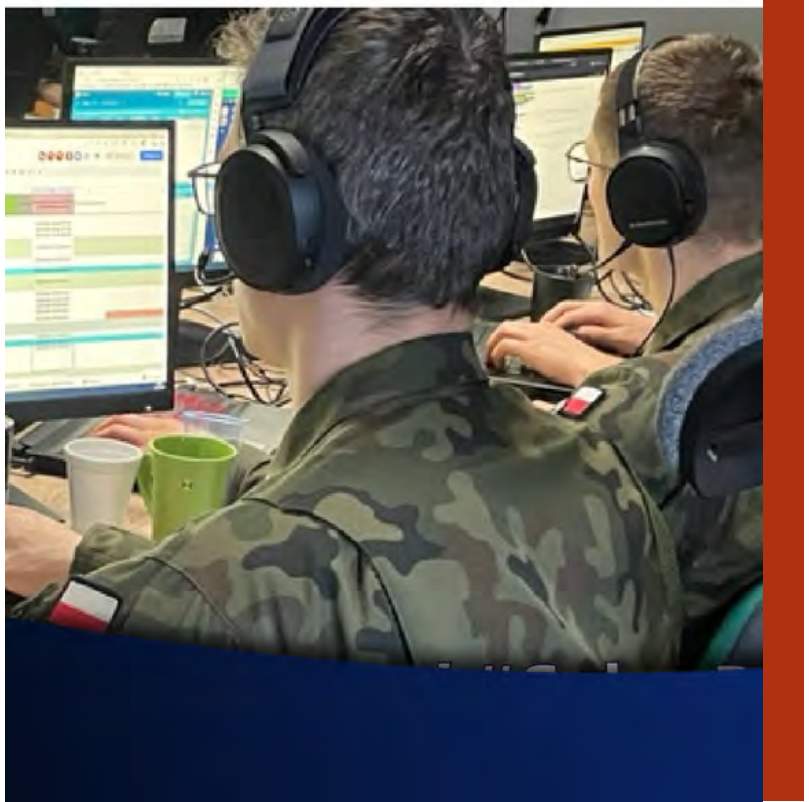
- *To zasługa między innymi tego, że konsekwentnie rozbudowujemy nasze struktury ds. cyberbezpieczeństwa, polscy specjaliści ds. cyberbezpieczeństwa reprezentują wysoki poziom wiedzy merytorycznej* - poinformował nas płk Grzegorz Wielosz.

- *Członków naszej drużyny charakteryzują również zaangażowanie i poczucie misji. Do LS23 przygotowali się przez wiele tygodni, ciężko pracowali tylko dla własnej satysfakcji, oczywiście nie zaniedbując swoich podstawowych obowiązków. Było to też możliwe dzięki zrozumieniu pracodawców, którzy niejednokrotnie pozwalali swoim ludziom na treningi w godzinach pracy, zdając sobie sprawę, że to bardzo ważne ćwiczenie dla wszystkich podmiotów funkcjonujących w ramach Krajowego Systemu Cyberbezpieczeństwa* - dodał szef Oddziału Współpracy Międzynarodowej z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni.

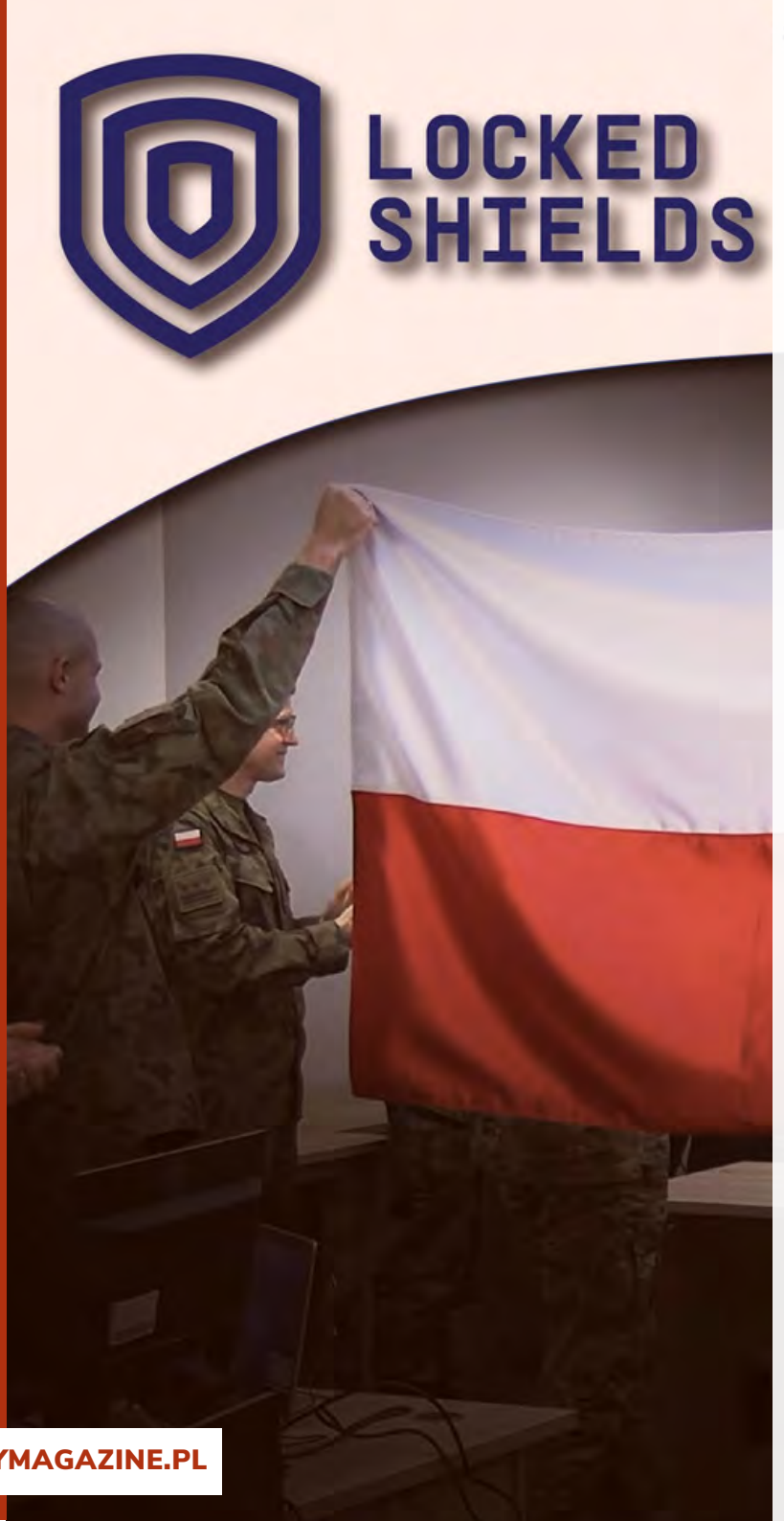
KLUCZ DO SUKCESU

Kiedy spytaliśmy o klucz do sukcesu Polski, odpowiedź była jasna: ciężka praca, zaangażowanie, ciągły rozwój zawodowy i i trening, a także zdolność do adaptacji i szybkiego podejmowania decyzji w warunkach presji.





Obrona cyberprzestrzeni: triumf Polski podczas ćwiczeń Locked Shields

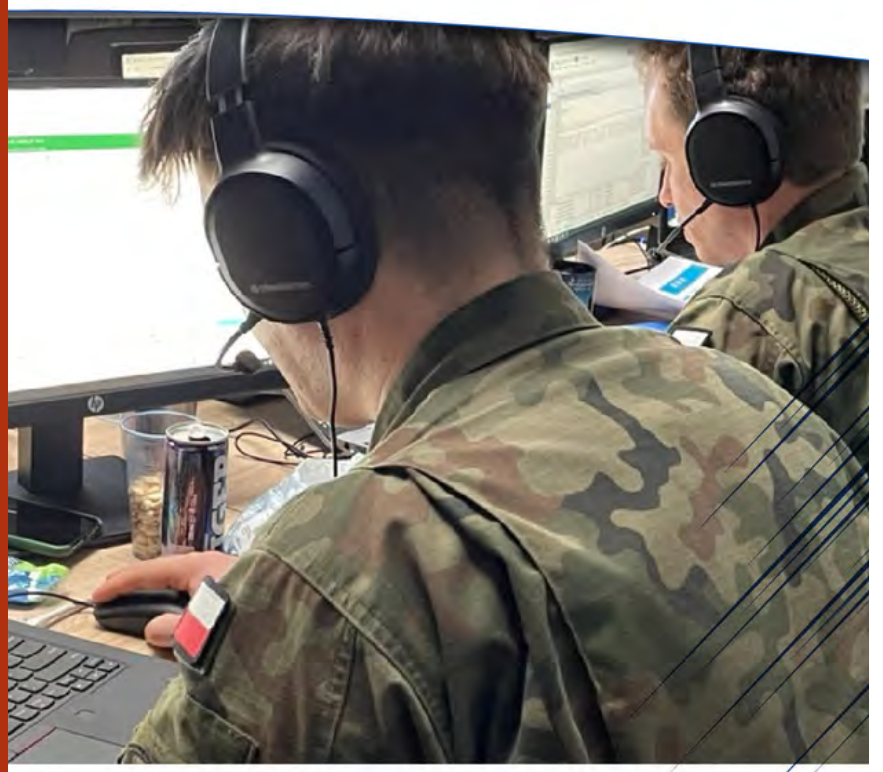


Drużyna Polski składała się z około 200 osób, co zdecydowanie zwiększało poziom skomplikowania operacji, ale jednocześnie otwierało szereg możliwości poprzez wykorzystanie szerszego spektrum umiejętności i doświadczeń.

- Wybierając członków polskiej drużyny, zależało nam, by reprezentowali jak najszerszy przekrój specjalistów zajmujących się cyberbezpieczeństwem. Wiele osób, które brały udział w tegorocznych zawodach było w drużynie w latach poprzednich. W tym roku jednak zależało nam, by pojawiły się nowe twarze, nowi eksperci z nowymi umiejętnościami. Miało to na celu zwiększenie liczby osób przeszkolonych spośród pracujących w instytucjach Krajowego Systemu Cyberbezpieczeństwa - zaznaczył płk Grzegorz Wielosz.

Zawody dają unikalną możliwość przetestowania umiejętności w realnych, choć symulowanych, warunkach. Największym wyzwaniem, jak przekazał nam rzecznik prasowy DKWOC, było zapewnienie sprawnego przepływu informacji w celu szybkiego podejmowania decyzji. Tego rodzaju ćwiczenia służą również jako ważna forma edukacji, pozwalając uczestnikom na rozwijanie i doskonalenie swoich umiejętności.

- Kolejną rzeczą z którą musieliśmy się zmierzyć było wyrównanie wiedzy pomiędzy zawodnikami, co w tak dużym zespole było wyzwaniem - przekazał naszej redakcji przedstawiciel DKWOC.



MIĘDZYNARODOWE ZNACZENIE UDZIAŁU W LOCKED SHIELDS

Udział Polski w tak prestiżowym konkursie ma duże znaczenie na arenie międzynarodowej, choć jak stwierdził płk Grzegorz Wielosz:

- Nasi eksperci należą do światowej czołówki, w międzynarodowych zawodach zdobywają czołowe miejsce, w tym roku zajęliśmy w Locked Shields 3 miejsce, w poprzednim - 2. Można powiedzieć, że dla wielu nasz poziom stanowi punkt odniesienia.

Trzecie miejsce to ogromny sukces. Zasługa leży w konsekwentnym rozbudowywaniu struktur ds. cyberbezpieczeństwa, wysokim poziomie wiedzy merytorycznej polskich specjalistów, oraz ich zaangażowaniu i poczuciu misji. Sukces ten pokazuje, że Polska jest ważnym graczem w dziedzinie cyberbezpieczeństwa, nie tylko na arenie krajowej, ale także międzynarodowej.

- Dołączenie do elitarnej grupy ekspertów z dziedziny bezpieczeństwa IT w ramach Wojsk Obrony Cyberprzestrzeni wymaga nie tylko doświadczenia, ale także samodzielności, kreatywności, analitycznego umysłu i zdolności do pracy w grupie. Uczestnicy muszą być gotowi na ciężką pracę, zważywszy na wymagające zadania i intensywność służby - poinformował rzecznik prasowy DKWOC, dodając:

- Wyznajemy zasadę, że kluczem do utrzymania cyberbezpieczeństwa jest wymiana informacji oraz doświadczeń z naszymi sojusznikami i taka współpraca w trybie roboczym ma miejsce. Żołnierze biorą też udział w licznych szkoleniach i zawodach zarówno krajowych jak i międzynarodowych.

CHCESZ DOŁĄCZYĆ DO ELITARNEJ GRUPY WOC?

- Poszukujemy osób które mają nie tylko wymagane doświadczenie, ale też są samodzielne, kreatywne, mają analityczne umysły, lubią wyzwania i potrafią pracować w grupie. Służący u nas żołnierze bardzo szybko zdobywają doświadczenie, zadania stawiane przed nimi są wymagające, a służba w DKWOC, zwłaszcza na pierwszej linii wsparcia – bardzo intensywna - zaznaczył płk Grzegorz Wielosz.

Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni szuka utalentowanych specjalistów posiadających wiedzę oraz umiejętności w dziedzinie informatyki, matematyki, teleinformatyki i cyberbezpieczeństwa, gotowych dołączyć do zespołu ekspertów Sił Zbrojnych RP i służyć swoim doświadczeniem Państwu Polskiemu. Oferuje stanowiska dla osób cywilnych i żołnierzy zawodowych.

Jeśli chcesz spróbować swoich sił, napisz: **kontakt@cyber.mil.pl** lub zadzwoń na infolinię rekrutacyjną w dni robocze pomiędzy godziną 8 a 20 pod numer telefonu: **509 677 777**.


Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?
Sprawdź ofertę
PATRONATU
MEDIALNEGO
SECURITY MAGAZINE
Napisz do nas:
redakcja@securitymagazine.pl

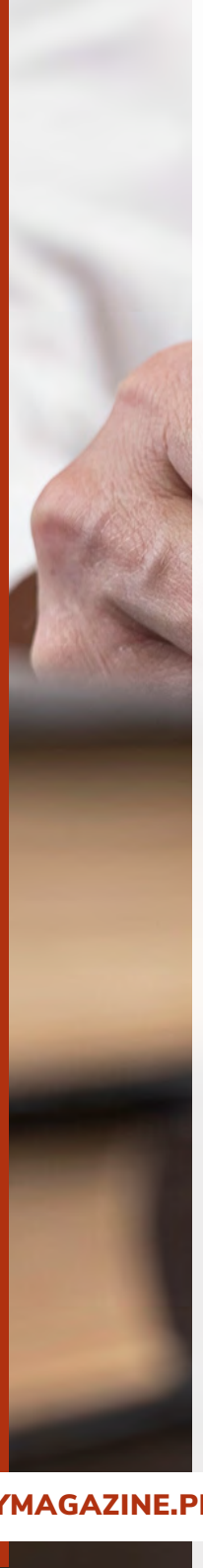
SECURITYMAGAZINE.PL

ZGŁOŚ NAJLEPSZĄ PRACĘ NAUKOWĄ W KONKURSIE IM. MARIANA REJEWSKIEGO

Redakcja
SECURITY MAGAZINE

Departament Cyberbezpieczeństwa MON ogłosił rozpoczęcie piątej, jubileuszowej edycji konkursu im. Mariana Rejewskiego. Ten prestiżowy konkurs, który od 2019 roku stanowi integralną część naukowej sceny Polski, służy do wyłaniania najbardziej innowacyjnych i wpływowych prac naukowych z obszaru cyberbezpieczeństwa i kryptologii.

Zgłoś najlepszą pracę naukową w Konkursie im. Mariana Rejewskiego



SPRAWY FORMALNE

O konkursie im. Mariana Rejewskiego wie każdy, kto choć raz zagłębiał się w świat kryptologii i cyberbezpieczeństwa. Rozpoczęty jako hołd dla Mariana Rejewskiego, genialnego matematyka, który przyczynił się do złamania kodu niemieckiej maszyny szyfrującej Enigma podczas II wojny światowej, konkurs ten nabrał swojego unikalnego charakteru i prestiżu, przyciągając co roku setki ambitnych uczestników.

Konkurs jest przeprowadzany w dwóch kategoriach: na najlepszą pracę inżynierską, licencjacką i magisterską oraz na najlepszą rozprawę doktorską. W tym roku nagrody pieniężne wynoszą od 5 do 15 tys. złotych, co jest wyrazem uznania dla znaczących osiągnięć laureatów.

Uczestnictwo w konkursie jest otwarte dla wszystkich, którzy obronili swoją pracę inżynierską, licencjacką, magisterską lub rozprawę doktorską na uczelni mającej siedzibę na terytorium Rzeczypospolitej Polskiej. Prace muszą być poświęcone cyberbezpieczeństwu lub kryptologii i mogą być przygotowane w języku polskim lub angielskim.

Co ciekawe, do konkursu mogą zostać zgłoszone prace, które nie przeszły poprzednio etapu oceny formalnej lub zostały zgłoszone po terminie. Ta elastyczność przyciąga wielu młodych naukowców, którzy mają okazję poprawić i doszlifować swoje prace, aby przyciągnąć uwagę jury.

Zgłoś najlepszą pracę naukową w Konkursie im. Mariana Rejewskiego

Zgłoszenie do konkursu powinno zawierać wypełniony oraz podpisany formularz zgłoszeniowy, pracę i jej streszczenie w wersji elektronicznej oraz zaświadczenie z uczelni potwierdzające złożenie i obronę przesłanej pracy. Wszystkie te dokumenty powinny zostać wysłane mailowo lub pocztą do Departamentu Cyberbezpieczeństwa MON do 31 lipca 2023 roku.

NAGRODY

Rozpiętość nagród jest atrakcyjna i zasługuje na uwagę. W kategorii prac inżynierskich, licencjackich i magisterskich, I nagroda wynosi 10.000 zł, II nagroda to 7.000 zł, a III nagroda to 5.000 zł.

W kategorii rozpraw doktorskich, I nagroda wynosi 15.000 zł, II nagroda to 11.000 zł, a III nagroda to 8.000 zł. Te nagrody pieniężne stanowią wartościowy bodziec dla naukowców, którzy poświęcają wiele godzin na swoje badania.

Nagrodami dodatkowymi, które można wybrać, są wizyta na terenie garnizonu Dęblin z przelotem symulatorami, zwiedzaniem Muzeum Sił Powietrznych i możliwością obejrzenia statków powietrznych, szkolenie na "Symulatorze lotów na otwartej czaszy", przejazd czołgiem Leopard, czy szkolenie ratownicze po awaryjnym lądowaniu na wodzie.

Te wyjątkowe nagrody dodatkowe umożliwiają laureatom konkursu zyskanie cennego doświadczenia, które wzbogaci ich wiedzę i umiejętności.

Prace są oceniane przez doświadczonych ekspertów współpracujących z Departamentem, wybranych spośród osób o dorobku naukowym, wiedzy i doświadczeniu w dziedzinach odpowiadających tematyce prac. Kapitułę konkursu tworzą specjaliści pełniący najwyższe funkcje w strukturach Sił Zbrojnych. Ten unikalny zestaw ekspertów sprawia, że laureaci mają możliwość zyskać uznanie i nawiązać cenne kontakty.

FORUM DLA MŁODYCH NAUKOWCÓW

Od czasu pierwszej edycji konkursu w 2019 roku, nadesłano ponad 120 prac, w ubiegłym roku 2022 wpłynęło aż 43 prace. Wybieranych jest średnio 7 prac w kategoriach prac licencjackich – magisterskich oraz doktorskich.

Zwycięskie prace z ostatniej edycji dotyczyły takich zagadnień jak identyfikacja rodziny złośliwego oprogramowania na podstawie wygenerowanego ruchu sieciowego, użycie techniki Moving Target Defence do walki z aktywnym rekonesansem czy orkiestracja narzędzi bezpieczeństwa w sieci operatora telekomunikacyjnego z wykorzystaniem technik uczenia maszynowego oraz metod przetwarzania języka naturalnego.

Konkurs im. Mariana Rejewskiego stanowi ważne forum dla młodych naukowców, dając im możliwość pokazania dorobku, zdobycia uznanie i nagród, a przede wszystkim - zdobycia wartościowej wiedzy i doświadczenia w dziedzinie cyberbezpieczeństwa i kryptologii. Konkurs służy nie tylko promocji i rozwoju młodych talentów, ale przede wszystkim inspirowaniu ich do dalszych badań i pracy na

Zgłoś najlepszą pracę naukową w Konkursie im. Mariana Rejewskiego

rzecz poprawy bezpieczeństwa cyfrowego kraju.

Jedną z najważniejszych kwestii, które wyłaniają się z tego konkursu, jest znaczenie badań i rozwoju w dziedzinie cyberbezpieczeństwa. W obecnych czasach, kiedy technologia cyfrowa jest nierozerwalnym elementem naszego codziennego życia, kwestie związane z bezpieczeństwem cyfrowym stają się coraz bardziej istotne. Dlatego też inicjatywy takie jak Konkurs im. Mariana Rejewskiego odgrywają kluczową rolę w promowaniu oraz zachęcaniu do badań i innowacji w tej dziedzinie.

Marian Rejewski, do którego nawiązuje nazwa konkursu, był jednym z najwybitniejszych polskich matematyków i kryptologów, znany przede wszystkim z udziału w złamaniu kodu niemieckiej maszyny szyfrującej Enigma. Jego wkład w rozwój kryptologii jest nieoceniony, dlatego wartość nagrody jest hołdem dla jego niezwykłego dziedzictwa.

Zapraszamy do zgłaszania prac do konkursu. Jest to niepowtarzalna okazja, by wziąć udział w inicjatywie, która łączy naukę, innowacje i patriotyzm. Ostateczny termin nadsyłania prac to 31 lipca. Zachęcamy do zgłaszania prac, które są poświęcone cyberbezpieczeństwu i kryptologii - dziedzinom, które mają kluczowe znaczenie dla bezpieczeństwa narodowego i są nieodzowne w dzisiejszym cyfrowym świecie. Niezależnie od tego, czy jesteś studentem, absolwentem czy doktorantem, twoja praca ma szansę na zdobycie uznanie i nagrody na piątej jubileuszowej edycji konkursu.

ZAPOZNAJ SIĘ ZE SZCZEGÓŁAMI I WYŚLIJ ZGŁOSZENIE

PATRONAT
SECURITY MAGAZINE

CONFIDENCE 2023

KONFERENCJA W KRAKOWIE

Pełna agenda wydarzenia oraz bilety

Z kodem rabatowym "CONFI23xSecurityMagazine" można odebrać 10% zniżki na bilety.

Czym zajmują się polscy cyberżołnierze, jak obejść zabezpieczenia nowoczesnych programów antywirusowych i jak za darmo przejechać się komunikacją miejską? 5 i 6 czerwca stolica Małopolski ponownie stanie się centrum branży cyberbezpieczeństwa. Na konferencji CONFidence w EXPO Kraków wystąpią eksperci z całego świata.

Konferencja skierowana jest do wszystkich osób związanych z cyberbezpieczeństwem - w wydarzeniu biorą udział setki specjalistów reprezentujących bardzo różnorodne branże. Program też jest bardzo bogaty i wielopoziomowy, lecz wszystkie prezentacje mają wspólną cechę - wysoką jakość merytoryczną oraz gwarancję aktualności i praktyczności prezentowanych informacji.

Uczestnicy mają szansę poznać możliwości narzędzi: Raspberry Robin czy wipers, prześledzić metodyki działania grup cyberprzestępczych lub szczegółowe analizy głośnych ataków. Program konferencji odpowiada potrzebom branży z perspektywy szkoleniowej i ze względu na sytuację geopolityczną i jej wpływ na cyberbezpieczeństwo.

Wiedzą podzielą się eksperci o międzynarodowej renomie i specjaliści doskonale znający realia lokalnego rynku security. Dowiesz się m.in.:

- co zrobić, żeby ransomware czuło się w Twojej sieci komfortowo? **(Maciej Broniarz)**,
- dlaczego północnokoreańskie grupy APT są ważnym źródłem dochodu reżimu Kim Jong-Una? **(Mateusz Ossowski)**,
- jakie narzędzia, taktyki i techniki są przydatne w red teamingu systemów kontroli dostępu? **(Julia Zduńczyk)**,
- czy można przeoczyć złośliwy kod w odpowiedzi wygenerowanej przez GPT-4? **(Michał Sarnowski)**.

Aby skorzystać z możliwości, jakie daje udział w wydarzeniu, należy się zarejestrować.

SECURITYMAGAZINE.PL

CYBERGOV 2023. BUDOWANIE CYBER-ODPORNOŚCI PAŃSTWA TO PRIORYTET

PATRONAT
SECURITY MAGAZINE

Podczas konferencji CyberGOV 2023, eksperci cyberbezpieczeństwa, przedstawiciele administracji centralnej i samorządowej, podkreślali znaczenie cyberodporności jako priorytetu strategicznego. Nawiązali do konieczności reagowania na dynamicznie zmieniające się otoczenie. Zwrócili uwagę na fakt, że budowanie cyberodporności jest procesem wymagającym zaangażowania na wielu poziomach administracji.

CYBERZAGROŻENIA W NOWEJ RZECZYWISTOŚCI

Konferencja CyberGOV 2023 - 18 i 19 maja - zorganizowana przez firmę Evention, zgromadziła rekordowe grono specjalistów od cyberbezpieczeństwa. Prelegenci zwrócili na niej uwagę na aktualne wyzwania, które stoją przed administracją publiczną w Polsce, ze szczególnym uwzględnieniem wpływu pandemii oraz konfliktu zbrojnego na Ukrainie. Jako narzędzia walki z zagrożeniami wskazane zostały m.in. wprowadzane rozwiązania legislacyjne i technologiczne.

CYBERODPORNOŚĆ JAKO PRIORYTET

Janusz Cieszyński, Minister Cyfryzacji, podkreślił, że budowanie cyberodporności państwa jest obowiązkiem i odpowiedzialnością. Chwalił zaangażowanie ekspertów ds. cyberbezpieczeństwa, usprawniających istniejące rozwiązania i tworzących nowe. Podkreślił także, że pojawiły się nowe instytucje, takie jak Wojska Obrony Cyberprzestrzeni czy Centrum Cyberbezpieczeństwa Ministerstwa Sprawiedliwości.

- Istnieje jednak wiele wysp, do których pojęcie cyberbezpieczeństwa się nie przebiło. Dlatego cieszę się, że udało się przeznaczyć istotne fundusze dla samorządów, ministerstw i instytucji na budowę kompetencji cyfrowych - zaznaczył minister.

ROLA FUNDUSZY W BUDOWANIU CYBERODPORNOŚCI

Szczególne znaczenie dla budowy odporności IT ma alokacja odpowiednich funduszy. Marcin Romanowski, podsekretarz stanu w Ministerstwie Sprawiedliwości, powiedział, że nakłady na cyfryzację administracji publicznej są niezbędne do budowy zrębów państwa cyfrowego. Wskazał na sukcesy Ministerstwa

CyberGOV 2023. Budowanie cyberodporności państwa to priorytet

Sprawiedliwości, które przeszło cyfrową rewolucję, wprowadzając e-płatności, e-doręczenia, rozprawy zdalne i powołując Centrum Cyberbezpieczeństwa.

WZMOCNIENIE SAMORZĄDÓW I BUDOWA NARODOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Podczas konferencji Łukasz Wojewoda z Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji zaznaczył, że jednym z głównych celów rządu jest wsparcie jednostek samorządu terytorialnego w zapobieganiu i reagowaniu na incydenty bezpieczeństwa w IT. Projekt o wartości 1,9 mln zł ma na celu przekazanie grantów jeszcze w tym roku.

Kolejnym priorytetem jest podłączenie nowych podmiotów do krajowego systemu cyberbezpieczeństwa i do zintegrowanego systemu zarządzania cyberbezpieczeństwem (systemu S46). Planowane jest wsparcie dla prawie 500 jednostek w zakresie rozbudowy systemów bezpieczeństwa, co ma kosztować łącznie 163 mln euro (ponad 700 mln zł). Realizacja projektu ma zakończyć się pod koniec 2024 roku.

EDUKACJA I SZKOLENIA W OBSZARZE CYBERBEZPIECZEŃSTWA

W prezentacji Wojewoda podkreślił również znaczenie szkoleń. Te mają obejmować różne poziomy administracji, od instytucji centralnych, przez samorządowe, aż po pracowników placówek opieki zdrowotnej. W ramach tego projektu zaplanowano program zwiększenia świadomości pracowników administracji publicznej w zakresie cyberbezpieczeństwa.

Pierwszy moduł szkolenia z podstaw cyberhigieny ma zostać uruchomiony już

w czerwcu na platformie szkolenia.obywatele.gov.pl. W planach są również kolejne moduły szkolenia.

REGULACJE PRAWNE I KRAJOWE CENTRUM KOMPETENCJI CYBERBEZPIECZEŃSTWA

Na konferencji przedstawiciele Ministerstwa Cyfryzacji poinformowali o powstaniu Krajowego Centrum Kompetencji Cyberbezpieczeństwa, które będzie częścią europejskiej społeczności zajmującej się ochroną IT. Ośrodek ma służyć jako źródło wsparcia dla wszystkich zainteresowanych udziałem w konkursach w zakresie bezpieczeństwa informatycznego.

Przedstawiciele Ministerstwa Cyfryzacji mówili również o pracach nad regulacjami prawnymi dotyczącymi bezpieczeństwa IT. Projekt noweli ustawy o Krajowym Systemie Cyberbezpieczeństwa jest gotowy do przekazania do dalszych prac w parlamencie. Zasady zawarte w unijnej dyrektywie NIS2 mają być uwzględnione w kolejnej nowelizacji ustawy o KSC lub w zupełnie nowym akcie prawnym.

Łukasz Wojewoda zachęcał do zapoznania się z europejskimi regulacjami dotyczącymi cyberbezpieczeństwa, aby wiedzieć, czego można się spodziewać w najbliższej przyszłości. Wspomniał również o innowacyjnej Ustawie o Zwalczaniu Nadużyć w Komunikacji Elektronicznej, która ma na celu przeciwdziałanie phishingowi SMS i połączeń głosowych, a także nakłada na podmioty publiczne obowiązek instalacji systemów zapobiegających nadużyciom w poczcie elektronicznej.

LEKCJE Z WOJNY NA UKRAINIE

W zeszłym roku CERT Polska zanotował drastyczny wzrost zgłoszeń dotyczących bezpieczeństwa IT - aż dziesięciokrotnie więcej niż w 2020 roku. Ekspert od bezpie-

CyberGOV 2023. Budowanie cyberodporności państwa to priorytet

czeństwa, Sebastian Kondraszuk, powiązał ten wzrost z rozpoczęciem konfliktu na Ukrainie.

- Internauci zauważają więcej, jest również większa otwartość w urzędach. Duży wpływ na liczbę zgłoszeń mają również ułatwienia w sposobie ich przekazywania, w tym incydentów z SMS-ami. Kolosalne znaczenia ma wojna za naszą wschodnią granicą - tłumaczył te dane Kondraszuk.

CYBERZAGROŻENIA W SEKTORZE ZDROWIA

Roman Łożyński z Centrum e-Zdrowia zwrócił uwagę na szczególną dziedzinę działalności sektora publicznego, jaką jest ochrona zdrowia. Stan cyberbezpieczeństwa polskich szpitali można ocenić jako średni. - *To oznacza, że można je skutecznie zaatakować, dysponując średnimi zasobami* - mówił Roman Łożyński.

OCHRONA KLUCZOWYCH ZASOBÓW I DANYCH

Podczas debaty na temat ochrony kluczowych zasobów i danych w sektorze publicznym uczestnicy zastanawiali się, w jakim stopniu ochrona zasobów powinna być scentralizowana, a w jakim - działać na poziomie lokalnym.

Adam Marczyński, zastępca dyrektora NASK PIB, porównał to do systemu straży pożarnej, gdzie działanie na poziomie centralnym i lokalnym musi być zbalansowane. Natomiast Bartosz Kamiński z SentinelOne argumentował, że odpowiedzią na pytanie o scentralizację czy działanie na poziomie lokalnym jest hybryda - działanie wspólne pozwala na obniżenie kosztów i radzenie sobie z brakami kadrowymi w obszarze IT.

CyberGOV 2023. Budowanie cyberodporności państwa to priorytet

Fot. Evention (25)

POTRZEBA DECENTRALIZACJI

Marek Krzyżanowski z ICSec przekonywał, że podejście wyłącznie scentralizowane może być niewystarczające w przypadku bezpieczeństwa dużych jednostek należących do samorządów, takich jak wodociągi, kanalizacja czy ciepłownie. Wskazał, że państwo może okazać się trochę za daleko, aby w optymalny sposób zarządzać tymi systemami, co stanowi argument za większym zaangażowaniem na poziomie lokalnym.

Jan Kostrzewa, dyrektor Centrum Cyberbezpieczeństwa MS, podkreślił, że centralizacja jest korzystna, kiedy narzuca standardy i stwarza pewną potrzebę biznesową. Zauważył tendencję spychania cyberbezpieczeństwa na drugi plan, podczas gdy wymogi ministerialne tworzą presję na podnoszenie jakości działań.

Łożyński wyraził obawy co do stanu cyberbezpieczeństwa w polskich szpitalach. Wskazał na ich podatność na ataki ransomware oraz brak odpowiednich systemów kopii zapasowej oraz planów zarządzania podatnościami. Dodatkowo, szkolenia kadry w dziedzinie cyberbezpieczeństwa należą do rzadkości.

REGULACJE PRAWNE

Dyskutowano także o regulacjach prawnych związanych z cyberbezpieczeństwem. Prof. Grzegorz Sibiga zaznaczył problem z interpretacją przepisów dotyczących dostępu do informacji publicznej, a zwłaszcza tych związanych z bezpieczeństwem teleinformatycznym.

Innym zagadnieniem były przepisy dotyczące pracy zdalnej. Chociaż organizacje komercyjne dostosowały się do tego modelu pracy podczas pandemii, dopiero teraz pojawiły się przepisy obejmujące wszystkie miejsca pracy, w tym urzędy i jednostki samorządowe. Wprowadzenie tych regulacji ma na celu zapewnienie bezpiecznego przepływu informacji.

Podczas sesji roundtables poruszono m.in. temat przygotowania organizacji do ataku ransomware, konieczności szkolenia pracowników i przełożenia koncepcji "ciągłości biznesowej" na pracę urzędów administracji publicznej. Omówiono również zagadnienia związane z wykorzystywaniem prywatnych urządzeń do pracy (BYOD) oraz oporami wobec korzystania z rozwiązań chmurowych w polskich urzędach.

PATRONAT
SECURITY MAGAZINE

Zapraszamy na pierwszą na polskim rynku konferencję z zakresu cybersecurity, która jest skupiona ściśle na tej tematyce.

W innowacyjnej formule konferencji, która zakłada większy niż zazwyczaj aktywny udział uczestników, skupimy się na kluczowych elementach systemu cyberbezpieczeństwa – organizacji zarządzania incydentami oraz zagrożeniami.

Konferencja jest adresowana do menedżerów bezpieczeństwa, ekspertów specjalizujących się w Threat Hunting, Threat Intelligence, Incident and Response Management oraz efektywności i organizacji SOC, a także do osób, które zajmują się szeroko pojętym cyberbezpieczeństwem.

Pogłębisz swoją wiedzę w obszarach takich jak:

- Budowa, rozwój, utrzymanie, optymalizacja i opomiarowanie Security Operations Center,
- Poziomy dojrzałości SOC i nowe obszary rozwoju zależnie od specyfiki organizacji,
- Droga od SIEM do SOAR, przyszłość rozwiązań SIEM i ich obecne słabości, SIEM w chmurze,
- SOC nowej generacji – jak może wyglądać przyszłość?
- Wdrażanie programów Threat Intelligence i ich potencjał, zewnętrzne źródła danych,
- Współpraca w branżach i między branżami w obszarze zarządzania incydentami i analizowania zagrożeń,
- Praktyka Threat Hunting,
- Automatyzacja w cyberbezpieczeństwie i autonomiczny SOC – co automatyzować i w jaki sposób, by było to efektywne i służyło wszystkim?

KOGO SPOTKASZ NA KONFERENCJI?

Menedżerów cyberbezpieczeństwa, ekspertów specjalizujących się w Threat Hunting, Threat Intelligence, Incident and Response Management oraz specjalistów i managerów do spraw efektywności, organizacji i funkcjonowania SOC, a także zajmujących się aspektami dotyczącymi jakości pracy i komfortu osób pracujących w cyberbezpieczeństwie, w szczególności w obszarze SOC.

ZAREJESTRUJ SIĘ TUTAJ!

incidentbusters.pl

SECURITYMAGAZINE.PL

KTÓRA Z KOBIET ZOSTAŁA RISING STAR IN CYBERSECURITY?

PATRONAT
SECURITY MAGAZINE

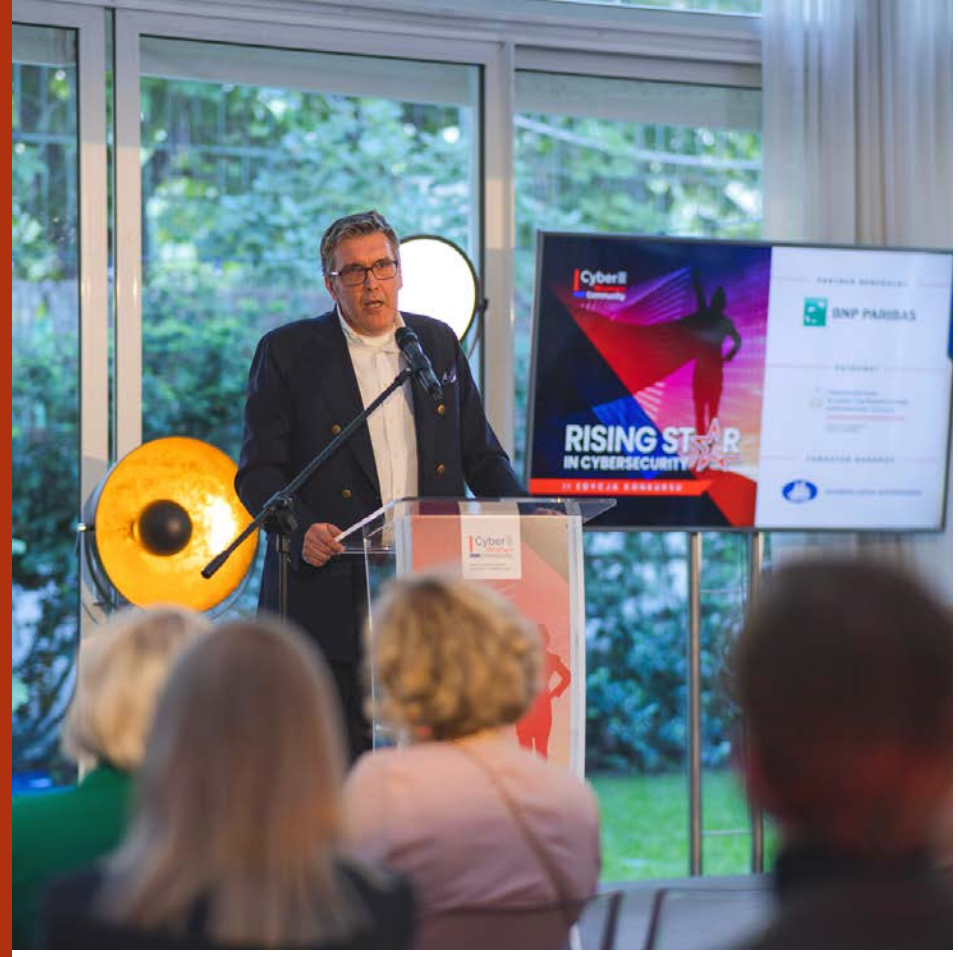
25 maja poznaliśmy laureatkę konkursu Rising Star in Cybersecurity. Przed publicznością wystąpiły cztery finalistki, prezentując swoje projekty związane z cyberbezpieczeństwem. Poziom prezentacji pokazał, że wszystkie uczestniczki to niezwykle utalentowane i zaangażowane kobiety, które zasługują na uznanie w dziedzinie cyberbezpieczeństwa.

Która z kobiet została Rising Star in Cybersecurity?

Główną nagrodę zdobyła charyzmatyczna Magdalena Jakimiuk, liderka zespołu usług bezpieczeństwa IT w DB Schenker, która przekonała jury swoim podejściem do zagadnień związanych z cyberbezpieczeństwem. Jej prezentacja, która koncentrowała się na narzędziu do tworzenia raportów, zasłużyła na szczególne uznanie jury. W opinii oceniających, Magdalena Jakimiuk nie tylko wykazała ogromne zrozumienie dla problemów związanych z cyberbezpieczeństwem, ale również zaprezentowała efektywne rozwiązanie, jakim był właśnie program Power BI. Co prawda, do tej pory nie był stosowany w cyberbezpieczeństwie, jednak pani Magdalena zaczęła go używać do danych o podatnościach. Okazało się, że dzięki niemu odzyskała czas na inne działania, na których jej zależało.

- Okazało się, że całkiem nieźle mi to wyszło, ponieważ dziś narzędzie rozrosło się do potężnego "ekspresu" który codziennie pozwala przemielić ogromne ilości danych z wielu źródeł. (...) Ten ekspres przyczynił się do tego, że dzisiaj mamy w dziale bezpieczeństwa inżynierów danych i żadne analizy nie są nam straszne. Przyczynił się do poprawy dostępności naszego skanera podatności, do automatyzacji zarządzania tym skanerem. (...) Dziś z moim zespołem odpowiadam nie tylko za rozwój tego narzędzia, ale odpowiadam przede wszystkim za skaner podatności, który monitoruje blisko 100 tys. urządzeń na całym świecie, odpowiadam za edukacyjne kampanie phishingowe na poziomie globalnym, za identyfikację i egzekucję domen

Która z kobiet została Rising Star in Cybersecurity?



zagrażających marce oraz naszym klientom - mówiła Magdalena Jakimiuk.

Pozostałe finalistki: Katarzyna Skrobek (trzecie miejsce), Małgorzata Widera (super wyróżnienie) i Magdalena Wrzosek (drugie miejsce), również prezentowały bardzo wysoki poziom. Wszystkie ich projekty zasługują na uwagę, a ich zaangażowanie w zabezpieczanie świata cyfrowego jest niezwykle inspirujące.

A co najważniejsze udowadniają, że kobiet w cyberbezpieczeństwie jest zdecydowanie zbyt mało. Ponadto są do dziś niedoceniane w branży technologicznej. Co prawda, stereotypy dotyczące kobiet zmieniają się, ale nadal w wielu firmach, organizacjach panuje przekonanie, że cybersecurity przeznaczone jest dla mężczyzn, a sama branża jest zmaskulinizowana. To zamyka drogę wielu niezwykle zaangażowanym, ambitnym kobietom.

A przecież mają masę pomysłów na to, co zrobić, by w świecie online było bezpiecznie. Bo oprócz pomysłu, który zaprezentowała laureatka, pozostałe panie również pokazały prawdziwy potencjał. Katarzyna Skrobek zaprezentowała niezawodność chmury, Małgorzata Widera mówiła o potrzebie ochrony dzieci, młodzieży i projekcie Be.Net - ogólnopolskim programie edukacyjnym skierowanym do nauczycieli, uczniów, szkół podstawowych i ponadpodstawowych z całej Polski. Magdalena Wrzosek przekonywała, że to nie prezentacje w PowerPoincie przekonają firmy, by inwestować w cyberbezpieczeństwo, ale... gry. Pokazała, że to naprawdę działa.

Wśród pań największe uznanie publiczności zdobyła Małgorzata Widera, która trafiła do przekonania oglądających galę w serwisie LinkedIn, jak istotne jest kształcenie młodych w zakresie cyberbezpieczeństwa. Ale również jak ważne

Która z kobiet została Rising Star in Cybersecurity?

jest dzielenie się wiedzą z nauczycielami, którzy przecież też muszą wiedzieć, co swoim uczniom przekazać.

W kontekście jednego z naszych artykułów dotyczących cyberbezpieczeństwa w edukacji, mało powiedzieć, że w Polsce mamy jedynie 17 tys. wakatów związanych z cyberbezpieczeństwem, a do matury z informatyki przystąpiło ledwo 18 uczniów (ani jedna uczennica). W grę wchodzi również umiejętność walki z hejtem i dezinformacją.

Podczas Gali Rising Star in Cybersecurity obecnością zaszczycili ambasador Stanów Zjednoczonych w Polsce, Mark Brzezinski, Monika Pieniek, zastępca Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, Krzysztof Słotwiński z BNP Paribas oraz prof. dr hab. Grzegorz Mazurek, rektor Akademii Leona Koźmińskiego - fundator nagrody głównej. Koordynatorką konkursu była Agnieszka Wielądek z firmy Evention.

- *Wierzę, że takie projekty jak Rising Star pomagają przełamać stereotypy. Budują potencjał do rzeczywistych zmian* - podsumował Przemysław Gamdzyk, Meeting Designer oraz prezes spółki Evenfion.

Konkurs Rising Star in Cybersecurity to ważne wydarzenie dla całej branży, podkreślające znaczenie kobiet w dziedzinie cyberbezpieczeństwa. To także okazja do zwrócenia uwagi na ważność inwestowania w badania i rozwój w tej dziedzinie. Laureatka rozpocznie studia podyplomowe na kierunku “Zarządzanie bezpieczeństwem” na Akademii Leona Koźmińskiego. Głównym celem studiów jest przekazanie praktycznej wiedzy z zakresu zarządzania cyberbezpieczeństwem w organizacjach z sektora publicznego i prywatnego. Jak zapewnił rektor Grzegorz Mazurek, inicjatywę tę uczelnia będzie wspierać tak długo, jak trwać będzie konkurs. Bo uczelnia chce mieć w swoich murach ambitne, twórcze, utalentowane osoby - takimi bez wątpienia są finalistki Rising Star in Cybersecurity.

Która z kobiet została Rising Star in Cybersecurity?

Fot. Evention (18)

PATRONAT
SECURITY MAGAZINE

24. KONFERENCJA BRANŻY OCHRONY

POTENCJAŁ I ROLA SEKTORA PRYWATNEGO W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO

ZAREJESTRUJ SIĘ TUTAJ

28-29 września, w Hotelu Windsor w Jachrance, odbędzie się 24. Konferencja Branży Ochrony. Wydarzenie jest nieodłącznym elementem kalendarza ekspertów, przedsiębiorców i instytucji związanych z sektorem ochrony i zabezpieczeń w Polsce.

Tegoroczne spotkanie, organizowane pod hasłem „Potencjał i Rola Sektora Prywatnego w Systemie Bezpieczeństwa Narodowego" to okazja, by zapoznać się z wystąpieniami ekspertów, panelami dyskusyjnymi, prezentacjami produktów oraz networkingu.

PIO, jako lider w branży ochrony, zrzesza około 180 firm, współpracujących z podmiotami prywatnymi i publicznymi. Organizacja ta odgrywa kluczową rolę w realizacji zadań ochronnych w Polsce, szczególnie na poziomie lokalnym.

Głównymi obszarami omawianymi podczas konferencji będą technologie dla narodowego bezpieczeństwa, współpraca z mieszkańcami i partycypacja społeczna w tworzeniu bezpiecznych przestrzeni, bezpieczeństwo społeczności, cyberbezpieczeństwo, oraz rola i potencjał branży ochrony dla bezpieczeństwa narodowego.

Konferencja jest adresowana do przedstawicieli władz, ośrodków bezpieczeństwa, jak również jednostek odpowiedzialnych za bezpieczeństwo oraz zarządzanie kryzysowe w sektorze prywatnym. Celem spotkania jest pokazanie potencjału branży ochrony oraz jej znaczącego wpływu na bezpieczeństwo na szczeblu narodowym.

Partnerami konferencji są prestiżowe instytucje takie, jak Wojskowa Akademia Techniczna, Securex oraz Akademia WSB, a wsparcie merytoryczne zapewnia Centrum Prewencji Terrorystycznej, Agencja Bezpieczeństwa Wewnętrznego.

WIĘCEJ NA STRONIE PIO

SECURITYMAGAZINE.PL

PŁEĆ I WIEK NIE MOGĄ WYKLUCZAĆ Z BRANŻY CYBERSECURITY

Magdalena Jakimiuk
Leader of IT Security Services Team

To ona zwyciężyła w drugiej edycji konkursu Rising Star in Cybersecurity. Jej charyzma, wiedza i pomysł, jak przekazać jurorom to, czym zajmuje się na co dzień zrobiły na nich ogromne wrażenie. Przekonała nie tylko swoją pasją i profesjonalizmem, ale także innowacyjnym podejściem do poruszanych zagadnień. Oto Magdalena Jakimiuk w rozmowie z "Security Magazine".

Czym się Pani zajmuje na co dzień? Co zdecydowało, że podjęła Pani pracę w cyberbezpieczeństwie?

Magdalena Jakimiuk: Przede wszystkim odpowiadam za globalny proces zarządzania podatnościami. Oprócz tego za edukacyjne kampanie phishingowe na poziomie globalnym oraz identyfikację i egzekucję domen zagrażających firmie, jej pracownikom i klientom. Zmieniłam branżę ponieważ, zależy mi na rozwoju intelektualnym, realizowaniu czegoś znaczącego i współpraca z profesjonalistami, którzy są autentyczni. Kombinację tych elementów znalazłam dopiero w cyberbezpieczeństwie.

W swojej prezentacji wspomniała Pani o przeszkodzie na drodze do pracy w cyberbezpieczeństwie, jaką był wiek. Konkurs z kolei ma przełamywać stereotypy dotyczące płci. Płeć i wiek – choć wydaje się to abstrakcją – mogą być przeszkodami do kariery. Co powiedziałaby Pani rekruterom, którzy wciąż wykluczają kandydatów tylko ze względu na wiek czy płeć?

M.J.: Zacznę od tego, że jeżeli ktoś pozwala na to, aby wiek czy płeć przysłaniały wiedzę i doświadczenie, to nie jest profesjonalistą. By zostać profesjonalistą, trzeba się szkolić, i to byłaby pierwsza uniwersalna rekomendacja.

Co do rekruterów, to należy pamiętać, że często są pośrednikami przekazującymi decyzję managerów, którzy też muszą doskonalić swoje umiejętności.

Czy uważa Pani, że inicjatywy jak Rising Star in Cybersecurity są skutecznym narzędziem do promowania większego udziału kobiet w cyberbezpieczeństwie?

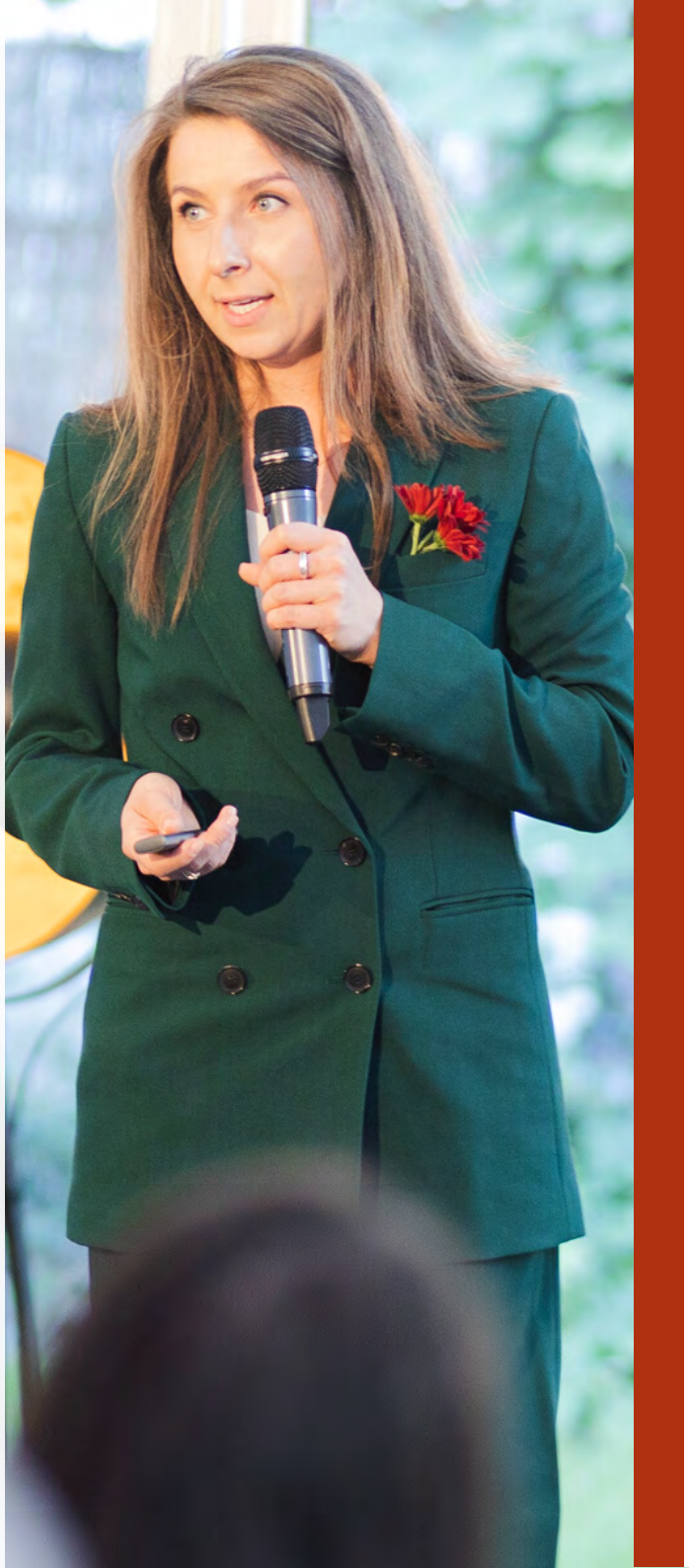
M.J.: Zdecydowanie. Konkurs jest genialną inicjatywą, która pozwoliła mi poznać wspaniałe kobiety z branży. Teraz o nich mogą się dowiedzieć moje koleżanki i ich koleżanki. Tak coraz więcej kobiet może poznać możliwości, jakie daje ta branża oraz, że jeżeli zdecydują się dołączyć do naszego grona, mogą liczyć na naszą pomoc.

Jakie rady dałaby Pani innym kobietom, które chcą wyruszyć na podobną ścieżkę kariery w cyberbezpieczeństwie?

M.J.: Bądź konsekwentna. Szukaj mądrych ludzi. Buduj wiedzę oraz dbaj o apetyt na nią.

Jako laureatka konkursu Rising Star in Cybersecurity rozpocznie Pani studia z zarządzania cyberbezpieczeństwem. Jak planuje Pani wykorzystać swoje doświadczenie i wiedzę zdobytą na studiach? Czy pomogą rozwijać Pani zainteresowania, karierę?

M.J.: Bez wątpienia. Praca w cyberbezpieczeństwie wymusza

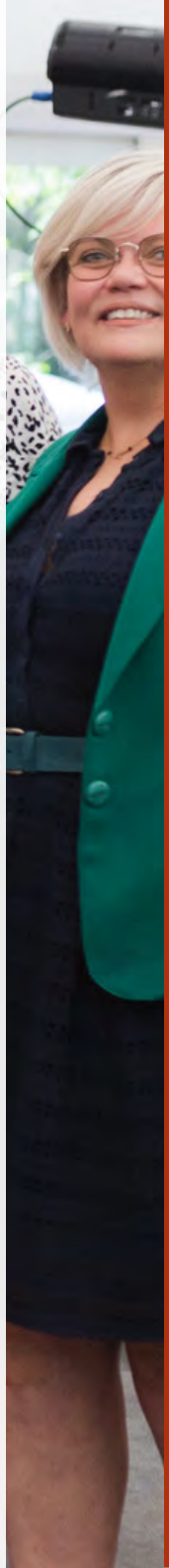


Fot. Evention (4)

nieustanne kształcenie się. Studia pozwolą mi dowiedzieć się jeszcze więcej, aby jeszcze lepiej realizować swoją pracę i budować mój profesjonalny warsztat.

Dziękujemy za rozmowę i gratulujemy zwycięstwa w konkursie.

Rozmawiała:
Monika Świetlińska



Rzetelny® Regulamin

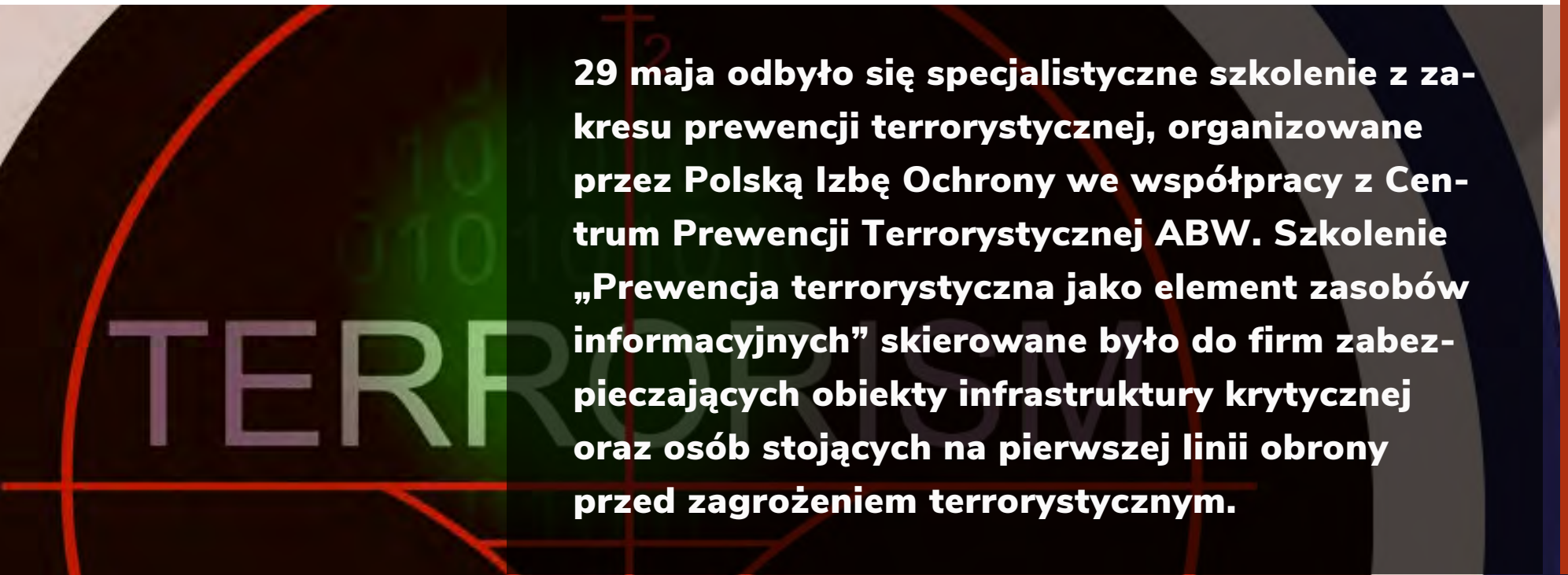
DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

PREWENCJA TERRORYSTYCZNA JAKO ELEMENT ZASOBÓW INFORMACYJNYCH

PATRONAT
SECURITY MAGAZINE



29 maja odbyło się specjalistyczne szkolenie z zakresu prewencji terrorystycznej, organizowane przez Polską Izbę Ochrony we współpracy z Centrum Prewencji Terrorystycznej ABW. Szkolenie „Prewencja terrorystyczna jako element zasobów informacyjnych" skierowane było do firm zabezpieczających obiekty infrastruktury krytycznej oraz osób stojących na pierwszej linii obrony przed zagrożeniem terrorystycznym.

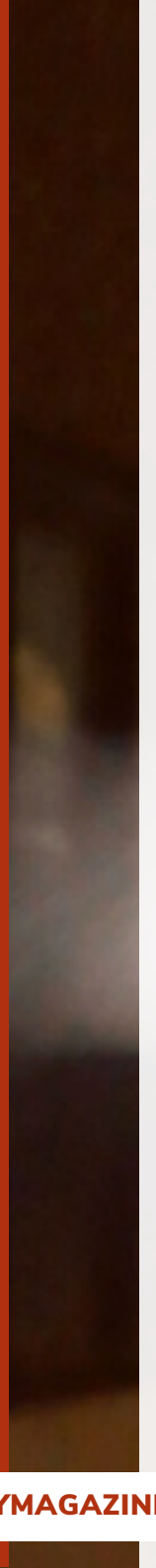
Prewencja terrorystyczna jako element zasobów informacyjnych

29 maja odbyło się specjalistyczne szkolenie z zakresu prewencji terrorystycznej, organizowane przez Polską Izbę Ochrony we współpracy z Centrum Prewencji Terrorystycznej ABW. Szkolenie „Prewencja terrorystyczna jako element zasobów informacyjnych" skierowane było do firm zabezpieczających obiekty infrastruktury krytycznej oraz osób stojących na pierwszej linii obrony przed zagrożeniem terrorystycznym.

Przygotowanie uczestników do szybkiego rozpoznawania i skutecznego reagowania na zagrożenia terrorystyczne, dywersyjne i szpiegowskie, zwłaszcza w obliczu aktualnych wyzwań geopolitycznych to główny cel organizatora.

Podczas szkolenia poruszane były tematy takie jak: rola informacji na temat zagrożeń terrorystycznych, typologia tych zagrożeń, poziom narażenia obiektów strategicznych, metody pozyskiwania informacji, identyfikowanie osób mogących stanowić zagrożenie, a także mechanizmy ochrony. Prowadzone przez doświadczonych specjalistów z Centrum Prewencji Terrorystycznej ABW odbyło się w Centrum Szkoleniowym WSPÓLNA.

Na temat tej inicjatywy rozmawiamy z rzecznikiem Polskiej Izby Ochrony, Wojciechem Stawskim.



Polska Izba Ochrony: „Prewencja terrorystyczna jako element zasobów informacyjnych" - skąd taka tematyka szkolenia dla branży ochrony?

Wojciech Stawski: Ostatnio żyjemy w dość niebezpiecznym otoczeniu. Wojna w Ukrainie oraz zaangażowanie Polski w pomoc naszym sąsiadom stwarza ryzyka, dawniej rozpoznawane wyłącznie jako teoretyczne, w coraz większym stopniu przybierające obraz faktycznych. Polska Izba Ochrony od wielu lat podkreślała rolę branży w systemie bezpieczeństwa państwa.

Bezpieczeństwo państwa kojarzone jest z organami państwowymi oraz służbami specjalnymi, natomiast branża ochrony wiązana jest bardziej z realizacją komercyjnych usług na rzecz osób prywatnych i podmiotów gospodarczych. Gdzie jest tu miejsce dla prywatnych ochroniarzy?

W.S.: Postawiona w pytaniu teza nie do końca jest prawdziwa. Branża ochrony świadczy w znacznej mierze usługi na rzecz osób i przedsiębiorców prywatnych, ale również ochrania obiekty infrastruktury krytycznej (energetyczne, paliwowe, zaopatrzenia w wodę, przechowujące substancje niebezpieczne, administracji publicznej), lotniska, porty, jednostki wojskowe, dworce, galerie handlowe itp. Wszystkie wymienione obiekty potencjalnie mogą stać się celem ataków terrorystycznych lub dywersyjnych. Służby państwowe, biorąc pod uwagę ich liczebność, nie są w stanie ich zabezpieczyć swoimi siłami, stąd potrzeba wsparcia przez prywatny sektor ochrony.

Kto był adresatem szkolenia?

W.S.: Szkolenie adresowane było przede wszystkim do średniego szczebla kierowniczego w firmach ochroniarskich, do osób, które zajmują się bezpośrednim nadzorem

nad realizacją zadań ochronnych w obiektach, które mogą być zagrożone aktami terroru, dywersji lub stać się obiektem zainteresowania obcego wywiadu.

Zakładamy, że wiedza zdobyta przez uczestników szkolenia zostanie uwzględniona w tworzeniu dokumentacji ochronnej oraz wykorzystana w instruktażu pracowników ochrony bezpośrednio wykonujących zadania na obiektach o strategicznym znaczeniu.

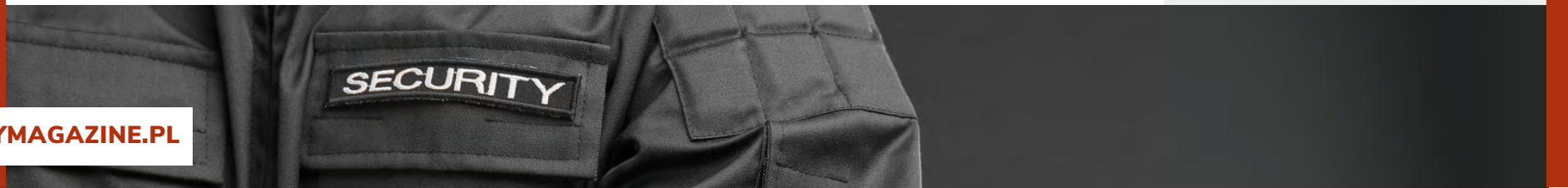
Mając w pamięci niedawny, niefortunny incydent w Naftoporcie (całe szczęście bez udziału pracowników ochrony), istnieje szansa, że m.in. dzięki szkoleniu zostanie podniesiony poziom bezpieczeństwa chronionych obiektów, a pracownik ochrony będzie przygotowany na właściwą ocenę symptomów zagrożeń i adekwatne działania.

Im więcej osób, bez względu na rodzaj formacji, które wypełniają zadania w systemie bezpieczeństwa będzie miało świadomość zagrożeń i właściwych reakcji, tym większe szanse na ograniczenie groźnych skutków.

Czy to to jedyna inicjatywa Polskiej Izby Ochrony w tym zakresie?

W.S.: 28-29 września w Jachrance odbędzie się 24. Konferencja Branży Ochrony pt. „Potencjał i rola sektora prywatnego w systemie bezpieczeństwa narodowego”. Organizatorem konferencji jest Polska Izba Ochrony, przy współudziale Wojskowej Akademii Technicznej. Uczestnicy konferencji będą mieli okazję zapoznać się z miejscem, jakie zajmuje oraz do jakiego aspiruje branża ochrony w systemie bezpieczeństwa państwa. Nie należy zapominać, że pod względem liczebności prywatny sektor ochrony przewyższa wszystkie formacje państwowe razem wzięte. Naszego kraju nie stać na niedostrzeganie tego potencjału. Szkolenie, będące przedmiotem naszej rozmowy, jest przykładem praktycznej realizacji wspomnianego potencjału.

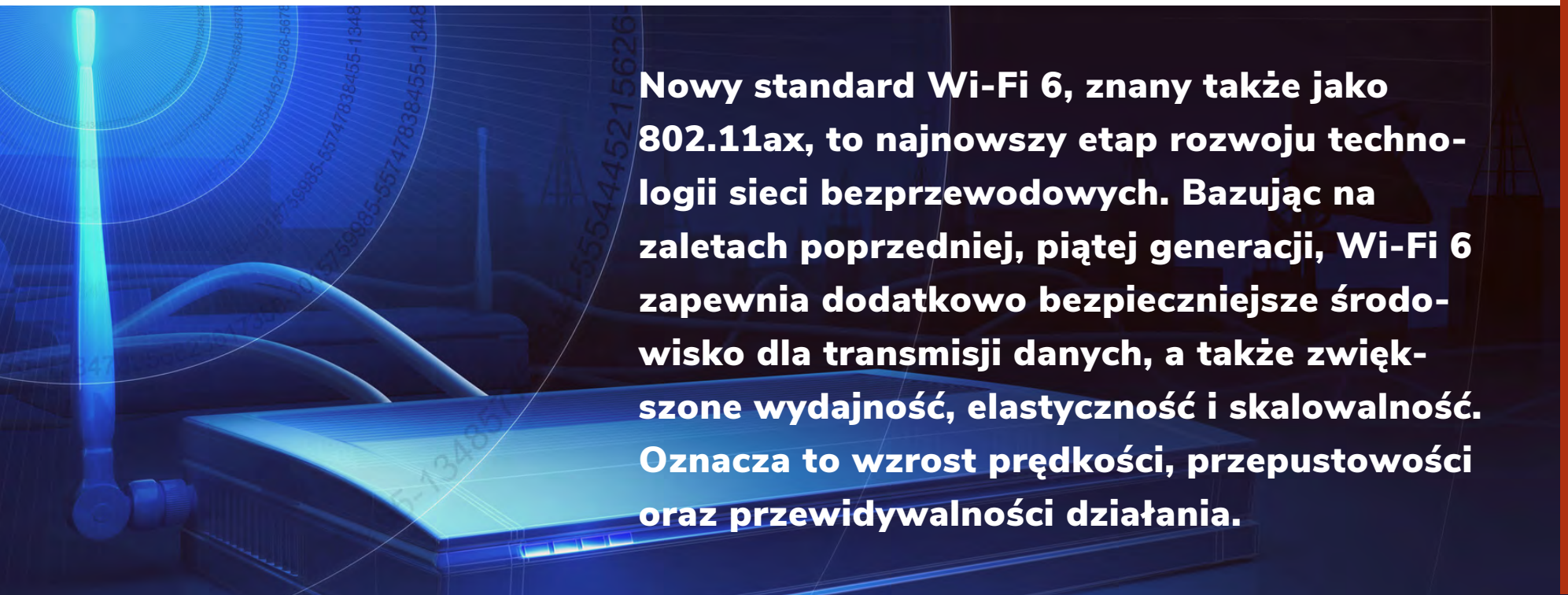
Dziękujemy za rozmowę.



DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

WI-FI 6 I WI-FI 6E - BEZPIECZNIEJSZE SIECI BEZPRZEWODOWE

Karol Goliszewski
Grandmetric



Nowy standard Wi-Fi 6, znany także jako 802.11ax, to najnowszy etap rozwoju technologii sieci bezprzewodowych. Bazując na zaletach poprzedniej, piątej generacji, Wi-Fi 6 zapewnia dodatkowo bezpieczniejsze środowisko dla transmisji danych, a także zwiększone wydajność, elastyczność i skalowalność. Oznacza to wzrost prędkości, przepustowości oraz przewidywalności działania.

Nowy standard Wi-Fi 6, znany także jako 802.11ax, to najnowszy etap rozwoju technologii sieci bezprzewodowych. Bazując na zaletach poprzedniej, piątej generacji, Wi-Fi 6 zapewnia dodatkowo bezpieczniejsze środowisko dla transmisji danych, a także zwiększone wydajność, elastyczność i skalowalność. Oznacza to wzrost prędkości, przepustowości oraz przewidywalności działania.

Obecnie większość punktów postępowych nowych serii obsługuje standardy Wi-Fi 6 oraz Wi-Fi 6E. Przykładem niech będzie seria urządzeń Catalyst 9100 od Cisco czy Meraki MR56 i MR57.

Wi-Fi 6 odpowiada na potrzeby zaawansowanych aplikacji, służących np. do odtwarzania wideo w jakości 4K lub 8K, sterowania procesami w zautomatyzowanych fabrykach przemysłu 4.0 czy Internetu Rzeczy (IoT). Standard ten pozwala na bardziej efektywną obsługę sieci zatłoczonych przez wiele urządzeń łączących się jednocześnie i przekazujących duże ilości danych.

Poza zwiększoną prędkością przesyłania danych czy możliwością obsługi środowisk o dużej gęstości, Wi-Fi 6 oraz Wi-Fi 6E to również kilka ulepszeń, które mają duży wpływ na zwiększenie bezpieczeństwa sieci.

Z pewnością skorzystają na tym różnego rodzaju instytucje obracające danymi wrażliwymi (jak banki, instytucje rządowe czy placówki medyczne), a także obiekty o wysokim znaczeniu strategicznym (np. elektrownie, lotniska, bazy wojskowe).

Z czego wynika zwiększone bezpieczeństwo standardu Wi-Fi 6 oraz jego rozszerzenia Wi-Fi 6E?

WYKORZYSTANIE SZYFROWANIA WPA3

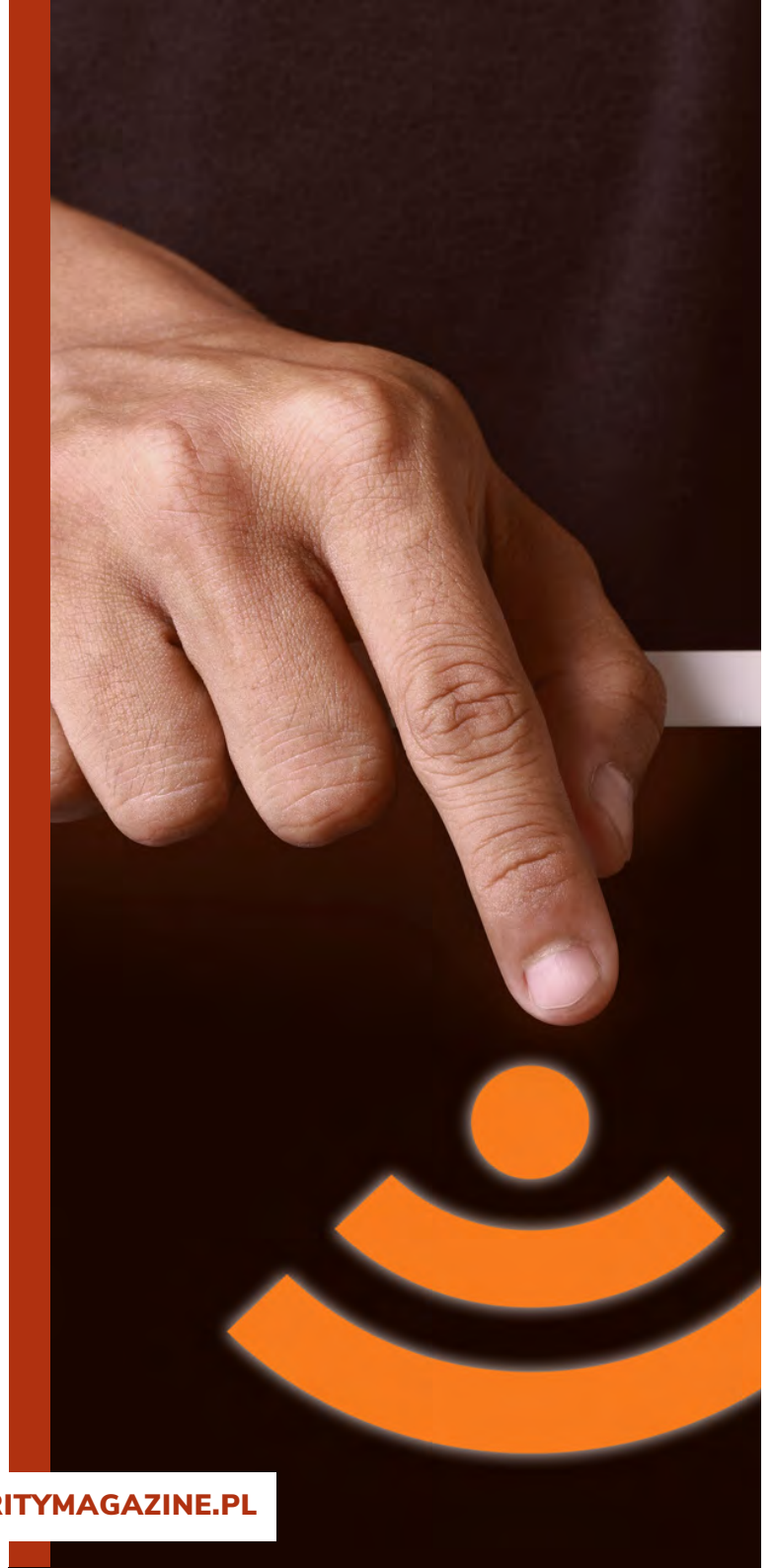
Najważniejszym ulepszeniem w Wi-Fi 6 jest obsługa najnowszego standardu szyfrowania – WPA3 (Wi-Fi Protected Access 3). WPA3 oferuje silniejsze protokoły bezpieczeństwa oraz zastępuje dotychczasowy standard WPA2, wykorzystywany w pasmach 2.4 GHz i 5 GHz. WPA3 występuje w dwóch wariantach - WPA3-Personal i WPA3-Enterprise.

WPA3-Personal

Największą zmianą w WPA3-Personal jest zastąpienie klucza współdzielonego Pre-shared Key (PSK) przez metodę Simultaneous Authentication of Equals (SAE). Nowa metoda opiera się na wymianie kluczy o wdzięcznej nazwie Dragonfly zapewnia znacznie lepszą ochronę przed atakami typu brute-force, polegającymi na odgadywaniu przez hakerów haseł w trybie offline.

	WEP	WPA	WPA2	WPA3
Krótki opis	Zapewnia prywatność taką jak sieci przewodowe	Oparty na standardzie 802.11i, nie wymaga nowego sprzętu	Zawiera wszystkie wymagane funkcje 802.11i oraz wymaga nowego sprzętu	Opcjonalny dla pasm 2.4GHz i 5GHz, wdrożony dla 6GHz
Szyfrowanie	RC4	TKIP + RC4	CCMP / AES	GCMP-256
Uwierzytelnianie	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA23Personal WPA3-Enterprise
Integralność danych	CRC-32	algorytm MIC	Cipher Block Chaining Message Authentication Code (w oparciu o AES)	256-bitowy kod Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Zarządzanie kluczem	brak	4-way handshake	4-way handshake	wymiana Elliptic Curve Diffie-Hellman (ECDH) i algorytm Elliptic Curve Digital Signature Algorithm (ECDSA)

GRANDMETRIC
STAY CONNECTED.



WPA3-Enterprise

W przeciwieństwie do WPA3-Personal, które wykorzystuje nową metodę uwierzytelniania, WPA3-Enterprise wciąż bazuje na WPA2, wprowadzając do niego kilka usprawnień.

- Uwierzytelnione szyfrowanie jest realizowane za pomocą 256-bitowego protokołu Galois/Counter Mode Protocol (GCMP-256).
- Funkcja wyprowadzenia klucza wykorzystuje 384-bitowy tryb Hashed Message Authentication Mode (HMAC) oraz algorytm Secure Hash Algorithm (SHA).
- Wymiana kluczy szyfrujących odbywa się z użyciem Elliptic Curve Diffie-Hellman (ECDH) i Elliptic Curve Digital Signature Algorithm (ECDSA).
- Integralność danych opiera się na 256-bitowym kodzie Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256).

ULEPSZONE UWIERZYTELNIANIE I OBSŁUGA KLUCZY SZYFROWANIA

Wi-Fi 6 wprowadza również nowy protokół uwierzytelniania o nazwie Enhanced Open, który eliminuje ograniczenia bezpieczeństwa otwartych sieci Wi-Fi. Zapewnia indywidualne szyfrowanie danych dla każdego użytkownika, nawet w sieciach, które nie wymagają hasła. Pomaga to chronić użytkowników sieci przed nieautoryzowanym dostępem.

Dodatkowo Wi-Fi 6 zawiera ulepszenia w sposobie obsługi kluczy szyfrowania. Wykorzystuje mechanizm o nazwie Op-

portunistic Wireless Encryption (OWE), który generuje unikalne klucze szyfrowania dla każdego urządzenia klienckiego, zapobiegając ponownemu użyciu klucza i zmniejszając ryzyko nieautoryzowanego dostępu.

DOCELOWY CZAS BUDZENIA (TWT)

Funkcja TWT, która umożliwia urządzeniom zaplanowanie określonych godzin dostępu do sieci i oszczędzanie energii w stanie uśpienia w przypadku Wi-Fi 6 nie tylko poprawia wydajność energetyczną, ale także zwiększa bezpieczeństwo. TWT pozwala urządzeniom zaplanować dostęp do sieci, skracając czas, jaki spędzają na aktywnym przesyłaniu lub odbieraniu danych. Zmniejsza to narażenie na potencjalne luki w zabezpieczeniach, które mogą wynikać z długotrwałej aktywności w sieci.

OFDMA I MU-MIMO

Wi-Fi 6 zawiera funkcje OFDMA oraz MU-MIMO, o których również należy wspomnieć w kontekście cyberbezpieczeństwa. To technologie, które umożliwiają urządzeniom jednoczesną komunikację na różnych podkanałach, poprawiając ogólną odporność sieci na ataki.

WZGLĘDY BEZPIECZEŃSTWA IOT

Możliwości szóstej generacji Wi-Fi uwzględniają specyficzne potrzeby dotyczące bezpieczeństwa urządzeń Internetu rzeczy (IoT). Dzięki funkcji TWT umożliwia urządzeniom IoT oszczędzanie energii przy jednoczesnym zachowaniu łączności. Ponadto Wi-Fi 6 wprowadza mechanizmy chroniące przed niektórymi typami ataków na urządzenia IoT, takimi jak protokół Neighbor Awareness Networking (NAN) do bezpiecznej komunikacji między urządzeniami.

WDROŻENIE WI-FI 6

Wdrażając Wi-Fi 6, firmy mogą korzystać z najnowszych rozwiązań w technologii sieci bezprzewodowych, zapewniając bezpieczniejsze środowisko dla swoich danych, urządzeń oraz użytkowników. Warto jednak pamiętać, że wprowadzenie WPA3 wymaga obsługujących go urządzeń końcowych, co może stanowić wyzwanie, szczególnie w modelu BYOD.

Ponadto używanie nowej generacji Wi-Fi to wzmocnienie tylko jednego elementu krajobrazu składającego się na cyberbezpieczeństwo. Aktywna i skuteczna obrona przed hakerami to kompleksowe działanie, które odbywa się na wielu polach i kierunkach jednocześnie.


/GDPSYSTEM.EU
ZGODA NA COOKIES
Czy Twoja strona WWW spełnia wymogi prawne i daje możliwość elastycznego zarządzania cookies osobom, które ją odwiedzają?
SPRAWDŹ
SPEŁNIJ WYMOGI PRAWNE

DUE DILIGENCE W CYBERBEZPIECZEŃSTWIE. DLACZEGO JEST WAŻNY?

Redakcja
SECURITY MAGAZINE

Firmy, niezależnie od swojej wielkości, są narażone na ataki hakerów i inne cyberzagrożenia. Właśnie dlatego due diligence, czyli staranne badanie i analiza w zakresie cyberbezpieczeństwa, odgrywa kluczową rolę w ochronie firm. Jednak jak dokładnie ono działa i jak możesz to wdrożyć?

CZYM JEST DUE DILIGENCE?

Due diligence to należyta staranność w cyberbezpieczeństwie. Jest to proces, w którym Twoja firma dokładnie analizuje swoje systemy, infrastrukturę, polityki bezpieczeństwa i procedury, aby zidentyfikować i zminimalizować ryzyko wystąpienia cyberzagrożeń. Firmy nierzadko przeprowadzają ją np. przed podejmowaniem ważnych decyzji jak chociażby inwestycji, przejmowania konkurencyjnych podmiotów, zawierania nowych umów itd. itp. Jednak zasady due diligence warto stale podtrzymywać.

Celem due diligence jest identyfikacja, ocena oraz zrozumienie ryzyka związanego z cyberbezpieczeństwem w zakresie systemów informatycznych, sieci, infrastruktury i procedury związane z bezpieczeństwem Twojej organizacji.

W ramach tego procesu powinieneś przeprowadzić audyty bezpieczeństwa, przeglądy polityk bezpieczeństwa, analizę zarządzania dostępu, monitorowania zdarzeń, ochronę przed zagrożeniami, sprawdzić zabezpieczenia techniczne oraz inne aspekty bezpieczeństwa informatycznego.

Wyniki due diligence w cyberbezpieczeństwie mogą Ci dostarczyć wiedzy na temat potencjalnych luk i słabości w systemach i procedurach Twojej firmy. To pozwala na identyfikację obszarów wymagających wzmocnienia, takich jak aktualizacja zabezpieczeń, wprowadzenie nowych procedur, szkolenie personelu czy zwiększenie budżetu na cyberbezpieczeństwo.

Taki proces jest kluczowy – zarówno ze względu na Twój biznes, jak i biznesy Twoich klientów. Zwłaszcza jeśli np. gromadzisz czy przetwarzasz poufne dane kontrahentów lub konsumentów. To też ważne z punktu widzenia pracowników. Pamiętaj, że cyberzagrożenia z roku na rok są coraz poważniejszym problemem.

KIEDY WARTO PRZEPROWADZIĆ ANALIZĘ DUE DILIGENCE?

Analiza due diligence może być przeprowadzana w różnych sytuacjach. Choć o cyberbezpieczeństwo firmy powinieneś dbać stale, to są momenty, w których warto przeprowadzić analizę due diligence w szczególności, np. przed inwestycją lub fuzją, by ocenić stan infrastruktury technologicznej, polityk bezpieczeństwa oraz ryzyka związanego z cyberbezpieczeństwem.

Dzięki temu oceniasz potencjalne zagrożenia i problemy, które mogą wpływać na wartość transakcji. Podobnie jest w przypadku, kiedy planujesz przejąć inną firmę. Due diligence pozwoli wtedy ocenić stan bezpieczeństwa firmy, ryzyka związanego z cyberatakami i potencjalnych wycieków danych, a także polityki bezpieczeństwa i procedury.

Przed podpisaniem umowy z dostawcą technologicznym lub usługowym, też powinieneś przeprowadzić analizę due diligence w zakresie cyberbezpieczeństwa. W ten sposób możesz ocenić, czy dostawca spełnia odpowiednie standardy bezpieczeństwa i jest w stanie chronić dane i systemy Twojej firmy.

Również, jeśli zamierzasz zainwestować w nowe technologie lub rozwiązania informatyczne, ważne jest przeprowadzenie due diligence w zakresie cyberbezpieczeństwa tych rozwiązań. Pozwoli to ocenić ich potencjalne zagrożenia, luki w zabezpieczeniach i ryzyko dla Twojej organizacji.

To jednak nie koniec. Jeśli planujesz wprowadzić znaczące zmiany w infrastrukturze IT swojej firmy, takie jak migracja do chmury, to też nie obejdzie się (a przynajmniej nie powinno) bez dokonania takiej analizy.

W każdym przypadku due diligence powinna być przeprowadzona przed podjęciem decyzji, aby zidentyfikować potencjalne ryzyka i podjąć odpowiednie działania w celu minimalizacji zagrożeń.

JAK PRZYGOTOWAĆ SIĘ DO DUE DILIGENCE?

Aby dokonać analizy w swojej firmie, musisz podjąć odpowiednie kroki (tyczy się

to też weryfikacji Twoich dostawców czy podmiotu, który planujesz przejąć lub zainwestować w niego pieniądze), w tym:

- **zidentyfikowanie potencjalnych zagrożeń**, jak phishing, ransomware czy malware. Dokładnie przeanalizuj swoje systemy, infrastrukturę i procesy biznesowe, aby zrozumieć, gdzie może wystąpić ryzyko;
- **sprawdzenie, z jakich zabezpieczeń korzystasz.** Mowa tutaj o wszelkich firewallach, antywirusach, VPN-ach, szyfrowaniu danych itd. itp.;
- **przeprowadzenie testów penetracyjnych**, które polegają na symulowaniu ataków hakerów na swoje systemy, aby zidentyfikować ewentualne słabe punkty. Dzięki nim ocenisz, które aspekty Twojej organizacji są słabymi ogniwami;
- **skontrolowanie swojej polityki bezpieczeństwa i procedur**. Upewnij się, że są one aktualne, zgodne z najlepszymi praktykami branżowymi oraz dostosowane do specyfiki Twojej firmy. Weryfikuj, czy są one skutecznie egzekwowane i czy pracownicy są świadomi swoich obowiązków w zakresie cyberbezpieczeństwa;
- **organizowanie regularnych szkoleń** z zakresu cyberbezpieczeństwa dla swojego personelu. Zapewnij im wiedzę na temat identyfikowania zagrożeń, jak wykrywać ataki phishingowe czy jak przetwarzać dane (w tym te dostępowe, tj. np. nie podawać ich na komunikatorach, a korzystać z menedżerów haseł czy programów, które kasują wiadomości po ich wyświetleniu). Świadomi pracownicy są ważnym elementem ochrony przed incydentami cybernetycznymi;
- **wdrożenie systemów monitorowania zdarzeń,** co pozwoli Ci na ciągłą analizę i wykrywanie nieprawidłowości w systemach. Dzięki temu można szybko zareagować na potencjalne ataki i minimalizować skutki incydentów;
- **regularne aktualizowanie oprogramowania oraz zabezpieczenia swoich systemów.** Wiele cyberataków wykorzystuje znane luki w oprogramowaniu, dlatego ważne jest, aby być na bieżąco z aktualizacjami;
- **przeanalizowanie, czy organizacja przestrzega odpowiednich przepisów prawnych** oraz regulacji dotyczących bezpieczeństwa danych, takich jak chociażby RODO;
- **utworzenie inwentaryzacji zasobów obejmujących systemy fizyczne** (smartfony itp.), czy oprogramowania;

- **posiadanie planu reagowania na cyberincydenty,** planu ciągłości biznesowej i odzyskiwania (np. danych) po awarii czy cyberataku;
- **sprawdzanie zewnętrznych dostawców,** np. oprogramowania typu SaaS. Analizuj łańcuchy dostaw, dowiedz się, kto kontroluje i ma dostęp do danych w Twojej firmie itd.

WYZWANIA W DUE DILIGENCE

Choć praktyki due diligence są niezwykle ważne, to, oczywiście, i tu mogą pojawić się pewne wyzwania czy problemy. Dla części przedsiębiorców będzie to już czas trwania tak rozbudowanej analizy. Nie ma co ukrywać, że due diligence nie przeprowadza się w dzień czy dwa.

To proces, który może trwać tygodniami lub miesiącami. Dodatkowo, często wymaga pomocy dobrze przeszkolonego zespołu. Twoja firma, dostawca lub podmiot, który chcesz przejąć – niekoniecznie muszą je mieć. I tu w grę często wchodzą zewnętrzne organizacje, które oferują analizę due diligence albo przynajmniej część z usług wymaganych do jej przeprowadzenia (np. pentesty).

Wyzwania pojawiają się także w momencie np. braku wsparcia ze strony organizacji docelowej. Tj. jeśli podmiot, który chcesz przejąć (albo Twój dostawca) niekoniecznie tak ochoczo podchodzą do weryfikacji swoich zabezpieczeń czy przetwarzania danych. Choć powinien to być dla Ciebie wy-

raźny sygnał.

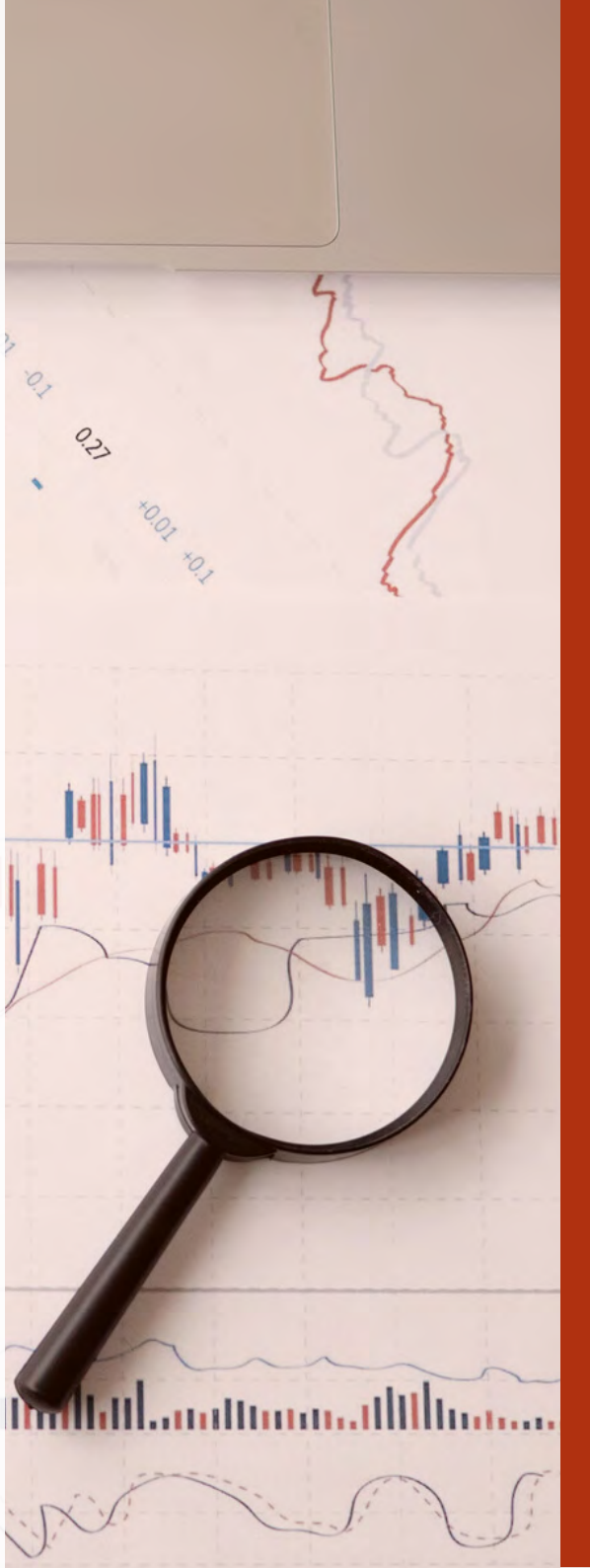
W takich sytuacjach może się też okazać, że dany podmiot nie zawsze prowadził szczegółową dokumentację np. naruszeń czy incydentów cyberbezpieczeństwa. Tym bardziej jeśli np. dotychczas pracownicy tej konkretnej organizacji nie byli jakoś szczególnie wyedukowani w aspektach cyberbezpieczeństwa.

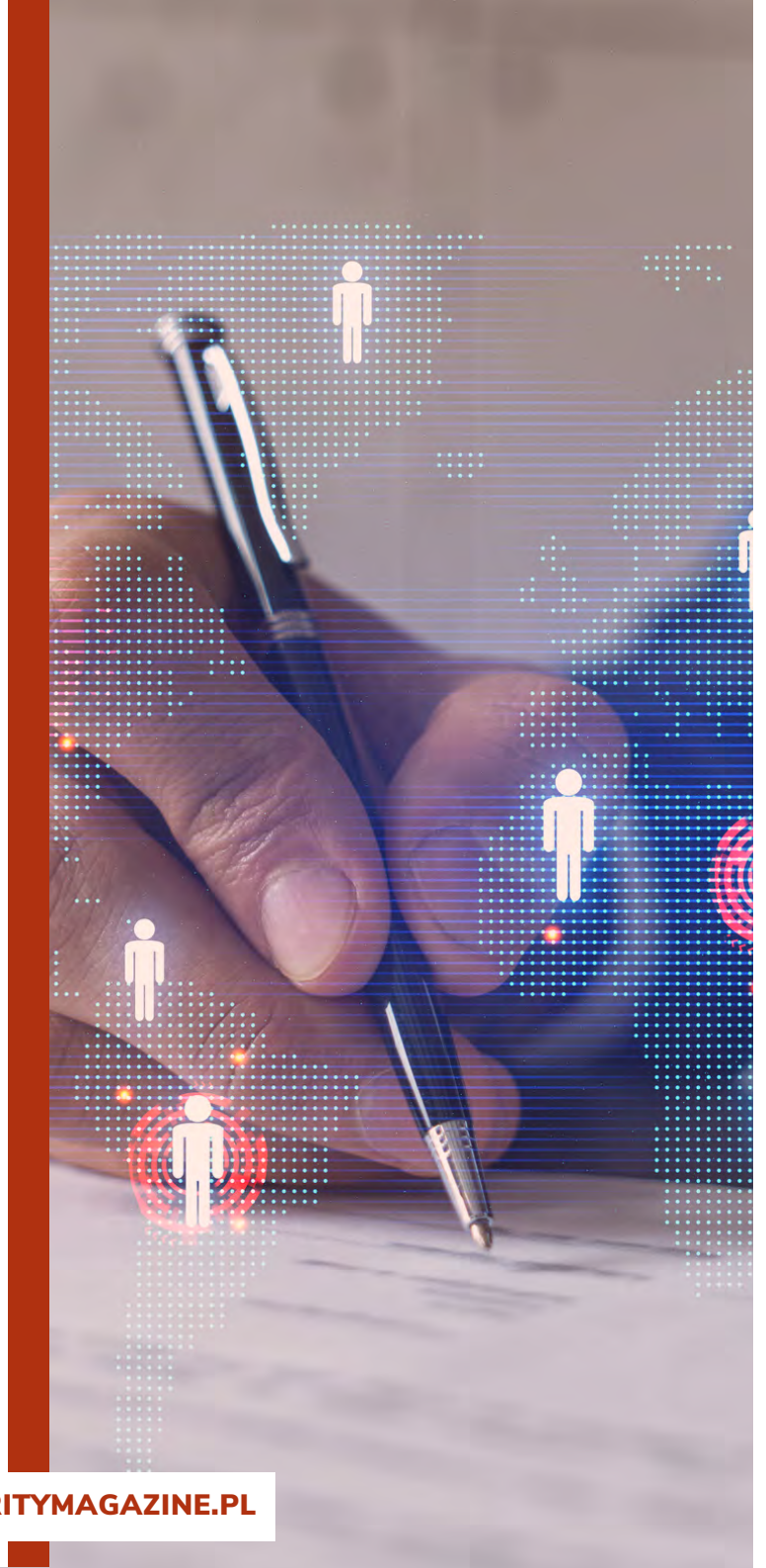
W tym wszystkim nie pomaga też brak regulacji czy konkretnych wytycznych co do due diligence. Owszem, z tego artykułu dowiadujesz się, jakie kroki powinieneś podjąć (albo jakie powinny być kroki docelowej organizacji), ale nie oznacza to, że koniecznie tak będzie. Analizy due diligence to sprawy bardzo indywidualne i nie każdy podmiot stosuje wszystkie wspomniane praktyki. A to przekłada się właśnie na jego cyberbezpieczeństwo.

CO PO ANALIZIE DUE DILIGENCE?

W zależności od tego, jakie wnioski można wyciągnąć z przeprowadzonej analizy due diligence – czekają Cię kolejne kroki. Pierwszą podstawową rzeczą, jaką należy wówczas zrobić – jest opracowanie strategii i kosztorysu przyszłych inwestycji. Może się w końcu okazać, że Twoja organizacja (lub podmiot, z którym dokonujesz fuzji czy przejęcia) mają poważne luki w zabezpieczeniach. Co to oznacza? Koszty, koszty i jeszcze raz koszty.

Mogą Cię czekać zaawansowane szkolenia pracowników, zmiany dotychczasowych systemów czy oprogramowań, powołanie do życia specjalnych zespołów (np. działu IT) itd. Finalnie może się okazać (chociażby w przypadku fuzji czy przejęcia), że gra nie jest warta świeczki, bo koszty takiej inwestycji mogą być





spore i znacząco wpłynie to na transakcję.

Musisz jednak pamiętać, że każde badanie due diligence jest inne, a jego intensywność i wyniki zależą od wielu czynników. Dlatego trudno tutaj o jakieś konkretne, jednoznaczne wytyczne. Jednak bez niej narażasz się na znaczące ryzyko w każdym procesie biznesowym, jaki przeprowadzasz. Od podpisania umowy z nowym kontrahentem, przez współpracę z dostawcą aż po fuzję, integrację, przejęcie czy inwestycję w nowy podmiot.

ZAMÓW AUDYT BEZPIECZEŃSTWA

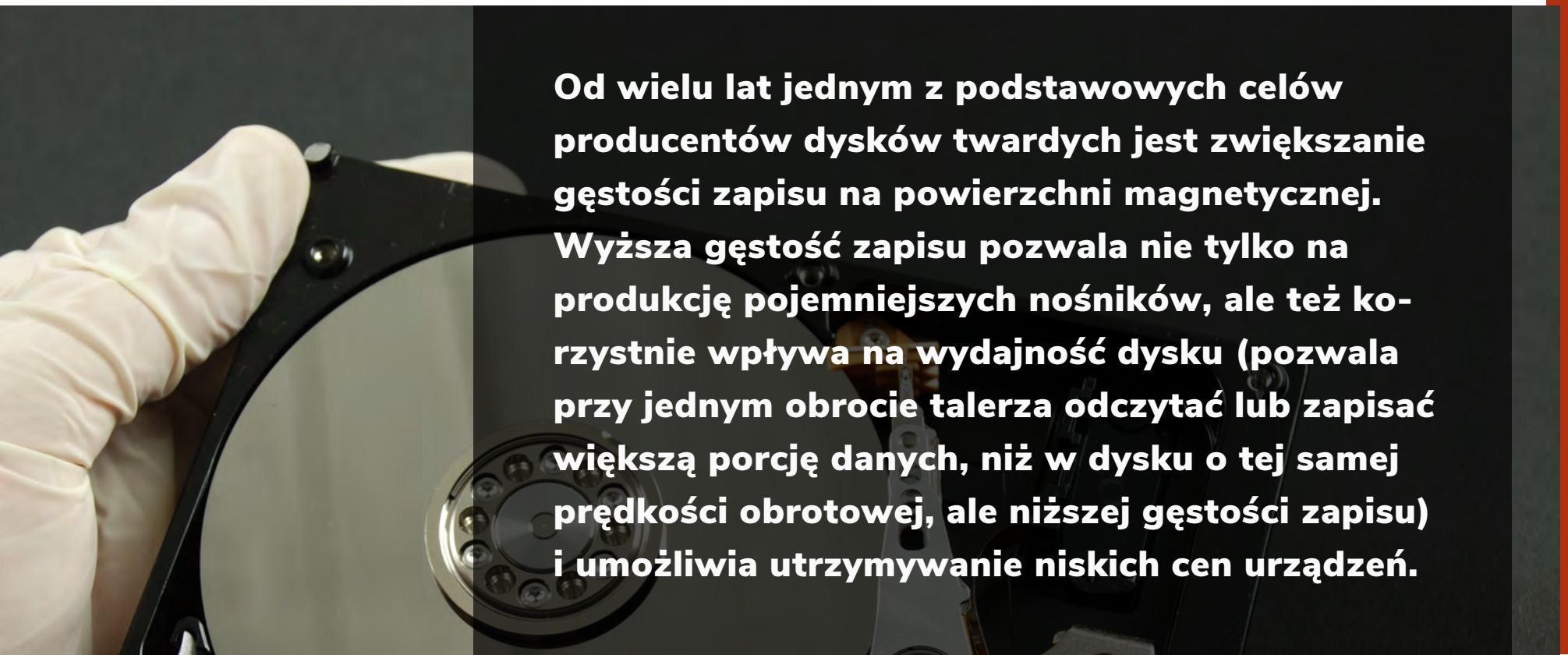
I PRZEKONAJ SIĘ, JAK OPTYMALIZACJA PRZETWARZANIA DANYCH MOŻE DAĆ CI PRZEWAGĘ KONKURENCYJNĄ

DOWIEDZ SIĘ WIĘCEJ!

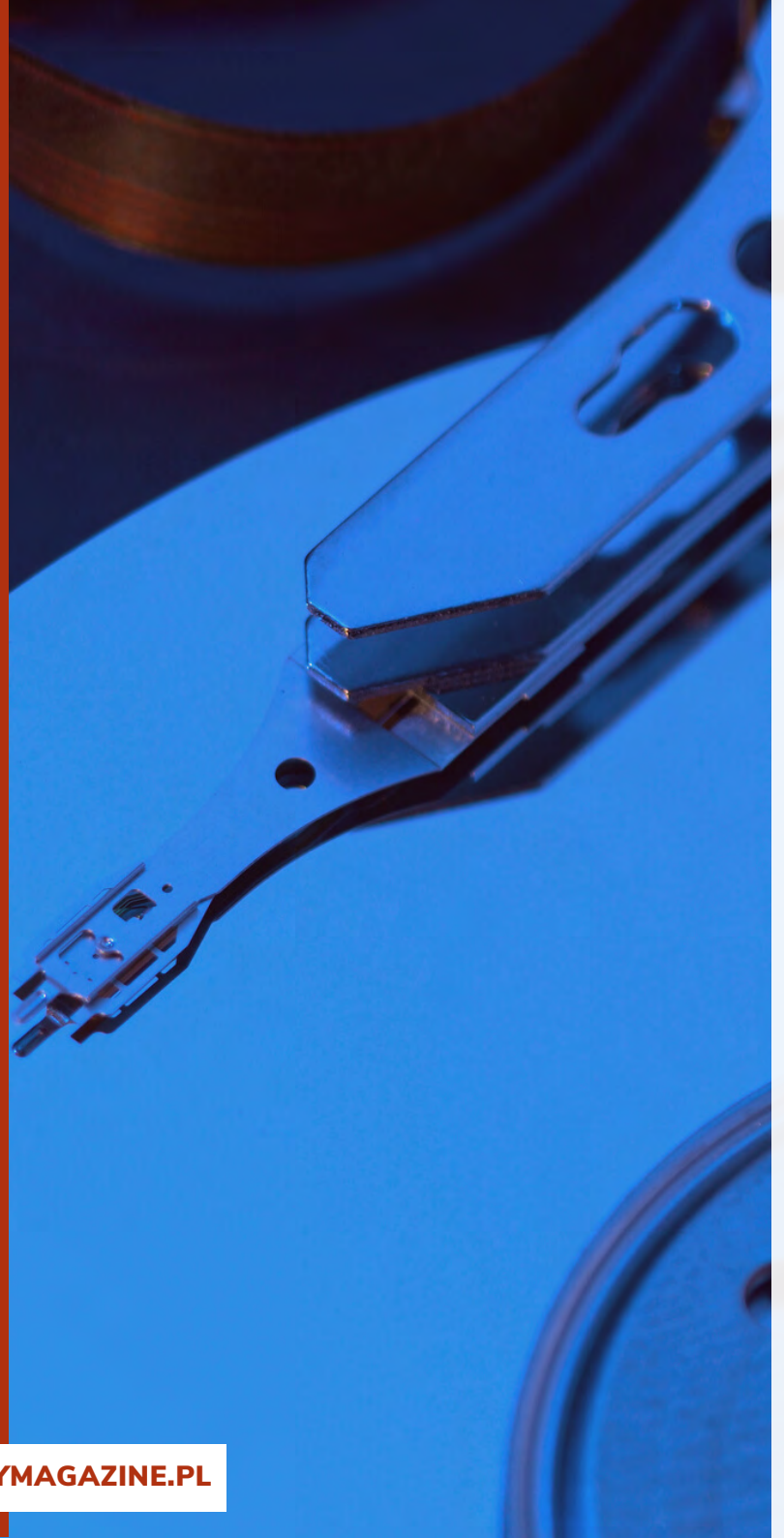
Polityka® Bezpieczeństwa

PRZEWAGI I PROBLEMY ZAPISU SMR

Paweł Kaczmarzyk
Serwis komputerowy Kaleron



Od wielu lat jednym z podstawowych celów producentów dysków twardych jest zwiększanie gęstości zapisu na powierzchni magnetycznej. Wyższa gęstość zapisu pozwala nie tylko na produkcję pojemniejszych nośników, ale też korzystnie wpływa na wydajność dysku (pozwala przy jednym obrocie talerza odczytać lub zapisać większą porcję danych, niż w dysku o tej samej prędkości obrotowej, ale niższej gęstości zapisu) i umożliwia utrzymywanie niskich cen urządzeń.



Jednym ze sposobów zwiększania gęstości zapisu jest tzw. zapis dachówkowy (lub gontowy – Shingled Magnetic Recording) wprowadzony na rynek w 2013 r. Obecnie zdecydowana większość dostępnych na rynku dysków wykorzystuje tę technologię, jednak często użytkownicy nawet nie zdają sobie z tego sprawy. Nie bez powodu – istnieją przyczyny, dla których producenci nie śpieszą się, by chwalić się rozwiązaniami wykorzystywanymi w ich produktach.

POSTĘPY W ZWIĘKSZANIU GĘSTOŚCI ZAPISU W DYSKACH TWARDYCH

Z biegiem lat producenci wprowadzili wiele innowacji pozwalających na zwiększenie gęstości zapisu. Do najważniejszych z nich należy zastąpienie odpowiedzialnych za pozycjonowanie głowic silników krokowych silnikami liniowymi umożliwiającymi bezstopniową regulację położenia głowic. Dzięki temu udało się setki razy zwiększyć liczbę ścieżek na powierzchni talerza.

Ewoluowały też stopy używane, jako warstwa magnetyczna przechowująca dane. Poprawa struktury krystalicznej warstwy magnetycznej oraz użycie stopów o wyższej koercji umożliwiło stopniowe zmniejszanie domen magnetycznych. Istotnym przełomem było zastąpienie zapisu równoległego bardziej odpornym na efekt superparamagnetyzmu zapisem prostopadłym.

Nie bez znaczenia była także ewolucja systemów kodowania danych pozwalających na zwiększenie gęstości upakowania strumienia danych w domenach magnetycznych.

Zastąpienie systemów kodowania FM/MFM samotaktującym kodowaniem RLL wyeliminowało konieczność uwzględniania w sygnale składowej zegarowej. Pozwoliło także upakować w domenach więcej bitów danych.

Rosnąca gęstość zapisu wpłynęła także na optymalizację innych aspektów funkcjonowania dysków. Mniejsze odstępy pomiędzy impulsami sygnału i niższe ich amplitudy wymusiły zastąpienie detekcji szczytów metodą detekcji PRML (Partial Response – Maximum Likelihood częściowa odpowiedź – maksymalne prawdopodobieństwo). Wprowadza się także bardziej zaawansowane metody detekcji i korekcji błędów bitowych. Powierzchnię talerzy dla lepszego wykorzystania podzielono na strefy o różnej liczbie sektorów na ścieżkę.

PODSTAWY KONCEPCJI TECHNOLOGII SMR

Nazwa zapisu dachówkowego pochodzi od sposobu wyznaczania ścieżek tak, aby kolejna ścieżka częściowo nadpisywała poprzednią. Już dawno zauważono, że głowice zapisujące indukują pole magnetyczne znacznie szerzej, niż jest to niezbędne dla odczytu przez głowicę odczytującą.

Jednak zwężanie ścieżek tradycyjnymi metodami ma swoje granice.
Jednak zwężanie ścieżek tradycyjnymi metodami ma swoje granice.

Żeby skutecznie namagnesować powierzchnię podczas zapisu, musimy operować dostatecznie silnym polem magnetycznym, które maleje proporcjonalnie do kwadratu odległości i rozchodzi się na szerokość po obu stronach ścieżek. Ścieżki można zwężać obniżając wysokość lotu głowicy nad powierzchnią talerza, co daje możliwość precyzyjnej magnesować pożądane obszary oraz indukować dostatecznie silne pole przez coraz mniejsze głowice.

Aby możliwe było zastosowanie technologii zapisu dachówkowego, konieczna była zmiana sposobu konstrukcji głowic zapisujących. Pola indukowane w zapisie dachówkowym nie mogą się rozchodzić równomiernie, gdyż zapis kolejnej ścieżki uszkadzałby poprzednią. Dlatego głowice zapisujące konstruuje się, jakby były „połówką” tradycyjnych głowic z wstawionym ekranem, do którego zamykają się li-

nie pola, chroniąc przed przemagnesowaniem tę część poprzedniej ścieżki, która powinna pozostać nienaruszona.

Dzięki temu namagnesowanie kolejnej ścieżki jest asymetryczne względem jej środka i obszar dający największą odpowiedź sygnału może się znaleźć znacznie bliżej sąsiedniej ścieżki (tego, co z niej zostanie po częściowym nadpisaniu), jednocześnie pozostawiając następnej ścieżce obszar, który może być przemagnesowany bez utraty danych. Równocześnie ekranowanie pozwala operować silniejszym polem bez ryzyka uszkodzenia sąsiednich ścieżek. Rozwiązanie to umożliwia zmniejszenie szerokość ścieżki z kilkudziesięciu do ok. 10 nm, co odpowiada szerokości wystarczającej dla odczytu przez głowicę odczytującą.

NAJWAŻNIEJSZE PROBLEMY ZWIĄZANE Z ZAPISEM DACHÓWKOWYM

Jednym z problemów związanych z rosnącą gęstością zapisu są efekty skosu związane z przemieszczaniem głowic po łuku względem powierzchni talerza w poszukiwaniu właściwych ścieżek. W pewnym momencie odchylenia położenia głowic od równoległego względem ścieżek nie można było już ignorować. Stąd konieczna była modyfikacja konstrukcji aktuatorów i wyposażenie ich w elementy piezoelektryczne ustawiające ślizgacze równolegle do przebiegu ścieżki w dowolnym miejscu talerza. Wprawdzie takie dwustopniowe aktuatory nie są ściśle związane z zapisem dachówkowym, jednak przy tej gęstości zapisu są obowiązkowe.

Inna kategoria problemów dotyczy zakłóceń odczytywanego sygnału. Ze względu na znaczne zmniejszenie odstępu pomiędzy ścieżkami rośnie wpływ interferencji międzyścieżkowych, co utrudnia odfiltrowanie sygnału od szumu. Rośnie też znaczenie fluktuacji wysokości lotu głowic nad powierzchnią talerza, co wymusza stosowanie rozwiązań pozwalających na obserwowanie oraz stabilizację wysokości ich lotu.

Jednak najważniejszą przyczyną problemów związanych z zapisem dachówkowym jest utrata swobodnego dostępu do sektora podczas zapisu. O ile możemy swobodnie odczytywać dowolne sektory, to przy zapisie różnica szerokości ścieżek odczytywanej i zapisywanej powoduje, że nie możemy zapisać wybranego sektora bez zmiany namagnesowania sąsiedniej ścieżki.

W praktyce oznacza to konieczność przepisywania wielu ścieżek nawet wtedy, gdy potrzebujemy zmienić zawartość pojedynczego sektora. Oczywiście bardzo negatywnie odbija się to na wydajności dysku podczas zapisu.

SPOSOBY ROZWIĄZYWANIA PROBLEMÓW I OPTYMALIZACJI PRACY DYSKÓW SMR

Gdyby zapisać całą powierzchnię talerza, wykorzystując

technologię SMR, jakakolwiek zmiana któregokolwiek sektora wymagałaby przepisania wszystkich ścieżek począwszy od tej, na której ten sektor się znajduje aż do końca powierzchni talerza.

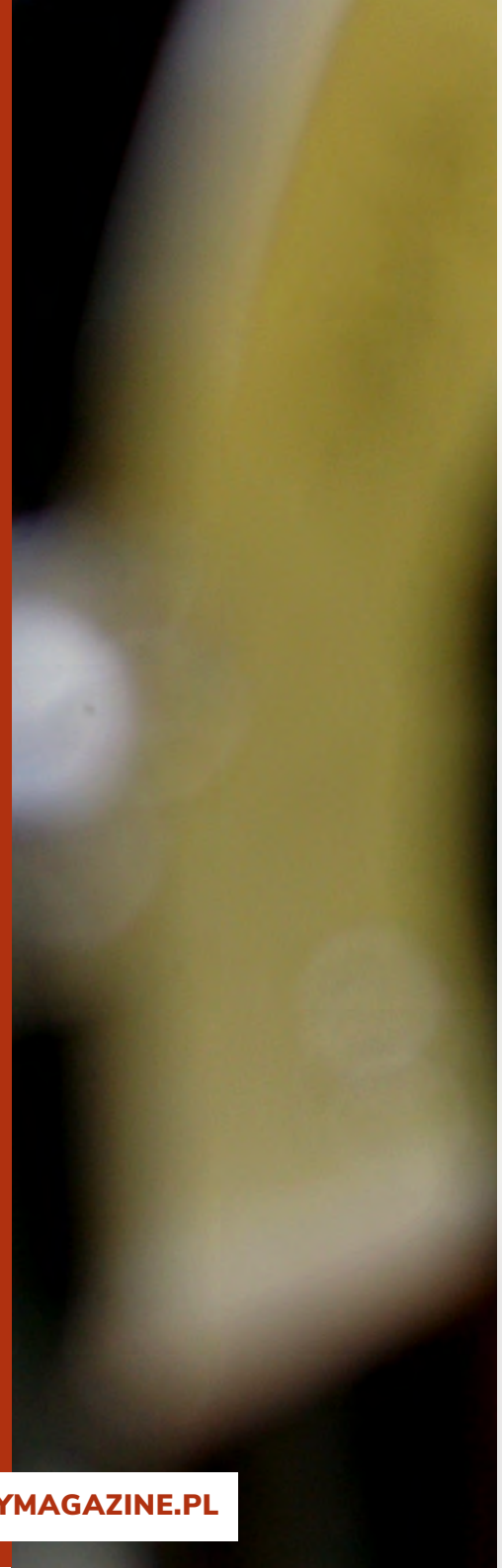
W praktyce taka sytuacja jest niedopuszczalna, dlatego ścieżki dzieli się na grupy (strefy) oddzielone niewielkimi odstępami (ostatnia ścieżka strefy nie jest częściowo nadpisywana przez kolejną). Pozwala to na ograniczenie liczby zapisów, jednak i tak zmiana zawartości sektora leżącego w takiej strefie wymaga przepisania całej strefy.

Przepisywanie całych stref za każdym razem przy zmianie zawartości pojedynczych sektorów byłoby bardzo uciążliwe dla użytkowników, natomiast wykorzystanie ulotnego buforowania DRAM do przechowywania większych ilości danych obciążone jest ryzykiem ich utraty w przypadku zaniku zasilania. Dlatego opracowano szereg rozwiązań pozwalających na względnie normalne korzystanie z dysków SMR.

Rozwiązania te sprowadzają się do różnych zabiegów pozwalających na umieszczanie logicznych sektorów w różnych fizycznych miejscach dysku, co skutkuje zerwaniem tradycyjnego dla wcześniejszych generacji dysków twardych względnie trwałego przywiązania adresów logicznych do adresów fizycznych. Metody zarządzania adresacją danych można podzielić na trzy zasadnicze kategorie:

- **Host Managed (HM-SMR)** – zarządzane przez komputer, w którym dysk się znajduje,
- **Disk Managed (DM-SMR)** – gdzie ciężar zarządzania adresacją danych w całości spoczywa na oprogramowaniu układowym dysku i odbywa się w sposób niezauważalny dla użytkownika,
- **Host Awared (HA-SMR)** – łączący powyższe podejścia, w których za część informacji o adresowaniu danych odpowiada oprogramowanie układowe dysku, a część jest przechowywana przez komputer zarządzający w tzw. buforze H.

Rozwiązania DM-SMR z racji obciążenia zarządzaniem adresacją oprogramowania układowego dysku są najłatwiejsze w implementacji. Nie wymagają obsługi dodatkowych funkcji od BIOS-u oraz systemu operacyjnego komputera. Poza tym pozwalają one na podłączanie dysku do różnych komputerów nie powodując ryzyka utraty danych, gdyż wszystkie niezbędne dla ich adresowania informacje są zapisane w strefie serwisowej dysku.

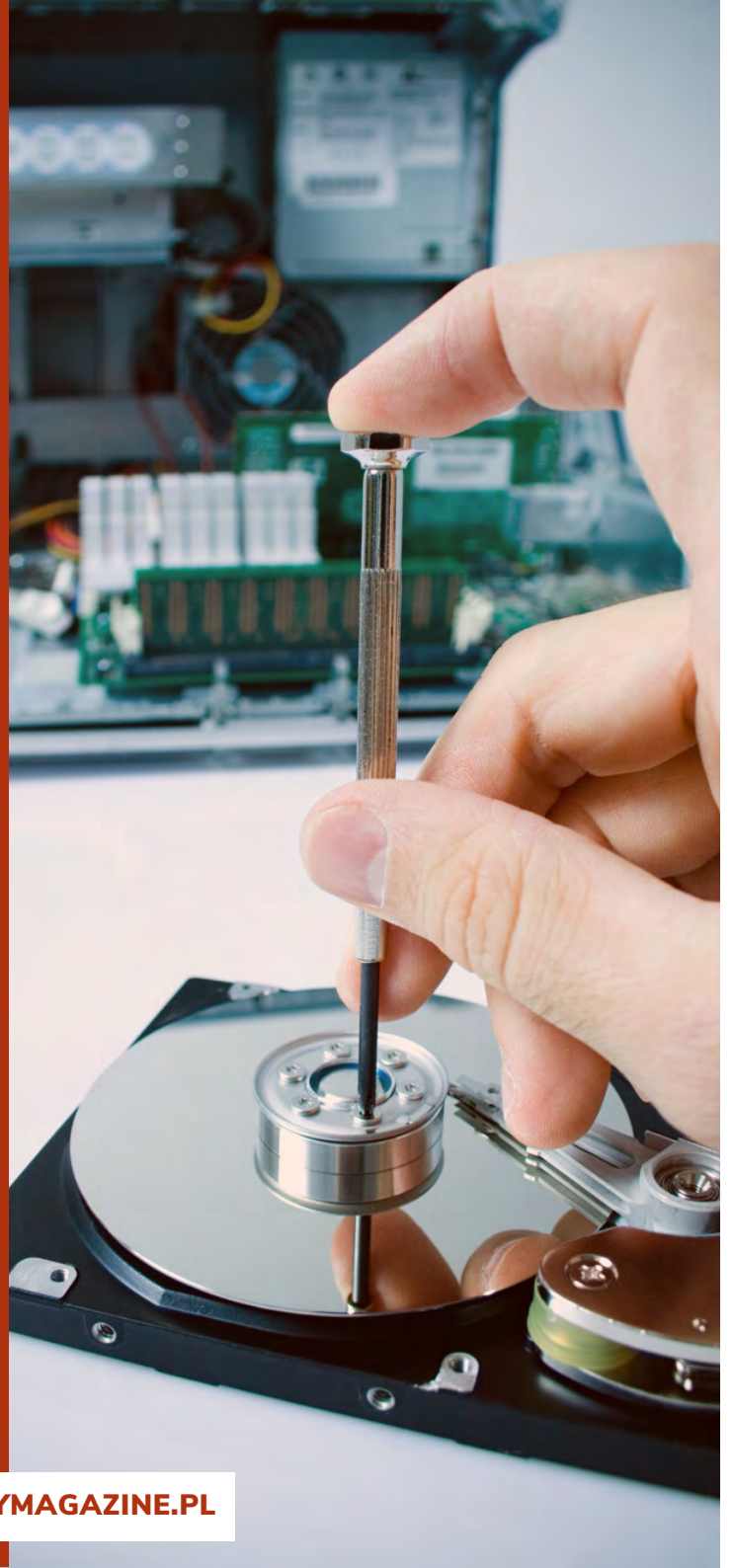


Nie dziwi więc, że w praktyce to z nimi najczęściej będziemy się spotykać i to właśnie na nich skupimy się w dalszej części artykułu. Rozwiązania HM-SMR i HA-SMR można spotkać jedynie w dużych centrach danych.

Rozwiązania DM-SMR opierają się na dwustopniowej translacji adresów logicznych na fizyczne. Pierwszy stopień, podobnie, jak i w przypadku dysków z zapisem konwencjonalnym (bez SMR), odpowiada za omijanie defektów i realokację uszkodzonych sektorów. Drugi pozwala na ustalanie, w której fizycznej lokalizacji znajduje się aktualna wersja danej jednostki LBA.

Jest to związane z faktem buforowania danych napływających do dysku w strefie zapisu konwencjonalnego, co jest rejestrowane w odpowiednich tablicach oprogramowania układowego dysku. Dane te są przenoszone do właściwych stref zapisu SMR, gdy dysk nie jest obciążony innymi operacjami. Ale dopóki sektor nie trafi w swoje docelowe miejsce, podsystem translacji musi wiedzieć, gdzie go szukać na wypadek, gdyby użytkownik chciał go odszukać. Większość dysków SMR wspiera także obsługę funkcji TRIM, która pozwala zwracać wartości 0x00 w odpowiedzi na żądanie odczytania sektorów niezaalokowanych w strukturach logicznych systemu plików (wolne miejsce partycji – zob. „Rola metadanych w przechowywaniu plików”, Security Magazine 5(14) 2023 bez konieczności ich fizycznego odnajdywania i odczytywania.

Tym niemniej tak skomplikowany podsystem translacji adresów logicznych na fizyczne istotnie wpływa na awaryjność dysków SMR.



Jest to dodatkowa rzecz, która może się zepsuć, a z racji dużej liczby zapisów w odpowiednich tablicach oprogramowania układowego, ryzyko wystąpienia w nich błędów jest całkiem spore.

Jeśli diagnostyka dysku (zob. „Podstawy diagnostyki dysków twardych" Security Magazine 2(11) 2023) wskazuje na uszkodzenie oprogramowania układowego, w przypadku dysków SMR z bardzo dużym prawdopodobieństwem ucierpiała translacja adresów logicznych na fizyczne.

Z uwagi na fakt, że podsystem translacji nie tylko jest bardzo złożoną częścią oprogramowania układowego, ale też jest unikalny dla każdego egzemplarza dysku, trzeba zachować dużą ostrożność przy próbach jego naprawy. Bezwzględnie należy zabezpieczyć stan wyjściowy zgrywając zawartość strefy serwisowej dysku. Większość modeli wymaga przy tym dodatkowych, specyficznych dla producenta i rodziny modeli, ingerencji w oprogramowanie układowe. Trzeba też zwracać uwagę na to, że wiele opisywanych w różnych źródłach sposobów naprawy dysku jest destrukcyjnych dla zawartości i może utrudnić lub wręcz w praktyce uniemożliwić jej odzyskanie.

30,5 TYSIĘCY

TYLE POBRAŃ MAJOWEGO WYDANIA

"SECURITY MAGAZINE"

CHCESZ Z WIEDZĄ, USŁUGAMI LUB PRODUKTAMI Z BRANŻY SECURITY
DOCIERAĆ DO TAKIEGO GRONA POTENCJALNYCH KLIENTÓW?

NAPISZ DO NAS

REDAKCJA@SECURITYMAGAZINE.PL

SECURITYMAGAZINE.PL

KAMERY AI, ANALIZA CYBER-BEZPIECZEŃSTWA I BEZPIECZNE POŁĄCZENIE

Redakcja
SECURITY MAGAZINE

W Polsce i na świecie nie brakuje startupów, które dostarczają rozwiązań z zakresu cyber, jak i tradycyjnego bezpieczeństwa. Dzięki nim Twoja firma, pracownicy czy klienci nie muszą obawiać się ataków cyberprzestępców, czy fizycznych zagrożeń. Sprawdź, jakie startupy pomogą Ci w tym zakresie.

KAMERY AI – TRASEE

Trasee to wrocławska spółka, która dostarcza rozwiązania wizyjne oparte o sztuczną inteligencję. Mówiąc prościej – dzięki temu startupowi możesz zamontować kamery, które rozpoznają np. ruch, ale też i wiele więcej.

Dzięki rozwiązaniu od Trasee możesz np. zarządzać miejscami parkingowymi, tzn. sprawdzać, kiedy ktoś parkuje w niedozwolonym miejscu, odczytywać tablice rejestracyjne pojazdów, anonimizować przechodniów, wykrywać niepożądane zachowania (chociażby bójki) czy niedozwolone przedmioty – np. broń palną, ale też chociażby zwierzęta czy wypadki. Możliwości jest jednak znacznie więcej.

Wszystko to przekłada się na szybsze, sprawniejsze i lepsze wykrywanie potencjalnych zagrożeń, a także reagowanie na nie. itp. Z usług Trasee korzystają obecnie PKP Polskie LInie Kolejowa S.A., Gdańsk Lech Wałęsa Airport, Miasto Rzeszów, NFZ i wiele, wiele innych.

Startup dostarcza swoje rozwiązanie głównie dla branż z zakresu przemysłu 4.0, sprzedaży detalicznej, obrotu nieruchomościami, transportu i organizacji państwowych. Ponadto spółka chwali się, że ich usługa jest nawet do sześciu razy tańsza niż rozwiązania chmurowe.

POPRAWA CYBER-BEZPIECZEŃSTWA – 1STRIKE

Warszawski 1Strike, na którego czele stoi Lucyna Szaszkiewicz to startup zajmujący się standardowym cyberbezpieczeństwem. Spółka oferuje rozwiązanie, dzięki któremu możliwe jest analizowanie bezpieczeństwa firmy poprzez zautomatyzowane symulacje kluczowych cyberataków. Dzięki temu 1Strike wykryje luki i słabe punkty w cyberbezpieczeństwie Twojej firmy. To pomoże w poprawie tych najsłabszych ogniw.

To jednak nie koniec, bo 1Strike oferuje też informacje o najnowszych cyberzagrożeniach dzięki stale rosnącej bazie technik ataków. A dodatkowo startup raportuje na bieżąco stan ochrony firmy. SaaS stworzony przez 1Strike jest skierowany przede wszystkim do sektora MMŚP, czyli mikro, małych i średnich przedsiębiorstw, które nierzadko nie mogą sobie pozwolić na pełnoetatowy zespół ze względu na niewielki budżet.

Rozwiązanie korzysta, oczywiście, ze sztucznej in-

teligencji i symuluje potencjalne zagrożenia na podstawie profilu ryzyka firmy. Pozwala to na zmniejszenie ryzyka cyberataku, ale też na monitorowanie tzw. ekspozycji zewnętrznej.

Oprócz tego startup zajmuje się też testowaniem złośliwego oprogramowania punktów końcowych, bramek poczty e-mail itd., itp.

PEER-TO-PEER VPN – HUSARNET

Coraz więcej przedsiębiorstw wykorzystuje VPN-y do szyfrowania połączeń pomiędzy urządzeniem pracownika a firmową siecią. To pozwala chronić przed atakami nieuprawnionych osób. I jest przydatne, zwłaszcza kiedy sieci WiFi w firmie są ogólnodostępne. Problem w tym, że nie wszystkie VPN-y są skuteczne, a nierzadko też sprawiają, że połączenie internetowe jest wolniejsze.

W tym aspekcie pomóc ma startup Husarnet. Urządzenia z zainstalowanym Husarnet Client mogą bezpośrednio komunikować się między sobą, bez konieczności przekierowania ruchu przez centralny serwer. To oznacza, że połączenia odbywają się bezpośrednio pomiędzy urządzeniami za pośrednictwem internetu. Startup chwali się, że to minimalizuje opóźnienia.

Husarnet jest siecią zdefiniowaną programowo (SDN), co oznacza, że całe przesyłanie danych odbywa się za

pośrednictwem klientów Husarnet i serwerów bazowych Husarnet.

Konfiguracja i zarządzanie odbywają się poprzez Husarnet Dashboard i Husarnet Websetup.

Dzięki takiemu rozwiązaniu urządzenia mogą bezpośrednio wymieniać się danymi, a cała kontrola sieci jest łatwo konfigurowalna i dostępna poprzez wspomniane narzędzia. To pozwala na płynne działanie sieci oraz umożliwia prostą konfigurację i monitorowanie połączeń między urządzeniami

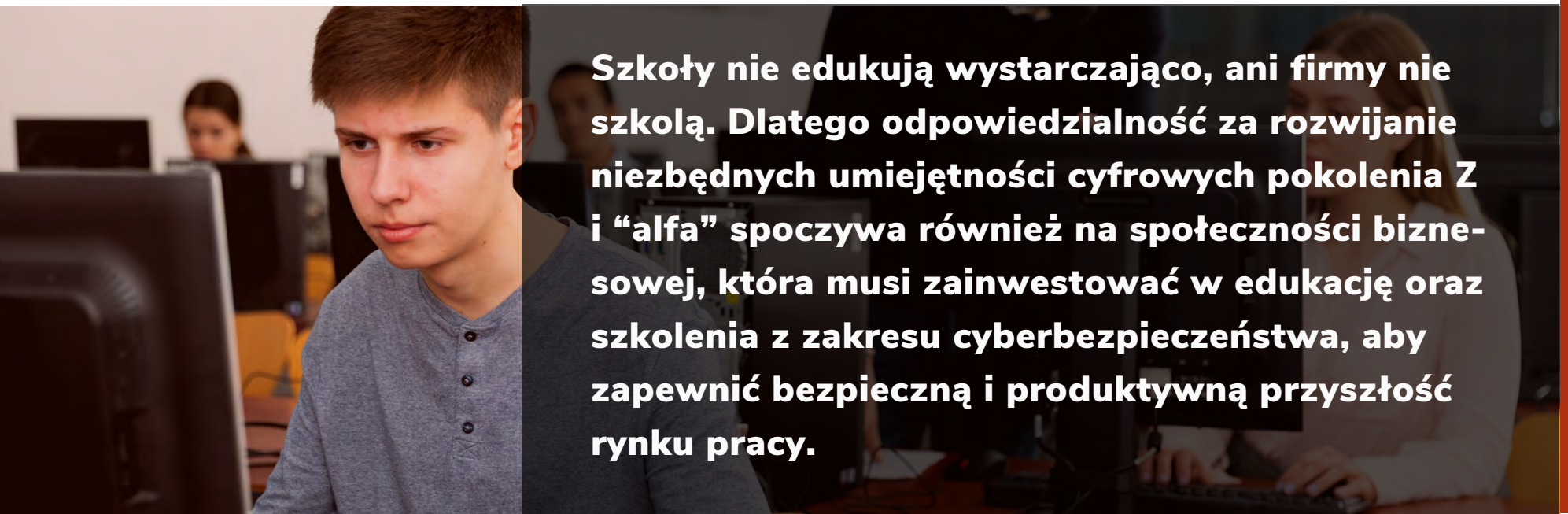
Dodatkowo Husarnet działa w tle i nie trzeba modyfikować istniejącego kodu. Z perspektywy ROS Husarnet to po prostu sieć LAN. Dzięki temu rozwiązanie startupu obsługuje ROS i może pomóc w jego konfiguracji i monitorowaniu. Startup dostarcza swoje rozwiązanie dla branż robotyki, IoT, motoryzacyjnej i wielu, wielu innych.

To, rzecz jasna, nie wszystkie startupy, które wspierają firmy w zakresie cyberbezpieczeństwa. Na rynku funkcjonuje wiele spółek opartych o różne technologie. Warto podkreślić, że startupy oferujące usługi z zakresu cyberbezpieczeństwa są kluczowym ogniwem w dziedzinie ochrony przed zagrożeniami w sieci. Ich innowacyjne podejście, wykorzystanie zaawansowanych technologii i wsparcie dla klientów przyczyniają się do podniesienia poziomu bezpieczeństwa danych i systemów w dzisiejszym cyfrowym świecie. A zarówno Ty, jak i Twoja firma, powinniście dbać o swoje, swoich pracowników i klientów – cyberbezpieczeństwo.


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

E-KOMPETENCJE DZIECI A PRZYSZŁOŚĆ TWOJEJ FIRMY. POWIĄZANIE, KTÓRE MUSISZ ZROZUMIEĆ

Redakcja
SECURITY MAGAZINE



Szkoły nie edukują wystarczająco, ani firmy nie szkolą. Dlatego odpowiedzialność za rozwijanie niezbędnych umiejętności cyfrowych pokolenia Z i "alfa" spoczywa również na społeczności biznesowej, która musi zainwestować w edukację oraz szkolenia z zakresu cyberbezpieczeństwa, aby zapewnić bezpieczną i produktywną przyszłość rynku pracy.

Cyfryzacja staje się codziennością, a technologia nieustannie przyspiesza tempo naszego życia – w tej rzeczywistości najmłodsze pokolenia są na pierwszej linii zmian. Przedstawiciele pokolenia Z już teraz stanowią ważną część siły roboczej, a ich wpływ na rynek pracy będzie tylko rósł. Za nimi idzie generacja alfa, która choć wciąż jest w okresie edukacji, już za dekadę dołączy do świata pracy.

Niezależnie od roli, jaką te pokolenia będą pełnić – czy to jako menedżerowie, dyrektorzy czy brygadziści – ich umiejętności i kompetencje w dziedzinie cyberbezpieczeństwa będą nieocenione. Jednak to samo tyczy się „szeregowych" pracowników. Jedną z najczęstszych przyczyn udanego cyberataku wcale nie są słabo zabezpieczone informacje czy przestarzała infrastruktura, a człowiek.

Dlatego chcemy przybliżyć Ci znaczenie cyberbezpieczeństwa w kontekście tych nowych pokoleń na rynku pracy i podkreślić, jak istotne jest przygotowanie młodych ludzi do wyzwań, które niesie ze sobą cyfrowa rzeczywistość, i reakcji na cyberzagrożenia.

NIE LEKCEWAŻ CYBERBEZPIECZEŃSTWA

Polskie przedsiębiorstwa niechętnie szkolą swoich pracowników. Co pokazuje raport „COVID-19 Business Pulse Survey – Polska". Według niego umiejętności cyfrowe polskich pracowników są poniżej średniej europejskiej. Mimo to 33% przedsiębiorców uważa, że są... zadowalające. Co więcej – 49% polskich firm nie szkoliło swoich pracowników, chociażby w 2020 roku. Dlaczego? Właśnie ze względu na to, że uważało, iż ich kompetencje są wystarczające. Albo tłumaczyło się tym, że szkoliło się w poprzednich latach lub że koszty takich warsztatów są zbyt duże.

Tylko czy bezpieczeństwo to coś, na czym powinno się oszczędzać? Według raportu „Cyberwarfare In The C-Suite" cyberprzestępczość będzie kosztować świat 10,5 bilionów (odpowiednika angielskiego trillion) rocznie do 2025 r.

Jeśli nie chcesz dokładać pieniędzy do kieszeni cyberprzestępców – lepiej zadbaj o kompetencje pracowników. Tym bardziej, że ci najmłodsi niekoniecznie są tak dobrze przygotowani w kontekście cyberbezpieczeństwa. Co pokazuje przykład szkół. Do dziś w Polsce nie ma przedmiotu w szkołach, jak "cyberbezpieczeństwo" (choć kwestie cyberbezpieczeństwa jako tako przewijają się w placówkach), a same placówki, jak wynika z informacji UODO, również nie dbają o przetwarzanie i przechowywanie danych. Zdarza się że nauczyciele naprzemiennie używają swoich niezabezpieczonych prywatnych i służbowych urządzeń, przez co dane ich uczniów znajdują się raz tu, raz tu. I dobrym przykładem tego jest przypadek Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie, gdzie w 2019 roku doszło do wycieku. Wypłynęły dane nawet 100 tys. osób. Z tego tytułu UODO nałożyło na uczelnię karę finansową. Pytanie nasuwa się samo: skoro nauczyciele nie mają wiedzy na temat cyberbezpieczeństwa, ochrony danych, to w jaki sposób, chronić mają dzieci? Jak zapewnić dzieciom bezpieczeństwo w szkołach, skoro w całym kraju jest ledwo 17 tys. wakatów związanych z cyberbezpieczeństwem?

NAWET 10 TYS. CYBERPRZESTĘPSTW PRZECIWKO DZIECIOM W USA, A W POLSCE?

Stany Zjednoczone to kraj, który uchodzi za jeden ze wzorów, jeśli chodzi o naukę cyberbezpieczeństwa. Jednak i tam nie jest tak kolorowo, jak mogłoby się wydawać. To również kraj, który wyjątkowo często jest na celowniku cyberprzestępców. I nie każdy obywatel umie sobie z tym poradzić.

Według raportu FBI „Internet Crime Center Report 2015–2020" w 2020 r. cyberprzestępczość dotykająca dzieci wzrosła o 144% względem 2019 r. Jest to niewątpliwie w jakimś stopniu wpływ pandemii koronawirusa. Ta, wywołując przyspieszoną cyfryzację, spowodowała też wzrost cyberzagrożeń. Jednak to i tak było nieuniknione.

To zwiększenie się cyberprzestępczości – trzeba przyznać – jest zatrważające. W latach 2015–2019 w Stanach Zjednoczonych cyberzagrożenia wymierzone w dzieci wzrastały o 5–9% rok do roku.

Do FBI w latach 2015–2020 zgłoszono 10 tys. skarg związanych z cyberprzestępczością dotykającą dzieci. A straty z powodu cyberzagrożeń wymierzonych w najmłodszych oceniono na 2 mln dolarów. Z kolei według globalnych badań DQ Institute 2020 6 na 10 dzieci w wieku od 8 do 12 lat jest narażona w sieci na cyberzagrożenia. Ponadto 1 na 2 dzieci spotyka się z cyberprzemocą, a blisko ⅓ doświadczyła innych zagrożeń, takich jak phishing czy hakowanie.

Jak sytuacja wygląda w Polsce? Mamy świeże dane badania od ClickMeeting, z którego wynika, że aż 88% rodziców dzieci w wieku od 7 do 18 lat obawia się o ich bezpieczeństwo online. 4% rodziców przyznało, że ich pociechy były celami prób wyłudzenia danych, natomiast 6% stwierdziło, że przestępcy próbowali wyłudzić od nich pieniądze. Ponadto, 6% dzieci padło ofiarą złośliwego oprogramowania, a kolejne 6% stało się celem fałszywych osób, próbujących nawiązać z nimi kontakt. Łącznie, 22% respondentów miało doświadczenie z różnymi formami cyberprzestępstw wymierzonych w ich dzieci.

Przerażające jest to, że aż 13% rodziców przyznało, że nie wie, czy ich dzieci były narażone na działania cyberprzestępców. Tylko 67% ankietowanych zadeklarowało, że na pewno ich dzieci nigdy nie miały takiego problemu.

Z drugiej strony, tylko ⅓ rodziców przyznała, że zna i korzysta z narzędzi poprawiających bezpieczeństwo online ich dzieci. 32% respondentów stwierdziło, że zna takie narzędzia i planuje z nich skorzystać, podczas gdy 27% przyznało, że nie zna, ale chce się z nimi zapoznać. Tylko 7% rodziców stwierdziło, że nie zna tych rozwiązań i nie widzi powodów, aby z nich korzystać.

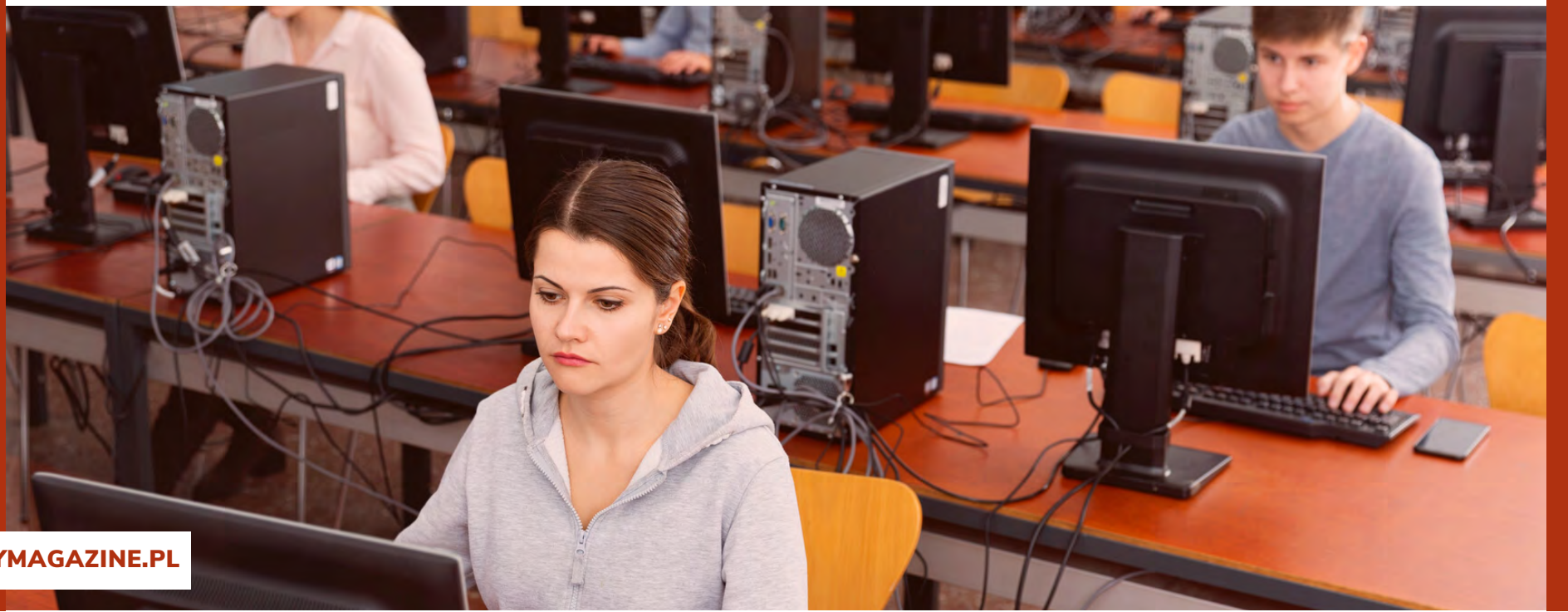
CYFROWE KOMPETENCJE DZIECI – NIE JEST DOBRZE

DQ Institute prowadzi „Child Online Safety Index", który ma na celu ocenianie i analizę potencjalnego cyberbezpieczeństwa dzieci w poszczególnych krajach. Polska wypada na jego tle dość blado, choć są kraje niżej ocenione od nas – w tym też w Europie. Jednak to, co przemawia za niską pozycją Polski, są cyfrowe kompetencje naszych najmłodszych.

Instytut przyznał nam w tej kategorii 20,4 pkt (na 100 możliwych), co uplasowało nas niżej od takich krajów jak Peru (54,2), Rumunia (49 pkt), Rosja (35,7 pkt), czy Sri Lanka (29,8 pkt). Mimo że najmłodsi często określani są jako tzw. digital natives, czyli osoby, które „rodzą się ze smartfonem w ręce", to ich rzeczywiste kompetencje nie wypadają już tak dobrze. Dlaczego? Nie ma tutaj konkretnych badań, ale dzieje się tak zapewne z kilku powodów.

DLACZEGO POLSKIE DZIECI MAJĄ GORSZE KOMPETENCJE?

Po pierwsze – Polska jest dość bezpiecznym krajem. Zarówno, jeśli chodzi o przestępstwa w świecie rzeczywistym, jak i cyfrowym. Owszem – one się



zdarzają - przez ostatni rok częściej - ale daleko nam do wielu innych krajów na tym polu. Z tego względu nasza podejrzliwość, a zwłaszcza rodziców, jest nieco uśpiona - mimo toczącej się cyberwojny.

Po drugie – rodzice dzieci w Polsce często sami nie mają lepszych cyfrowych kompetencji. Nie tylko pod względem cyberbezpieczeństwa, ale w ogólnym, szerszym kontekście. I to mimo że nasz kraj jest naprawdę dość dobrze scyfryzowany, natomiast my sami możemy się poszczycić dość dużą liczbą wykwalifikowanych programistów, czy równego rozkładu płci wśród absolwentów i absolwentek kierunków STEM (nauka, technologia, inżynieria i matematyka).

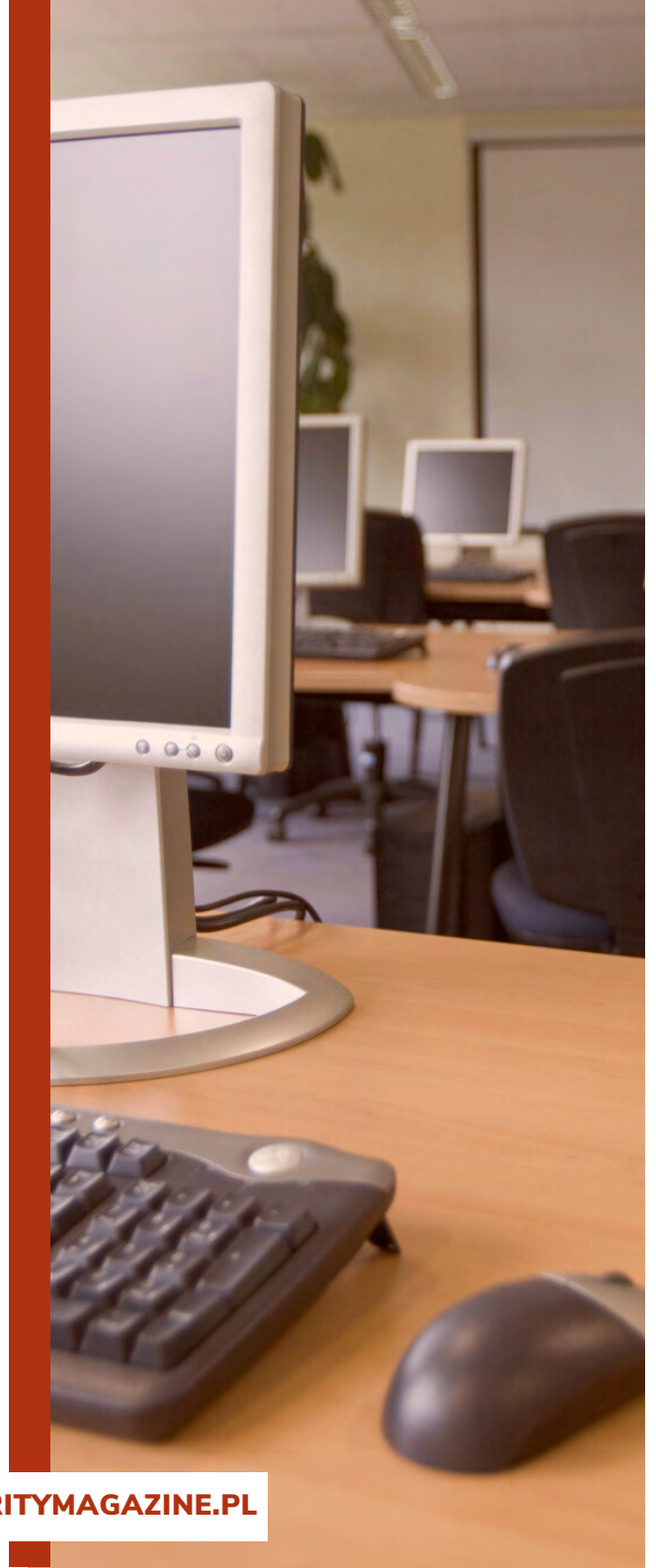
Po trzecie – dzieci w Polsce, jeśli chodzi o cyberprzestępczość najczęściej borykają się z mową nienawiści (48% według raportu EU Kids Online 2020). I to najwyższy taki wynik w Europie. Jest to oczywiście złe, ale to inny rodzaj cyberzagrożenia niż np. hakowanie. Mimo to polskie dzieci najczęściej zgłaszają cyberprzestępstwa w porównaniu do swoich rówieśników w innych krajach (35%).

Niestety, wygląda na to, że nasza młodzież zdecydowanie zawyża też swoje cyfrowe kompetencje. Przeważnie polskie dzieci lepiej je oceniają niż ich rówieśnicy w pozostałych państwach.

Co kłóci się z wynikami wspomnianego wcześniej „Child Online Safety Index". Dla przykładu – najczęściej bardzo kiepsko swoje kompetencje dotyczące cyberbezpieczeństwa oceniają Japończycy. Ponad 70% z nich (według badań firmy Norton) twierdzi, że nie wie, jak chronić się przed cyberzagrożeniami. Mimo to są oceniani jako jeden z najlepiej przygotowanych do tego państw.

Po czwarte – problemem jest też wymieniona na początku edukacja. Choć coraz większa część kadry dostrzega, jak ważne jest wykorzystanie nowoczesnej technologii i edukowanie o niej, to nie zawsze działa w tym kierunku. Przyznać jednak trzeba, że temat cyberbezpieczeństwa stopniowo wkracza do oświaty. I przykładem tego jest podstawa programowa informatyki. Uczniowie uczą się teraz m.in. profilaktyki antywirusowej i zabezpieczania komputerów wraz z zawartymi w nim informacji przed zagrożeniami.

9 lutego stał się też Dniem Bezpiecznego Internetu, kiedy to dzieci uczą się o zagrożeniach online. Pytanie tylko, czy skutecznie.



– *Stereotypowe myślenie o lekcjach informatyki, tzn. że podczas ich trwania, uczniowie uczą się jedynie tworzenia prezentacji w PowerPoint czy korzystania z Worda, jest krzywdzące dla tych, którzy w szkołach dbają o bezpieczeństwo w sieci. Ostatnie lata pokazują, że spory nacisk kładzie się na edukację dzieci w tym zakresie. Odbywają się konferencje poświęcone cyberbezpieczeństwu dla uczniów ale też dla pedagogów i rodziców. Nauczyciele nawiązują współpracę z wieloma fundacjami i organizacjami, które zajmują się tą tematyką. Otrzymują wsparcie merytoryczne np. w formie materiałów dydaktycznych, które mogą wykorzystać w pracy z uczniami, a także z rodzicami. Popularne stało się organizowanie cykli zajęć w formie projektów z udziałem ekspertów w dziedzinie bezpieczeństwa* – powiedziała nam **Elżbieta Kołodziejczuk, wicedyrektorka Szkoły Podstawowej nr 185 IM. UNICEF w Warszawie.**

IM WCZEŚNIEJSZA EDUKACJA, TYM LEPIEJ

Aby przyszli pracownicy mogli skutecznie działać we współczesnym świecie, muszą być dobrze przeszkoleni. I to już na poziomie wczesnej edukacji. Przekonuje o tym chociażby raport firmy badawczej Gartner „Leverage the K-12 Education Digital Learning Maturity Model", który wskazuje na konieczność przeniesienia nauki cyfrowej na wyższy poziom dojrzałości.

Raport ten podkreśla, że dostarczanie szkołom cyfrowych narzędzi to potencjał do tworzenia spersonalizowanych metod uczenia się. Z kolei z badania Gallupa dowiadujemy się, że 57% nauczycieli i 65% dyrektorów uważa, że cyfrowe narzędzia do nauki są skuteczniejsze niż inne. A co więcej – przekładają się na zaangażowanie dzieci w naukę. Mowa tu zarówno o cyfrowym uczeniu się, jak i o edukacji w tym zakresie.

EDUKACJA W SZKOŁACH – SĄ KRAJE, KTÓRE ROBIĄ TO LEPIEJ

W amerykańskich czy australijskich szkołach funkcjonuje przedmiot „cyberbezpieczeństwo" – niekiedy jest to inicjatywa oddolna, czasem wymagana od szkół publicznych (np. w Dakocie Północnej w Stanach Zjednoczonych. Szkoli się tam nie tylko dzieci, ale też kadrę pedagogiczną). Państwa te wiedzą, jak ważne jest to w kontekście bezpieczeństwa zarówno sektora prywatnego, jak i publicznego. Zwłaszcza, patrząc na przykład Ukrainy, która boryka się nie tylko z wojną fizyczną, ale też cyfrową.

Problem cyberzagrożeń dobrze adresuje też Estonia. Tamtejszy Uniwersytet Technologiczny w Tallinnie mocno stawia na edukację w zakresie cyberbezpieczeństwa. Dodatkowo Estonia w raporcie „Cybersecurity Education Initiatives in the EU Member States" została wskazana jako kraj, który chętnie promuje aspekt cyberbezpieczeństwa wśród swoich obywateli. W kraju tym istnieje rada ekspertów zarządzająca tego typu inicjatywami, wspierana przez nauczycieli.

Dodatkowo Estonia chętnie współpracuje z Norwegią, współorganizując np. letnie obozy edukacyjne, by Norwedzy i Estończycy razem podnosili swoje kompetencje w zakresie cyberbezpieczeństwa. W tych trzech krajach współpraca na poziomie rządu, szkół i sektora prywatnego w promocji i edukacji w cyberbezpieczeństwie działa naprawdę przyzwoicie.

CYBERBEZPIECZEŃSTWO JAKO PRZEDMIOT? TYLKO NA UCZELNIACH

W naszym kraju również można się natknąć na przedmiot „cyberbezpieczeństwo", ale dopiero na studiach, np. w Szkole Głównej Handlowej w Warszawie czy na Akademii Leona Koźmińskiego. Choć kadra pedagogiczna niekoniecznie uważa, że dodatkowy przedmiot w szkolnictwie podstawowym i średnim mógłby tu coś zmienić.

– Na naukę w tej dziedzinie poświęcana jest nie tylko informatyka, ale także inne przedmioty np. godziny wychowawcze, technika, wiedza o społeczeństwie, edukacja dla bezpieczeństwa i inne. Fakt, że nie ma takiego przedmiotu jak "cyberbezpieczeństwo" nie oznacza, że szkoły o nim nie uczą, czy nie uświadamiają. Muszę jednak przyznać, że to, co realizujemy w szkołach, to wciąż zbyt mało, by uchronić dzieci przed negatywnymi skutkami korzystania z internetu. Chodzi mi tu w szczególności

o hejt, z którym się spotykają, i z którym sobie nie radzą. Trudno się nie zgodzić, że jeśli nie radzą sobie z tym rodzajem cyberzagrożenia, to w przyszłości mogą nie poradzić sobie z innymi formami cyberoszustw, np. socjotechnikami, w tym phishingiem – stwierdziła wicedyrektorka Szkoły Podstawowej nr 185 IM. UNICEF w Warszawie.

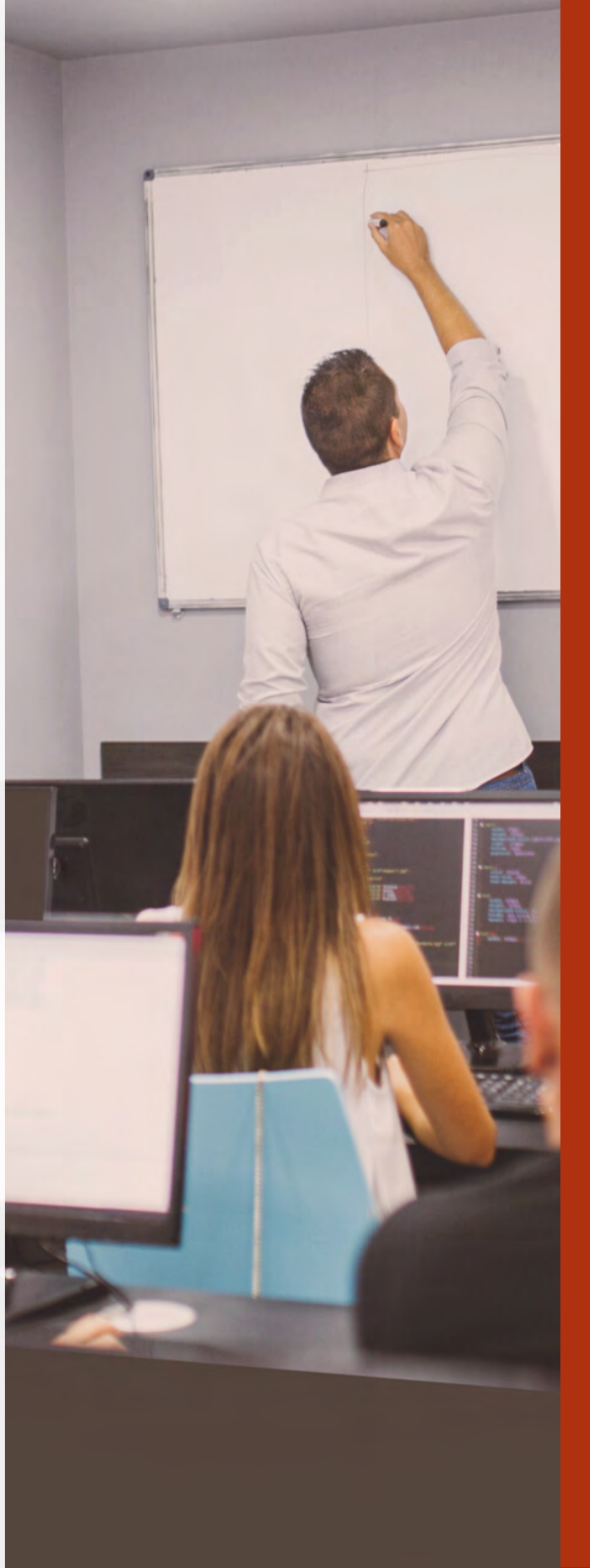
Nie jest też najlepiej w kontekście kampanii państwowych. W 2022 r. w trakcie wakacji w radiach pojawiały się spoty edukujące o phishingu, ale... cyberprzestępców stosujących tę metodę nazywano „hakerami", choć w zasadzie nie muszą nimi być.

Są też organizacje, które starają się poszerzać wiedzę dzieci i młodzieży w zakresie cyberbezpieczeństwa, np. NASK realizuje CYBER lekcje - projekt edukacyjny, który powstał w ramach współpracy Ministra Cyfryzacji oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego. A Stowarzyszenie ISSA od dawna co miesiąc organizuje Akademie Cyberbezpieczeństwa, ponadto realizuje program "Cyfrowy Skaut". Powstał serwis Sieciaki.pl, który opiera się na przygodach czwórki szkolnych przyjaciół, którzy dzięki umiejętnościom potrafią sprawnie i bezpiecznie korzystać z sieci. Jest również wiele komercyjnych szkoleń dla szkół, a nawet dla przedszkoli. Działa platforma Be.Net z ogólnopolskim programem edukacyjnym skierowanym do nau-

czycieli, uczniów, szkół podstawowych i ponadpodstawowych z całej Polski. Są szkolenia, które prowadzi prof. Jacek Pyżalski, pedagog specjalny, profesor na Wydziale Studiów Edukacyjnych Uniwersytetu im. A. Mickiewicza w Poznaniu, nauczyciel i wychowawca z wieloletnim doświadczeniem, ekspert w programie EduAkcja. Jest wiele kampanii np. kampania edukacyjna FakeHunter-Edu, i wiele innych inicjatyw, ale są one w większości oddolne.

Czy w związku z tak, wydawać by się mogło, szerokimi możliwościami nauki o cyberbezpieczeństwie, przedmiot taki to konieczność? Jak zauważyła nasza rozmówczyni, szkoły robią wiele, ale to wciąż zbyt mało. Jednak jej zdaniem tworzenie nowego przedmiotu „cyberbezpieczeństwo" przy już i tak dużym obciążeniu uczniów, nie rozwiąże problemu.

- Ważne jest, aby oddziaływanie na młodego człowieka było współproporcjonalne do potrzeb związanych z wciąż rozwijającymi się technologiami informatycznymi. Ogromną funkcję pełnią rodzice, na których barkach leży odpowiedzialność, i co dziecko robi w sieci, na co ma przyzwolenie. Z badań wynika, że rodzice mają niewielką świadomość, jakiego rodzaju aktywność w internecie realizuje ich dziecko. Podstawowym i najlepszym sposobem na wzmocnienie działań hamujących cyberprzemoc jest współpraca domu i szkoły. Nauczyciele na bazie podstawowych kierunków realizacji polityki oświatowej państwa, mają obowiązek rozwijać umiejętności metodyczne w zakresie prawidłowego i skutecznego wykorzystywania technologii informacyjno-komunikacyjnych w edukacji, a także wspierać uczniów w kształtowaniu krytycznego podejścia do treści publikowanych w internecie i mediach społecznościowych. Widać to w wielu szkołach. Czeka nas jeszcze jednak długa i niełatwa droga, aby osiągnąć satysfakcjonujące efekty – zauważyła Elżbieta Kołodziejczuk.



ZAUFANIE DO EKSPERTÓW W BRANŻY

Ogromnym wsparciem mogą stać się firmy, tak jak już teraz robi to np. EY Polska. Zresztą, odpowiedzialność za rozwijanie tych niezbędnych umiejętności dzieci i młodzieży spoczywa teraz również na społeczności biznesowej, która musi zainwestować w edukację i szkolenia z zakresu cyberbezpieczeństwa, aby zapewnić bezpieczną i produktywną przyszłość rynku pracy. Firmy muszą zrozumieć, że cyfrowe umiejętności dzieci są przyszłością ich biznesu. Dlatego powinny jeszcze bardziej włączać się w projekty skierowane nie tyle do szkół, a do uczniów i ich rodziców.

JAK FIRMY MOGĄ EDUKOWAĆ MŁODZIEŻ?

Wiemy dobrze, że cyberprzestępczość będzie rosnącym problemem. Z tego powodu narodzi się luka pomiędzy poszczególnymi grupami wiekowymi, które edukacji z zakresu cyberbezpieczeństwa nie odbyły. Co w tym przypadku mogą robić firmy?

Edukować młodzież na własną rękę, zanim ta jeszcze pojawi się w ich przedsiębiorstwach. Już teraz wiele organizacji przeprowadza bezpłatne webinary, organizuje kursy (niekiedy ze zniżką dla studentów) itd.

A co Ty możesz zrobić?

- Masz eksperta do spraw cyberbezpieczeństwa w swojej firmie? Zaproponuj lokalnej szkole, że ten przeprowadzi warsztaty dla dzieci i młodzieży, ucząc ich jak chronić się w internecie. Albo pomoże w szkoleniu samej kadry nauczycielskiej;
- W ramach swoich działań CSR czy ESG – przeprowadź kampanię edukującą o cyberzagrożeniach w mediach czy internecie;
- Możesz też wejść we współpracę z zasięgowym influencerem, który nagłośni kwestię cyberbezpieczeństwa;
- Przyjmujesz nowych, młodych pracowników? Poszerz szkolenie BHP o zagadnienia z zakresu cyberbezpieczeństwa;
- Wysyłaj tych pracowników na warsztaty, kursy i webinary poświęcone cyberzagrożeniom;
- Twórz edukacyjne programy dla dzieci, wykorzystując ich ulubione formaty, np. gaming.

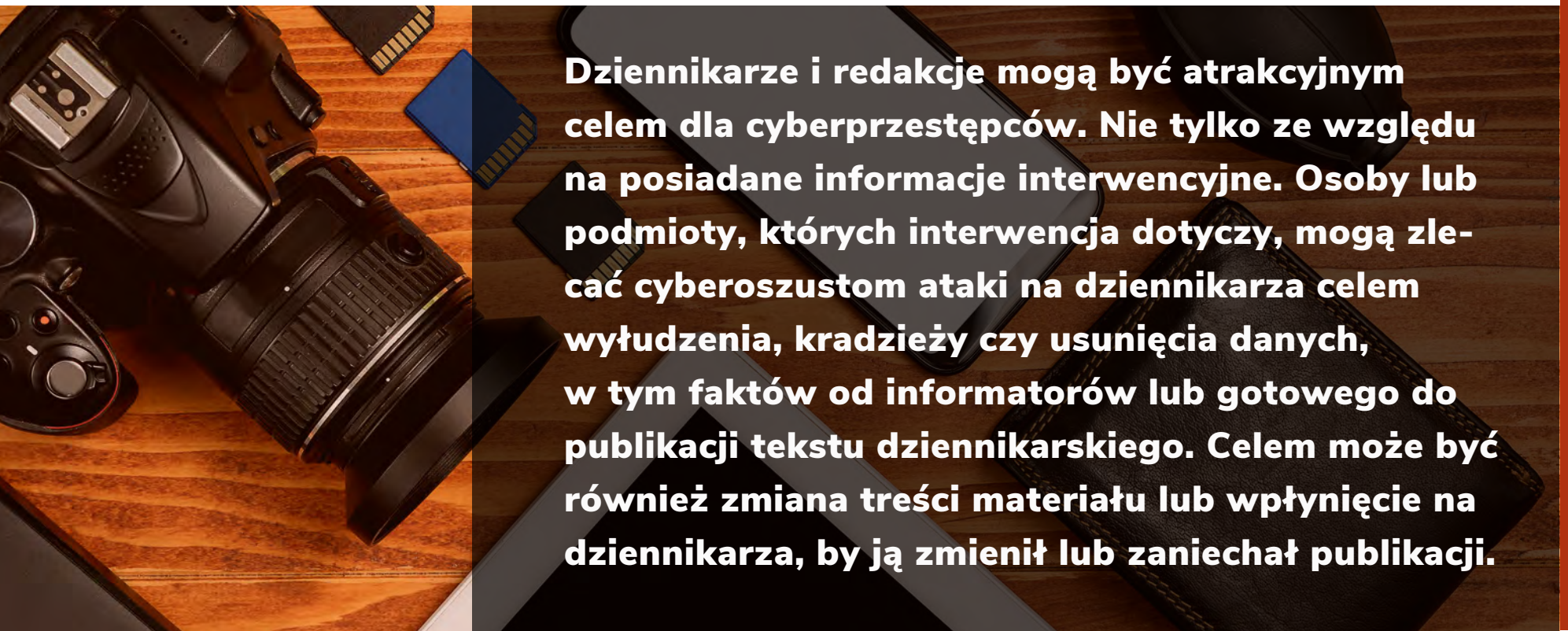
Popatrz na Miasteczko ING w Robloxie, w którym dzieci nie tylko się bawią, ale też edukują o finansach, a także bezpieczeństwie.

Edukacja z zakresu cyberbezpieczeństwa ma kluczowe znaczenie dla przyszłych pracowników firm. Pomaga im zrozumieć zagrożenia, które mogą napotkać, i daje im narzędzia do ochrony swoich danych i systemów. A to wszystko z korzyścią zarówno dla samych pracowników, jak i firm czy klientów. W końcu – niestety – cyberzagrożenia będą tylko się zwiększać.

SECURITYMAGAZINE.PL

CYBERZAGROŻENIA W BRANŻY MEDIALNEJ

Redakcja
SECURITY MAGAZINE



Dziennikarze i redakcje mogą być atrakcyjnym celem dla cyberprzestępców. Nie tylko ze względu na posiadane informacje interwencyjne. Osoby lub podmioty, których interwencja dotyczy, mogą zlecać cyberoszustom ataki na dziennikarza celem wyłudzenia, kradzieży czy usunięcia danych, w tym faktów od informatorów lub gotowego do publikacji tekstu dziennikarskiego. Celem może być również zmiana treści materiału lub wpłynięcie na dziennikarza, by ją zmienił lub zaniechał publikacji.

To, że cyberatki na media zdarzały się i wciąż się zdarzają wiemy nie od dziś.

Jednym z przykładów cyberataku na redakcję, jest atak na serwery Associated Press w 2013 roku. W wyniku tego ataku, hakerzy uzyskali dostęp do oficjalnego konta Twittera agencji i opublikowali fałszywe wiadomości o ataku na Biały Dom, co spowodowało krótkotrwały szok na giełdach finansowych.

W 2013 roku chińscy hakerzy przeniknęli do sieci New York Times, kradnąc hasła wszystkich jego pracowników i próbując uzyskać dostęp do komputerów 53 z nich. Atak prawdopodobnie miał na celu odnalezienie źródeł informacji, które posłużyły do przygotowania artykułu o premierze Chin Wen Jiabao.

W 2014 roku doszło do ataku na Sony Pictures. Hakerzy z Korei Północnej ujawnili tysiące poufnych dokumentów i e-maili z Sony Pictures. Atak miał na celu zapobiegnięcie wydaniu filmu "The Interview", który miał premierę w tym samym roku.

Kanał wiadomości Al Jazeera w 2020 roku padł ofiarą skomplikowanego ataku cybernetycznego, który miał na celu dostarczenie szkodliwego oprogramowania do telefonów 33 dziennikarzy i producentów pracujących dla stacji.

Atak prawdopodobnie był próbą inwigilacji pracowników Al Jazeera i dostępu do ich kontaktów i komunikacji.

W czerwcu 2021 roku Polska Agencja Prasowa poinformowała o cyberataku na jej serwery. Pomimo tego, że atak nie naruszył bezpieczeństwa danych klientów agencji, przerwał on działanie niektórych usług świadczonych przez PAP.

W marcu 2022 w Chorwacji doszło do prorosyjskiego ataku hakerskiego na stronę internetową dziennika "Slobodna Dalmacija". W efekcie na portalu gazety wydawanej w Splicie można było zobaczyć artykuły z rosyjską propagandą o wojnie na Ukrainie pod nazwiskami redaktorów. Teksty hakerów zostały usunięte.

W maju 2023 roku doszło do masowego ataku DDoS najprawdopodobniej rosyjskich grup hakerskich na strony polskich portali informacyjnych. Hakerzy mieli zaatakować strony: polityka.pl, niezalezna.pl, ceneo.pl, wyborcza.pl, rp.pl, se.pl, wpolityce.pl, wprost.pl oraz login.gremi-media.pl i login.wyborcza.pl. Niektóre z portali informowały o chwilowych trudnościach z wejściem na strony.

Ministerstwo Cyfryzacji wiedziało o nadchodzących atakach i z wyprzedzeniem informowało redakcje portali o takim ryzyku.

I to zaledwie garstka, bo w samym 2022 roku zostało zarejestrowanych niemal 50 ataków na świecie, których celem były wydawnictwa medialne. Od czasu rozpoczęcia wojny w Ukrainie mamy do czynienia głównie z atakami DDoS, które mają zakłócać funkcjonowanie portali informacyjnych. Ale jest też masa akcji związanych z dezinformacją, którą niestety wiele redakcji powiela bez sprawdzenia i weryfikacji lub weryfikacji niewystarczającej, niedokładnej. W ubiegłym roku najwięcej ataków przeprowadzono, co wydaje się oczywiste, w lutym i były one skierowane na media... rosyjskie. W kwietniu tego samego roku sporo było również ataków na media izraelskie.

CO CENNEGO MAJĄ DZIENNIKARZE I REDAKCJE?

Skoro ataków na media i dziennikarzy jest aż tyle, to warto wiedzieć, że są oni opiekunami informacji, które mogą być atrakcyjne dla różnych stron, w tym zarówno legalnych, jak i nielegalnych. Tymi informacjami bez wątpienia są:

- **Dane osobowe**, takie jak adresy e-mail, numery telefonów czy adresy zamieszkania. Mogą one być wykorzystywane do celów kradzieży tożsamości, wymuszeń czy dalszych ataków phishingowych.
- **Dane źródeł.** Dziennikarze często pracują z poufnymi źródłami. Dane tych źródeł są niezwykle cenne, a ich ujawnienie może narażać źródła na ryzyko.
- **Nieopublikowane jeszcze materiały.** Materiały dziennikarskie, takie jak artykuły, reportaże, zdjęcia, filmy czy audio, które nie zostały jeszcze opublikowane, są atrakcyjne dla hakerów. Mogą one być wykorzystywane do manipulacji informacjami, szantażu lub do uzyskania przewagi konkurencyjnej.
- **Informacje korporacyjne i rządowe.** Redakcje mogą posiadać cenne informacje o działaniach firmy czy urzędu, takie jak strategie biznesowe, plany marketingowe, informacje finansowe, które mogą być atrakcyjne dla konkurencji, hakerów lub innych stron zainteresowanych takimi danymi.
- **Infrastruktura IT**. Wiele redakcji przechowuje duże ilości danych na swoich serwerach, co może stanowić atrakcyjny cel dla hakerów. Atak na infrastrukturę IT może mieć poważne konsekwencje, w tym utratę danych, przerwę w dostawie treści lub uszkodzenie sprzętu.
- **Dostęp do kanałów dystrybucji.** Dziennikarze i redakcje mają dostęp do platform dystrybucyjnych o dużym zasięgu. Hakerzy mogą próbować zdobyć dostęp do tych kanałów, aby rozpowszechniać dezinformacje lub propagandę.

Dla cyberprzestępców lub osób, które zlecają atak, cenny jest również dostęp do zaufania, jakim społeczność obdarza media. Przejęcie kontroli nad tym zaufaniem, na przykład poprzez sianie dezinformacji, może być cennym narzędziem dla tych, którzy chcą manipulować opinią publiczną. Dla mediów kolejne ataki - zresztą jak w każdej branży - wiążą się z utratą tego zaufania, które i tak od 2022 roku jest mocno nadszarpnięte.

MEDIA: JAK WIDZĄ JE INNI, JAK WIDZĄ SAME SIEBIE?

Według badania Edelman Trust Barometer przeprowadzonym w 2023, zaufanie do mediów na całym świecie rok do roku nie spadło, ale ten poprzedni nie pokazał branży w najlepszym świetle. Wówczas obok rządów największym spadkiem zaufania nie cieszyły się właśnie media. Na całym świecie większość ludzi uważała, że jest okłamywana przez dziennikarzy (67%, wzrost o 8 punktów). Prawie co drugi respondent postrzegał media (46%) obok rządów jako siły dzielące społeczeństwo. Nie napawa optymizmem to, że wobec takich danych oraz coraz częstszych ataków, media, niestety pozostają bierne.

Wiązać się to może między innymi z tym, jak dziennikarze w swojej branży postrzegają samych siebie. Uważają bowiem, że cyberprzestępczość... ich nie dotyczy. Badanie "Postrzeganie cyberbezpieczeństwa przez dziennikarzy w Polsce", które wśród redakcji przeprowadziła w 2022 roku Polska Agencja Prasowa, wskazało, że, według dziennikarzy, grupą najbardziej narażoną na ataki są klienci banków, później politycy i urzędnicy państwowi. Swoją grupę umiejscowili na 7. pozycji z 13. Czyli ocenili się, jako tych, którymi cyberprzestępcy raczej nie są zainteresowani.

Ogromny odsetek respondentów zgodził się ze zdaniem, że na przestrzeni ostatnich lat obserwują stały wzrost zagrożeń w sieci związanych z utratą lub przejęciem danych. Równie często deklarowali, że umieją rozpoznać maile z zagrożeniem, ale przyznali też, że wszędzie stosują to samo hasło do logowania. Równocześnie byli zdania, że cyberbezpieczeństwo jest w większym stopniu realną koniecznością niż modnym tematem.

37% badanych przyznało, że ich redakcje nie informują ich na bieżąco o zagrożeniach i nie ins-

truują, jak się zabezpieczać.

W szkoleniach z zakresu cyberbezpieczeństwa wzięło udział zaledwie 40% ankietowanych. Pozostałe 60% nigdy nie brało udziału w spotkaniach edukacyjnych. Nie dziwić więc powinno, że dziennikarze nie potrafili odpowiedzieć na pytanie, czy redakcje prasowe w Polsce, ich zdaniem, są dobrze zabezpieczone przed atakami cybernetycznymi. Odpowiedź twierdzącą w tym temacie podało 13,5% badanych, przy czym żaden z nich nie zrobił tego w sposób zdecydowany. 28% pytanych zdecydowanie przyznało, że polskie redakcje nie są dobrze zabezpieczone przed cyberatakami.

KONSEKWENCJE CYBERATAKÓW NA DZIENNIKARZY

Jest niepokój i niepewność, warto zatem, by dziennikarze mieli świadomość, jakie konsekwencje mogą przynieść cyberataki i dlaczego tak ważna jest świadomość i szczypta krytycyzmu względem siebie oraz swojej wiedzy na temat cyberbezpieczeństwa.

Przyjrzyjmy się skutkom cyberataku w branży medialnej:

- W przypadku naruszenia poufnych informacji, anonimowe źródła mogą zostać ujawnione, co naraża je na ryzyko i podważa zaufanie do dziennikarza. Dlatego ochrona tajemnic dziennikarskich jest jednym z podstawowych warunków wolności prasy.
- Cyberataki mogą prowadzić do fałszowania informacji lub manipulowania danymi, co z kolei wpływa na jakość pracy dziennikarskiej i może prowadzić do dezinformacji.

- Dziennikarze są szczególnie narażeni na phishing ze względu na wartość informacji, które posiadają. Mogą napotkać na swojej drodze osoby podszywające się pod informatorów i zebrać niewłaściwe informacje, co z kolei rzutuje na jakość artykułu i dalsze, również finansowe i prawne konsekwencje.
- Dziennikarze otrzymują wiele e-maili dziennie, wśród których mogą pojawić się zainfekowane załączniki lub linki. Kliknięcie na taki link lub otwarcie załącznika może prowadzić do instalacji ransomware na urządzeniu dziennikarza.
- Cenzura i blokowanie dostępu - tu przykładem mogą być ataki DDoS, które powodują czasowe wyłączanie witryn internetowych, ograniczając dostęp do informacji dla czytelników, ograniczając swobodę wypowiedzi oraz narażając wydawcę na straty finansowe oraz wizerunkowe.
- Stałe cyberzagrożenia mogą wpływać na zdrowie psychiczne dziennikarzy, prowadząc do stresu, lęku czy obaw o własne bezpieczeństwo, życie czy prywatność. Szczególnie w przypadku dziennikarzy zajmujących się tematami kontrowersyjnymi, ryzyko naruszenia ich cyberbezpieczeństwa może prowadzić do zwiększonego napięcia i niepokoju.
- Cyberzagrożenia mogą zniechęcić dziennikarzy do zajmowania się kontrowersyjnymi tematami lub krytykowania władz, co prowadzi do samocenzury i ograniczenia swobody wypowiedzi.
- Zarówno dla dziennikarzy, jak i dla wydawców, jest potrzeba zainwestowania w technologie zabezpieczające. Często jednak te grupy mogą być niechętne do przyjęcia nowych technologii, biorąc pod uwagę czas potrzebny na naukę obsługi tych narzędzi.

Wobec tych wyzwań, konieczne jest wdrożenie skutecznych narzędzi zabezpieczających i strategii cyberbezpieczeństwa. Jest to jednak trudne, gdy zarówno dziennikarze, jak i wydawcy często są niechętni wdrażaniu nowych technologii. W związku z tym, istnieje pilna potrzeba podniesienia świadomości na temat zagrożeń cyberbezpieczeństwa wśród dziennikarzy i wydawców, a także zainwestowania w skuteczne narzędzia i strategie zabezpieczające, aby chronić integralność zawodu dziennikarskiego.

Monika Świetlińska

EKSPERCI WYDANIA

KAROL GOLISZEWSKI
Consulting Engineer
Grandmetric

Consulting Engineer z doświadczeniem w komercyjnych obszarach network oraz network & data security. Aktywny w obszarze komunikacji z Klientami, pomoże w rozpoznaniu problemu, doborze rozwiązań i zaproponuje efektowny model wdrożenia. Jego kompetencje potwierdzają certyfikaty techniczne z rozwiązań marek Cisco, Sophos, Palo Alto czy Fortinet.

MAGDALENA JAKIMIUK
Leader of IT Security
Services Team

Leader zespołu IT Security Services, będący cześcią globalnego zespołu IT Security Competence Center w DB Schenker. Odpowiadam za zarządzanie podatnosciami, kampanie phishingowe oraz identyfikację i egzekucję domen naruszających prawo i bezpieczeństwo DB Schenker, i jego partnerów.

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.

WOJCIECH STAWSKI
Wiceprezes, rzecznik prasowy
Polska Izba Ochrony

Rzeczoznawca Polskiej Izby Ochrony w zakresie ochrony osób i mienia i zarządzania bezpieczeństwem, współautor projektu ustawy z dnia 22 sierpnia 1997 r o ochronie osób i mienia i większości aktów wykonawczych wydanych na jej podstawie. Autor podręczników oraz licznych publikacji, programów e-learningowych i filmów szkoleniowych.

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

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

al. Jana Pawła II 61 lok. 212
01-031 Warszawa

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

Redaktor Naczelny: Rafał Stępniewski

Redaktor prowadzący: Monika Świetlińska
Redakcja: Damian Jemioło, Anna Petynia-Kawa
Projekt, skład i korekta: Monika Świetlińska

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL