3(12)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Już rok z nami jesteście

Działania security awareness w organizacji

Zagrożenia i kryzysy wizerunkowe w sieci w 2023

Podstawowe metody hakowania a wzmacnianie ochrony tożsamości

Pamięci zmiennofazowe

SPIS TREŚCI

SZANOWNI PAŃSTWO,

już rok jesteście z nami i za to dziękujemy. Te ostatnie dwanaście miesięcy były czasem sprawdzianu dla większości firm, bo cyberprzestępcy na każdym kroku dają o sobie znać. Niezależnie czy mówimy o atakach na podmioty prywatne czy publiczne - cyberprzestępstwa zdarzają się każdego dnia.

W ciągu ostatniego roku byliśmy świadkami wielu znaczących incydentów, które wykazały, że żadna firma nie jest nietykalna. Ataki na dostawców usług chmurowych, naruszenia danych w sektorze zdrowia, a nawet incydenty dotyczące infrastruktury krytycznej - to tylko niektóre z przykładów. Dlatego w dzisiejszych czasach, kiedy większość firm działa w przestrzeni cyfrowej, bezpieczeństwo informacji staje się kluczowym elementem biznesowym.

W tym roku "Security Magazine" będzie kontynuowało swoją misję - bo tak traktujemy naszą pracę - dostarczania najświeższych informacji i wiedzy dotyczącej zagrożeń szeroko pojętego bezpieczeństwa oraz najlepszych praktyk w zakresie ochrony informacji.

Pierwsze 12 numerów to dawka rzetelnej, unikalnej wiedzy i możecie je pobrać bezpłatnie w każdej chwili. Wszystkie nasze wydania zawierają linki kierujące do poprzednich numerów. Chcąc wyróżnić naszych ekspertów, przygotowaliśmy konkurs "Artykuł Roku Security Magazine". W finale znalazły się cztery materiały, a zwycięzcę wyłoni głosowanie na naszych kanałach na LinkedIn i Facebooku. Głosowanie właśnie ruszyło, a szczegóły i regulamin znajdziecie na str. 9.

Zapraszamy do lektury naszego rocznicowego wydania i głosowania w konkursie.

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

SECURITYMAGAZINE.PL

JUŻ ROK Z NAMI JESTEŚCIE

Redakcja
SECURITY MAGAZINE

Już od roku możecie polegać na "Security Magazine" - e-pismie, które jest źródłem nie tylko praktycznych porad, ale również case studies, analiz zagrożeń oraz sposobów ich przeciwdziałania. Dzięki wiedzy naszych ekspertów możecie w sposób realny zminimalizować zagrożenia w swojej firmie i wdrożyć odpowiednie rozwiązania i procedury zapewniające maksymalne bezpieczeństwo dla pracowników, klientów oraz danych. Dziękujemy, że jesteście z nami.

To, że bezpieczeństwo w firmach, administracji, organizacjach było i nadal jest traktowane z przymrużeniem oka, wiadomo nie od dziś. Nie wynika to jednak z ignorancji, ale z faktu, że dostęp do wiedzy w tym zakresie jest (a na pewno był) mocno ograniczony. Kursy z szeroko pojętego bezpieczeństwa, a z cyberbezpieczeństwa w szczególności, są niezwykle drogie.

KOMU UFAMY?

Do tej pory branża cybersecurity była mocno hermetyczna - eksperci nieszczególnie dzielić się chcieli cenną wiedzą, a o case-study firm nikt nie chciał głośno mówić. Z jednej strony to zrozumiałe - dlaczego ktoś miałby chcieć dzielić się swoim kapitałem i własnością, rozwiązaniami, nad którymi pracował długie lata. Takie wydarzenia, jak chociażby Kongres Profesjonalistów PR poświęcony ostatnio komunikowaniu zdarzeń związanych z cybersecurity i współpracy między "komunikacją" firmy a "bezpieczeństwem" firmy są niezwykle cenne. Przełamują bowiem bariery między tymi kluczowymi filarami przedsiębiorstw, pokazują, że rola bezpieczników zmienia się. Bo komu innemu uwierzymy, jak ważne jest traktowanie bezpieczeństwa priorytetowo, jak nie bezpiecznikowy? Komuś, kto ma wiedzę, doświadczenie? Kto sam gasił pożary, opracował skuteczne sposoby, by walczyć z hackingiem i tak dalej?

Pracownicy, kadra zarządzająca każdej jednej firmy mogą

mieć dostęp do rzetelnej, solidnej, potwierdzonej doświadczeniem wiedzy. Dostęp ten, dający możliwość poznania powodów, dla których bezpieczeństwo powinno stać się priorytetem każdego jednego podmiotu są pierwszym i najważniejszym krokiem uświadomienia sobie, ile i co możemy stracić bez traktowania kwestii bezpieczeństwa jako jednego z najistotniejszych elementów istnienia, funkcjonowania i rozwoju. I mówimy tu zarówno o sektorze prywatnym, jak i publicznym. O mikroprzedsiębiorstwach, jak i korporacjach. O branży finansowej, jak i opiece zdrowotnej, o e-commerce, jak i produkcji. O bezpieczeństwie fizycznym, jak i bezpieczeństwie IT.

ROŚNIE ZAINTERESOWANIE

Jako wydawca serwisu “Polityka Bezpieczeństwa” dostrzegliśmy zainteresowanie tematyką security końcem 2021 roku. Powód był oczywisty. Wojna Rosji z Ukrainą z każdym tygodniem stawała się coraz bardziej realna. Poszukiwanie treści w tym zakresie było naturalnym odruchem tych, którzy chcieli chronić swój biznes.

Badanie rynku pokazało nam, że brakuje w Polsce łatwo dostępnego i przystępnego pisma, które poświęcone będzie stricte bezpieczeństwu podmiotów zarówno prywatnych, jak i publicznych. Pisma, które pomogłoby firmom, na wstępie, rozeznać się w tej kwestii, ocenić ryzyko, a następnie wdrożyć odpowiednie rozwiązania z zakresu bezpieczeństwa, dostosowane do specyfiki ich działalności.

“W SŁUŻBIE BEZPIECZEŃSTWU”

Zgodnie z naszym hasłem “W służbie bezpieczeństwu” stworzyliśmy e-pismo "Security Magazine", które stało się odpowiedzią na potrzeby przedsiębiorców i pracowników każdej branży chcących dowiedzieć się więcej na temat najnowszych trendów oraz rozwiązań w dziedzinie bezpieczeństwa.

- Nasze czasopismo to źródło cennych informacji, praktycznych porad i case studies, które pozwolą czytelnikom na rozwój i poszerzenie wiedzy na temat ochrony przed różnymi zagrożeniami - powiedział **Rafał Stępniewski, redaktor naczelny "Security Magazine".**

- Publikujemy artykuły ekspertów z różnych dziedzin szeroko rozumianego bezpieczeństwa, którzy dzielą się swoją wiedzą i doświadczeniem, a także analizy zagrożeń i sposoby ich przeciwdziałania. W magazynie znajdują się również informacje na temat bezpieczeństwa fizycznego, zarządzania ryzykiem oraz ochrony danych osobowych zaznaczył redaktor naczelny, dodając, że najważniejszym celem "Security Magazine" jest pomaganie firmom w identyfikacji i minimalizacji zagrożeń, a także wdrożenie odpowiednich rozwiązań i procedur zapewniających maksymalne bezpieczeństwo dla ich pracowników, klientów oraz danych - dodał redaktor naczelny.

WARTOŚCIOWE NARZĘDZIE DO DZIAŁANIA

- Chcemy dostarczyć czytelnikom wartościowe narzędzie do działania, które pozwoli na zwiększenie świadomości związanej z bezpieczeństwem i poprawę skuteczności działań podejmowanych w tym zakresie - powiedział Rafał Stępniewski.

"Security Magazine" jest pismem bezpłatnym, bo chcemy, aby wiedza naszych ekspertów była dostępna dla jak największej liczby osób zainteresowanych tematyką bezpieczeństwa. Jesteśmy przekonani, że publikacje zawarte w e-piśmie mogą przyczynić się do poprawy bezpieczeństwa w Polsce oraz pomóc w zmniejszeniu zagrożeń, którym każdego dnia muszą stawić czoła zarówno firmy, jak i osoby prywatne.

POTENCJAŁ "SECURITY MAGAZINE"

Wiedza 70 autorów na łącznie 1080 stronach "Security Magazine" zawarta jest w 130 artykułach 11 wydań. Opisaliśmy łącznie 18 startupów wspierających bezpieczeństwo w firmach, zrelacjonowaliśmy 7 wydarzeń związanych z bezpieczeństwem, które objęliśmy patronatem medialnym.

W ciągu pierwszego roku na łamach naszych wydań online pojawiło się 51 zewnętrznych reklam. 11 wydań zanotowało 253 tysiące pobrań, z czego najwięcej przypadło na wydanie styczeń 2023 (31 tys.) i paź-dziernik 2022 - (29,9 tys.).

Te liczby pokazują, że po pierwsze - przedsiębiorcy - nasi Czytelnicy - dostrzegają potencjał “Security Magazine” i chętnie po niego sięgają. Wysoki standard merytoryczny to wpływ naszych ekspertów i zaangażowania na-szych redaktorów. Stawiamy na unikalność, profesjonalizm, skrupulatność oraz rzetelność treści, które otrzymujemy.

Wierzymy, że między innymi dzięki temu nasi Czytelnicy poprzez zaufanie do autorów mogą do zagadnienia, jakim jest bezpieczeństwo, podejść poważniej oraz włączać go do swojej strategii biznesowej.

Pismo "Security Magazine" staje się więc cennym źródłem wiedzy i inspiracji dla osób odpowiedzialnych za bezpieczeństwo w organizacjach, pomagając im w realizacji celów związanych z ochroną przed zagrożeniami.

Przystępność, na której nam zależało, to nie tylko bezpłatny dostęp do pisma, ale przede wszystkim jego format, tzn. jest on wydawany w formie elektronicznej, nie papierowej jako PDF poziomego A4. Wszystko po to, by ułatwić Czytelnikowi lekturę i dopasować się do urządzeń, z których korzysta najczęściej (smartfon, laptop). Każde wydanie można ściągnąć bez-pośrednio na swoje urządzenie.

Wierzymy, że nasze wydawnictwo może pomóc Czytelnikom w lepszym zrozumieniu dziedziny bezpieczeństwa oraz w podejmowaniu bardziej świadomych decyzji związanych z ich bezpieczeństwem.

DO 3 KWIETNIA 2023 TRWA GŁOSOWANIE NA

PRZECZYTAJ: REGULAMIN

ARTYKUŁ ROKU SECURITY MAGAZINE

"INFORMACYJNE BEZPIECZEŃSTWO PRZEDSIĘBIORSTWA PRZY OGRANICZONYM BUDŻECIE"

intellias

"E-HANDEL NA MUSZCE CYBERPRZESTĘPCÓW. JAK POWINIEN BRONIĆ SIĘ RYNEK?"

tpay

"KORZYŚCI KONTROLOWANYCH ATAKÓW HAKERSKICH"

GRANDMETRIC

"TECHNOLOGIZACJA BRANŻY SECURITY. OSZCZĘDNOŚCI A ROSNĄCA PRESJA PŁACOWA"

seris konsalnet

ODDAJ SWÓJ GŁOS NA:

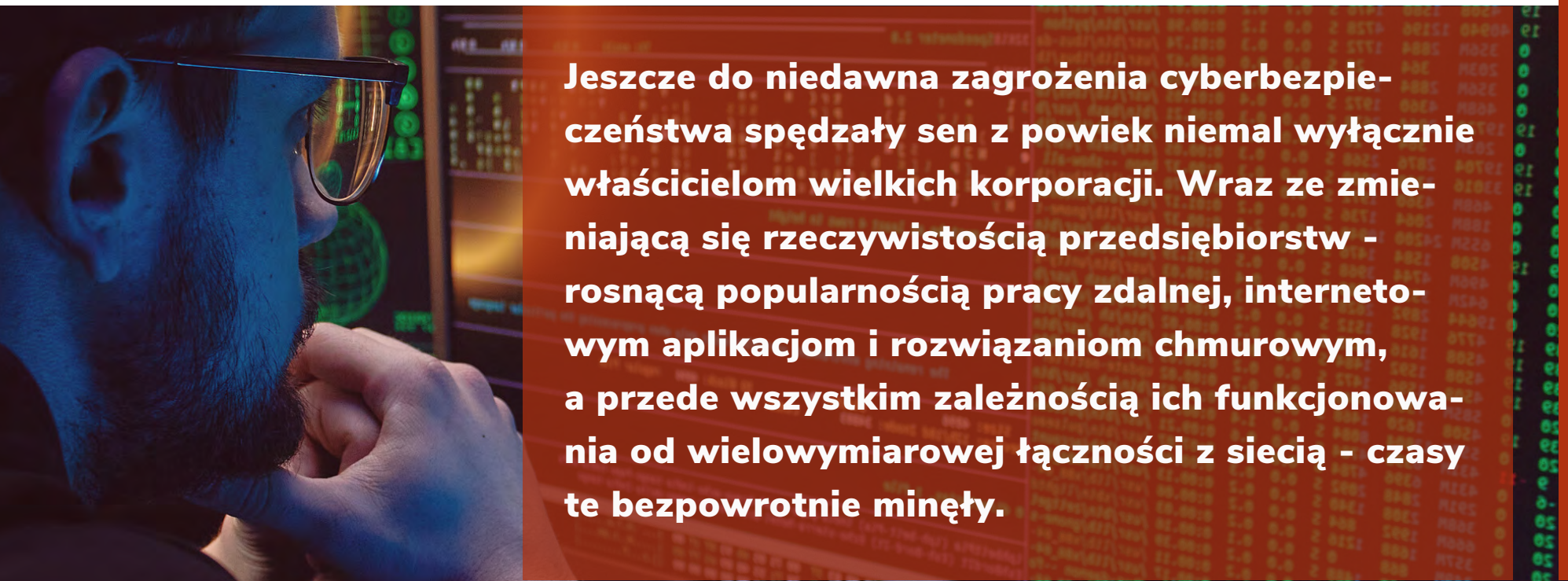
LUB:

ARTYKUŁ KONKURSOWY

KORZYŚCI KONTROLOWANYCH ATAKÓW HAKERSKICH

GRANDMETRIC
STAY CONNECTED.

Oddaj swój głos na:



Jeszcze do niedawna zagrożenia cyberbezpieczeństwa spędzały sen z powiek niemal wyłącznie właścicielom wielkich korporacji. Wraz ze zmieniającą się rzeczywistością przedsiębiorstw - rosnącą popularnością pracy zdalnej, internetowym aplikacjom i rozwiązaniom chmurowym, a przede wszystkim zależnością ich funkcjonowania od wielowymiarowej łączności z siecią - czasy te bezpowrotnie minęły.

AUTOMATYZACJA ATAKÓW HAKERSKICH

W dobie automatyzacji wielu procesów, które dotąd były mozolnie wykonywane ręcznie, swoje działania automatyzują również przestępcy działający w świecie wirtualnym. Są w stanie jednocześnie atakować setki, jeśli nie tysiące firm w tym samym czasie. Ze względu na mniej restrykcyjne polityki bezpieczeństwa, skromniejsze nakłady finansowe i niższy poziom świadomości ryzyka, szczególnie małe i średnie przedsiębiorstwa są dla nich atrakcyjnym targetem.

Wg raportu "Cost of Cybercrime" firmy Accenture, 43% cyber-ataków jest wymierzona w małe biznesy, ale tylko 14% z nich jest przygotowanych do tego, by skutecznie się przed nimi obronić.

To właśnie nieduże firmy mają sporo do stracenia, szczególnie, jeśli przechowują patenty, dane osobowe chronione prawnie czy opierają się na produkcji, której zatrzymanie i ponowne uruchomienie wiąże się z kosztami rzędu setek tysięcy złotych. Należy pamiętać, że prócz okupu dla którego działają hakerzy, w sytuacji cyberataku firmy ponoszą również inne koszty, takie jak straty wizerunkowe czy utrata zaufania klientów i partnerów biznesowych.

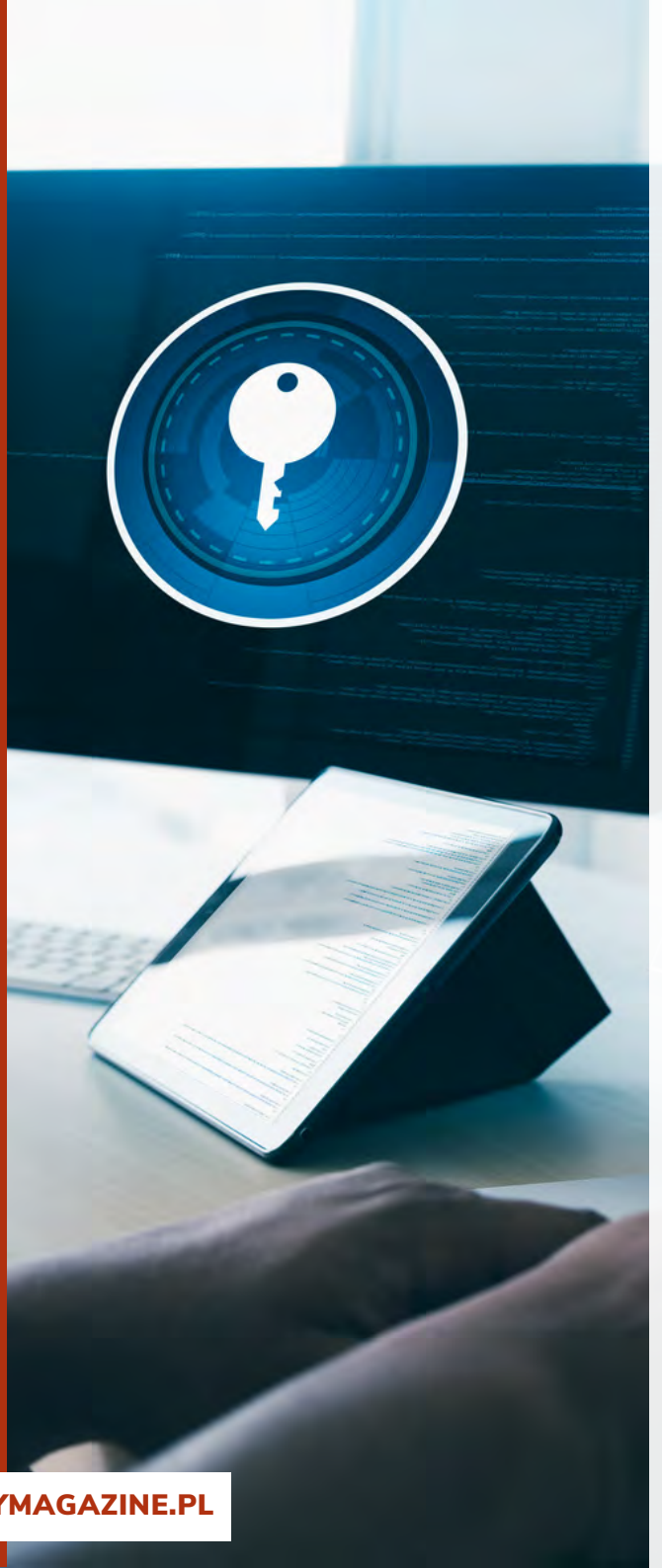
Badanie przeprowadzone przez Cisco wykazało, że 40% małych firm, które padły ofiarą cyberataku musiało mierzyć się z przestojem trwającym ponad 8 godzin, co stanowiło dużą część poniesionych kosztów.

PRZYCZYNY BŁĘDÓW BEZPIECZEŃSTWA

W przeciwieństwie do konsekwencji przyczyny błędów bezpieczeństwa bywają trywialne.

Przyjrzyjmy się najczęstszym z nich:

- **NIEAKTUALNE OPROGRAMOWANIE LUB JEGO KOMPONENTY**
- **NIEWYSTARCZAJĄCE PROCEDURY BEZPIECZEŃSTWA**
- **LUKI W OPROGRAMOWANIU ALBO W SPRZĘCIE**
- **NIEWŁAŚCIWA KONFIGURACJA**
- **NIEDOCIĄGNIĘCIA TECHNICZNE**
- **NIEOSTROŻNOŚĆ UŻYTKOWNIKÓW**



JAK PRZYGOTOWAĆ SIĘ NA POTENCJALNY CYBERATAK?

Przede wszystkim nie dać się zaskoczyć i zadbać o to, by firmowa infrastruktura informatyczna była bezpieczna. Podstawowym narzędziem służącym do sprawdzenia stanu cyberbezpieczeństwa jest przeprowadzenie testu penetracyjnego, nazywanego w skrócie pentestem.

Test penetracyjny to atak hakerski przeprowadzany w sposób kontrolowany, na zlecenie właściciela infrastruktury teleinformatycznej, sieci, strony internetowej czy aplikacji. Służy do wykrycia błędów, które zagrażają bezpieczeństwu badanego systemu.

Pentester wciela się w tej sytuacji w hakera, który działa **„w białych rękawiczkach”**. Jego zadaniem jest wykrycie luk systemu, wskazanie miejsc wrażliwych na potencjalny atak i zaproponowanie rozwiązań, które wyeliminują zagrożenie.

Pentesty powinny być przeprowadzane w sposób systematyczny i mogą mieć różny zakres, najczęściej też stanowią część szerszego audytu cyberbezpieczeństwa systemów i infrastruktury IT. Ich głównym celem jest zbadanie, na ile dana sieć jest odporna na włamanie i jaka jest skuteczność zastosowanych zabezpieczeń.

Niezbędną częścią każdego testu jest raport, opisujący zidentyfikowane problemy. Jego bardzo ważną częścią są rekomendacje, które mają na celu ich skuteczne wyeliminowanie.

Testy bezpieczeństwa dzielą się na trzy typy na podstawie ilości wiedzy na temat badanego systemu, jaka jest udostępniana pentesterom przez klienta:

1. **testy white box** - pełna wiedza pentesterów, mających do dyspozycji dokumentację projektu infrastruktury, informacje dotyczące konfiguracji urządzeń w sieci czy kod źródłowy strony
2. **testy black box** - minimalna wiedza pentesterów – najlepiej odzwierciedlają rzeczywisty cyberatak i wymagają dużego nakładu pracy ze strony testerów, a ich wiedza może ograniczać się tylko do adresu strony czy nazwy firmy, której zabezpieczenia testują.
3. **testy gray box** - częściowa wiedza pentesterów, hybryda obu wyżej wymienionych metod.

Wybierając firmę, której zlecimy przeprowadzenie testów naszej infrastruktury, warto zwrócić uwagę na to, jakie metody wykorzystuje. Ważne, by testy penetracyjne były wykonywane nie tylko w sposób automatyczny z użyciem oprogramowania, ale przede wszystkim ręcznie, w sposób dostosowany do konkretnego przypadku.

Należy pamiętać o tym, że kluczowy wpływ na sukces pentestu ma **doświadczenie, kreatywność, wiedza i wytrwałość pentestera**, który go przeprowadza. To rola wymagająca szerokiego zakresu kompetencji nie tylko technicznych, potwierdzonych certyfikatami, ale też komunikacyjnych czy z zakresu zarządzania.

JAK PROGNOZUJE STEVE MORGAN, REDAKTOR NACZELNY CYBERCRIME MAGAZINE, W 2025 ROKU GLOBALNE CYBERPRZESTĘPSTWA BĘDĄ WYMAGAŁY NAPRAWY STRAT RZĘDU 10,5 TRYLIONA DOLARÓW (!). WARTO ZADBAĆ, BY NIE DZIAŁO SIĘ TO KOSZTEM MAJĄTKU NASZEGO I NASZEJ FIRMY.

TESTY PENETRACYJNE – FAQ

1. Jakie są fazy testu penetracyjnego?

- **Rekonesans** – kluczowy etap, polegający na zebraniu jak największej ilości danych niezbędnych do przeprowadzenia testu
- **Skanowanie** – sprawdzanie istniejących mechanizmów zabezpieczeń
- **Eksploatacja** – próba złamania zabezpieczeń systemu, czyli usługi bądź aplikacji
- **Eskalacja** – rozszerzenie uprawnień i dalsze kroki w sieci lub systemie
- **Raport** – zawiera szczegółowy opis metod zastosowanych w symulacji cyberataku, wykrytych błędów i podatności oraz rekomendacje działań, które mają na celu ich eliminację.

2. Jakie korzyści wynikają z wykonania testów penetracyjnych?

- Weryfikacja skuteczności zabezpieczeń systemu
- Zbadanie podatności systemu na potencjalny cyberatak
- Uzyskanie rekomendacji dotyczących poprawy bezpieczeństwa systemu
- Uniknięcie ogromnych kosztów związanych z zakłóceniem działania systemu w przedsiębiorstwie.

3. Jak często należy przeprowadzać pentesty?

Najlepszym rozwiązaniem jest przeprowadzanie testów penetracyjnych cyklicznie, przynajmniej raz do roku, a także w przypadku wprowadzania zmian w systemach. Po fazie pentestów warto również wykonać **re-test**, czyli weryfikację wprowadzonych zmian (sprawdzenie, czy zostały poprawnie zaimplementowane i nie doprowadziły do powstania nowych luk bezpieczeństwa).

4. Jak długo trwa test penetracyjny?

Pentest, w zależności od rodzaju, wielkości i poziomu skomplikowania badanej struktury może trwać od kilku dni do kilku tygodni.

SECURITYMAGAZINE.PL

E-HANDEL NA MUSZCE CYBER-PRZESTĘPCÓW. JAK POWINIEN BRONIĆ SIĘ RYNEK?

tpay

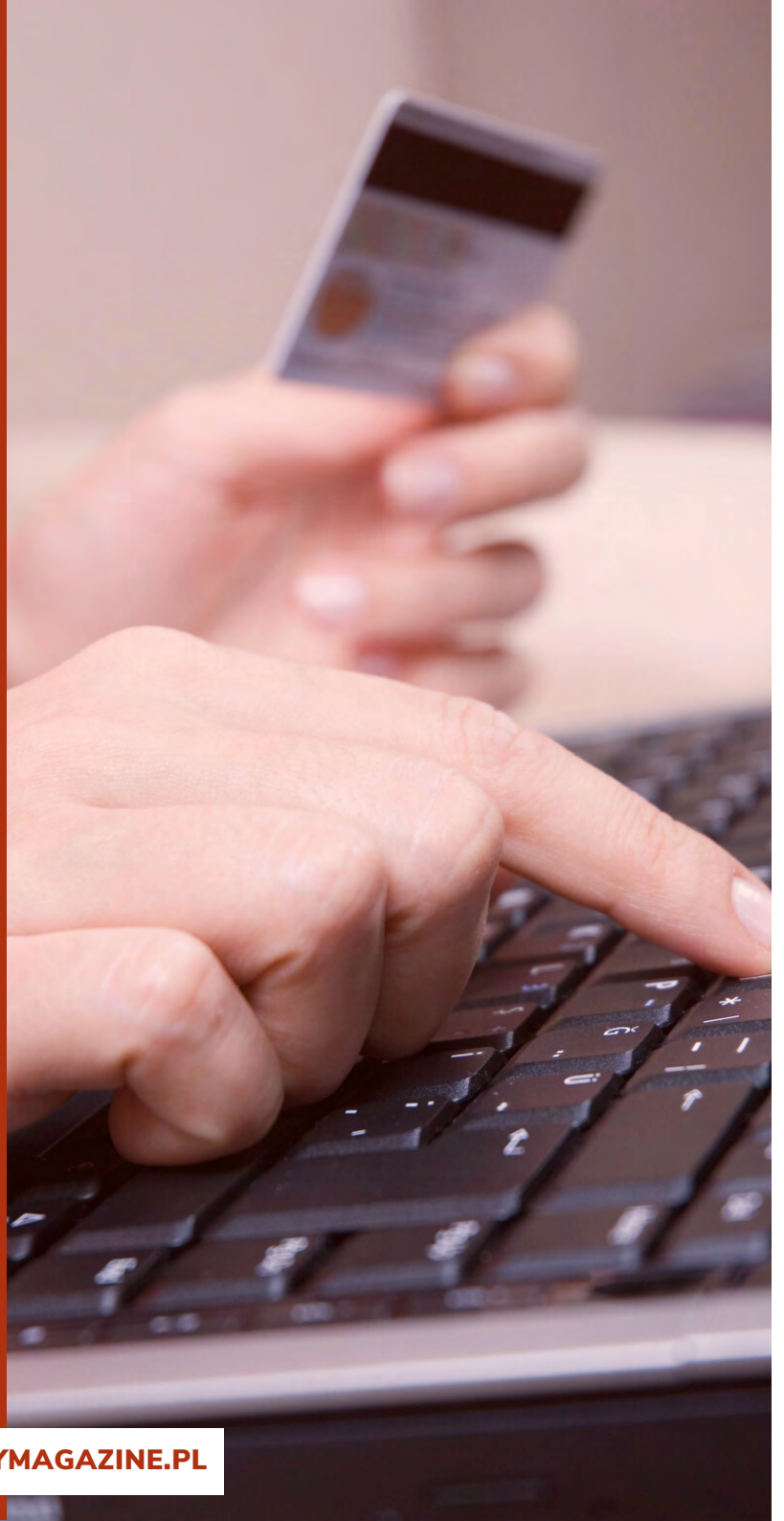
ARTYKUŁ KONKURSOWY

Oddaj swój głos na:

O tym, czy i jak Polacy dbają o bezpieczeństwo w trakcie aktywności w sieci, w jaki sposób bronić się przed cyberatakami i co w sprawie bezpiecznych zakupów robią właściciele sklepów internetowych we współpracy z operatorami płatności, rozmawiamy z Maciejem Pawlakiem odpowiedzialnym za zarządzanie ryzykiem i bezpieczeństwem informacji w Tpay.

ŻYJEMY W CZASACH, KIEDY LICZNE SPRAWY MOŻNA ZAŁATWIĆ ONLINE: ZAKUPY, OPŁACENIE RACHUNKÓW ETC. NIE MA PAN WRAŻENIA, ŻE POLACY TROCHĘ ZBYT MOCNO PRZESZLI DO PORZĄDKU DZIENNEGO NAD SWOJĄ AKTYWNOŚCIĄ W SIECI I WCIĄŻ ZBYT RZADKO PAMIĘTAJĄ O BEZPIECZEŃSTWIE, KTÓRE PRZECIEŻ JEST TAK ISTOTNE?

Przejście kupujących do kanału online to zupełnie naturalny proces, który dynamicznie przyspieszył w trakcie pandemii. Temat dotyczący bezpieczeństwa nieco nam jednak spowszedniał, a nadmiar informacji spowodował, że wiele kwestii zaczęło po prostu umykać. Choć więc informacji samych w sobie jest bardzo dużo, to mam wrażenie, że Polacy nie wiedzą, z jakich korzystać narzędzi, aby w tym natłoku wiadomości czuć się bezpiecznie. Warto zwracać uwagę na to, co i u kogo kupujemy oraz jaką metodę płatności wybieramy. Jeśli wchodzimy na stronę sklepu, w którym nie robiliśmy wcześniej zakupów, musimy zachować czujność, sprawdzić opinie o nim oraz poznać model płatności, z jakim jest zintegrowany. Nie uciekniemy przed rozwojem i kierunkiem, w jakim podążają aktywności online. To, co możemy i powinniśmy zrobić, to zadbać o ochronę w sieci. Jak wynika z badania Tpay, mimo że aż dla 90 proc. Polaków bardzo ważne jest bezpieczeństwo transakcji podczas e-zakupów, to jednak wielu konsumentów wciąż pada ofiarą różnych, coraz bardziej wymyślnych metod cyberprzestępców.



WŁAŚNIE. JAK POKAZUJĄ ANALIZY RYNKOWE, ŚWIADOMOŚĆ POLAKÓW W TAKIM OBSZARZE WIEDZY FINANSOWEJ, JAKIM JEST CYBERBEZPIECZEŃSTWO, Z ROKU NA ROK ROŚNIE, JEDNAK NA TLE INNYCH OBSZARÓW, JAK NP. OSZCZĘDZANIE, PŁATNOŚCI BEZGOTÓWKOWE CZY KREDYTY I POŻYCZKI, W TYM ASPEKCIE WYPADAMY NAJSŁABIEJ. JAK PAN SĄDZI, DLACZEGO TAK JEST?

To być może wynika z tego, że zbyt szybko i w zasadzie nagle przeszliśmy do kanału e-commerce. Sam przeskok był dynamiczny, nie był procesem płynnym, tzn. wiele osób nie było ani przygotowanych na tego typu aktywności, ani nie miało wystarczającej wiedzy, jak to zrobić. Warto zauważyć, że nasze nawyki w sieci nie dotykają wyłącznie zakupów czy płatności, ale także sposobu, w jaki poruszamy się w internecie w ogóle. Cyberbezpieczeństwo dotyczy całej naszej działalności online, a to z kolei przekłada się na to, jak w takich wrażliwych procesach będziemy się zachowywać. Jeśli więc Polakom brakuje podstawowej wiedzy na temat bezpiecznego poruszania się w internecie, to później nawet z pozoru drobny błąd, jak na przykład za słabe hasło do poczty e-mail, może kosztować bardzo wiele.

Często wydaje nam się, że skoro jesteśmy we własnym domu, a komputer ląduje na naszych kolanach, to jesteśmy bezpieczni. Tymczasem świadomy użytkownik jest mniej narażony na ataki, a jeśli zdarzy się przykry incydent, to wie, gdzie w pierwszej kolejności szukać pomocy.

AŻ JEDNA TRZECIA INTERNAUTÓW DEKLARUJE, ŻE ZOSTAŁA OSZUKANA PODCZAS ZAKUPÓW W SIECI. NA CO POLACY POWINNI ZWRÓCIĆ WIĘC UWAGĘ, ABY NIE DAĆ SIĘ OSZUKAĆ? SKĄD MOGĄ CZERPAĆ WIEDZĘ NA TEMAT CYBERBEZPIECZEŃSTWA?

Badania rynkowe pokazują, że jednym z pierwszych celów cyberprzestępców jest m.in. przejęcie skrzynki mailowej, dlatego z pozoru błahą kwestią, o której powinniśmy pamiętać, jest zarządzanie hasłami. Istnieje wiele narzędzi, które nam w tym pomogą, np. dedykowane aplikacje typu KeePass, przechowujące wszystkie hasła czy też autoryzacja SMS. Niestety często można spotkać się z opinią, że posiadanie wielu różnych haseł do różnych portali, bankowości etc. jest sporym utrudnieniem. Bezpieczna aktywność w sieci zawsze będzie kwestią kompromisu pomiędzy wygodą a odpowiednią ochroną. Jeśli chodzi o czerpanie wiedzy, to większość instytucji finansowych opracowuje i udostępnia własne poradniki. Często obszerne informacje są także publikowane na stronach WWW banków i instytucji finansowych w zakładce dotyczącej bezpieczeństwa. Na rynku jest również kilka portali internetowych, które udostępniają wiedzę w tym temacie, informują o aktualnych, popularnych wśród cyberprzestępców akcjach phishingowych. Rzeczywistość pokazuje jednak, że cyberataki to problem nie tylko dla zwykłego Kowalskiego, ale mogą one dotknąć też każdy biznes.

WEŹMY NA TAPET WŁAŚCICIELI E-SKLEPÓW – ONI TAKŻE SĄ UCZESTNIKAMI RYNKU FINANSOWEGO. JAK POKAZUJĄ DANE, TYLKO W UBIEGŁYM ROKU W 47 PROCENTACH ZA STRATY ZWIĄZANE Z CYBER-OSZUSTWAMI DOTYCZĄCYMI PŁATNOŚCI CYFROWYCH ODPOWIEDZIALNE BYŁY ZAKUPY ONLINE. JAKIEGO RODZAJU CYBERPRZESTĘPSTWA NAJCZĘŚCIEJ DOTYKAJĄ SEKTOR E-COMMERCE?

Pierwszą grupą ryzyka są dane kartowe, które mogą zostać wykradzione od konsumenta. W tym przypadku merchant, tj. właściciel e-sklepu, nie wie o tym, że ten proces ma miejsce, a co za tym idzie – jest on z punktu widzenia sprzedawcy bardzo trudny do wykrycia. Inny, również popularny mechanizm oszustwa, to klasyczny phishing – konsument otrzymuje np. maila z oszukańczej strony internetowej z pozornie bardzo atrakcyjną ofertą produktową. Konsument – dając się nabrać i klikając w link zawarty w mailu – zostaje przekierowany na fałszywą stronę płatności i bankowości, a ktoś wyprowadza jego środki finansowe. Mimo że wektor ataku jest w tym przypadku inny, to tego typu oszustwo również jest bardzo trudne do wykrycia.

W ostatnim czasie bardzo popularne jest też oszustwo metodą „na BLIKA". Oszust, przejmując należący do kogoś profil w mediach społecznościowych, kontaktuje się ze znajomymi osoby, której profil przejął, prosząc ich o wsparcie finansowe (uzasadnione nagłą, wyjątkową sytuacją) i podanie kodu do płatności mobilnych (BLIK). Reasumując, wszystkie strony sektora e-commerce muszą zachować należytą czujność – konsumenci powinni zwiększać swoją świadomość na temat metod i działań cyberprzestępców i wiedzieć, jak się przed nimi chronić, a właściciele e-sklepów muszą zapewniać swoim klientom bezpieczeństwo.

CO ZATEM MOŻE ODPOWIADAĆ ZA SZEROKO ROZUMIANE CYBERBEZPIECZEŃSTWO W TEJ BRANŻY?

Pojawia się szereg rygorystycznych regulacji prawnych, które są gwarancją jakości i bezpieczeństwa obsługiwanych transakcji. Przykładowo my, tj. Tpay, jako operator płatności musimy mieć całkowitą pewność, że właściciel e-sklepu, który jest aktywnym uczestnikiem rynku finansowego, jest w stu procentach zaufany: jego sklep istnieje, sprzedaje produkty/usługi i będzie wywiązywał się ze wszystkich zobowiązań na rzecz swoich klientów. Taka skrupulatna weryfikacja to przede wszystkim wymóg prawny. W przypadku właścicieli e-sklepów, poza zwiększeniem wydatków na cyberbezpieczeństwo, bardzo istotna jest edukacja – zarówno wśród nich samych, jak i płatników. Tym, co musi zrobić e-sprzedawca, jest umieszczenie regulaminu sklepu w widocznym miejscu – zobowiązuje go do tego Ustawa o prawach konsumenta. Zwiększone zaufanie wzbudza także informacja o dostępnych metodach płatności oraz współpracy z operatorem płatności. Warto więc umieścić logo, link i nazwę operatora, z którego usług korzysta sklep. Przydatne są również wszelkie instrukcje i poradniki dotyczące procesu zakupowego, które ułatwią konsumentowi zakupy i zwiększą jego zaufanie do sklepu. Sporo na ten temat piszemy na naszym blogu Tpay.

POROZMAWIAJMY ZATEM O KONIECZNYCH REGULACJACH RYNKU FINANSOWEGO. JAKIE MAMY OBECNIE REGULACJE, MAJĄCE ISTOTNY WPŁYW NA BEZPIECZEŃSTWO UCZESTNIKÓW PROCESU PŁATNOŚCI?

Instytucje płatnicze, aby świadczyć swoje usługi, muszą posiadać stosowną licencję. W Polsce taką licencję wydaje Komisja Nadzoru Finansowego w ramach Ustawy o usługach płatniczych. Zadaniem tego typu regulacji jest sprawienie, by sposób działania w internecie był bezpieczny i zrozumiały dla wszystkich uczestników rynku finansowego. Operatorzy płatności odpowiedni poziom ochrony zapewniają poprzez certyfikaty, jak chociażby PCI DSS (Payment Card Industry Data Security Standard), który jest potwierdzeniem spełniania norm wymaganych przez instytucje płatnicze VISA i MasterCard do dostarczania płatności kartami. Na kształt rynku finansowego ma także wpływ Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML), która zobowiązuje do identyfikowania i weryfikowania tożsamości właścicieli e-commerce, ustawa o świadczeniu usług drogą elektroniczną czy też ustawa RODO, normalizująca zakres i sposób przetwarzania danych osobowych.

DLACZEGO MERCHANT MUSI PRZEJŚĆ PROCES WERYFIKACJI I JAK MUSI ON BYĆ ZORGANIZOWANY?

Pomijając wcześniej wspomniany przeze mnie aspekt, jakim jest odgórny wymóg ustawowy, to wszystkie regulacje mają za zadanie zapewnić szeroko rozumiane bezpieczeństwo, zarówno merchantowi, jak i klientowi. Dla właściciela e-sklepu jednym z celów jest chociażby zbudowanie zaufanie ze strony płatnika. Posiadanie licencji jest bowiem równoznaczne z pozytywnym przejściem procesu licencyjnego.

DLACZEGO I W JAKI SPOSÓB REGULACJE MAJĄ SŁUŻYĆ BEZPIECZEŃSTWU KLIENTA, TJ. PŁATNIKA, A W JAKIM MERCHANTA?

Ideą jest bezpieczeństwo całego sektora i zabezpieczenie wszystkich uczestników rynku, tym samym budując efektywną i elastyczną przestrzeń do prowadzenia działalności e-commerce. Z jednej strony, ma to być bezpieczeństwo płatnika, który kupując daną usługę, chce mieć pewność, że środki, jakie przekaże za usługę lub produkt trafią do merchanta. Z drugiej zaś, merchant również powinien być pewny, że taka transakcja zostanie zrealizowana w sposób niezakłócony. Regulacje mają więc na celu zbudowanie efektywnej i elastycznej przestrzeni, zarówno do prowadzenia działalności e-commerce, jak i aktywności zakupowych.

JAKIE ZAGROŻENIA I RYZYKA POWSTAJĄ W MOMENCIE BRAKU POPRAWNIE PRZEPROWADZONEGO PROCESU WERYFIKACJI?

To pytanie trochę prowokacyjne (śmiech). Proces weryfikacji powinien być tak skonstruowany, żeby takich zagrożeń nie było. Proszę sobie wyobrazić sytuację, gdybyśmy jako operator płatności chociażby nie weryfikowali merchantów. Oczywiście, zdarza się, że fałszywe sklepy powstają i funkcjonują, sprzedając produkty w pozornie atrakcyjnych cenach. I faktycznie, dany sklep jakiś czas działa, buduje zaufanie u swoich klientów, po czym, gdy skala zamówień rośnie do poziomu dla niego intratnego, to zaczyna on przyjmować bardzo dużo zamówień, ale ich nie realizuje. To jest tylko jeden z wielu przykładów nadużyć, przestępstw, które w świecie e-commerce'owym mogą zaistnieć, dlatego też proces weryfikacji musi być dokładny i precyzyjny, aby takich sytuacji uniknąć.

Rozmawiała: Izabela Świątkowska

SECURITYMAGAZINE.PL

ARTYKUŁ KONKURSOWY

INFORMACYJNE BEZPIECZEŃSTWO PRZEDSIĘBIORSTWA PRZY OGRANICZONYM BUDŻECIE

Oleksandr Chyzhykov

intellias

Oddaj swój głos na:

Jeśli zastanawiałeś się nad wzmocnieniem bezpieczeństwa informacyjnego w swojej firmie, prawdopodobnie spotkałeś się ze stwierdzeniem, że wymaga to znacznych inwestycji. Rzeczywiście, oprogramowanie, infrastruktura i zespół specjalistów potrzebują finansowania, czasem - dużego. Ale co, jeśli pieniądze i ludzie nie wystarczą?

INWENTARYZACJA, OCENA I SKUPIENIE SIĘ NA TYM, CO WAŻNE

Przy ograniczonym budżecie nie rób wszystkiego na raz. Efektywniej jest skoncentrować się bardziej na ochronie najbardziej ważnych aktywów, takich jak dane osobowe, hasła, klucze, bazy danych, serwery, konta i tak dalej. Zrób inwentaryzację aktywów i przejdź do oceny ryzyka.

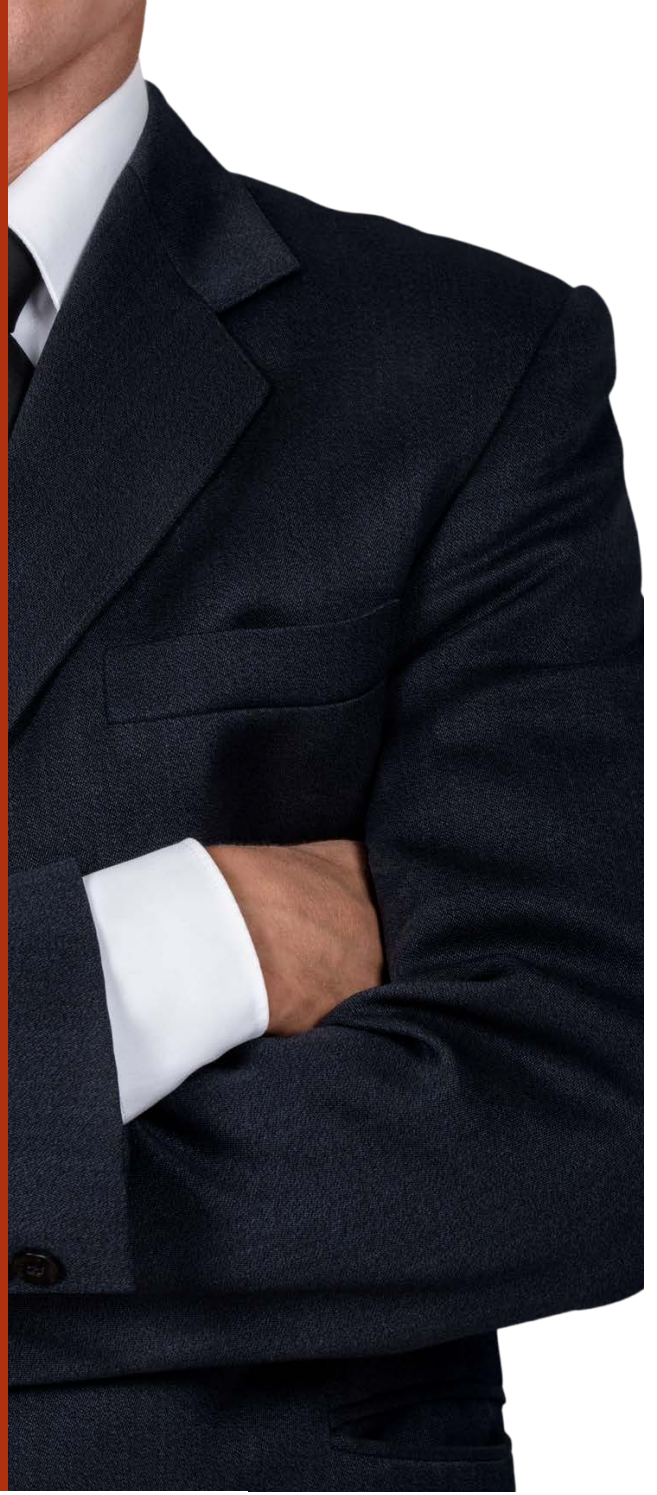
Podczas oceny ryzyka ważne jest, aby dokładnie zidentyfikować wrażliwości, zagrożenia i możliwe wektory ataku. Przykład:

- Utrata danych osobowych - RYZYKO.
- Kradzież laptopa specjalisty - ZAGROŻENIE.
- Kradzież miała miejsce na terenie firmy - WEKTOR.
- Laptop ma nieograniczony dostęp i brak szyfrowania dysku - WRAŻLIWOŚĆ.
- Następnie przejdź do PLANU postępowania z ryzykiem.

PLAN POSTĘPOWANIA Z RYZYKIEM

Priorytetem w twoim planie powinny być te ryzyka, które będą miały największy wpływ i prawdopodobieństwo. Nie zapomnij o wartości aktywów. Do obliczenia ryzyka można użyć następującego wzoru:

Kwota ryzyka = prawdopodobieństwo + wpływ * wartość aktywów.



Plan postępowania z ryzykiem powinien składać się z co najmniej trzech elementów:

ŚRODKI ORGANIZACYJNE

Zakaz lub ograniczenia na poziomie organizacyjnym, takie jak zakaz pracy z danymi osobowymi na urządzeniu prywatnym.

ŚRODKI TECHNICZNE

Ograniczenia techniczne, takie jak szyfrowanie dysku z danymi osobistymi, umożliwienie uwierzytelniania dwuskładnikowego i tak dalej.

ŚRODKI BEZPIECZEŃSTWA

Kontrola nad bezpieczeństwem informacji, monitorowanie zdarzeń związanych z bezpieczeństwem, incydentów, zarządzanie lukami w zabezpieczeniach i zmianami, zgodność itp.

W celu wzmocnienia bezpieczeństwa informacji przy ograniczonym budżecie zwróć także uwagę na następujące zalecenia:

1. Dobrze znane praktyki. Nie musisz wymyślać koła na nowo, aby wybudować wszystkie rodzaje bezpieczeństwa informacji. Korzystaj ze znanych i sprawdzonych praktyk, takich jak ISO 27001, ISO 27002 i NIST 800-53. Nie komplikuj polityk, standardów i wymagań - zrób je jasnymi i przejrzystymi, aby ułatwić wdrożenie. Każda komplikacja może stworzyć dodatkowe ryzyko, na przykład specjaliści nie rozumieją wymagań i po prostu je ignorują.

2 **Konta i uprawnienia.** Realizuj scentralizowany system zarządzania kontami i uprawnieniami (Identity and Access management). Jeśli Twój system będzie w stanie realizować SSO z Twoimi systemami i aplikacjami innych firm, uwierzytelnianie dwuskładnikowe i Role or Attribute based access model, będziesz w stanie zamknąć większość „standardowych" ryzyków przy minimalnym budżecie. Jeśli pracujesz z Office 365, użyj Azure AD do zarządzania kontami i szeregiem innych usług, które przydadzą się w zarządzaniu ryzykiem. Google G Suite ma również podobne usługi.

3 **Wendorzy i dostawcy.** Zawsze pytaj swoich wendorów i dostawców o dodatkowe opcje lub usługi w zakresie bezpieczeństwa informacji. Często możesz nawet nie wiedzieć, że masz już pod ręką narzędzia zabezpieczające, za które nie musisz płacić. Na przykład wendorzy mogą zapewnić usługi ochrony antywirusowej, monitorowania i zgłaszania incydentów.

4 **Macierz dostępu.** Stwórz macierz dostępu, aby zrozumieć funkcje i obowiązki swojego zespołu. W tym celu wystarczy zwykła tabela, w której wpiszesz stanowiska specjalistów i jakie dostępy powinni mieć.

Następnie za pomocą Identity and Access management stwórz niezbędne role i przydziel je specjalistom. Wraz z usprawnieniem procesów ta macierz będzie się uzupełniać, a Ty będziesz kontrolować dostęp całego zespołu.

5 **Centralizacja**. Korzystaj ze scentralizowanych rozwiązań do zarządzania zdarzeniami technicznymi i nie rób tego ręcznie. Dzięki temu zaoszczędzisz dużo czasu i zredukujesz tzw. „prostój”. Ponadto centralizacja pozwoli Ci szybko reagować na incydenty i redukować wpływ szybkich zmian.

6 **Kopie zapasowe.** Zorganizuj regularny proces tworzenia kopii zapasowych i przetestuj odzyskiwanie krytycznych danych. Nie warto robić kopii zapasowej wszystkiego. Zamiast tego zidentyfikuj krytyczne aktywy i skopiuj je. To zmniejszy budżet.

7 **Szukaj wrażliwości technicznych.** Zorganizuj regularny proces wyszukiwania wrażliwości technicznych w sieci, systemach operacyjnych i aplikacjach za pomocą narzędzi budżetowych, takich jak OpenVAS, Wazuh, Burp Suite, Software from Kali Linux. Korzystanie z tych narzędzi pozwoli zaoszczędzić i pokryć większość zagrożeń związanych z identyfikacją wrażliwości technicznych.

8 **Logging and Monitoring.** Zorganizuj proces Logging and Monitoring zdarzeń związanych z bezpieczeństwem z krytycznych systemów, aplikacji i serwerów za pomocą narzędzi budżetowych, takich jak ELK, Wazuh.

Narzędzia te zapewniają szeroką gamę narzędzi nie tylko do zbierania zdarzeń związanych z bezpieczeństwem, ale także pozwalają budować analitykę, aby reagować na incydenty i identyfikować zagrożenia z wyprzedzeniem.

8

Antywirus. Jeśli nie masz środków na zakup scentralizowanego systemu antywirusowego, skorzystaj z wbudowanego antywirusa w systemie Windows OS (Defender)

9

Szyfrowanie dysku. Aby zaoszczędzić pieniądze, możesz zrezygnować ze scentralizowanego systemu szyfrowania dysków. Zamiast tego użyj native szyfrowania Bitlocker w OS Windows, FileVault na MacOS i bezpłatnego Fscrypt lub Lux w systemie Unix

10

Poziomy reagowania. Podziel proces reagowania na incydenty na poziomie (Tiers). Zwyczajny IT Support Specialist będzie mógł pracować z incydentami bezpieczeństwa na pierwszej linii - na przykład analizować wiadomości o incydentach. Na innych poziomach konieczne będzie zaangażowanie zespołu ds. bezpieczeństwa informacji. Dzięki temu będziesz mógł reagować na incydenty całodobowo i podłączyć bardziej kompetentnych i wysoko opłacanych pracowników tylko wtedy, gdy jest to konieczne.

11

Automatyzacja. Maksymalnie zautomatyzuj procesy bezpieczeństwa informacji. Dzięki temu ominiesz zarówno czynnik ludzki, jak i zaoszczędzisz czas zespołu ds. bezpieczeństwa informacji.

Mając takiej celowej oceny i planu zarządzania ryzykiem, będziesz w stanie zbudować system bezpieczeństwa, który będzie potrzebował tylko procesów, systemów i ludzi. Po uporaniu się z krytycznymi ryzykami, opracowuj te, które są mniej priorytetowe. W ten sposób będziesz w stanie konsekwentnie radzić sobie ze wszystkimi zagrożeniami, równomiernie rozdzielając budżet i wysiłki.
Nie zapomnij również rozpocząć proces regularnego przeglądu aktywów, identyfikacji nowych wrażliwości i zagrożeń oraz ponownej oceny ryzyka. Powinieneś również regularnie oceniać już wdrożony plan, aby upewnić się, że został wybrany prawidłowo. Do oceny ryzyka zalecam stosowanie następujących metodologii i frameworków - ISO 27005, ISO 27001, IRAM2, NIST SP800-30, OCTAVE.

SECURITYMAGAZINE.PL

ARTYKUŁ KONKURSOWY

TECHNOLOGIZACJA BRANŻY SECURITY. OSZCZĘDNOŚCI A ROSNĄCA PRESJA PŁACOWA

Tomasz Wojak

Oddaj swój głos na:

Rozwój nowych technologii, digitalizacja, zmiany wywołane przez pandemię i wzrost kosztów dla przedsiębiorców spowodowały duże zmiany na rynku usług. Szczególnie dotknęły one branżę security.

Coraz więcej firm w ramach szukania oszczędności skłania się ku inwestycjom w nowe technologie obok zatrudniania nowych pracowników fizycznych. Czy monitoring, zdalny nadzór obiektów i szeroko pojęta technologizacja jest przyszłością sektora bezpieczeństwa?

Przed marcem 2020 roku branża security notowała wzrosty rok do roku (według Frost& Sullivan nawet 7-9% rocznie). Jednak pandemia i dynamiczny wzrost nowych technologii diametralnie zmieniły sytuację – w zaledwie pół roku od jej rozpoczęcia aż 77% spółek tego sektora dotknęły poważne cięcia. Zwłaszcza firmy z branży handlowej, transportowej i związane z edukacją ograniczały koszty związane z zabezpieczeniem.

Co więcej, eksperci przewidują, że w najbliższym czasie sytuacja nie tylko nie zmieni się, ale że firmy security będą szukać kolejnych oszczędności. Innymi słowy, niewiele wskazuje na to, że rynek z 2019 roku będzie możliwy do odbudowania. Na popularności zyskują natomiast rozwiązania zdalne oraz pomagające zabezpieczyć pracę zdalną.

Wyzwaniem stały się przede wszystkim rosnące koszty utrzymania firmy i presja płacowa. Oszczędzanie na ochronie i systemach bezpieczeństwa staje się wyjątkowo trudne także z innego powodu. Wraz z rozwojem technologii rośnie zuchwałość sprawców. Dotyczy to nie tylko drobnych kradzieży w sklepach, ale przede wszystkim poważnych zdarzeń, takich jak włamania i przywłaszczenie mienia

w większym zakresie. Istnieje jeszcze inny aspekt, do którego przyczyniła się pandemia: rozwój technologiczny i wysyp nowych narzędzi IT dla branży security.

OCHRONA TECHNICZNA W NOWEJ RZECZYWISTOŚCI

Obserwacja w czasie rzeczywistym, zdalny nadzór obiektów, czy monitoring wideo zapewniają firmom dostęp do informacji o bezpieczeństwie w wygodny i prosty sposób. Jednak technologizacja branży security staje się odpowiedzią także na rosnącą presję płacową.

Aktualnie branża ochrony osób i mienia dotkliwie odczuwa skutki sytuacji gospodarczo-ekonomicznej w Polsce. Galopująca inflacja, czy waloryzacja wynagrodzenia minimalnego wymuszają na firmach zajmujących się bezpieczeństwem zmiany. Przedsiębiorstwa branży security podnoszą stawki za swoje usługi, ale jednocześnie poszukują nowych rozwiązań. **Wśród nich jest przejście od ochrony fizycznej do technicznej.** Jak wskazują badania, ochrona techniczna na koniec 2020 roku uzyskała poziom 40-50% rynku ochrony fizycznej (dla porównania przed 2016 rokiem miała szczątkowy udział w ochronie mienia).

Według prognoz udział ochrony technicznej będzie tylko wzrastał, a już na koniec 2025 roku znacząco przewyższy udział klasycznej ochrony fizycznej. Wśród przyczyn jest między innymi oszczędność finansowa.

Pracownicy ochrony fizycznej to często osoby, które zarabiają najniższą krajową. To powoduje, że nadchodzące wraz z nowym rokiem podwyżki płacy minimalnej mocno uderzą w firmy security. Szacuje się, że w efekcie pracę może stracić nawet 25 tys. osób, zwłaszcza, że rozwój nowych technologii daje coraz większe możliwości wykorzystania rozwiązań smart w branży security.

FIRMY INWESTUJĄ W ROZWIĄZANIA SMART SECURITY

Nowe technologie mają istotny wpływ na całe nasze życie: od pracy i nauki, aż po wsparcie w codziennych czynnościach. Pojawia się więc pytanie, dlaczego w branży security miałoby być inaczej? Tym bardziej, że systemy zdalnego monitoringu sprawdzają się w wielu organizacjach – szczególnie w firmach o regularnych godzinach pracy lub w takich, które nie wymagają obecności fizycznej w da-

nej lokalizacji (na przykład zamknięte place budowy, hurtownie, składy budowlane, magazyny czy salony samochodowe).

To powoduje, że z roku na rok rośnie popularność usług ochrony w postaci monitoringu i zdalnego dozoru obiektów. Firmy decydują się na usługi monitoringu w oparciu, na przykład, o systemy telewizji przemysłowej czy systemy sygnalizacji włamania. Poza rosnącymi wynagrodzeniami tendencja ta jest efektem wzrostu cen za usługi ochrony. Te z kolei wynikają z rosnących kosztów ochrony fizycznej oraz z wprowadzania nowych, tańszych rozwiązań technologicznych. Wydaje się, że inwestycja w rozwój zwiększający potencjał centrum monitorowania staje się nieunikniona dla większości przedsiębiorstw.

W branży security zwrot w kierunku nowych technologii jest szczególnie zauważalny. Po zmianach wywołanych pandemią zwiększyło się zainteresowanie rozwiązaniami technologicznymi jako wsparciem obecności człowieka przy chronionej osobie czy w obiekcie.

Coraz częściej przedsiębiorcy wybierają rozwiązania ze zdalnym nadzorem wideo, zastosowaniem nowoczesnych technologii również w kontroli dostępu, nadzorze wideo czy detekcji ruchu.

Co więcej, zwrot z inwestycji w monitoring może nastąpić zaledwie po kilku miesiącach użytkowania..

SZTUCZNA INTELIGENCJA, CHMURY I DRONY W SŁUŻBIE BRANŻY SECURITY

Nieoceniona w nowoczesnych narzędziach do monitorowania, nadzoru i zapewniania bezpieczeństwa okazuje się być sztuczna inteligencja. Pozwala ona, na przykład, na rozpoznanie ruchomych obiektów, takich jak człowiek, zwierzę czy pojazd. Ponadto umożliwia rozróżnienie fałszywych alarmów, które mogą zostać wywołane przez obiekty, takie jak ruchome gałęzie, liście, zwierzęta, nagłe zmiany poziomu oświetlenia, cienie, opady atmosferyczne i wiele innych.

Jednym z filarów transformacji branży security w stronę nowych technologii jest wykorzystanie rozwiązań chmurowych.

W Polsce jak dotąd narzędzie to nadal traktowane jest przez przedsiębiorców branży ochroniarskiej ostrożnie, choć, jak wskazują prognozy, istnieje duża szansa, że ulegnie to zmianie. Rozwiązania chmurowe doskonale sprawdzą się w komunikacji marketingowej, obsłudze klienta czy jako wsparcie grup i patroli interwencyjnych. To nowoczesne narzędzie umożliwia również zastosowanie automatyzacji żmudnych oraz czasochłonnych procesów, a tym samym oszczędność

czasu. Na szybką i skuteczną weryfikację fałszywych alarmów pozwolą również drony, obsługiwane przez odpowiednio przeszkolony personel. Urządzenia te umożliwiają także sprawne patrolowanie nawet rozległego terenu przy niewielkich kosztach operacyjnych.

Firmy z branży security, które chcą zoptymalizować rozwiązania, z których korzystają, a także przygotować się na wyzwania, jakie niesie przyszłość, już teraz mogą rozważyć zastosowanie innowacyjnych technologii, które pozwolą stworzyć skuteczne systemy zabezpieczenia technicznego.

Przy tym należy pamiętać, że nowe technologie, choć niosą ogromną wartość dla branży security, nie zastąpią w pełni człowieka, który często podejmuje trudne decyzje i odpowiada za działania wedle procedur i przepisów prawa.

Szczególne znaczenie ma to w sytuacjach nagłych, kiedy trzeba na przykład przeprowadzić ewakuację, udzielić pierwszej pomocy, czy też użyć środków przymusu bezpośredniego.

PATRONAT
SECURITY MAGAZINE

POLSECURE 2023

MIĘDZYNARODOWE TARGI 25-27 KWIETNIA

Zaplanowane w terminie od 25 do 27 kwietnia Międzynarodowe Targi POLSECURE będą okazją do zapoznania się z ofertą firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania łączności, dowodzeniu czy kontroli oraz do wymiany doświadczeń i rozmów o rzeczywistych potrzebach służb mundurowych.

Wydarzenie odbędzie się po raz drugi pod Honorowym Patronatem Ministra Spraw Wewnętrznych i Administracji i po raz kolejny organizowane jest przy wsparciu Komendy Głównej Policji. Partnerem strategicznym jest Grupa WB. Wśród wystawców, którzy do tej pory potwierdzili swój udział w wydarzeniu są m.in. Enigma Systemy Ochrony Informacji Sp. z o.o., GLOMEX-MS POLSKA Sp.z o.o., Griffin Group S.A. Defence Sp. k., Grupa WB, HOLSTERS HPE Polska Grzegorz Szymański, KLIMAWENT S.A., , LUBAWA, MEGMAR LOGISTICS & CONSULTING Sp. z o.o., MODULAR SYSTEM, Spółki Polskiej Grupy Zbrojeniowej, TRANSCOM INTERNATIONAL, TVPRZEMYSLOWA NOWAK SPÓŁKA KOMANDYTOWA, WORKS 11 Sp.z o.o., ZDUNEK PREMIUM Sp. z o.o. i inne.

Targi dedykowane są służbom odpowiedzialnym za bezpieczeństwo publiczne, w tym Policji, Straży Granicznej, Straży Pożarnej, a także Służbie Ochrony Państwa i Służbie Więziennej. Ofertą mogą też być zainteresowane służby specjalne, Krajowa Administracja Skarbowa oraz organizacje ratownicze GOPR, TOPR, WOPR. POLSECURE 2023 będzie miało też ofertę skierowaną do ratowników medycznych. Merytorycznym uzupełnieniem wystawy będzie międzynarodowa konferencja organizowana przez KG Policji.

POLSECURE dołączyło w 2022 roku do portfolio Targów Kielce obok wystaw skierowanych do służb mundurowych.

Targi Kielce
exhibition & congress centre
30 LAT YEARS

polsecure

II Międzynarodowe Targi POLSECURE

25-27.04.2023

WYDARZENIA TOWARZYSZĄCE

- **Międzynarodowa Konferencja Policyjna**
  Zakres tematyczny: cyberbezpieczeństwo, laboratorium kryminalistyczne, logistyka
- **Pokazy dynamiczne**
- **Prezentacje sprzętu**

Więcej informacji na **polsecure.targikielce.pl**

Patronat Honorowy

Minister Spraw Wewnętrznych i Administracji

POLICJA

SŁUŻBA WIĘZIENNA

RCB

LOTNICZE POGOTOWIE RATUNKOWE

NCBR
Narodowe Centrum Badań i Rozwoju

INSPEKCJA TRANSPORTU DROGOWEGO

ABW

DZIAŁANIA SECURITY AWARENESS W ORGANIZACJI

Aleksandra Kornecka

Świadomość o bezpieczeństwie (z ang. security awareness) praktykowana w poprzek całej organizacji staje się coraz ważniejsza nie tylko pod kątem stricte cyberbezpieczeństwa, ale również z powodu potrzeb zapewnienia ciągłości biznesowej organizacji.

W dobie powszechności ataków phishingowych, ataków typu ransomware, czy prób spowodowania odmowy dostępu (ataki DDoS) podstawowa wiedza o tym, jak się chronić, powinna zagościć u pracowników na stanowiskach zarówno inżynierskich, jak i biznesowych.

W niniejszym artykule opiszę jak zbudować zestaw działań, które pomagą zadbać o świadomość o (cyber)bezpieczeństwie dla organizacji, nawet kiedy dysponuje ona niewielkim zespołem ds. cyberbezpieczeństwa i budżetem. Podzielę się pomysłami na regularne szkolenia, jak i okazjonalne działania, kampanie oraz ich przykładowe implementacje.

DEFINIOWANIE OBSZARU

Świadomość o bezpieczeństwie (z ang. security awareness) w organizacji oznacza wiedzę pracowników o realnych zagrożeniach, umiejętność ich rozpoznania oraz odpowiedniego zareagowania na nie.

Zagospodarowanie tego obszaru w organizacji będzie oznaczało zaprojektowanie go w tak, by utrzymywać poziom tej wiedzy u pracowników na satysfakcjonującym poziomie. Drugim elementem jest maksymalizacja odporności czyn-

nika ludzkiego w organizacji na zagrożenia.

Każda organizacja w zależności od swego kontekstu, skali oraz potrzeb biznesowych powinna dokonać wyboru praktyk z obszaru security awareness w odniesieniu do swoich realiów. Również sposób realizacji praktyk przytoczonych w niniejszym artykule powinien zostać skrojony na miarę potrzeb danej organizacji, w zależności od kultury organizacji, narzędzi oraz możliwości budżetowych.

W celu doboru środków, treści i formatów działań warto postawić na współpracę działu ds. cyberbezpieczeństwa oraz działu komunikacji, marketingu, Public Relations, bądź dowolnego działu, którego punktem skupienia jest dopasowywanie treści do ludzkiego odbioru.

Stan, do którego organizacje powinny dążyć, to stan wbudowania świadomości o bezpieczeństwie w kulturę organizacji i promowanie postawy odpowiedzialności każdego pracownika, menedżera i lidera za bezpieczeństwo ze swojej pozycji i w ramach swoich obowiązków. Aby taka sytuacja miała miejsce należy dostarczyć im odpowiednich narzędzi oraz wzorców zachowań i dobrych praktyk, oraz nagradzać za ich stosowanie w różny sposób (nie tylko za pomocą środków pieniężnych).

By świadomość o bezpieczeństwie zagościła na stałe w kulturze organizacji, strategia tego obszaru musi być zbieżna z wizją organizacji najwyższego kierownictwa i przez nie promowana. Z kolei działania oddolne wpływają na zrozumienie i rozpowszechnianie dobrych praktyk w codziennych obowiązkach.

W kolejnych sekcjach prezentuję pomysły na po-

szerzanie świadomości o bezpieczeństwie w organizacji.

DOSTĘP DO DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA

Ważnym aspektem dbania o świadomość o bezpieczeństwie w organizacji jest łatwy dostęp do dokumentów zawierających polityki bezpieczeństwa oraz zasady panujące w organizacji dotyczące takich kwestii, jak:

- kontrola dostępu,
- szyfrowanie,
- kopie zapasowe,
- praca zdalna,
- zarządzanie urządzeniami mobilnymi i stacjami roboczymi,
- zgłaszanie incydentów.

DEDYKOWANY KANAŁ KOMUNIKACJI DOTYCZĄCY BEZPIECZEŃSTWA

Istotnym czynnikiem zwiększającym propagację oraz zasięg wiedzy oraz aktualnych informacji o bezpieczeństwie oraz zagrożeniach jest stworzenie dedykowanego kanału komunikacji w medium używanym przez całą organizację np. na czacie firmowym bądź w intranecie firmowym.

Treści pojawiające się na takim kanale komunikacji to przykładowo:

- cykliczne informacje o obowiązkowych szkoleniach do wykonania przez pracowników,

- ostrzeżenia ad hoc o zaistniałych niebezpieczeństwach (np. wyciekach danych w zewnętrznym oprogramowaniu, które mogą wpłynąć na pracę naszej organizacji),
- informacje o nowych podatnościach (vulnerabilities) dotyczących oprogramowania używanego w naszej organizacji,
- artefakty okazjonalnych kampanii z zakresu świadomości o bezpieczeństwie, takie jak na przykład Miesiąc Świadomości Cyberbezpieczeństwa, Dzień Prywatności, Dzień Bezpiecznego Internetu itp.,
- okazjonalne pytania pracowników do zespołu ds. cyberbezpieczeństwa, na które odpowiedzi często pozwalają im szybciej internalizować wiedzę i lepiej stosować się do polityk bezpieczeństwa.

Kolejnym istotnym czynnikiem jest regularne prowadzenie takiego kanału komunikacji. W znacznym stopniu można zautomatyzować prowadzenie kanału dzięki dostępnym integracjom w ramach używanych narzędzi, bądź gotowych wzorców automatów, a także dodaniu zewnętrznych skryptów automatyzujących działania.

Czy będzie to format newslettera mailowego, kanału na komunikatorze Slack bądź Teams, czy też grupy na zamkniętym forum firmowym, z pewnością pomoże to pracownikom odszukać i śledzić informacje.

SZKOLENIE DLA NOWYCH PRACOWNIKÓW (SECURITY ONBOARDING)

Zagadnienia bezpieczeństwa systemów informatycznych oraz poufność danych powinny znaleźć się w programie obowiązkowych szkoleń dla nowych pracowników, niezależnie od ich roli oraz pozycji w hierarchii organizacji. Każdy może być obiektem ataku lub źródłem podatności.

W wersji minimalnej powinno być to kilka punktów lub slajdów w szkoleniu ogólnym, a w wersji idealnej osobne dedykowane szkolenie prowadzone przez pracownika zespołu ds. cyberbezpieczeństwa. Najważniejsze dokumenty polityki bezpieczeństwa organizacji powinny zostać załączone do szkolenia lub włączone w treści samego szkolenia.

Dobrą praktyką jest stosowanie quizu lub testu sprawdzającego na koniec szkolenia, bądź inne formy wzmocnienia przekazu. Takie szkolenie powinno zostać przypominane co najmniej raz do roku dla aktualnych pracowników.

SECURITY CHAMPIONS PROGRAMME (PROGRAM LIDERÓW BEZPIECZEŃSTWA)

Program ten jest kluczowy do utrzymania wysokiej świadomości o zagrożeniach wśród kadry technicznej, ale może świetnie posłużyć również osobom piastującym stanowiska stricte biznesowe. Dzięki niemu można odciążyć zespół ds. cyberbezpieczeństwa pod względem dbania o pojedyncze projekty i zespoły oraz wzmocnić oddolnie postawę bezpieczeństwa (security posture) w całych zespołach.

Istotą programu security champions jest zbudowanie w organizacji społeczności (community) osób zainteresowanych tematyką cyberbezpieczeństwa, które chcą pogłębiać swoją wiedzę w tym zakresie oraz być liderami bezpieczeństwa w swoich zespołach. Stają się oni również pierwszymi punktami kontaktu dla zespołu ds. cyberbezpieczeństwa (points of contact).

Członkowie społeczności mogą uzyskiwać rozmaite korzyści (niekoniecznie finansowe) w zamian za swoje zaangażowanie oraz krzewienie zasad bezpieczeństwa w zespołach.

Poza swego rodzaju prestiżem wśród zespołów, security champion może otrzymać:

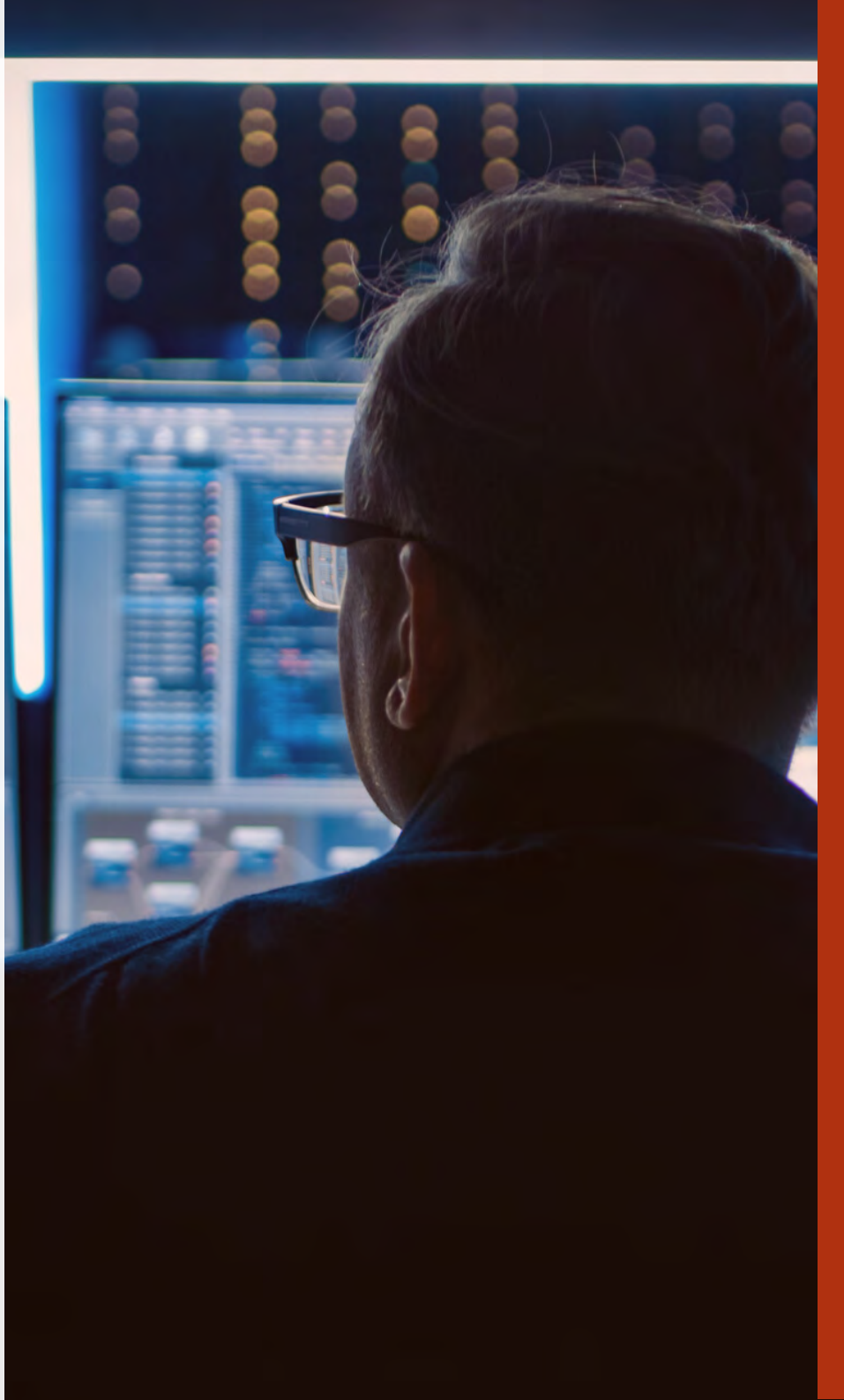
- możliwość uczestnictwa w wymarzonych szkoleniach,
- wyjazd na konferencje branżowe,
- dostęp do platform treningowych typu HackTheBox
- subskrypcję albo udział w zawodach typu Capture The Flag.

Oczywiście, jeśli budżet organizacji na to pozwala, można również nagradzać okresowymi nagrodami rzeczowymi, które są praktycznymi pomocnikami w pracy. Mogą to być przykładowo słuchawki, gadżety chroniące komputer, brandowane gadżety firmowe itp.

Szkolenia i zawody Capture The Flag mogą być też organizowane w samej organizacji przez zespół ds. cyberbezpieczeństwa, jeśli pozwalają na to zasoby zespołu.

Dobry program powinien zawierać formę grywalizacji, w wyniku której członek społeczności może zdobywać kolejne poziomy wtajemniczenia, poziomy wiedzy, a tym samym poziomy korzyści.

W przytoczonych poniżej przykładach zakładamy, że program security champions dedykowany jest pracownikom na stanowiskach inżynierskich.



Każdy kandydat na security championa powinien zrealizować podstawowe zadania wymagane do otrzymania miana security championa. Przykładowo, wykonać podstawową analizę ryzyk dla swojego zespołu albo sprawdzić, czy jego zespół spełnia podstawowe wymogi nakładane przez zespół ds. cyberbezpieczeństwa na proces wytwórczy aplikacji.

Przykładem takiej grywalizacji może być przyznawanie odznak (lub tzw. badges) o różnych kolorach symbolizujących zaawansowanie security championa. Kolejne odznaki (np. biała > żółta > zielona > niebieska > czarna) można osiągać po spełnieniu warunków przewidzianych na dany kolor. Im wyższa odznaka, tym ilość odznak do zdobycia powinna być bardziej limitowana. Po osiągnięciu czarnej odznaki security champion może ubiegać się o przyjęcie do zespołu ds. cyberbezpieczeństwa.

Warunki do spełnienia, by uzyskać konkretną odznakę, mogą być różne. Udokumentowane ukończenie poszczególnych szkoleń, realizacja konkretnych zadań dla swojego zespołu, aktywności w ramach samego programu security champions.

Przykład zestawu warunków na uzyskanie pierwszego poziomu wtajemniczenia i pierwszej odznaki:

- ukończenie szkolenia uczącego jak wykorzystać program statycznej analizy kodu skanujący repozytoria zespołu pod kątem podatności aplikacji na zagrożenia wylistowanie w OWASP Top Ten,
- zintegrowanie wspomnianego programu w cykl wydania kodu w repozytoriach zespołu,
- monitorowanie znajdowanych przez program podatności i egzekwowanie ich naprawy w zespole,

- przygotowanie i przeprowadzenie prezentacji na temat aspektu bezpieczeństwa istotnego dla organizacji.

Warunki pozwalające uzyskać kolejne kolory odznak powinny charakteryzować się coraz większą złożonością lub stopniem trudności, ale pozostawać nadal przydatne dla bezpieczeństwa organizacji oraz zespołów.

Prowadzenie programu security champions jest sporym obciążeniem czasowym, ale może mieścić się w ramach etatu osoby, najlepiej z zespołu ds. cyberbezpieczeństwa, która dysponuje dobrymi umiejętnościami miękkimi i komunikacyjnymi.

W zależności od ilości członków programu, zasobów szkoleniowych oraz aktywności członków społeczności, zaangażowanie może się wahać między 5 a 10 roboczogodzin tygodniowo.

INNE FORMY WZMACNIANIA ŚWIADOMOŚCI O BEZPIECZEŃSTWIE W ORGANIZACJI

Poza opisanymi już szerzej działaniami, inne warte realizacji to:

- **CyberSecurity Awareness Month** (Miesiąc Świadomości o Cyberbezpieczeństwie) - miesiąc, na przykład październik, pełen prezentacji, filmów i materiałów edukacyjnych na tematy bezpieczeństwa najważniejsze aktualnie dla organizacji,
- **Privacy Day** (Dzień Świadomości o Prawie do Prywatności),
- **trening rozpoznawania i reagowania na wiadomości phishingowe,** próby wyłudzeń danych (email, smishing, vishing, social media),
- **kampanie wewnątrz organizacji** symulujące phishing (a potem trening wzmacniający dla pracowników, którzy ulegli oszustwom),
- **wykorzystanie ogólnofirmowych spotkań wymiany wiedzy** (Technical Exchange, Knowledge Sharing sessions itp.) do prezentacji uświadamiających o bezpieczeństwie oraz zagrożeniach.

PODSUMOWANIE

W obecnych czasach warto inwestować w odpowiednie zabezpieczenia. Jednym z “nietechnicznych”, ale niezwykle istotnych zabezpieczeń jest świadomość członków organizacji o zagrożeniach oraz sposobach ochrony.

PATRONAT
SECURITY MAGAZINE

DRUGA EDYCJA
CYBERTEK TECH FESTIVAL

DOŁĄCZ DO NAS
I ENJOY THE CYBER!

CyberTek Tech Festival to II edycja profesjonalnego, międzynarodowego, wyjątkowego wydarzenia budującego społeczność specjalistów w zakresie cyberbezpieczeństwa sieci przemysłowych. Tegoroczna konferencja odbędzie się pod hasłem: ENJOY THE CYBER.

Wymieniaj doświadczenia, dyskutuj o dobrych praktykach w doborowym towarzystwie i atmosferze sprzyjającej kreatywności oraz nawiązywaniu znajomości, które zaprocentują.

CyberTek Tech Festival jest w całości poświęcony cyberbezpieczeństwu systemów przemysłowych, natomiast jego nadrzędnym celem jest upowszechnianie wiedzy i budowanie partnerstwa wokół idei „Ekosystemu cyberbezpieczeństwa", która propaguje pryncypia współpracy na rzecz cyberbezpiecznego przemysłu, w tym kontekście wdrażania w życie Ustawy o KSC.

Wydarzenie kierowane jest przede wszystkim do osób, na których spoczywa odpowiedzialność za stworzenie, skuteczne wdrożenie lub realizację programów bezpieczeństwa obejmujących sieci i systemy przemysłowe.

To konferencja tworzona dla ekspertów przez ekspertów w dziedzinie cyberbezpieczeństwa.

Tematyka poruszana podczas konferencji:

- Red Team, Pentesty, Offensive Security w OT
- Blue Team (GRA, branżowe scenariusze)
- Incident Response, Security Operations Center (SOC), Security, Orchestration and Automation (SOAR) dla OT
- Specyfika Digital Forensics/Incident Response dla elementów systemów automatyki (PLC, HMI)
- Śledzenie zagrożeń w OT, szacowanie ryzyka i ciągłość działania
- Zapewnienie zgodności, Audyt Cyber w OT, KSC, NIS2, IEC62443
- Nadzór i zarządzanie bezpieczeństwem OT/IT; Cyberprogram w firmie
- Architektura i narzędzia (cyber)bezpieczeństwa w OT
- Monitorowanie OT; #SBOM
- Dostęp zdalny
- Historie i wpadki z obszaru bezpieczeństwa IT/OT, doświadczenia z wdrożeń
- Trendy i technologie, zmieniające sieci przemysłowe, czyli jak na paradygmaty cyber w OT wpływają: chmura, 5G, IoT
- Zero Trust vs. IoT
- Software Defined Network (SDN) w ICS
- Migracja z SDH – MPLS-TP
- i wiele innych.

CyberTek Tech Festival

Muzeum Śląskie, Katowice

24-26.05.2023

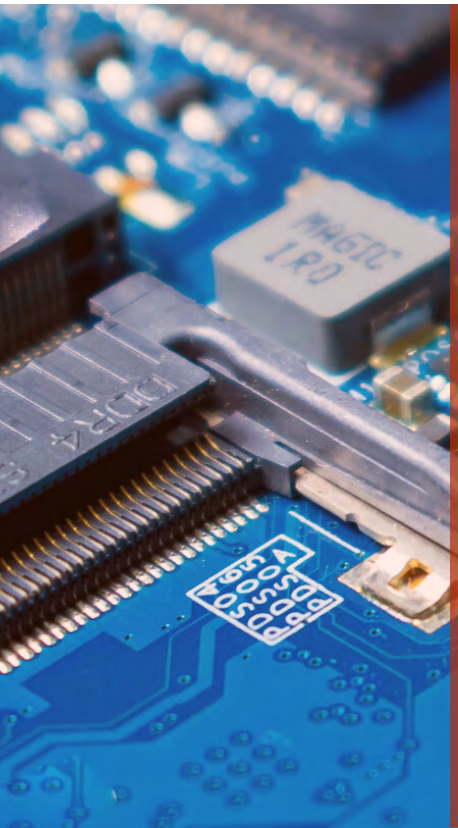
10% ZNIŻKI DLA NASZYCH CZYTELNIKÓW

Skontaktuj się z organizatorem mailowo, aby otrzymać rabat: konferencja@cybertek.com.pl

Szczegóły s. 47

PAMIĘCI ZMIENNOFAZOWE

Paweł Kaczmarzyk
Serwis komputerowy Kaleron



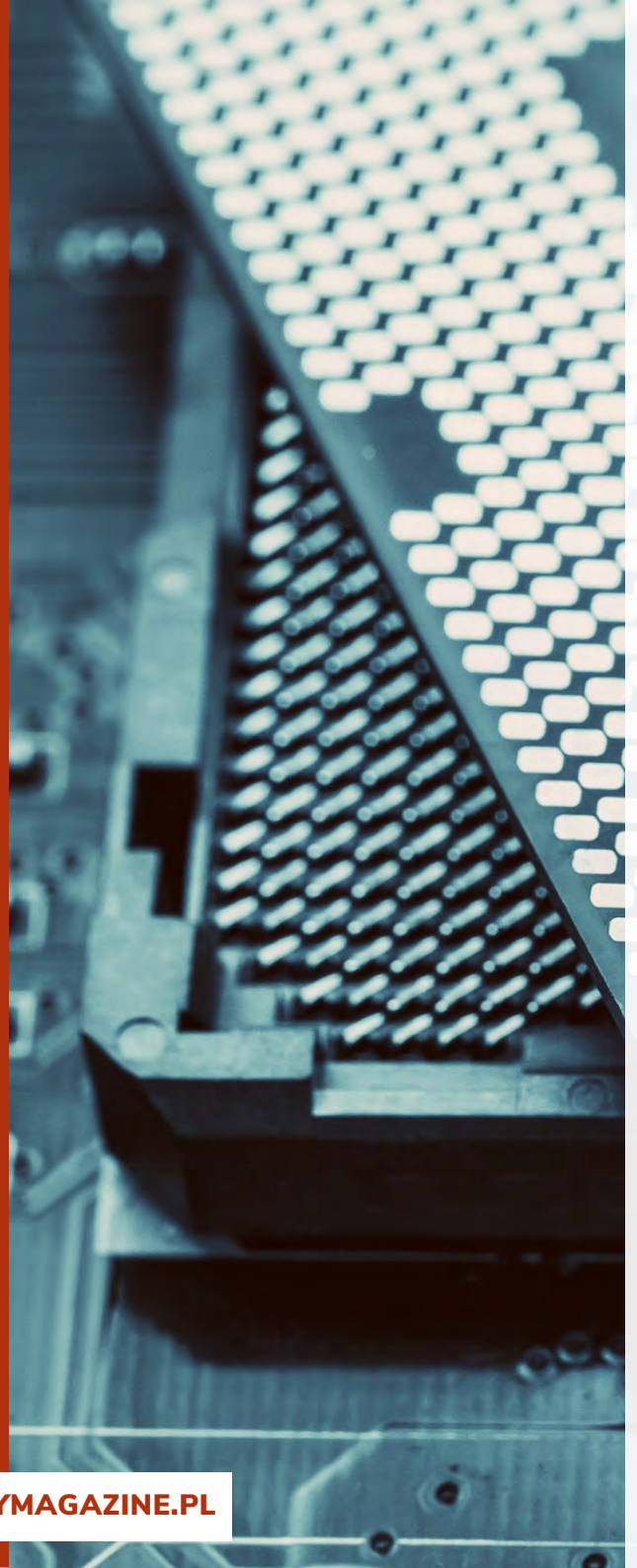
Kiedy rozmawiamy o nośnikach danych, zwykle mamy na myśli nośniki magnetyczne: dyski twarde i taśmy, lub półprzewodnikowe, wykorzystujące układy typu Flash-NAND: SSD, pendrivy, karty pamięci oraz układy pamięci wbudowane w różnego rodzaju urządzenia mobilne, internetu rzeczy, przemysłowe itd. Tymczasem trochę niepostrzeżenie wśród nas pojawiła się nowa technologia przechowywania danych. Pamięci zmiennofazowe. Jeśli ktoś korzystał z rozwiązania Intela Optane, to często bez pełnej świadomości tego, co ma w komputerze.

STAN FIZYCZNY I JEGO LOGICZNA INTERPRETACJA

Podstawą funkcjonowania techniki cyfrowej są stany fizyczne interpretowane jako logiczne zera i jedynki. W zależności od tego, z jakim urządzeniem mamy do czynienia, takim stanem fizycznym mogą być np. określone poziomy napięć, zgromadzony ładunek elektryczny, namagnesowanie powierzchni lub rezystancja. Pamięci zmiennofazowe (ang.: Phase Change Memory – PCM) należą do kategorii pamięci rezystywnych, w których stany logiczne i ich zmiany powiązane są z rezystancją. Wykorzystują one odwracalne zmiany fazy pomiędzy stanem krystalicznym, a amorficznym chalkogenków – zazwyczaj stopu germanu (Ge), antymonu (Sb) i telluru (Te). Od pierwszych liter symboli chemicznych stop ten zwykle jest nazywany GST.

Komórka bitowa pamięci zmiennofazowej składa się z tranzystora oraz z rezystora wykonanego z umieszczonego pomiędzy dwiema elektrodami chalkogenku. Najpopularniejsze rozwiązanie nazywane jest potocznie lancą lub grzybkiem. W niektórych wariantach otwierających drogę do stworzenia trójwymiarowych pamięci zmiennofazowych dodaje się także diodę pełniącą funkcję selektora. Rozgrzanie chalkogenku może następować poprzez przepuszczenie przez niego prądu elektrycznego lub z wykorzystaniem specjalnego elementu podgrzewającego.

Przyjęło się logiczne zero wiązać ze stanem amorficznym, który charakteryzuje się wysoką rezystancją. Z kolei logicznej jedynce odpowiada stan krystaliczny o znacznie niższej rezystancji. Ze względu na duże różnice rezystancji pomiędzy stanem krystalicznym, a amorficznym możliwe jest uzyskiwanie pośrednich stanów rezystancji, co pozwala na przechowywanie w jednym rezystorze więcej, niż jednego bitu informacji.



PODSTAWOWE OPERACJE W PAMIĘCIACH ZMIENNOFAZOWYCH

W pamięciach zmiennofazowych wykonywane są dwie podstawowe operacje: odczyt i zapis. W odróżnieniu jednak od pamięci typu Flash, nie ma konieczności przeprowadzania kasowania przed zapisem nowej zawartości. Odczyt następuje poprzez pomiar rezystancji rezystora wchodzącego w skład komórki bitowej. Z kolei zapis wymaga roztopienia rezystora i jego odpowiedniego wychłodzenia.

Podgrzanie chalkogenku do temperatury ok. 600 ° C przez impuls elektryczny z użyciem prądu o natężeniu ok. 1 mA w krótkim, niepozwalającym na krystalizację materiału, czasie (poniżej 100 ns) powoduje jego przejście w charakteryzujący się wysoką, liczoną w MΩ, rezystancją stan amorficzny. Przełączenie w stan krystaliczny następuje przez impuls elektryczny o natężeniu prądu ok. 0,1 mA w czasie ok. 500 ns. Dłuższy czas trwania impulsu umożliwia krystalizację materiału w czasie wystudzenia. Rezystancja w stanie krystalicznym jest znacząco niższa niż w stanie amorficznym i liczona jest w kΩ.

PRZEWAGI I PROBLEMY PAMIĘCI ZMIENNOFAZOWYCH

Układy zmiennofazowe są znacznie bardziej niezawodne od popularnych układów NAND. Ich szacowana trwałość wynosi ponad milion zapisów, a przy zachowaniu odpowiednich warunków eksploatacji może przekroczyć nawet bilion zapisów. Istnieje też metoda naprawy uszkodzonych komórek pamięci z wykorzystaniem impulsu elektrycznego o odpowiednio wysokim natężeniu i długim czasie trwania. Inną różnicą na korzyść pamięci zmiennofazowych jest możliwość adresowania pojedynczych komórek bitowych tak podczas zapisu, jak i odczytu, co istotnie poszerza potencjalny zakres ich zastosowań.

Możliwość bezpośredniego nadpisywania wybranych komórek korzystnie wpływa na skrócenie czasu zapisu. Nie wymaga implementacji tak złożonego oraz podatnego na awarie systemu translacji adresów logicznych na fizyczne, jak to ma miejsce w przypadku nośników półprzewodnikowych. Operacje na danych w układach zmiennofazowych odbywają się kilkukrotnie szybciej niż w układach typu NAND.

Jednym z podstawowych problemów technicznych w rozwoju pamięci zmiennofazowych jest minimalizacja rozmiaru tranzystora przy jednoczesnym zachowaniu zdolności do operowania prądami niezbędnymi do zmian stanu materiału, z którego jest zbudowany rezystor.

Ponieważ ze zmniejszaniem rozmiaru komórek bitowych możliwe jest także znaczne obniżenie natężenia prądu programowania, jest to najważniejsze zagadnienie przy optymalizacji rozmiaru komórki bitowej oraz zużycia energii przez cały układ pamięci.

Kolejnym problemem zagrażającym stabilności układu i przechowywanym w nim danym jest oddziaływanie termiczne pomiędzy sąsiadującymi komórkami bitowymi. Dążenie do minimalizacji rozmiarów komórek i odstępów między nimi wymaga uwzględnienia tych oddziaływań tak, aby przeprogramowanie jednej komórki nie wpływało na stan sąsiednich.

Komórki pamięci zmiennofazowych są także narażone na zewnętrzne oddziaływania termiczne. Przykładowo, podczas lutowania układów. Chalkogenki w postaci amorficznej zaczynają krystalizować już przy temperaturze ok. 150 ° C. Prowadzone są prace nad materiałami, które zapewnią wyższą stabilność termiczną komórek bitowych.

URZĄDZENIA WYKORZYSTUJĄCE PAMIĘCI ZMIENNOFAZOWE

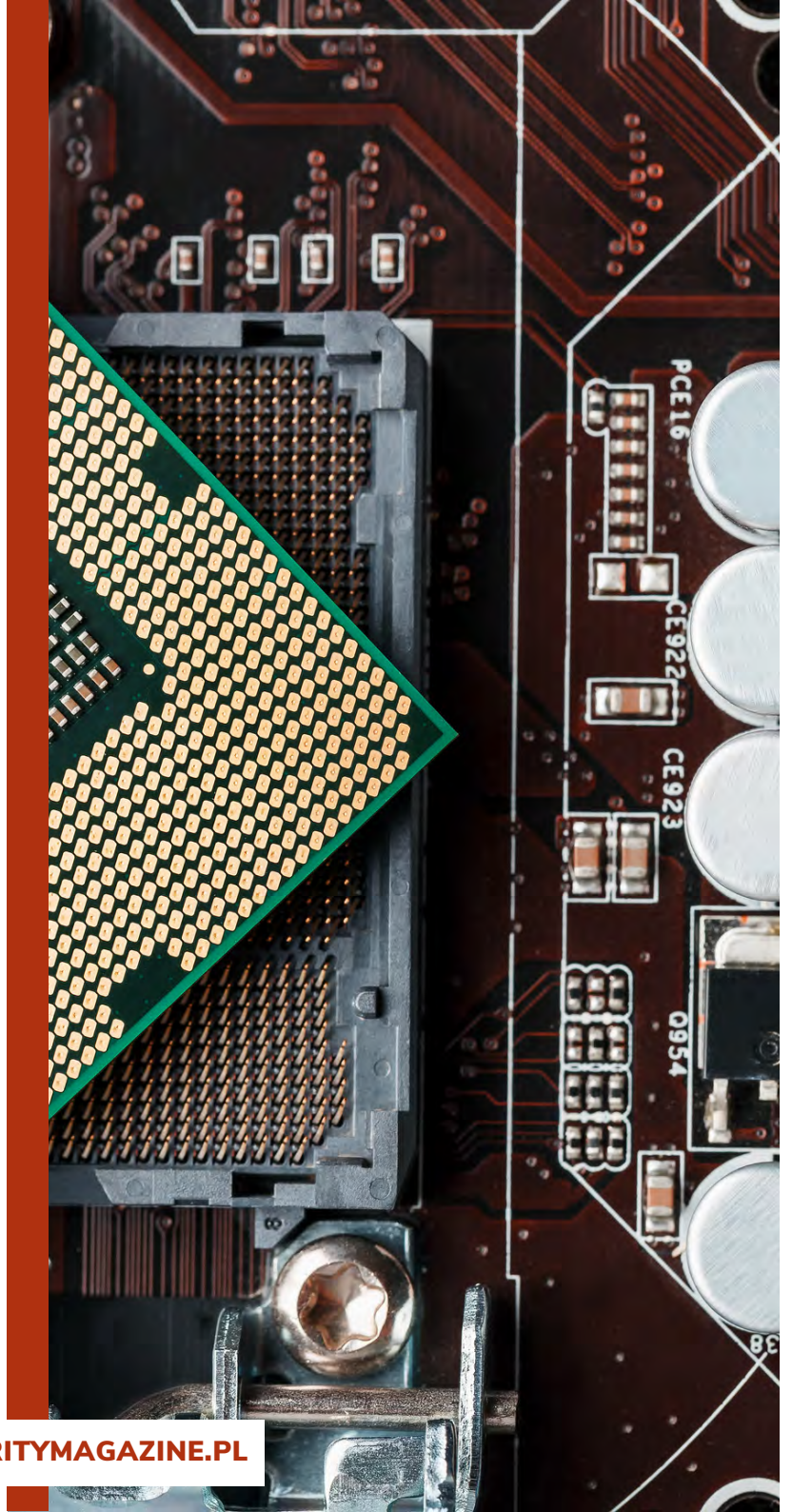
Pierwsze prototypy pamięci zmiennofazowych zostały opracowane w 2002 r. Pierwsze urządzenia komercyjne to pamięci buforowe Optane, które współpracują z procesorami Intela począwszy od siódmej generacji. To urządzenia podłączane przez interfejs M.2 i wykorzystujące protokół NVMe. Przechowują one informację najczęściej odczytywaną z dysków twardych lub SSD, co przekłada się na przyspieszenie pracy komputera.

Działanie bufora zmiennofazowego jest zbliżone do działania bufora NAND w przypadku dysków SSHD. Różnica polega na tym, że za zarządzanie pracą znajdującego się na elektronice dysku bufora NAND odpowiada oprogramowanie układowe tego dysku, zaś buforem Optane zarządza sterownik systemowy.

Dlatego wykorzystanie bufora zmiennofazowego jest obwarowane szeregiem wymagań sprzętowych i programowych, podczas gdy podłączenie dysków SSHD jest możliwe praktycznie do każdego komputera.

Najprawdopodobniej jednym z celów urządzeń Optane było przetestowanie działania nowego typu układów w praktyce, nim przeznaczono je do wykorzystania w nośnikach danych. Takie nośniki Optane SSD pojawiły się w sklepach pod koniec 2020 r., jednak ich wysoki koszt sprawił, że nie odniosły sukcesu rynkowego - obecnie bardzo trudno je spotkać. Do rynkowej porażki tego rozwiązania niewątpliwie przyczyniło się wprowadzenie szeregu rozwiązań obniżających koszt produkcji układów NAND-owych, a tym samym końcową cenę SSD-ków.

Czy to oznacza, że układy zmiennofazowe umarły? Ludzie, którzy polowali na dinozaury, a wieczorami siedzieli przed jaskiniami i patrzyli, jak powstaje węgiel mogą pamiętać dys-



kietki ED.

Były to bardzo mało popularne dyskietki, bo choć pojemność 2,88 MB robiła wrażenie w porównaniu z typową pojemnością 1,44 MB, to jeszcze większe wrażenie robiła cena. W dodatku dyskietki ED wymagały specjalnego napędu. Nie były obsługiwane przez zwykłe stacje dyskietek, bo były pierwszymi komercyjnymi produktami wykorzystującymi zapis prostopadły. W dodatku pechowo trafiły na okres bardzo szybkiego rozwoju dysków twardych.

Dyskietki zostały zepchnięte do bardzo niszowych zastosowań, ale sam zapis prostopadły po kilkunastu latach powrócił. W momencie, gdy to dyski twarde zmierzyły się z barierami wzrostu gęstości zapisu. Podobna sytuacja jest prawdopodobna i w przypadku układów zmiennofazowych, których rynkowy debiut trafił na niezbyt sprzyjające okoliczności.

Tymczasem Intel znalazł dla swojego wynalazku inne zastosowanie. Wykorzystuje układy zmiennofazowe do produkcji nieulotnych pamięci operacyjnych – Optane Persistent Memory. Szybkie, niezawodne i energoniezależne układy mogą z czasem zatrzeć granicę pomiędzy pamięcią operacyjną, a pamięcią masową.

Z przyjemnością ogłaszamy, że zostaliśmy Partnerem konkursu Rising Star in Cybersecurity organizowanym przez Cyber Women Community.

To świetna okazja do promowania projektów związanych z cyberbezpieczeństwem, tworzonych lub realizowanych przez kobiety! Nagrodą główną jest miejsce na studiach podyplomowych: Zarządzanie Cyberbezpieczeństwem na Akademii Leona Koźmińskiego.

Konkurs adresowany jest do kobiet, które:

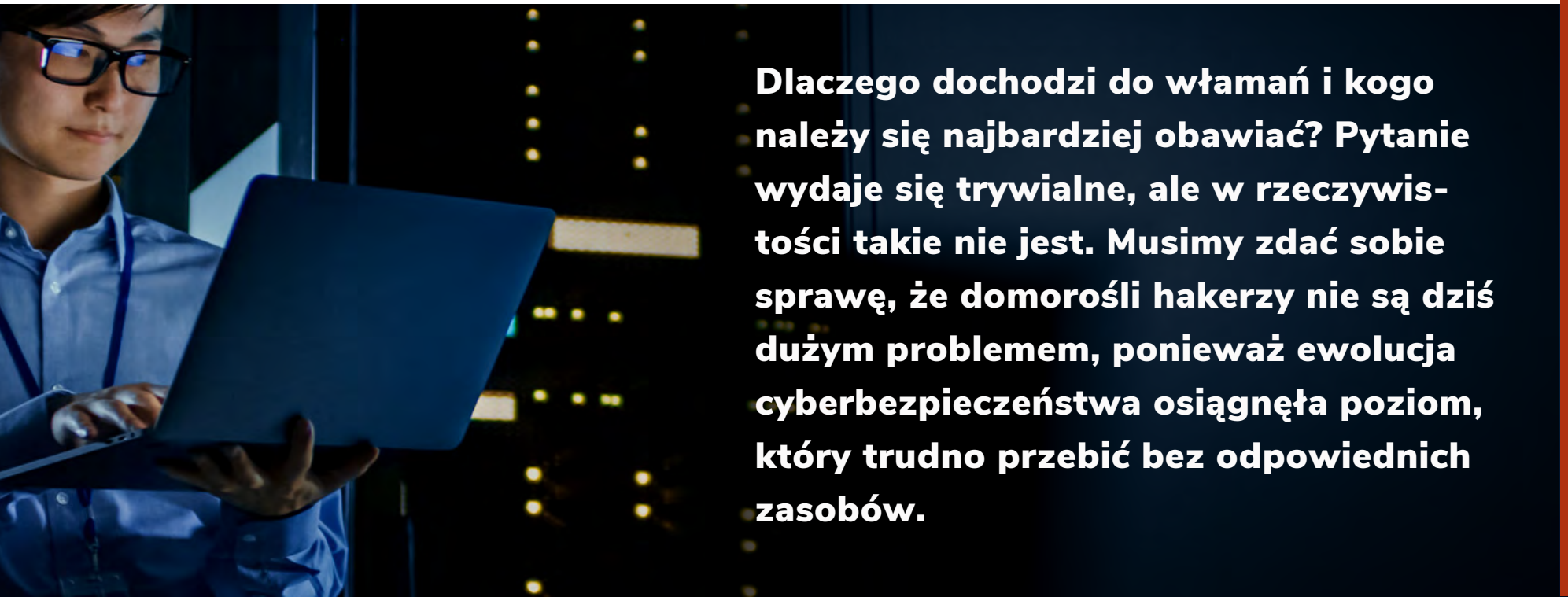
- znalazły rozwiązanie, które sprawiło że ich organizacja jest bardziej niedostępna niż warowna cybertwierdza,
- usprawniły proces lub narzędzie, dzięki któremu przepływ danych jest bezpieczniejszy,
- zorganizowała szkolenie z cyberbezpieczeństwa, wydarzenie lub zespół, który skutecznie odpiera cyberataki, albo służy wiedzą innym,
- za chwilę będą realizować super-cyber-pomysł.

Zgłoszenia przyjmowane są do 18 marca!
Więcej szczegółów oraz formularz zgłoszeniowy znajdziesz TUTAJ.


/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

PODSTAWOWE METODY HAKOWANIA A WZMACNIANIE OCHRONY TOŻSAMOŚCI

Kris Durski
Vault Security



Dlaczego dochodzi do włamań i kogo należy się najbardziej obawiać? Pytanie wydaje się trywialne, ale w rzeczywistości takie nie jest. Musimy zdać sobie sprawę, że domorośli hakerzy nie są dziś dużym problemem, ponieważ ewolucja cyberbezpieczeństwa osiągnęła poziom, który trudno przebić bez odpowiednich zasobów.

CORAZ BARDZIEJ ZALEŻYMY OD CYBERPRZESTRZENI

Tak, nadal otrzymujemy wiadomości, które próbują nakłonić nas do ujawnienia naszych danych uwierzytelniających, ale są one dość naiwne (wystarczy spojrzeć na pochodzenie i treść) lub nasza przeglądarka jest nagle przekierowywana na znajomą stronę internetową, ale pod dziwnym adresem URL . Ogólnie rzecz biorąc, ochrona przed tymi technikami nie jest bardzo trudna; zwykle wystarczy być czujnym. Większość typowego złośliwego oprogramowania może zostać wykryta przed wejściem do naszej przestrzeni lub usunięta, gdy już się w niej znajduje, za pomocą oprogramowania antywirusowego.

Ponieważ nasze środki do życia, w tym zabezpieczenia i bezpieczeństwo, w coraz większym stopniu zależą od cyberprzestrzeni, podstępne, ale naturalne pragnienie ludzi, by wykorzystywać innych, zmieniło się dramatycznie. Większość transakcji finansowych odbywa się elektronicznie, więc napad na bank nie opiera się już na broni i fizycznej obecności, ale sprytne hakowanie może to zrobić i może przynieść znacznie większą wartość niż tradycyjne napady. Energia elektryczna nie jest już produkowana i dostarczana lokalnie, ale rozprowadzana na wszystkich kontynentach i równoważona elektronicznie.

Aby wyrządzić jak największe szkody konkretnemu krajowi, wróg może zaplanować zhakowanie systemów kontroli sieci, co może skutecznie zaciemnić cały region. Alternatywnie, tradycyjne bombardowanie sieci trakcyjnej jest bardziej ryzykowne, kosztowne i narażające bezpośrednio życia agresorów. Ruch lotniczy nie jest już sprawą lokalną, ale jest globalnie koordynowany elektronicznie.

Własność intelektualna, taka jak plany samolotów, samochodów, zaawansowanych systemów uzbrojenia i wiele innych, nie jest już dostarczana w pośpiechu

do podwykonawców w pojazdach opancerzonych, ale przenoszona cyfrowo przez cyberprzestrzeń. Moglibyśmy tak wymieniać ale obraz naszych słabych punktów jest już wyraźnie widoczny.

Praktycznie we wszystkich przypadkach zapewnienie bezpieczeństwa dostępu koncentruje się na chronionych obiektach, takich jak serwer, budynek, samochód itp., podczas gdy od użytkownika oczekuje się jedynie posiadania gadżetu/urządzenia lub zapamiętania sekretnych informacji/haseł. Nie trzeba wiele myśleć, aby zdać sobie sprawę, że najsłabszym elementem całego systemu jest użytkownik, człowiek ze wszystkimi wrodzonymi słabościami. Zdrowy rozsądek mówi, że system jest tak mocny, jak jego najsłabszy element, więc dlaczego ten element jest ignorowany?

Kolejnym elementem, którego nie możemy zignorować, jest fakt, że postęp technologiczny jest dziełem ludzi. Chociaż komputery są wszechobecne w wykonywaniu obliczeń, decyzje podejmują ludzie, więc ich wrodzone słabości przyczyniają się do niektórych nieplanowanych „funkcji" zwanych błędami, które mogą osłabiać bezpieczeństwo systemów. Firmy wydają mnóstwo zasobów, by być sumiennym w znajdowaniu tych błędów i ich poprawianiu. Jednak ulepszanie produktów jest procesem ciągłym, więc wprowadzanie nowych błędów również jest procesem ciągłym. To tam kwitną hakerzy. Wydaje się, że to niekończący się problem, prawda?

Cóż, tak i nie. Nie możemy zmienić człowieka, ale możemy zmienić środowisko, z którym człowiek wchodzi w interakcje. Wiemy, że kontrola dostępu opiera się głównie na zasadach i gadżetach oraz oczywiście na fizycznych strażnikach w świecie realnym. Naiwnością byłoby sądzić, że ten rodzaj zabezpieczeń działa dobrze, ponieważ działa w oparciu o rozsądne oczekiwania, co w efekcie oznacza, że tak nie jest. Musimy zrozumieć, że współczesne środki bezpieczeństwa stanowią wykalkulowane ryzyko, które odstrasza większość ludzi, ale nie „profesjonalnych" sprawców lub dobrze finansowane ataki organizowane przez zagraniczne rządy lub organizacje. Czy naprawdę możemy to zmienić?

Ponownie, nie możemy zmienić zachowania, ponieważ jest ono częścią ludzkości, ale możemy uzbroić ludzi w środki, które reprezentują ich lepiej niż zapamiętane dane do logowania lub posiadany przez nich gadżet/urządzenie. Jednym z najlepszych sposobów ochrony danych jest kryptografia. Nie myl jednak tego z szyfrowaniem, które jest procesem ukrywania wiadomości i jest dobre tylko wtedy, gdy klucz szyfrowania nie jest dostępny. Aby być bezpiecznym, trzeba zaangażować znacznie więcej. Kolejną rzeczą, którą należy w tym miejscu podkreślić, są dane chronione, co nie musi od razu oznaczać danych nieznanych odbiorcy, a zebranych w trakcie badań lub innych projektów, czy sprawozdań finansowych i tym podobnych.

Dobrze znaną cechą kryptografii asymetrycznej jest to, że chronione dane mogą służyć do udowodnienia tożsamości osoby, o ile posiadanie klucza prywatnego można powiązać z tą osobą. Chronionymi danymi może być zarówno ich skrót (hash) zaszyfrowany kluczem prywatnym zwanym podpisem cyfrowym, jak i klucz efemeryczny, np. klucz symetryczny, zaszyfrowany kluczem publicznym, który można odszyfrować tylko odpowiednim kluczem prywatnym. W obu przypadkach tylko właściciel klucza prywatnego może je rozszyfrować.

Ta technika ma wyraźną przewagę nad powszechnymi praktykami dotyczącymi haseł nawet z dowo-

dem posiadania urządzenia, takim jak w przypadku MFA (Multi-Factor Authentication).

Hasło podróżuje po sieci, więc w ten czy inny sposób haker może je ukraść, aby podszyć się pod jego właściciela. MFA jest jedynie dowodem posiadania urządzenia lub dostępu do niego, a nie tego, przez kogo jest ono posiadane. Klucz prywatny jest znacznie trudniejszy do kradzieży, ponieważ nigdy nie podróżuje po żadnej sieci, aby potwierdzić tożsamość. Tożsamość jest dowodzona poprzez jego użycie, a nie jego ujawnienie. Inną cechą tego procesu jest to, że strona weryfikująca nie dowiaduje się niczego o kluczu prywatnym strony dowodzącej, więc jest to jakby ZKP (Zero-Knowledge-Proof).

Kolejną zaletą tożsamości kryptograficznej, zwłaszcza w porównaniu z biometrią, jest jej łatwość do zastąpienia. Zawsze można wygenerować nowy klucz prywatny, ale odcisk palca lub skan siatkówki są zawsze na całe życie. Pomiary biometryczne mogą być również znacznie łatwiejsze do kradzieży niż odpowiednio chronione klucze prywatne, ponieważ znowu dane biometryczne muszą zostać ujawnione, tak jak każda tajemnica, ale klucz prywatny może być używany bez uprzedniego ujawnienia. Niektórzy nazywają ten proces uwierzytelnieniem, a nie potwierdzeniem tożsamości. Nie popełnij błędu, uwierzytelnienie jest zawsze dowodem tożsamości lub autoryzacji strony uwierzytelniającej. Każda inna interpretacja to po prostu unikanie odpowiedzialności, ponieważ byłoby to potwierdzeniem tego, co i dlaczego ktoś miałby to robić? Rozszerzenie środowiska poprzez wzmocnienie tożsamości ludzi za pomocą technik kryptograficznych otwiera nowe możliwości ochrony zasobów cyfrowych i materialnych.

Środki kryptograficzne nie muszą ciągle się zmieniać, by czynić ciągły postęp w technologii produktów, a tym samym zmniejszać podatność systemów na luki w zabezpieczeniach spowodowane nowymi błędami. Po drugie, systemy mogą być bardziej restrykcyjne w dopuszczaniu użytkowników, zwiększając jeszcze bardziej ziarnistość dostępu bez angażowania „zaufanych” stron trzecich do zarządzania kontami użytkowników. Po trzecie, hakerzy musieliby ponownie skoncentrować się na konkretnych użytkownikach, nie zyskując nic na skradzionych środkach, by odnieść sukces w masowych naruszeniach.

Nigdy nie powinniśmy lekceważyć wroga, a starać się pozostać o krok przed nim.


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

JAK ZMIENIŁO SIĘ PODEJŚCIE FIRM DO CYBERBEZPIECZEŃSTWA?

Redakcja
SECURITY MAGAZINE

Rok 2022 znacząco wpłynął na kwestie cyberbezpieczeństwa. Choć hakowanie i cyberprzestępstwa towarzyszą nam od początku istnienia internetu, to z roku na rok zagrożenia te narastają. Dodatkowo rosyjska agresja na Ukrainę spotęgowała lęk przed wpływem zewnętrznych podmiotów na organizacje. Jak wygląda podejście do cyberbezpieczeństwa w 2023 roku?

CO LIDERZY BIZNESOWI MYŚLĄ O CYBERBEZPIECZEŃSTWIE?

Światowe Forum Ekonomiczne (WEF) wraz z Accenture sprawdziło, co eksperci biznesowi i IT z całego świata myślą o cyberbezpieczeństwie. Okazuje się, że 93% ekspertów ds. cyberbezpieczeństwa uważa, że globalne wydarzenia geopolityczne doprowadzą do umiarkowanego albo znaczącego wpływu na cyberkatastroficzne wydarzenia w ciągu najbliższych dwóch lat. Tak samo uważa 86% przebadanych liderów biznesowych.

Nie ma w tym nic dziwnego. Wojna w Ukrainie uświadomiła nas wszystkich, jakim poważnym zagrożeniem jest to, co dzieje się w cyberprzestrzeni. Z tego zresztą powodu państwa (np. Polska) podkreśliły wagę nienaruszalności cyberprzestrzeni i wskazały, że za incydenty są gotowe podjąć odwet. W ostatnim czasie również Unia Europejska ostrzegała np. przed chińskimi hakerami, którzy zagrażają europejskim instytucjom czy przedsiębiorstwom. A Belgia niedawno wystosowała prośbę do chińskiego rządu o ukrócenie takiej działalności.

A przecież po tej „drugiej stronie barykady" znajduje się też Rosja, która przy okazji agresji na Ukrainę, pokazała, co potrafi w cyberprzestrzeni. Ukraińskie (ale też europejskie) instytucje i przedsiębiorstwa były przez rosyjskich hakerów wielokrotnie atakowane. Co ważne – do większości takich grup, jak np. Killnet, Rosja oficjalnie się nie przyznaje, lecz wszyscy doskonale zdajemy sobie sprawę, że są one powiązane z Kremlem.

WEF i Accenture zapytali również, czy przedsiębiorstwa spodziewają się, że ryzyko geopolityczne wpłynie na ich strategie dotyczące cyberbezpieczeństwa. 29% respondentów przyznało, że będzie mieć ono znaczący wpływ. 44% wskazało, że wpłynie w jakiś umiarkowany sposób. 21% uważa, że będzie mieć to minimalne oddziaływanie, a jedynie 6% uważa, że nic się nie zmieni. Badania te pokazują, że przedsiębiorstwa na całym świecie zdają sobie sprawę z wagi sytuacji.

Dodatkowo podkreśla to fakt, jak liderzy biznesowi postrzegają cyberbezpieczeństwo - 37% respondentów wskazało, że jest to niezbędny koszt związany z prowadzeniem działalności gospodarczej. 51% myśli o nim jako o kluczowym czynniku biznesowym.

JAKIE ZMIANY W CYBERBEZPIECZEŃSTWIE ZAUWAŻAJĄ LIDERZY BIZNESOWI?

WEF i Accenture nie omieszkali zapytać liderów biznesowych, jakie zmiany wprowadzają w odpowiedzi na ryzyko geopolityczne. 73% wskazało, że zaostrzają swoją politykę i praktykę dotyczącą angażowania bezpośredniego połączenia third party z dostępem do danych. 71% również wzmacnia kontrolę dot. third party, które przetwarzają dane. 49% respondentów z kolei wskazało, że ponownie ocenia kraje, w których przedsiębiorstwo prowadzi jakąś formę działalności.

41% odpowiedziało, że dostosowuje praktykę wymiany informacji. 34% współpracuje z branżowymi grupami roboczymi w celu poprawienia swojego cyberbezpieczeństwa. 24% aktualizuje warunki dla third party. A jedynie 2% nie wprowadziło żadnych zmian w swojej strategii dotyczącej cyberbezpieczeństwa.

Świadomość związana ze zwiększeniem ryzyka z powodu sytuacji geopolitycznej jest zatem wysoka. Nie każdy jednak wprowadza wszystkie możliwe działania, aby zwiększyć swoje cyberbezpieczeństwo. Niektóre z nich mogą się też szybko zdezaktualizować. Np. wszystkie te działania, które tyczą się obecnie third party cookies, gdyż Google (choć kilkukrotnie to przekładało) niedługo z nich zrezygnuje. Oczywiście – pod nazwą „third party" kryje się też więcej kwestii. I może tu też chodzić o większą ostrożność wobec firm czy osób trzecich.

Z raportu WEF dowiadujemy się też, co zdaniem liderów biznesowych przyniesie najwięcej pozytywów na podejście do organizacji do cyberbezpieczeństwa w ciągu najbliższego roku. Zdaniem respondentów będzie to przede wszystkim zwiększenie świadomości pracowników o cyberprzestępczości.

Badani wskazali też, że organizacje będą częściej korzystać z usług opartych na chmurze.

CZY LIDERZY BIZNESOWI WIERZĄ W ODPORNOŚĆ SWOICH FIRM?

Od ostatniego roku wyraźnie zmieniło się też podejście liderów biznesowych do sprawności ich organizacji w kontekście cyberbezpieczeństwa. Na pytanie, czy czują, że ich przedsiębiorstwa są gotowe do zapewnienia cyberodporności w 2022 r. tylko 7% wskazało, że martwi się o tę kwestię. W 2023 r. było to już jednak 20%, czyli aż o 13 punktów procentowych więcej. W ubiegłym roku ponadto 4% respondentów odpowiedziało, że uważa, że ich firmy w ogóle nie są odporne na cyberzagrożenia. I tu też zauważamy wzrost do 7% w ciągu roku.

57% w 2022 r. odpowiedziało, że stosuje praktyki w zakresie cyberodporności, ale dostrzega potrzebę silnego wzrostu i doskonalenia w tej kwestii. Jednak rok później takich samych odpowiedzi udzieliło 46% osób. 32% z kolei wskazywało, że czuje, iż ich firmy są cyberodporne. W 2023 r. myśli tak tylko 27% liderów biznesowych.

W ciągu roku nastroje wyraźnie osłabły, a nieprzy-

gotowanie dostrzega znacznie więcej respondentów. I zdecydowanie ma to związek z rosnącą liczbą cybernaruszeń, ale też wymienianym w raporcie globalnym ryzykiem.

NAJWIĘKSZA OBAWA? KRADZIEŻ TOŻSAMOŚCI

Cyfrowa tożsamość jest obecnie niezwykle istotna. Dzięki niej legitymizujemy i autoryzujemy swoje działania. Dość powiedzieć, że w phishingu dość popularną metodą jest właśnie podszywanie się pod kogoś, czy kradzież tożsamości jakiejś osoby (np. poprzez zhakowanie jej konta w mediach społecznościowych albo właśnie udawania jej). I to właśnie w raporcie WEF znalazło się na pierwszym miejscu w kontekście obaw liderów biznesowych.

Jako drugą co do wielkości obawę wskazano utratę pieniędzy lub kluczowych danych z powodu cyberataku. Na trzecim miejscu wymieniono ataki typu ransomware. Na czwartym ex aequo znalazły się awaria infrastruktury krytycznej ze względu na cyberatak i geopolityczną niestabilność oraz cyberwojnę. Piątą największą obawą jest z kolei szantaż z powodu pozyskania kompromitujących danych. A szóstą kradzież lub sfałszowanie danych medycznych.

NA ŚWIECIE JEST CORAZ WIĘCEJ ATAKÓW HAKERSKICH

Wzrost cyberprzestępczości to nie żadna spekulacja. Potwierdzają to raporty, m.in. Google'a. W swoim badaniu zatytułowanym: „Fog of War. How the Ukraine Conflict Transformed the Cyber Threat Landscape" firma wskazuje, że odnotowujemy 300% wzrost cyberataków w porównaniu do 2020 r. Oczywiście, większość z nich wymierzona jest w kraje NATO. Jednak nie tylko w instytucje, ale też prywatne przedsiębiorstwa.

Google wymienia też kilka grup cyberprzestępczych powiązanych z rządem Rosji czy Białorusi. Są to m.in. Frozenbarents, Frozenlake, Coldriver, Frozenvista, Pushcha (Białoruś), czy Summit. Wszystkie one koncentrują swoje ataki przede wszystkim na kraje NATO i Ukrainę. Cyberprzestępcy uderzają w instytucje państwowe, militarne, spółki energetyczne, banki, przemysł ciężki, telecom, uniwersytety, media, NGOs-y, opiekę zdrowotną, prywatne frmy.

W samym tylko 2022 r. Google wykryło ponad 1950 przypadków rosyjskich prób zakłócenia działań platform ich rodzimej spółki – Alphabet Inc. Co ważne – Google wskazuje, że cyberprzestępcy (nie tylko ci rosyjscy) wykorzystują już nie tylko tradycyjne metody cyberataków. W internecie aż huczy od farm trolli czy używania sztucznej inteligencji do fałszowania wydarzeń. Jako przykład Google podaje filmik, w którym prezydent Ukrainy – Wołodymyr Zełenski twierdzi, że Ukraina powinna się poddać Rosji.

Oczywiście – materiał ten został sfabrykowany przez cyberprzestępców. Do jego powstania wykorzystano technologię deepfake, która pozwala m.in. na dość przekonujące "nałożenie cudzej twarzy" na inną osobę. W ten sposób powstają fałszywe materiały. Coraz częściej ofiarami takiej technologii padają osoby prywatne. Na przykład, streamerka QTCinderella, której twarz znalazła się w spreparowanym filmie pornograficznym.

NOWE FORMY CYBERPRZEMOCY

W tym momencie dochodzimy do sedna sprawy. Cyberprzestępczość to już nie tylko phishing czy złośliwe oprogramowanie. To już nawet nie jest wyłącznie klasyczny hacking.

Cyberprzestępczość w ciągu kilku lat znacząco się zmieniła. O ile dawniej (a w zasadzie nadal) obawiamy się głównie utraty pieniędzy czy przejmowania kont, o tyle coraz częściej powinniśmy zwracać uwagę na zupełnie nowe metody wykorzystywane zarówno przez zwykłych cyberprzestępców, jak i tych powiązanych z państwami czy cybersłużby.

Postępujący, niczym nieskrępowany postęp sztucznej inteligencji sprawia, że powstaje coraz więcej sposobów i metod na wyłudzenie pieniędzy, kradzież danych czy skuteczne podszywanie się pod innych ludzi.

Czego idealnym przykładem jest właśnie technologia deepfake. Problem w tym, że branża sztucznej inteligencji jest obecnie wyjątkowo nieuregulowana prawnie. Rynek ten robi w zasadzie „co chce". I jedynie w kontekście spółek o znaczeniu wojskowym czy dual-use można mówić o jakiejś regulacji, choć i tutaj nie zawsze jest wybitnie.

Sztuczna inteligencja może nam zarówno pomóc bronić się przed cyberprzestępczością, jak i ją ułatwić. Przykładowo, przez zautomatyzowanie skanowania sieci i odpierania cyberataków.

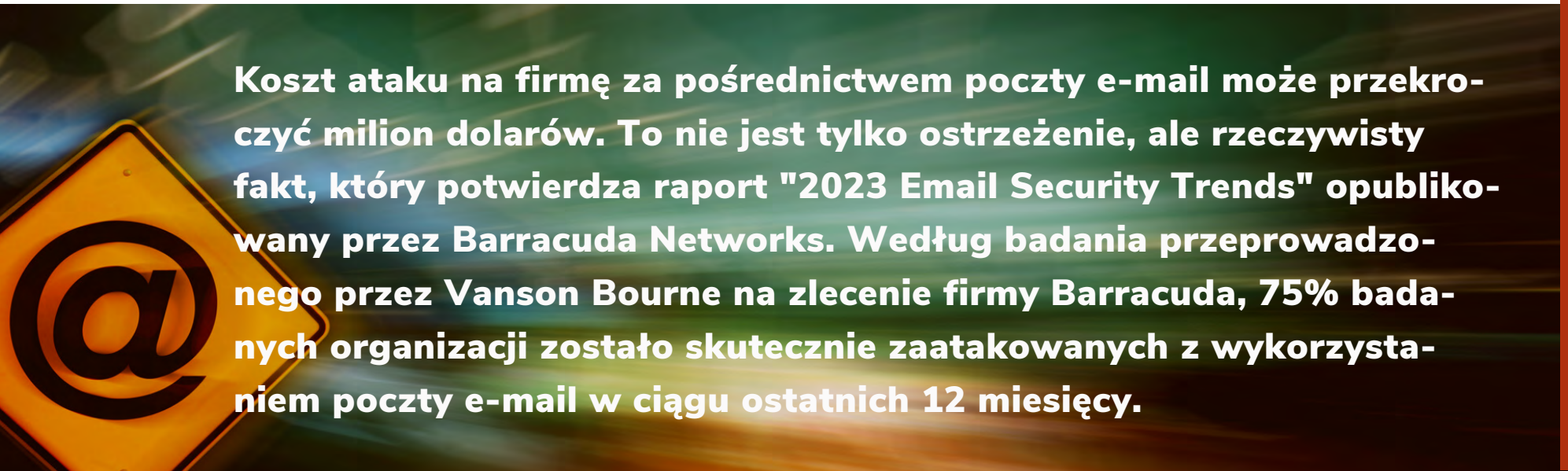
NATO przeprowadza, co prawda, ćwiczenia, które mają usprawnić bronienie się przed atakami z wykorzystaniem sztucznej inteligencji, ale czy zwykli obywatele i prywatne przedsiębiorstwa – zwłaszcza z sektora MMŚP – będą tak samo wprawne, jak żołnierze Sojuszu?


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

JAK ATAKI Z WYKORZYSTANIEM E-MAIL WPŁYWAJĄ NA SPRAWNOŚĆ BIZNESOWĄ FIRM?

Redakcja
SECURITY MAGAZINE

we współpracy z
Barracuda



Koszt ataku na firmę za pośrednictwem poczty e-mail może przekroczyć milion dolarów. To nie jest tylko ostrzeżenie, ale rzeczywisty fakt, który potwierdza raport "2023 Email Security Trends" opublikowany przez Barracuda Networks. Według badania przeprowadzonego przez Vanson Bourne na zlecenie firmy Barracuda, 75% badanych organizacji zostało skutecznie zaatakowanych z wykorzystaniem poczty e-mail w ciągu ostatnich 12 miesięcy.

SKUTKI CYBERATAKÓW Z WYKORZYSTANIEM POCZTY ELEKTRONICZNEJ

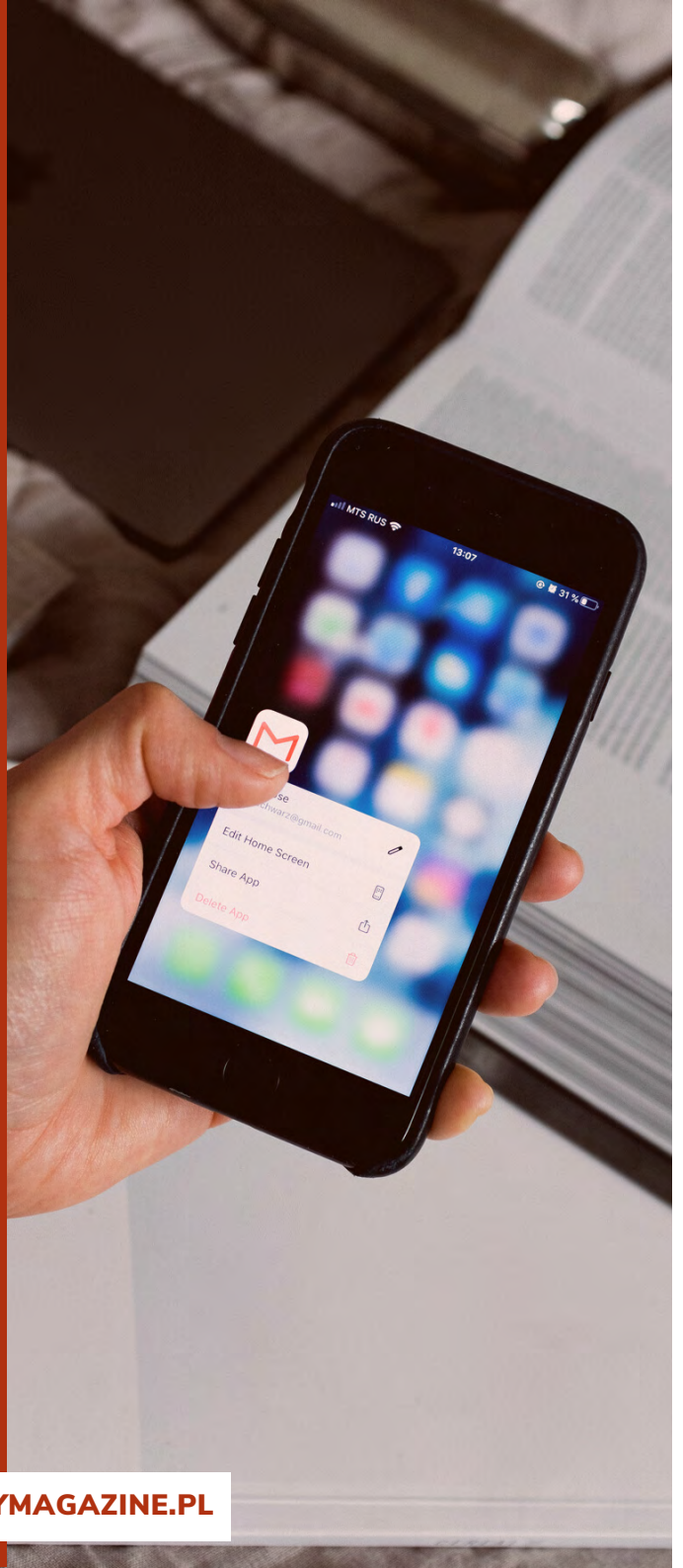
Skutki ataków z wykorzystaniem poczty elektronicznej mogą mieć znaczący wpływ na sprawność biznesową organizacji.

Do najczęściej zgłaszanych należą:

- **przestoje i zakłócenia w działalności firm** (które dotknęły 44% zaatakowanych organizacji). Ataki e-mailowe, takie jak phishing, mogą skutecznie zablokować lub zakłócić pracę w firmie, szczególnie, gdy większość pracowników korzysta z poczty e-mail jako głównego narzędzia do komunikacji. Przestój w pracy może prowadzić do opóźnień w realizacji projektów, wydłużania czasu reakcji na ważne kwestie biznesowe i spadku produktywności.
- **utrata wrażliwych, poufnych i krytycznych dla biznesu danych** (43%), tym bardziej katastrofalna, jeśli dane są związane z informacjami o klientach, pracownikach lub z działalnością biznesową. Jeśli dane wrażliwe lub poufne ujawnią się publicznie, firma może zostać oskarżona o naruszenie prywatności klientów i pracowników. Ostatecznie, to może prowadzić do poważnych konsekwencji prawnych i finansowych, takich jak kary i straty wizerunkowe.
- **uszczerbek na reputacji marki** (41%). Po pierwsze, ataki e-mailowe mogą prowadzić do utraty zaufania klientów do firmy. Jeśli atak e-mailowy prowadzi do wycieku danych klientów, klienci mogą stracić zaufanie do firmy i szukać alternatywnych usług lub produktów. Ostatecznie, to może prowadzić do spadku przychodów i utraty konkurencyjności. Trzeba też brać pod uwagę szkody wizerunkowe. Jeśli atak e-mailowy jest szeroko opisywany w mediach, firma może być kojarzona z incydentem i utracić prestiż w branży. Ostatecznie, to też może prowadzić do utraty klientów i przychodów.

Wyniki ataków z wykorzystaniem poczty e-mail różnią się wyraźnie w zależności od branży. Sektor finansowy jest najbardziej narażony na utratę cennych danych (59% badanych) i środków finansowych (51% badanych) ze względu na ich duże znaczenie dla działalności firmy. Firmy z tego sektora mają zwykle wrażliwe informacje finansowe, takie jak informacje o klientach, transakcjach finansowych i kontach bankowych, które są atrakcyjnym celem dla hakerów i cyberprzestępców.

Przedsiębiorstwa produkcyjne natomiast uznały, że najbardziej uciążliwym skutkiem ataków z wykorzystaniem poczty e-mail są zakłócenia w działaniu organizacji (53%). W tym sektorze firmy zwykle posiadają duże ilości danych dotyczących produkcji, logistyki i łańcucha dostaw, które są krytyczne dla utrzymania ciągłości działania firmy. Ataki mogą prowadzić do przerw w produkcji, opóźnień w dostawach, utraty zysków i problemów z zadowoleniem klientów.



Sektor służby zdrowia z kolei staje w obliczu kosztów przywrócenia sprawności systemów (44%) jako największego skutku ataków z wykorzystaniem poczty e-mail. Podmioty w tym sektorze zwykle posiadają duże ilości wrażliwych danych medycznych pacjentów, takich jak wyniki badań, diagnozy i historie chorób, które są cenne dla hakerów i cyberprzestępców. Utrata tych danych może prowadzić do poważnych problemów, w tym opóźnień w leczeniu, naruszeń prywatności i problemów z prawami pacjentów.

Wnioskiem jest, że różne branże wymagają różnych podejść do ochrony przed atakami z wykorzystaniem poczty e-mail. Firmy powinny zidentyfikować najważniejsze aktywa i dane, które wymagają ochrony, i dostosować swoje strategie ochrony przed atakami e-mailowymi, aby uwzględnić specyficzne potrzeby branżowe. Dodatkowo, szkolenia pracowników dotyczące rozpoznawania ataków e-mailowych oraz stosowanie odpowiednich narzędzi i procedur ochrony danych powinny być dostosowane do branży, aby zapewnić skuteczną ochronę przed cyberprzestępcami.

RYZYKO PRACY ZDALNEJ

Najbardziej niepokojącym faktem jest to, że im więcej pracowników wykonujących obowiązki zdalnie, tym większe zagrożenie ze strony cyberprzestępców i wyższy koszt usuwania skutków ich działań. Liczba pracowników zdalnych zwiększa się, a pracodawcy muszą być świadomi ryzyka związanego z takim modelem pracy.

Dotyczy to organizacji, w których ponad połowa pracowników wykonuje swoje obowiązki zdalnie niezależnie od wielkości i branży. Mimo to home office z tego powodu nie powinno być uważane za zagrożenie samo w sobie. Przeciwnie, praca zdalna jest coraz bardziej popularna i zyskała na znaczeniu.

- *Praca zdalna nie straci na popularności, tym bardziej że w Polsce została właśnie prawnie uregulowana. Pracodawcy muszą się liczyć z tym, że pracownicy będą wybierać home office. A to oznacza konieczność dostosowania strategii bezpieczeństwa firmy do takiej sytuacji. Liczba udanych ataków z wykorzystaniem poczty e-mail pokazuje, że wciąż jest bardzo dużo do zrobienia w obszarze zabezpieczenia podstawowych narzędzi pracy w firmach oraz w zakresie szkolenia pracowników* – mówił **Mateusz Ossowski, CEE Channel Manager w Barracuda Networks.**

Zatem praca zdalna wymaga od firm zwiększenia wysiłków w dziedzinie cyberbezpieczeństwa. Pracownicy zdalni często korzystają z prywatnych urządzeń, sieci WiFi i oprogramowania, co zwiększa ryzyko ataków z wykorzystaniem poczty elektronicznej.

Firmy muszą więc zapewnić swoim pracownikom narzędzia i szkolenia umożliwiające im bezpieczne korzystanie z poczty e-mail oraz innych narzędzi pracy.

Niezależnie od tego, czy firma działa zdalnie, czy nie, cyberbezpieczeństwo powinno być priorytetem dla każdej organizacji. Inwestycja w narzędzia zabezpieczeń i szkolenia pracowników to kluczowe kroki, które pomogą firmom uniknąć kosztownych konsekwencji ataków z wykorzystaniem e-poczty.

Warto również zauważyć, że koszty związane z usuwaniem skutków ataków z wykorzystaniem poczty elektronicznej nie są jedynym kosztem, który ponoszą firmy. Ataki te często powodują także straty finansowe w postaci utraconych klientów oraz zysków, co może wpłynąć na dalszy rozwój i stabilność organizacji.

Dlatego też, firma powinna podjąć działania w celu zabezpieczenia swoich systemów i danych, m.in. poprzez regularne aktualizacje oprogramowania, stosowanie zaawansowanych narzędzi zabezpieczeń oraz przeszkolenie pracowników w zakresie cyberbezpieczeństwa. Tylko w ten sposób można zminimalizować ryzyko ataku z wykorzystaniem poczty elektronicznej i chronić swoją organizację przed kosztownymi konsekwencjami.

NIEWYSTARCZAJĄCE PRZYGOTOWANIE FIRM DO WALKI Z ZAGROŻENIAMI

Z badania Barracuda Networks wynika również, że firmy czują się niedostatecznie przygotowane do radzenia sobie ze złośliwym oprogramowaniem i wirusami (34%), zaawansowanymi atakami na pocztę elektroniczną, takimi jak przejęcie konta (30%) i kompromitacja poczty biznesowej (28%), a nawet bardziej podstawowymi zagrożeniami, np. spamem (28%). - *Poczta e-mail jest zaufanym i rozpowszechnionym kanałem komunikacji, co czyni go atrakcyjnym celem dla cyberprzestępców. Spodziewamy się, że wyrafinowanie ataków opartych na poczcie elektronicznej wzrośnie. Atakujący będą wykorzystywać sztuczną inteligencję oraz zaawansowaną inżynierię społeczną, by uzyskać dostęp do pożądanych danych i ominąć zabezpieczenia* – wyjaśnił **Don MacLennan, SVP, Engineering & Product Management, Email Protection w Barracuda Networks.**

– *Ataki oparte na wiadomościach e-mail mogą być punktem wyjścia dla szerokiej gamy cyberzagrożeń, w tym ransomware, spyware, oprogramowania wyłudzającego informacje, wydobywającego kryptowaluty itd. Nie jest zaskakujące, że zespoły IT odpowiadające za bezpieczeństwo w firmach na całym świecie nie czują się w pełni przygotowane do obrony przed wieloma z nich. Rosnąca świadomość zagrożeń, których początkowym wektorem ataku może być poczta e-mail, oraz zrozumienie wagi solidnych zabezpieczeń będzie kluczem do utrzymania bezpieczeństwa organizacji i ich pracowników w 2023 roku i później* - zauważył Don MacLennan.

Rzetelny® Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

SECURITYMAGAZINE.PL

WERYFIKACJA KLIENTÓW I UTRZYMANIE SIECI IT

Redakcja
SECURITY MAGAZINE

W świecie cyberbezpieczeństwa funkcjonuje wiele startupów, które wspierają firmy na różne sposoby. Spółki te dostarczają rozwiązania, które między innymi pomagają utrzymać sieć IT, edukować pracowników, weryfikować klientów czy zabezpieczać organizację przed cyberatakami. Dziś przyjrzymy się kilku z nim.

AUTHOLOGIC – PRZECIWDZIAŁANIE OSZUSTOM

W sieci nie brakuje cyberprzestępców czy osób, które chcą w jakiś sposób oszukać przedsiębiorstwa lub prywatne osoby. Dzieje się to na różne sposoby, np. poprzez kradzież kont, kart płatniczych itp. Z tego powodu wiele przedsiębiorstw decyduje się na jakąś formę weryfikacji klientów. Najczęściej np. poprzez wysyłanie zdjęć dowodu osobistego wraz z fotografią twarzy, aby porównać, czy zdjęcia się zgadzają. Albo podawanie danych, o których mogą wiedzieć tylko właściciele kont.

Są jednak i inne sposoby. I tu z pomocą przychodzi warszawski startup Authologic. Spółka ta zajmuje się m.in. przeciwdziałaniem oszustwom chargeback, detekcją botów i tzw. fraudsterów. Startup przeprowadza szeroki proces weryfikacyjny oferujący m.in. analizę behawioralną (tj. zachowania użytkownika na stronie. Każde z nas nieco inaczej porusza się po witrynach), weryfikację mailową, telefoniczną, biometryczną, czy za pomocą cyfrowego dowodu osobistego lub ID w bankowości otwartej.

Produkt startupu pomaga też firmom weryfikować czy ich klienci znajdują się np. na listach sankcyjnych i weryfikują reputację użytkowników. Co ważne – rozwiązanie to dostępne jest dzięki API.

Startup kieruje swoje usługi do fintechów i banków, telekomów, ochrony zdrowia, e-commerców, branży nieruchomości, wynajmu aut, a także web3 i sektora kryptowalut. Z usług Authologic korzysta już m.in. siepomaga.pl, Santander Leasing, Europa Ubezpieczenia, czy Przelewy24.

NETHONE – AI WERYFIKUJĄCE KLIENTÓW

Usługę w podobnym zakresie oferuje też warszawski startup Nethone. Spółka ta działa już od 2016 r. i w swoim portfolio ma takich klientów jak LOT, Bank ING, BlaBlaCar, Booksy czy Ramp. Nethone łącznie posiada ponad 100 klientów, zatrudnia około 90 pracowników i działa w więcej niż 100 krajach.

Rozwiązanie spółki opiera się o sztuczną inteligencję – pasywnie i w czasie rzeczywistym. A co więcej – funkcjonuje zarówno na stronie www, jak również w systemach Android czy iOS. Sztuczna inteligencja Nethone pomaga m.in. zmniejszyć wskaźnik oszustw związanych z płatnościami

dzięki weryfikacji biometrii i zachowań behawioralnych.

Produkt startupu wykrywa nieoczywiste wzorce zachowań oraz automatyzuje proces decyzyjny. Nethone chwali się, że ich rozwiązanie jest szybsze od tradycyjnej heurystyki i ręcznych zestawów reguł. Startup nie skupia się jednak wyłącznie na płatnościach. Sztuczna inteligencja Nethone umożliwia też pasywną analitykę behawioralną, tworząc całościowy profil każdego użytkownika na podstawie odcisków palców, naciśnięć klawiszy, ruchów myszy czy ekranu dotykowego.

Startup twierdzi, że jego produkt jest w stanie zablokować 99,8% przejęć kont z wykorzystaniem danych biometrycznych i behawioralnych. A oprócz tego klienci Nethone odnotowali 66% spadek stawki obciążenia zwrotnego. Co ważne – rozwiązanie to jest zgodne z regulacjami PSD2.

GRANDMETRIC – PROJEKTOWANIE SIECI

Poznańskie Grandmetric jest zdecydowanie lepiej pasującym do opisu standardowego startupu, jeśli chodzi o kwestie związane z cyberbezpieczeństwem. Spółka specjalizuje się m.in. w szkoleniach technicznych, warsztatach produktowych czy kursach technologicznych dla inżynierów bezpieczeństwa i sieci. Grandmetric ponadto przeprowadza audyty bezpieczeństwa, licencji i testy penetracyjne (tzw. pentesty) z wykorzystaniem technik black box, gray box, white box i socjotechniki.

Oprócz tego startup specjalizuje się też w projektowaniu sieci. Pomaga w ten sposób zapewnić ciągłość operacyjną i poufność danych dla przedsiębiorstw. Spółka zabezpiecza firmowe sieci przewodowe (LAN) i WiFi. A dodatkowo dostarcza sprzęt sieciowy i serwerowy, realizując i konfigurując projekt sieci. Oprócz tego Grandmetric oferuje utrzymanie infrastruktury sieciowej, zajmuje się licencjami sprzętowymi, monitoringiem, polityką kopii zapasowych czy eliminowaniem zagrożeń.

Na liście startupu znajduje się też migracja do SD-WAN oraz projekty proof of concept dla sieci punktów usługowych, branży spożywczej, dostawców materiałów BHP czy producentów kruszyw. Mówiąc krótko – Grandmetric to cyberbezpieczeństwo 360°. Startup jest ponadto partnerem technologicznym Microsoftu i NetApp, a co więcej – został wyróżniony Diamentem Miesięcznika Forbes w 2022 roku.

Swoje usługi spółka świadczy zarówno w Polsce, jak i za granicą.

To tylko niektóre ze startupów, które wspierają cyberbezpieczeństwo w firmach. Takich spółek jest znacznie więcej – zarówno w Polsce, jak i za granicą. Grunt to dbać o cyberbezpieczeństwo swojej organizacji na każdym jej etapie.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

ZAGROŻENIA I KRYZYSY WIZERUNKOWE W SIECI W 2023

Beata Łaszyn
Alert Media Communications

Wojna i pandemia pokazały, jak wiele może się zmienić w otaczającej nas rzeczywistości. Nagle i bez ostrzeżenia. Czas ten pokazał również, że ludzie, społeczności, a nawet całe państwa i kontynenty potrafią się dostosować i zmienić pewne zasady.

Oba te wydarzenia wiele zmieniły w internecie – w zachowaniu internautów, dostępnych narzędziach i możliwościach. To z kolei wpłynęło na zagrożenia oraz możliwe kryzysy wizerunkowe.

Czego najbardziej boimy się w sieci w 2023 roku i jak się zmieniają obawy, wskazuje kolejny Kryzysometr – badanie Alert Media Communications. Został on zrealizowany wśród ekspertów komunikacji w firmach, instytucjach oraz organizacjach.

BIERZEMY MIARĘ Z KRYZYSÓW

Jak co roku, również pod koniec szczęśliwie zakończonego 2022 roku (przy czym głównym szczęściem jest, że się skończył), zrealizowaliśmy szóstą edycję badania Kryzysometr 2022/2023. Zapytaliśmy szerokie grono ekspertów komunikacji m.in. o to, gdzie spodziewają się kryzysów, by określić obszary, na jakie warto szczególnie uważać. Nauczeni doświadczeniem formujemy odrębne pytanie o kryzysy zrodzone w internecie. I w każdej edycji porównujemy wyniki, co pozwala nam ustalić pewne trendy.

Wnioski są naprawdę fascynujące i pozwalają na wcześniejsze poznanie terenów zagrożonych.

W Kryzysometrze pasjonujące jest porównywanie wyników poszczególnych pytań, by zobaczyć różnice w odpowiedziach między grupami respondentów. Najchętniej sięgam do porównania danych osób reprezentujących biznes oraz administrację państwową. Dlaczego jest to interesujące? Z wielu powodów. Obserwując z bliska lub daleka przebieg kryzysów, widzimy odmienności w potrzebach podmiotów obu kategorii. Wyraźnie widać różnice w przebiegu kryzysów – tym, co jest wyjątkowo bolesne, a co tylko „trudne”. Inny jest wpływ kryzysów na grupy docelowe, inny - na dalsze losy organizacji dotkniętej kryzysem.

KRYZYS ZWYKLE PRZEGLĄDA SIĘ W LUSTRZE POLITYKI

No i oczywiście jest kwestia polityki. W obu przypadkach gra jakąś rolę, ale rola ta jest odmienna i różnoplanowa. W kryzysach dotykających biznes polityka od pewnego czasu w mniejszym lub większym zakresie jest dodatkowym czynnikiem komplikującym.

Często polityka w różnych odmianach ma wpływ pośredni lub bezpośredni na efekt wydarzeń, dodatkowe epizody czy skutki. Nie pamiętam już przypadku kryzysu, gdzie nie trzeba było sięgnąć do tego obszaru, by uwzględnić ewentualny wpływ. Nawet w firmach, które zajmują się tematyką daleką od polityki. Takie mamy czasy i takie okoliczności społeczne.

W przypadku kryzysów w podmiotach administracji publicznej sprawy wyglądają inaczej. Tu występuje wysoki poziom wzajemności. Tu oczywiście polityka jest często na pierwszym miejscu, ale... kryzysy i ich skutki mogą mieć wpływ na politykę. I często mają. Oznacza to automatycznie dodatkowe bodźce, dodatkowe komplikacje i grupy mocnych interesariuszy. I to zarówno po stronie adwersarzy, sojuszników, jak i wreszcie grup docelowych. To dlatego wyniki Kryzysometru są tak ciekawe, bo wyraźnie mogą pokazać subtelności odmienności czy nawet mocne różnice.

Mają one statystyczny obraz w odpowiedzi na pytanie o spodziewane źródła kryzysów wizerunkowych w 2023 roku. W kategorii „administracja publiczna" znaczącego i negatywnego wpływu polityki obawia się co drugi ekspert (52%), tym samym jest to największa obawa środowiska. W biznesie ten faktor ma również wysoki współczynnik (jest na drugim miejscu), choć wskazał go mniejszy odsetek specjalistów – 37%. Tylko tyle i aż tyle. „Tylko tyle", bo wpływ tego obszaru jest z roku na rok coraz bardziej zauważalny. „Aż tyle", ponieważ polityka wywołująca strach w biznesie jest realną przeszkodą gospodarczą.

Namalowawszy tło obu kategorii, wracamy do źródeł... a przynajmniej e-źródeł kryzysów.

W szerokim panelu eksperckim badania Kryzysometr 2022/2023, przeprowadzonym przez agencję Alert Media Communications na przełomie listopada i grudnia 2022 r., wzięło udział 102 rzeczników, dyrektorów i managerów PR z wiodących polskich firm, instytucji państwowych i samorządowych oraz organizacji pozarządowych.

SKALA NAJWIĘKSZYCH STRACHÓW W SIECI, CZYLI E-OBAWY

Kryzysy, które mają swoje źródło w sieci, zajmują trzecie miejsce rankingu obaw, a więc podium – co ciekawe – w obu kategoriach: biznes osiągnął 27% wskazań, a administracja 12 punktów procentowych więcej – 39%. Jak widać, wszyscy obawiają się internetu, choć w odmiennych kwestiach, o czym opowiem szerzej. Tu na scenę wchodzi pytanie o źródła kryzysów powstających w internecie.

Od wielu lat z dużym zaciekawieniem przyglądamy się fake newsom, szczególnie na tle innych strachów internetowych. O ile wszystkie inne odpowiedzi z roku na rok przesuwają się na skali strachów, o tyle fake newsy zawsze i niezmiennie są bardzo wysoko. Każdego roku. Najświeższe dane dopełniają tendencje: strach przed fake newsami jest najczęściej wskazaną obawą – około 51% wszystkich specjalistów obawia się kryzysów wynikających z fake newsów.

To nie zaskakuje, znając utrzymujący się od lat trend, wzmocniony w świetle wydarzeń towarzyszących wojnie w Ukrainie. I w warunkach infodemii. Informacje o akcjach dezinformacyjnych, głównie w Rosji, ale i wielu innych środowisk, zwiększyły strach przed nimi. Z drugiej strony, co dobre, poniosły poziom świadomości w społeczeństwie. Jeśli jednak zajrzymy za kulisy tego pytania, robi się coraz bardziej ciekawie.

FAKE NEWSY I FALE NEGATYWNYCH KOMENTARZY

Eksperci komunikacji zatrudnieni w biznesie wskazali ex aequo fale negatywnych komentarzy oraz fake newsy jako najczęstsze przyczyny kryzysów powstałych w sieci (po 48%). W świetle powyższej dygresji o fake newsach, oraz oczywistego wpływu fali negatywnych komentarzy, dalszy komentarz jest zbędny. Natomiast opinie administracji wskazują już wyraźnie na różnice środowiskowe.

W tej kategorii obawy przed fake newsami wynoszą aż 55% (więc trochę więcej niż w drugiej grupie), a fale negatywnych komentarzy – tylko 39%. W porównaniu ze wskazaniami w sektorze prywatnym i znając poziom narzekania na instytucje administracji, to nie wydaje się dużo.

Skąd różnica? Firmy często są bardzo zależne od poziomu zadowolenia klienta/konsumenta, co oznacza, że negatywne komentarze zalewające „socjale" organizacji są koszmarną wizją i trudnym doświadczeniem.

Pracownicy administracji są już prawdopodobnie mocno uodpornieni, co wynika z przyzwyczajenia. Poza tym funkcjonowanie instytucji publicznych nie zależy od poziomu zadowolenia. Trzeba przyznać, że od kilkunastu już lat administracja dba właśnie o ten o poziom - wiele się zmieniło. Nie zmienia to jednak faktu, że sam strach jest dużo mniejszy, mimo że prawdopodobnie częściej zasadny.

Jednak jeszcze bardziej ciekawie robi się, analizując kolejne odpowiedzi obu środowisk. Różnice stają się znaczące.

KTO SIĘ BOI CYBERATAKÓW...

Choć właściwie powinnam napisać: kto ich nie docenia. 32% przedstawicieli biznesu wskazało cyberataki i akcje hackerów jako źródła potencjalnych kryzysów w 2023 roku*. Wielkość tego strachu oraz wskazanie jako 3. najczęściej spodziewanej przyczyny kłopotów nie dziwi, zważywszy na alarmujące statystyki organizacji polskich, europejskich i światowych, gdzie wskazywany jest znaczny wzrost ataków tego typu.

*Łączny wskaźnik wszystkich respondentów w pytaniu o cyberataki i akcje hakerskie to 26%.

Z roku na rok rosną również koszty ataków, uwzględniajace ewentualne okupy, koszty przestoju, naprawy infrastruktury, wzmocnienia zabezpieczeń etc. Wobec danych może zaskakiwać podejście do tego obszaru w administracji, w której tylko 15% ekspertów obawia się problemów wizerunkowych spowodowanych cyberatakami, co plasuje tę przyczynę na odległym, 8. miejscu na skali strachu.

Analizując przyczyny, wysuwa się wniosek analogiczny, jak w przypadku fali negatywnych komentarzy: administracja nie jest na nie mniej narażona, ale nieco przyzwyczajona i nieustannie spodziewająca się tego typu wydarzeń.

Podobnie jak w poprzednim przypadku – kwestie ataków wchodzą w spodziewane „wizerunkowe koszty". Zaintrygowana jednak tą kwestią, zapytałam specjalistów o opinię.

Michał Rosiak, ekspert zabezpieczeń systemów teleinformatycznych w Wydziale CERT w Orange Polska, skomentował: - *Tak znacząca różnica między biznesem a sektorem publicznym wydaje się wynikać z odpowiedzialności – nomen omen – biznesowej za efe-*

kty ataków. Myślę, że w firmie, dla której zachowanie ciągłości procesów jest kluczowe dla funkcjonowania i zysków, wiedza oraz świadomość cyberzagrożeń, także odpowiedzialność za działanie firmy, są na wyraźnie wyższym poziomie.

Security freelancer Mateusz Miniewicz zauważył: - *Inny wynik w sektorze prywatnym i publicznym może również wynikać ze stosunku do zespołów zajmujących się bezpieczeństwem. W biznesie, organizacji, której najistotniejszym celem jest zarabianie pieniędzy, inaczej traktuje się „bezpieczniki" niż w sektorze publicznym, którego istnienie nie zależy aż tak od opłacalności, a bardziej od użyteczności. Głównym zadaniem biznesu jest zarabiać, a urzędów służyć i chronić obywateli. Zrozumiała jest w takim razie różnica przykładanej wagi do zagadnień wokół cyberataków. Założeniem administracji jest ochrona danych, oznacza to, że nie jest to w oczach dyrektorów problem, któremu grozi zaniedbanie. W biznesach często bezpieczeństwo informacji wiąże się z dodatkowymi kosztami i niechęcią „góry", co spędza bezpiecznikom sen z powiek.*

ATAKI HYBRYDOWE I DEEP FAKE STRASZĄ INACZEJ

Znaczące różnice widać w przypadku analizy zagrożeń zorganizowanymi atakami hybrydowymi, łączącymi działania online i offline. Tu również występują interesujące odmienności.

Tym razem zdecydowanie większy strach to zjawisko wzbudza w administracji publicznej – 21% wskazań, co zważywszy na skomplikowany poziom działania jest wysokim wynikiem. Eksperci sfery biznesu rzadziej wskazują tego typu ataki jako zagrożenie – tylko 14% wskazało na ten element. Wydaje się, że odmienności w tej kwestii tłumaczy polityka i działania społeczne. Zdecydowanie częściej prowadzone są złożone działania, jak choćby kampanie społeczne, akcje aktywistów wal-

czących o zmiany przeciw administracji niż poszczególnym firmom. Bo i rzeczywiste zmiany bardziej należą i zależą od administracji właśnie. Zapewne stąd słuszna różnica w obawach, co Kryzysometr ładnie obrazuje, będąc swoistym papierkiem lakmusowym niepokojów kryzysowych. Różnicę również widać w obawach przed deep fake, gdzie biznes oba-wia się kłopotów z nimi związanych w 16%, natomiast administracja – tylko w 6%.

KRYZYS KOŁEM SIĘ TOCZY

Polityką zaczęłam analizę obaw kryzysowych zrodzonych w sieci i na polityce zamknę. Paradoksalnie pokazuje to jej wpływ nie tylko na same kryzysy, ale i e-kryzysy – te stricte wynikające z internetu.

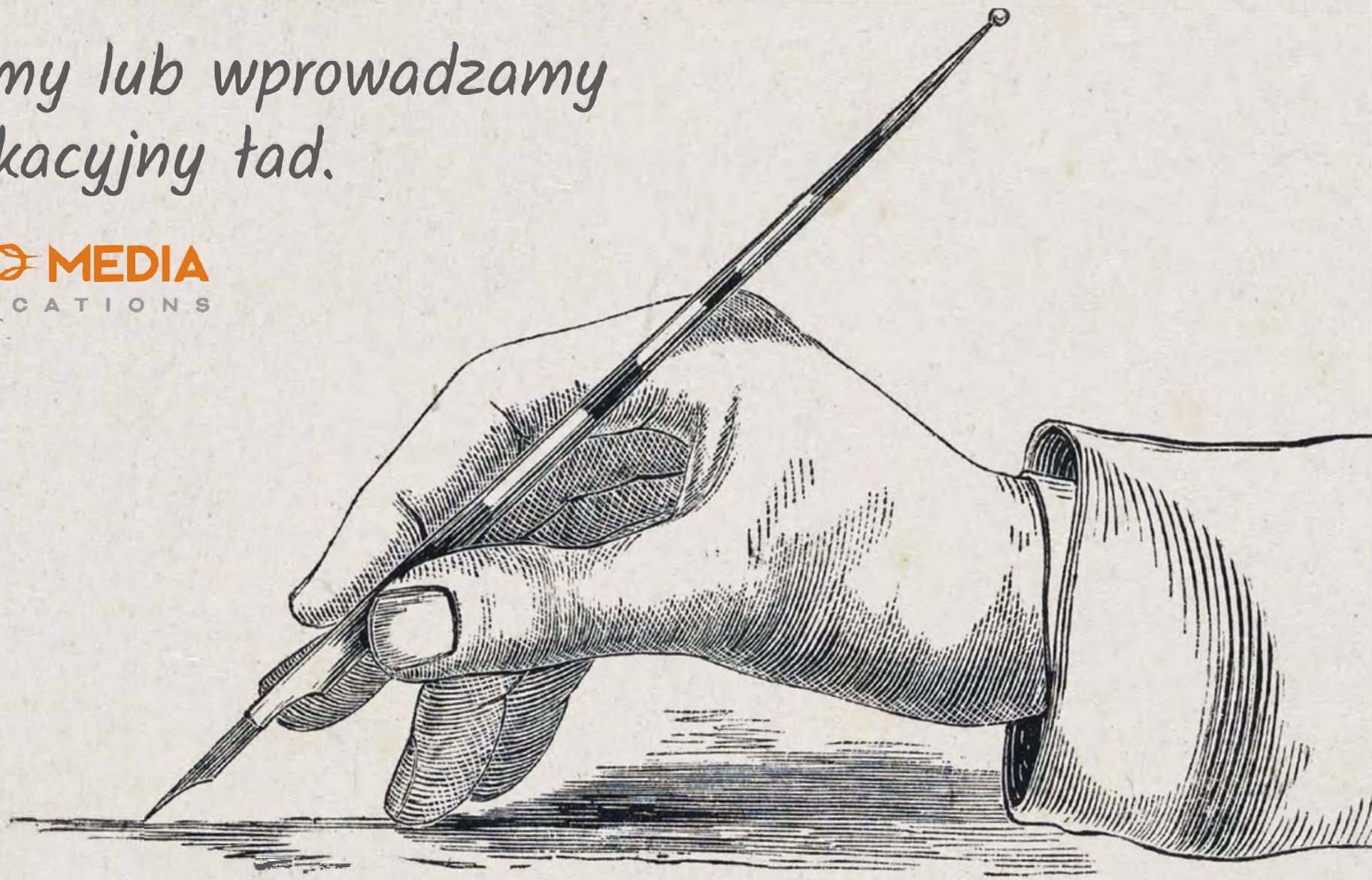
Co przyniesie rok, zobaczymy, choć już dziś, pamiętając o zbliżających się wyborach, można założyć, że kwestie dezinformacji oraz fake newsów będą wciąż żywe. Wiele do powiedzenia będzie miała rosyjska propaganda, w której zresztą o Polsce mówi się dosyć dużo. Dobrą wiadomością jest to, że istnieje wiele naprawdę prostych narzędzi do sprawdzania informacji i debunkowania fake newsów.

I wiele zależy od nas wszystkich, bo narzędzia są na wyciągnięcie ręki. A raczej dłoni na klawiaturze.

Jakub Śliż, prezes Stowarzyszenia Pravda, skomentował sytuację: - W społeczeństwie można zauważyć zwiększoną odporność na fake newsy. Jako Pravda za przyczynę stojącą za tego rodzaju odpornością wskazujemy pandemię i falę fake newsów, która zalała nas, kiedy pojawiły się pierwsze zakażenia czy pierwsza szczepionka. Z psychologicznego punktu widzenia społeczeństwo zostało zaszczepione wiedzą na temat tego, jak radzić sobie z wirusem, jakim są fałszywe informacje, co znacznie przekłada się na społeczną szybkość reakcji na danego fejka. Coraz więcej osób zdaje sobie sprawę, jak sprawdzić, czy zdjęcie jest fotomontażem lub czy zostało opublikowane przez „bota". Niestety, rozsiewacze dezinformacji też wyciągnęli wnioski z czasów pandemicznych - cały czas szukają nowych sposobów na to, jak nas oszukać. Oznacza to jednak małe prawdopodobieństwo spadku strachu przed fake newsami w najbliższym czasie, czego wszystkim jednak serdecznie życzę, zachęcając do czytania prawdy między wierszami newsów.

Tworzymy lub wprowadzamy komunikacyjny ład.

ALERT MEDIA
COMMUNICATIONS



Zapytaj o nas ludzi z branży lub wejdź na alertmedia.pl

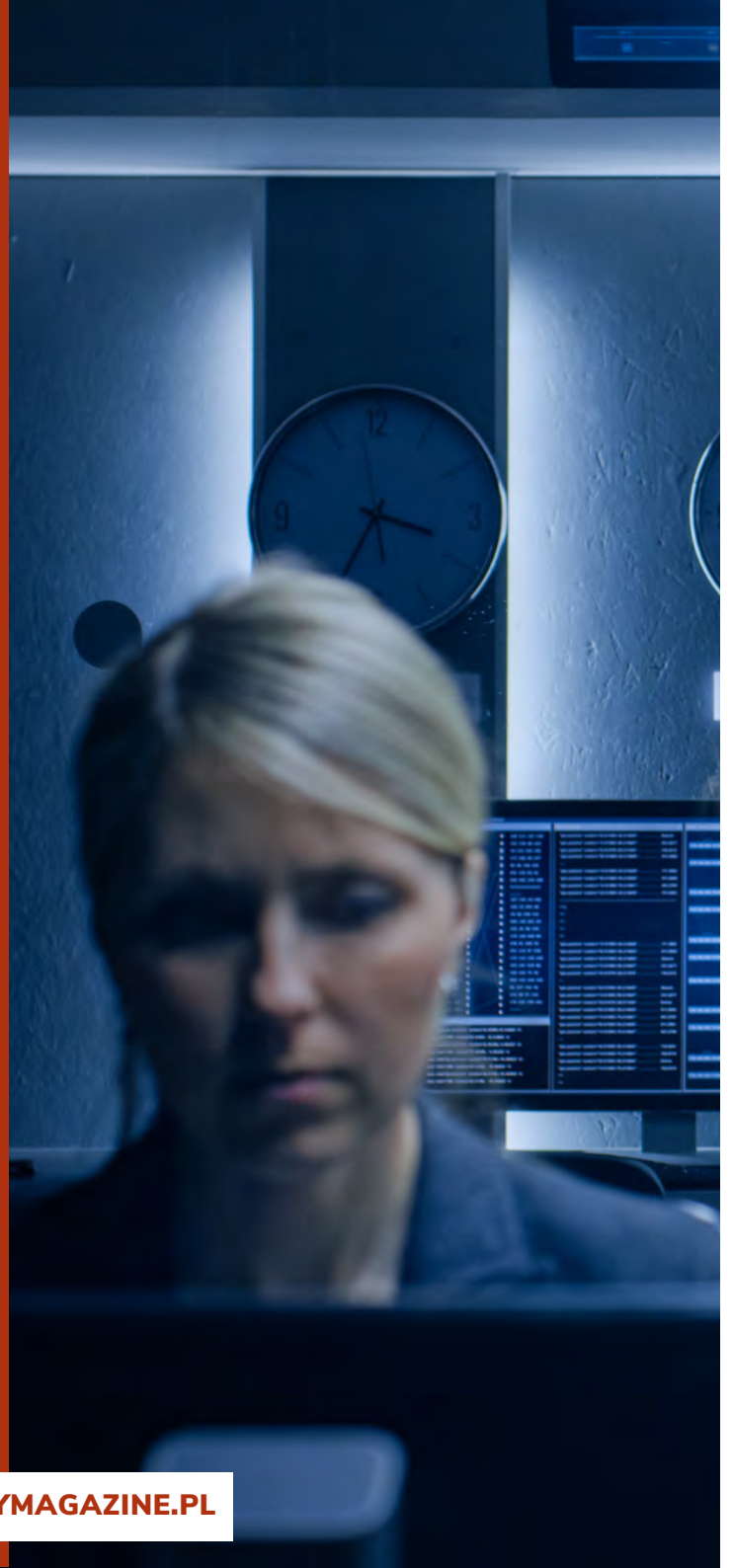
SECURITYMAGAZINE.PL

KOBIETY RATUNKIEM DLA CYBERBEZPIECZEŃSTWA

Redakcja
SECURITY MAGAZINE

we współpracy z
VECTRA

Według Cybersecurity Ventures, w 2021 roku na świecie brakowało około 3,5 miliona pracowników zajmujących się cyberbezpieczeństwem. Niepokój związany z niedoborem talentów technologicznych narasta od lat. Problem w tym, że obecnie nie mówimy już tylko o masowej transformacji cyfrowej przedsiębiorstw – digitalizuje się cały świat. Jeśli dodamy do tego wzmożoną działalność hakerów, ten niedobór pracowników jest szczególnie dotkliwy. Sytuację mogą uratować kobiety.



Tylko w 2020 roku cyberprzestępczość spowodowała globalne straty finansowe w wysokości biliona dolarów. Zagrożenie rośnie, 57% organizacji zgłasza nieobsadzone stanowiska w zakresie cyberbezpieczeństwa. Około 75% dzisiejszych pracowników cyberbezpieczeństwa to mężczyźni. Rozwiązaniem problemu mogłoby być zwiększenie liczby kobiet, które chcą pracować w tej branży. Od lat zresztą podejmowane są inicjatywy, żeby pracę na technicznych stanowiskach podejmowało jak najwięcej kobiet. Efekty co prawda są widoczne, ale wciąż nie wystarczające.

Nadzieją mogą napawać ostatnie wyniki badań — w tym ogólnoświatowa ankieta przeprowadzona wśród kobiet studiujących przedmioty z obszarów nauki, technologii, inżynierii i matematyki (STEM). Badanie uwidoczniło też przeszkody w zwiększaniu liczby pracowników ds. cyberbezpieczeństwa, ale ujawniło też zaskakujące możliwości postępu jeżeli chodzi o karierę kobiet.

DO POKONANIA WCIĄŻ JEST WIELE BARIER

Branża cyberbezpieczeństwa zmaga się z ogromnym niedoborem specjalistów. W latach 2020-2021 luka w talentach wzrosła o 13%. - *Częściowo wynika to z niedopasowania podaży i popytu. Sektor cyberbezpieczeństwa rozwija się bardzo szybko, a ze względu na rozwój technik hackerskich oraz nieustannie rozszerzającą się powierzchnię ataku, dyna-*

mika branży jest ogromna. Zdobycie specjalistycznej edukacji, certyfikacji i doświadczenia wymaganego do uzyskania wiedzy specjalistycznej wymaga nie tylko czasu, ale i pieniędzy – zauważył **Christian Putz, Country Manager w Vectra AI.**

Cybersecurity Ventures zwraca uwagę na jeszcze jeden czynnik - duże zróżnicowanie płci - kobiety stanowią obecnie tylko około 25% pracowników cyberbezpieczeństwa.

Dlaczego tak się dzieje? Według najnowszych badań przeprowadzonych przez (ISC)2, organizację non-profit, która koncentruje się na szkoleniach i certyfikacji w zakresie cyberbezpieczeństwa, większość kobiet, które pracowały w tej branży, zgłasza dyskryminację ze względu na płeć. Prawie wszystkie kobiety z którymi rozmawiano (87%) zgłosiły, że doświadczyły nieświadomej dyskryminacji, podczas gdy 19% stwierdziło, że były poddane jawnej dyskryminacji. Kobiety wskazywały również na nieuzasadnione opóźnienia w rozwoju kariery (53%) i przesadne reakcje na błędy (29%).

Dyskryminacja przejawia się też w luce płacowej. Badania (ISC)2 pokazują, że 32% mężczyzn pracujących w cyberbezpieczeństwie zarabia średnio od 50 do 100 tys. dol. rocznie. Ten sam przedział dochodów osiąga ledwie 18% kobiet.

BŁĘDY REKRUTACJI

Wyzwaniem pozostaje również zapewnienie równego trakto-

wania kobietom ubiegającym się o stanowiska z obszaru cyberbezpieczeństwa.

Jedną z kluczowych barier w dostępie, która pojawia się na tym etapie, jest tendencja do rekrutacji „idealnego kandydata" – tendencja, która zabija różnorodność. Rekruterzy poszukują kandydatów, którzy wyglądają jak obecni pracownicy, z odpowiednim stażem pracy, wykształceniem i wiedzą techniczną. Takie myślenie może wykluczać kobiety, zwłaszcza młode.

Zmiana podejścia pozwoliłaby znacznie zniwelować lukę pracowników – zamiast kierować się wyłącznie pilną potrzebą zatrudnienia, wystarczy wziąć pod uwagę kandydatów, którzy będą wymagać szkolenia. Czas na zdobycie odpowiednich kwalifikacji często będzie podobny do tego, ile zajmuje znalezienie „idealnego kandydata".

PORA ZACZĄĆ WYRÓWNYWAĆ SZANSE

Badanie obaliło wiele tradycyjnych poglądów, jak ten, że niski wskaźnik udziału kobiet w cyberbezpieczeństwie i ogólnie w dziedzinach STEM, wynika z wąskiej ścieżki rozwoju talentów, która sama w sobie jest konsekwencją niskiego udziału kobiet w edukacji STEM na poziomie wyższym. 58% badanych kobiet miało dostęp do edukacji z cyberbezpieczeństwa, 68% z nich brało udział w kursie związanym z cyberbezpieczeństwem.

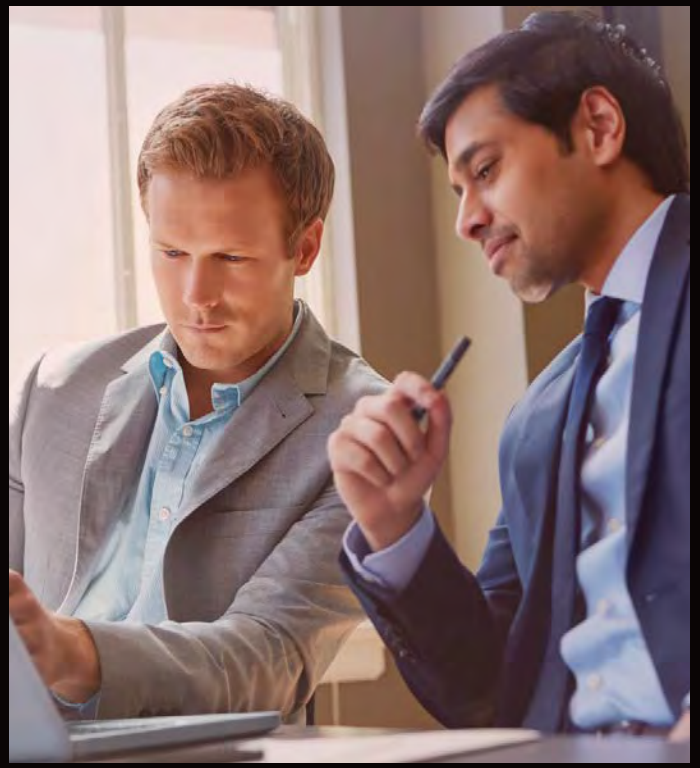
Nad dostępnością nadal trzeba pracować, ale wyniki są obiecujące. To co może niepokoić, to to, że mimo dostępności, część kobiet wciąż negatywnie ocenia wybór cyberbezpieczeństwa jako ścieżki kariery. Wynika to z priorytetów. Kobiety, planując swoją karierę, pod uwagę biorą przede wszystkim wkład w społeczeństwo, wysokość zarobków oraz równowagę między życiem zawodowym a prywatnym. 37% kobiet uważa cyberbezpieczeństwo za dziedzinę, w której osiągnięcie tej równowagi jest trudne, i dlatego rezygnuje z rozwoju w tej branży.

- Budowanie kariery w branży cyberbezpieczeństwa na pewno jest trudniejsze niż kariera w innych obszarach technologii, głównie ze względu na tempo zmian. Ale oferuje też wiele kierunków rozwoju, chociażby zapotrzebowa-

nie na rozwiązania oparte na AI, w których się specjalizujemy. Poszerzanie i wzmacnianie możliwości w zakresie bezpieczeństwa cybernetycznego poprzez wprowadzanie różnych perspektyw na kwestie rozwiązywania problemów i innowacji jest ważne i z pewnością wiele kobiet się w tym odnajdzie – mówił przedstawiciel Vectra AI.

CAŁA NADZIEJA W KOBIETACH

Trendy, które uwidoczniło badanie (ISC)2 są jednak obiecujące. Coraz więcej kobiet zaczyna przygodę z cyberbezpieczeństwem - ich udział podwoił się w latach 2017-2020. Co więcej, kobiety pracujące w cyberbezpieczeństwie mają zwykle wyższe wykształcenie, co zdecydowanie pozycjonuje je na stanowiskach kierowniczych. Zmniejsza się także luka w wynagrodzeniach, zwłaszcza wśród młodszych pokoleń. Jeżeli tylko branża wyjdzie naprzeciw potrzebom kobiet i usunie bariery, powstrzymujące przed rozpoczęciem kariery w branży, luka w zatrudnieniu zacznie się zmniejszać, i to szybko.



DOŁĄCZ DO GRONA EKSPERTÓW

BUDUJ SWOJĄ MARKĘ
I ROZPOZNAWALNOŚĆ
SWOJEJ FIRMY

PATRONAT
SECURITY MAGAZINE

CODEFRENZY

WIRTUALNA KONFERENCJA 27-31 MARCA

ZAREJESTRUJ SIĘ ZA DARMO

Tydzień z najlepszymi ekspertami z branży IT - za darmo i bez wychodzenia z domu. Kilkadziesiąt wykładów i panele dyskusyjne pięciu obszarach: Network, Security, DevOps, Java i Developers. Odbierz darmowy bilet na CodeFrenzy i poczuj klimat interdyscyplinarnego kodowania!

CodeFrenzy to wirtualna konferencja integrująca społeczność programistyczną. Od 27 do 31 marca programiści, sieciowcy, testerzy, devopsi, hakerzy oraz inne osoby związane z IT będą mogły wziąć udział w prezentacjach oraz sesjach Q&A na żywo z najlepszymi prelegentami polskiej oraz międzynarodowej sceny technologicznej.

Program wydarzenia obejmuje tematy z zakresu ICT, cyberbezpieczeństwa, kultury DevOps, języka Java oraz innych zagadnień programistycznych. Na wirtualnej scenie pojawią się eksperci reprezentujący konferencje organizowane przez PROIDEA: PLNOG, Oh My H@ck, CONFidence, 4Developers oraz JDD.

Udział potwierdzili m.in.: Łukasz Bromirski (Cisco), Adam Haertle (Zaufana Trzecia Strona), Piotr Godowski (IBM), Damian Mazurek (Chmurowisko) i Dominika Zając (Qualtrics).

Uczestnicy otrzymają dostęp do live streamingu wykładów, a po zakończeniu - do nagrań. W połączeniu z formułą online jest to bardzo elastyczne rozwiązanie - można dostosować udział w konferencji do swojego planu dnia, a wszystkie prezentacje, do których nie udało się dołączyć na żywo, obejrzeć w dogodnym terminie.

Kolejny atut? Udział nie tylko w wykładach z dziedzin, którymi zajmujemy się na co dzień, ale spoza zakresu specjalizacji. Brak opłaty otwiera drogę do swobodnego przetestowania ciekawie brzmiących tematów i zagadnień. Może to właśnie tu uczestnicy odkryją nowe ścieżki kariery lub wypróbują rozwiązania, które do tej pory wydawały im się tylko modnymi buzzwordami.

INTERDYSCYPLINARNA
KONFERENCJA DLA CAŁEJ
SPOŁECZNOŚCI IT

CODE FRENZY

27-31 MARCA 2023
ONLINE | ZA DARMO

EKSPERCI WYDANIA

ALEKSANDRA KORNECKA
Inżynier ds. cyberbezpieczeństwa

Inżynier ds. cyberbezpieczeństwa (security awareness, SecOps, CloudSec, SSDLC), lubiąca pracować i z maszynami, i z ludźmi. W IT od 2013 roku (testowanie, konsulting jakości, cyberbezpieczeństwo), magister kognitywistyki, prelegentka konferencji oraz meetupów w Polsce i zagranicą, mentorka, sprinterka.

BEATA ŁASZYN
Wiceprezeska
Alert Media Communications

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

KRIS DURSKI
Founder i dyrektor ds. technologii
Vault Security

Starszy analityk oprogramowania, programista, menedżer z ponad 20-letnim doświadczeniem w developingu i marketingu oprogramowania. Opracował koncepcję spersonalizowanego bezpieczeństwa w celu ochrony zasobów cyfrowych i materialnych. Współtworzył kilka start-upów z branży medycznej, technologii informacyjnej i cyberbezpieczeństwa.

MATEUSZ OSSOWSKI
CEE Channel Manager
Barracuda

Z branżą technologiczną związany jest od 2012 roku. Doświadczenie zdobywał w marketingu i sprzedaży produktów SaaS (Head of Sales, COO). Trener cyberbezpieczeństwa. Prelegent topowych konferencji. W Barracuda Networks odpowiedzialny za rozwój kanału partnerskiego w Europie Środkowo-Wschodniej.

EKSPERCI WYDANIA

TOMASZ WOJAK
Prezes Zarządu
Seris Konsalnet

W Grupie Seris Konsalnet od 1995 r. Od 2000 r. w zarządach spółek Grupy. Od 2018 r. Prezes Zarządu Seris Konsalnet Holding S.A. Wykształcenie wyższe, absolwent studiów MBA, wykładowca w Wyższej Szkole Bankowej. Prezes Polskiego Związku Pracodawców Firm Ochrony oraz Wiceprezes Federacji Przedsiębiorców Polskich.

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.

OLEKSANDR CHYZHYKOV
Information Security Manager
Intellias

Od 2014 roku związany z bezpieczeństwem informatycznym. Posiada ponad 8-letnie doświadczenie w dziedzinie Information Security & Business Continuity. Z firmą Intellias związany od 5 lat. Jako ekspert i menedżer przygotował kilka firm i z sukcesem pomógł im przejść przez certyfikacje ISO 27001, PCI DSS, TISAX.

CHRISTIAN PUTZ
Country Manager
Vectra AI

Odpowiada za działania firmy w Austrii i Europie Środkowo-Wschodniej. Jego rolą jest wspieranie ekspansji firmy w tym rejonie i rozwijanie jej rynkowej strategii. Od wielu lat pełni kluczowe funkcje wykonawcze w wiodących firmach z branży IT, odpowiadając za działy sprzedaży, rozwoju biznesu czy operacji biznesowych.

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

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

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

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL