7(16)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Bezpieczeństwo technologii generatywnej AI

Firma na wakacjach a cyberbezpieczeństwo

Jak zostać firmą cyberbezpieczną?

Pierwsza pomoc dla pracowników zdalnych: ochrona danych w dobie cyfryzacji

Cyberataki zagrożeniem dla branży marketingu i PR

SPIS TREŚCI

SZANOWNI PAŃSTWO,

wakacje to zazwyczaj okres mniejszej aktywności biznesowej, zmiany w dynamice pracy i ogólnej atmosferze w biurach. Często jesteśmy wtedy bardziej rozluźnieni, leniwi, a może nawet nieco rozkojarzeni.

Niemniej jednak, chociaż nasze biura mogą być mniej zatłoczone i tempo pracy może zwolnić, warto pamiętać, że zagrożenia w świecie cyberbezpieczeństwa nie biorą wolnego. Wręcz przeciwnie, hakerzy mogą próbować wykorzystać ten okres na swoją korzyść.

Są oni świadomi, że w okresie wakacyjnym kluczowi pracownicy mogą być na urlopach, a zespoły odpowiedzialne za bezpieczeństwo mogą być mniejsze przz wzgląd na czas urlopowy.

Ponadto, wakacyjny nastrój może wpłynąć na mniejszą czujność w kwestiach związanych z bezpieczeństwem. Hakerzy mogą skorzystać z tego, próbując przeprowadzać skoordynowane ataki na infrastrukturę IT firm.

Pamiętajmy, że bezpieczeństwo naszych danych i systemów nie powinno być lekceważone, latem również. Wakacje mogą być doskonałym czasem na relaks, ale nie powinny być okresem, kiedy obniżamy naszą czujność wobec zagrożeń, które nie biorą przerwy.

Bezpiecznych wakacji.

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

CYBERATAK NA USŁUGI MICROSOFT

Na początku czerwca użytkownicy pakietów Microsoft napotkali na zakłócenia w działaniu flagowego pakietu Outlook i aplikacji do udostępniania plików OneDrive. Okazało sie, że to atak DDoS przeprowadzony przez tajemniczą nową grupę haktywistów nazwaną przez Microsoft Storm-1359. Grupa haktywistów przyznała się, twierdząc, że zalała witryny śmieciowym ruchem w rozproszonych atakach typu „odmowa usługi".

OPERACJA „POWER OFF"

Dwie osoby zajmujące się wytwarzaniem i udostępnianiem płatnej usługi do przeprowadzania ataków DDoS, czyli tzw. usługi DDoS as a Service zatrzymane przez policję i prokuraturę. Korzystanie z usługi możliwe było po dokonaniu opłaty w kryptowalucie, co pozwalało na przeprowadzanie cyberataków, które w istotny sposób zakłócały pracę systemów informatycznych ulokowanych na terenie całego świata. Sprawa jest rozwojowa, nie wykluczone są dalsze zatrzymania.

DANE KONT CHATGPT NA SPRZEDAŻ

Od czerwca 2022 do maja 2023 roku ponad 101 100 zhakowanych danych uwierzytelniających do kont OpenAI ChatGPT znalazło się na nielegalnych rynkach w Dark Webie, przy czym same Indie odpowiadają za 12 632 skradzionych danych uwierzytelniających.

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

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

Redakcja "Security Magazine"

SECURITYMAGAZINE.PL

NA RZECZ CYBER-ODPORNOŚCI. CYBERSEC FORUM/EXPO 2023

PATRONAT
SECURITY MAGAZINE

W czerwcu Katowice stały się miejscem, w którym spotkali się specjaliści z różnych dziedzin, tworząc tym samym przestrzeń dla wymiany wiedzy i doświadczeń. Przez dwa dni Międzynarodowe Centrum Kongresowe tętniło życiem, a tematem przewodnim było cyberbezpieczeństwo. Właśnie odbyła się tam 17. edycja CYBERSEC FORUM/EXPO.

Konferencję oficjalnie otworzył prezydent Miasta Katowice, Marcin Krupa. Szybko stało się jasne, że jednym z głównych celów tego wydarzenia jest budowanie partnerstw na rzecz cyberodporności.

CYBERBEZPIECZNA POLSKA

Jednym z najbardziej oczekiwanych punktów pierwszego dnia był panel zatytułowany "CYBERBEZPIECZNA POLSKA. Priorytety na najbliższe lata". Podczas tej dyskusji, politycy reprezentujący różne opcje polityczne omawiali kierunki, w jakie powinno zmierzać cyberbezpieczeństwo kraju. W panelu udział wzięli: Paweł Lewandowski, Krzysztof Gawkowski, Grzegorz Napieralski, Mirosław Suchonia i Ziemowit Przebitkowski, a rozmowę prowadził Mirosław Maj, członek rady ds. Cyfryzacji.

MIEJSCE DLA PRZYSZŁOŚCI

Scena INNOVATION była w całości poświęcona wydarzeniu ECSO CYBER INVESTOR DAYS, z konkursami dla start-upów. Modino.io zwyciężyło, zdobywając tym samym nominację do finału europejskiej edycji turnieju.

ZMAGANIA W SIECI: P4 CAPTURE THE FLAG

Pierwszego dnia odbył się także p4 Capture The Flag, w którym drużyny z całego świata rywalizowały, rozwiązując zadania związane z cyberbezpieczeństwem. Zespół międzynarodowy okazał się najlepszy w tej rywalizacji.
Dla specjalistów IT firma Axence zorganizowała warsztaty o zabezpieczaniu się przed cyberatakami, zwłaszcza w kontekście pracy zdalnej.

OBRONA: DZIEŃ DRUGI

Drugi dzień konferencji, podobnie jak pierwszy, obfitował w szereg wydarzeń.

Rozpoczął się od wręczenia nagrody CYBERSEC AWARD 2023 Ministrowi Obrony Narodowej - Mariuszowi Błaszczakow. Zdobył wyróżnienie za swoje dążenie do zapewnienia cyberodporności Polsce.

LEKCJE Z UKRAINY

Jednym z najważniejszych paneli drugiego dnia była dyskusja na temat roli cyberoperacji w konflikcie zbrojnym. Panel zatytułowany "CYBER OPERATIONS IN WAR: LESSONS FROM UKRAINE" zgromadził ekspertów z różnych krajów. Gen. bryg. Oleksandr Potii, zastępca dyrektora Państwowej Służby Łączności Specjalnej i Ochrony Informacji Ukrainy, podzielił się swoimi doświadczeniami z linii frontu. Uczestnicy panelu omawiali także możliwości współpracy polsko-ukraińskiej w dziedzinie cyberbezpieczeństwa, a także roli NATO w tym kontekście.

INNOWACJE I DOSTĘP DO RYNKU

Scena INNOVATION również nie pozostawała bezczynna. 22 czerwca odbył się ACCES-TO-MARKET EVENT, podczas którego firmy prezentowały swoje rozwiązania w dziedzinie cyberbezpieczeństwa. Wśród nich firma Secfence wyróżniła się na tyle, że uzyskała nominację do finałów ECSO's CISO Choice Award.

WARSZTATY CYBER RANGE

W salach szkoleniowych odbywały się warsztaty Cyber Range, gdzie uczestnicy mieli okazję doskonalić swoje umiejętności w symulowanych warunkach realnego cyberataku. To doskonała okazja dla specjalistów, by zrozumieć, jakie są faktyczne wyzwania i jak można się przed nimi uchronić.

PRZYSZŁOŚĆ CYBERBEZPIECZEŃSTWA NA WYCIĄGNIĘCIE RĘKI

Oprócz paneli dyskusyjnych i prezentacji, CYBERSEC FORUM/EXPO zawierało również strefę EXPO. W tym miejscu uczestnicy mogli zapoznać się z najnowszymi trendami oraz rozwiązaniami w dziedzinie cyberbezpieczeństwa, które prezentowane były przez różne organizacje.

PARTNERSTWO NA RZECZ CYBERODPORNOŚCI

17. edycja CYBERSEC FORUM/EXPO okazała się być miejscem, gdzie specjaliści z różnych dziedzin mogli się spotkać i wymieniać wiedzą. Wydarzenie to dało nie tylko możliwość zrozumienia aktualnych wyzwań w dziedzinie cyberbezpieczeństwa, ale także inspirowało do budowania trwałych partnerstw w walce z cyberzagrożeniami. Ponad 1000 uczestników, 116 prelegentów i 118 partnerów stworzyło unikalną przestrzeń do nawiązania wartościowych kontaktów między przedstawicielami świata polityki, biznesu i nauki.

Strefa EXPO pozwoliła uczestnikom na zaznajomienie się z najnowszymi rozwiązaniami w dziedzinie cyberbezpieczeństwa. Wśród nich znalazły się innowacje, które mogą wpłynąć na kształtowanie się przyszłego bezpiecznego ekosystemu cyfrowego.

Niezwykle ważne było również nawiązanie współpracy międzynarodowej, co było widoczne zwłaszcza podczas paneli poświęconych kwestiom bezpieczeństwa w kontekście konfliktów zbrojnych, jak ten dotyczący sytuacji na Ukrainie. Połączenie wiedzy oraz doświadczenia z różnych regionów świata jest kluczowe dla skutecznego przeciwdziałania zagrożeniom w cyberprzestrzeni.

Na rzecz cyberodporności. CYBERSEC FORUM/EXPO 2023

Warsztaty, takie jak te organizowane przez firmę Axence oraz Cyber Range, były nieocenioną okazją dla specjalistów, aby pogłębić swoją wiedzę i umiejętności. W świecie, gdzie cyberzagrożenia są coraz bardziej zaawansowane, nieustanna edukacja i przygotowanie są niezbędne.

17 edycja CYBERSEC FORUM/EXPO nie tylko pozwoliła na wymianę wiedzy, ale również stanowiła inspirację dla uczestników do dalszego działania w dziedzinie cyberbezpieczeństwa. Współpraca, innowacja, edukacja i zaangażowanie to słowa klucze, które zarysowują drogę, jaką musimy podążać, aby budować świat bardziej odporny na cyberzagrożenia.


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

SECURITYMAGAZINE.PL

CYBERTEK - MERYTORYKA, KONKRETNA WIEDZA I DZIAŁANIA

PATRONAT
SECURITY MAGAZINE

24-26 maja w Muzeum Śląskim w Katowicach odbyła się Konferencja CyberTek Tech Festival. To były niezapomniane trzy dni spędzone pod hasłem #EnjoyTheCyber.

CyberTek - merytoryka, konkretna wiedza i działania

MERYTORYKA FUNDAMENTEM SPOTKANIA

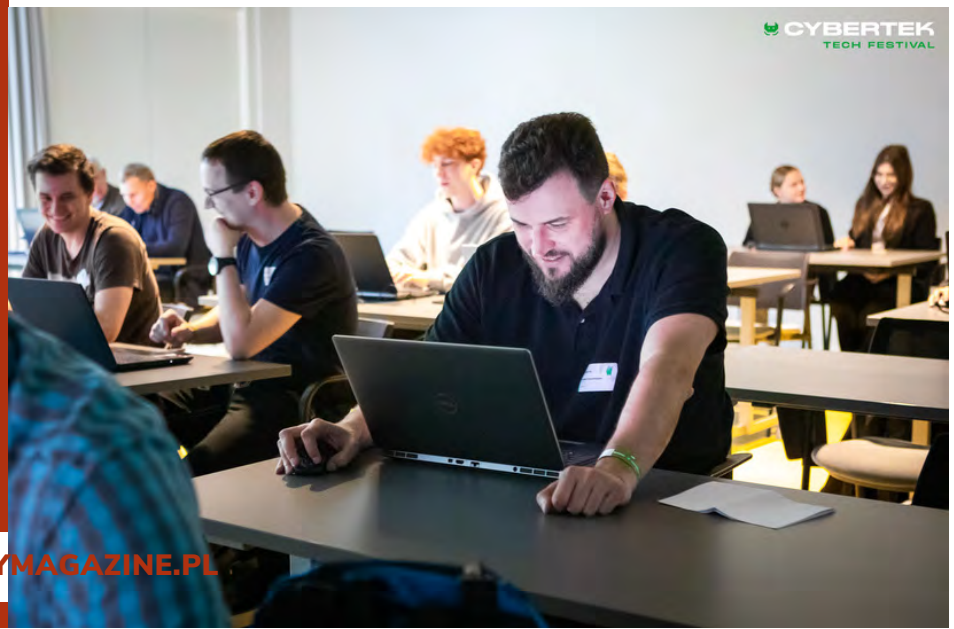
CyberTek to spotkanie, w którym liczyła się merytoryka, konkretna wiedza oraz działania. Organizator skupił się nad tym, aby zawartość merytoryczna odpowiadała aktualnym (i tym które pojawią się w najbliższej przyszłości) potrzebom poszczególnych grup odbiorców, a nadrzędnym celem konferencji było stworzenie wydarzenia budującego społeczność specjalistów w zakresie cyberbezpieczeństwa OT/ICS.

Konferencja miała charakter interdyscyplinarny, jej uczestnikami były przede wszystkim osoby, na których spoczywa odpowiedzialność za tworzenie, skuteczne wdrożenie lub realizację programów bezpieczeństwa obejmujących sieci i systemy przemysłowe.

W CyberTek Tech Festivalu wzięło łącznie udział 340 osób, w tym:

- przedstawiciele infrastruktury krytycznej, osoby odpowiedzialne za realizację zapisów ustawy KSC
- CISO IT/OT
- kadry zarządzające wyższego i średniego szczebla (liderzy zespołów OT, IT)
- specjaliści ds. cyberbezpieczeństwa technicznego (red / blue / purple)
- inżynierowie automatycy
- inżynierowie sieciowi odpowiedzialni za architekturę sieciową IT/OT
- audytorzy i specjaliści ds. zapewnienia zgodności, analizy ryzyka IT/OT oraz ciągłości działania
- entuzjaści cyberbezpieczeństwa i sieci OT oraz osoby, które chciałyby pokierować swoją karierą w tę stronę
- przedstawiciele dostawców rozwiązań i usług w obrębie automatyki przemysłowej i informatyki (integratorzy OT, IT)
- studenci oraz reprezentanci uczelni wyższych.

CyberTek - merytoryka, konkretna wiedza i działania



Pierwszego dnia CyberTek Tech Festivalu uczestnicy konferencji mieli możliwość wysłuchania wykładu wygłoszonego przez szczególnego gościa, którym był Daniel Ehrenreich, B.Sc., specjalista z ponad 30-letnim doświadczeniem w zakresie wdrażania systemów ICS, SCADA i OT. Daniel Ehrenreich poprowadził również 8 godzinny blok warsztatowy w dniu 24 maja (dzień „0" konferencji). W „Warsztatach na temat cyberbezpieczeństwa przemysłowych systemów sterowania (ICS)" wzięło udział wąskie grono specjalistów z branży cyberbezpieczeństwa (35 osób).

Łączenie w dniach 25-26 maja wygłoszono 32 prelekcje oraz podjęto 6 dyskusji na obu scenach Konferencji. Ważnym z praktycznego punktu widzenia elementem konferencji była część poświęcona różnym tematycznie warsztatom, które miały charakter edukacyjno-dyskusyjny, a przeprowadzono ich w sumie przez wszystkie dni konferencji 30.

Ważnym z praktycznego punktu widzenia elementem konferencji była część poświęcona różnym tematycznie warsztatom, które miały charakter edukacyjno-dyskusyjny.

Każdej sesji towarzyszyło duże zainteresowanie i znakomita atmosfera, ożywione dyskusje przenosiły się w przerwach z sal wykładowych / warsztatowych do kuluarów. Pomimo bardzo intensywnego planu zajęć nawet w godzinach popołudniowych sale wykładowe były pełne.

Miejsce konferencji – Muzeum Śląskie w Katowicach, sprzyjało owocnemu oraz sprawnemu przebiegowi obrad. Spotkanie towarzyskie, które odbyło się pierwszego dnia Konferencji w godzinach wieczornych było idealną okazją do nawią-

FOT. TEKNISKA POLSKA (12)

zania kontaktów, a także sprzyjało i przyczyniło się do zacieśnienia grona osób żywo zainteresowanych bezpieczeństwem przemysłu.

Konferencji towarzyszyły 3 merytoryczne wydarzenia specjalne:

1. spotkanie grupy CISO #Poland: spotkanie zamknięte dla członków grupy CISO #Poland pod patronatem Ministra Janusza Cieszyńskiego,
2. warsztaty na temat cyberbezpieczeństwa ICS: „Workshop on Industrial Control Systems (ICS) Cyber Security”,
3. spotkanie „Cyberbezpieczeństwo w motoryzacji” - sesja dedykowana cyberbezpieczeństwu w motoryzacji.

- Wierzymy, że takie wydarzenia jak CyberTek Tech Festival przyczyniają się do wykształcenia u uczestniczących w nich gości zasad cyberbezpieczeństwa, świadomości zagrożeń i sposobów obrony oraz pomagają lepiej zrozumieć, jak chronić obiekty przemysłowe, budowlane i użytkowe w Polsce - podsumowali organizatorzy, dodając: *- Prezes firmy Tekniska Zuzanna Wieczorek wraz z całym zespołem planują zorganizowanie kolejnej edycji konferencji CyberTek Tech Festival wiosną 2024 roku, na którą już teraz serdecznie zapraszamy wszystkich zainteresowanych.*

PATRONAT
SECURITY MAGAZINE

24. KONFERENCJA BRANŻY OCHRONY

POTENCJAŁ I ROLA SEKTORA PRYWATNEGO W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO

ZAREJESTRUJ SIĘ TUTAJ

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

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

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

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

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

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

WIĘCEJ NA STRONIE PIO

SECURITYMAGAZINE.PL

REKORDOWA EDYCJA KONFERENCJI CONFIDENCE

PATRONAT
SECURITY MAGAZINE

5 i 6 czerwca w EXPO Kraków odbyła się 23 edycja CONFidence, jednej z najstarszych i największych polskich konferencji poświęconej tematyce cybersecurity. Wydarzenie cieszy się rosnącym zainteresowaniem, w 2023 roku przyciągając niemal 1600 osób. Skąd taki wynik?

CONFIDENCE JEDNOCZY SPOŁECZNOŚĆ

Kultowa atmosfera i wieczorna integracja to nieodłączne elementy konferencji, które jak zawsze sprzyjały networkingowi. Uczestnicy mogli również spróbować swoich sił w licznych konkursach organizowanych przez towarzyszące wydarzeniu firmy technologiczne oraz skorzystać z atrakcji w strefie chill. Dużym zainteresowaniem cieszyły się również rozgrywki typu flag hunt, zorganizowane we współpracy ze stowarzyszeniem 17 53c oraz CTF School.

Jak wygląda taka konferencja na żywo?

Najlepiej obrazuje to relacja z CONFidence na YouTube.

CYBERBEZPIECZEŃSTWO WCIĄŻ NA TOPIE

Tematy związane z ochroną danych, bezpieczeństwem w sieci, kradzieżą tożsamości czy towarzyszą wszystkim użytkownikom Internetu, cyberbezpieczeństwo nie jest tematem zarezerwowanym wyłącznie dla specjalistów. Misją CONFidence jest edukowanie w tym zakresie na wielu poziomach. W programie konferencji znalazły się zarówno wysoce techniczne propozycje skierowane do ekspertów z branży IT, jak i wykłady prezentujące popularne mechanizmy ataków lub dobre praktyki bezpieczeństwa w sposób przystępny dla laików.

Uczestnicy mieli możliwość wzięcia udział w 47 warsztatach oraz 3 wykładach, swobodnie wybierając tematy, które odpowiadały ich aktualnym zainteresowaniom lub potrzebom zawodowym. Najlepiej ocenieni prelegenci mówili między innymi o hakowaniu systemów dostępu (**Julia Zduńczyk**), podatnościach 0day (**Or Yair**), trollach internetowych (**Adam Haertle i Piotr Zarzycki**), bezpieczeństwie macOS (**Wojciech Reguła**), kreatywnym wykorzystaniu PowerShell (**Paweł Maziarz**) oraz ochrony przed ransomware (**Maciej Jan Broniarz**).

Rekordowa edycja konferencji CONFidence

KOLEJNE SPOTKANIE JUŻ W GRUDNIU

Aby nadążyć za dynamiką branży cybersecurity, należy trzymać rękę na pulsie. Spotkania, warsztaty i prezentacje ekspertów to jedna ze ścieżek, którą warto obrać. Kolejna taka okazja będzie miała miejsce już 5 grudnia 2023 w Warszawie, gdzie w ramach konferencji Oh My H@ck spotkają się najlepsi polscy specjaliści cyberbezpieczeństwa.

Więcej o wydarzeniu można przeczytać TUTAJ.

Rekordowa edycja konferencji CONFidence

FOT. PROIDEA (13)


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

SECURITYMAGAZINE.PL

WYJĄTKOWE POMYSŁY I OGROMNA PASJA. TAK BYŁO NA HACKATHONIE UKNF!

PATRONAT
SECURITY MAGAZINE

Supervision_hack to hackathon, który odbył się po raz drugi, gromadząc liczne talenty z obszaru technologii i programowania. 19-21 maja ponad 250 uczestników przybyło do The Tides, aby podjąć wyzwania, które przygotował dla nich UKNF!

Wyjątkowe pomysły i ogromna pasja.
Tak było na hackathonie UKNF!

PRAWDZIWY SPRAWDZIAN DLA MŁODYCH PROGRAMISTÓW

Supervision_hack 2023 wzbudził ogromne zainteresowanie, a jego pula nagród wynosząca aż 150 000 PLN nie pozostawiła żadnego wątpliwości, że to prawdziwy sprawdzian dla młodych programistów. Zadanie nie było łatwe - uczestnicy rywalizowali o cenne nagród, ale prawdziwych zwycięzców mogło być tylko dwoje!

W tym roku UKNF stworzył dwa wyzwania:

- Zadanie nr 1. #FakeJobHunter - cel: walka z fałszywymi reklamami na rynku pracy
- Zadanie nr 2. #AdsDetect – cel: stworzenie mechanizmu wykrywania fałszywych reklam

Zgłoszono łącznie 15 projektów, które zapierały dech w piersiach swoją kreatywnością i innowacyjnością. Jury, złożone z uznanych ekspertów branży, miało trudne zadanie w wyborze najbardziej obiecujących rozwiązań.

Niezwykłe było nie tylko zaangażowanie i kreatywność uczestników, ale także energiczna atmosfera panująca na wydarzeniu. Kilkaset mocnych kaw dostarczonych przez niezawodnych baristów utrzymywało wszystkich w pełnym skupieniu przez cały hackathon. Nie zabrakowało również przekąsek - ponad 1500 kawałków pysznej pizzy pomogło uczestnikom zregenerować siły i nabrać nowej energii.

Druga edycja Supervision_hack okazała się nie tylko okazją do zdobycia cennych nagród, ale także do nawiązania kontaktów, dzielenia się wiedzą i tworzenia inspirujących rozwiązań technologicznych.

Wyjątkowe pomysły i ogromna pasja. Tak było na hackathonie UKNF!

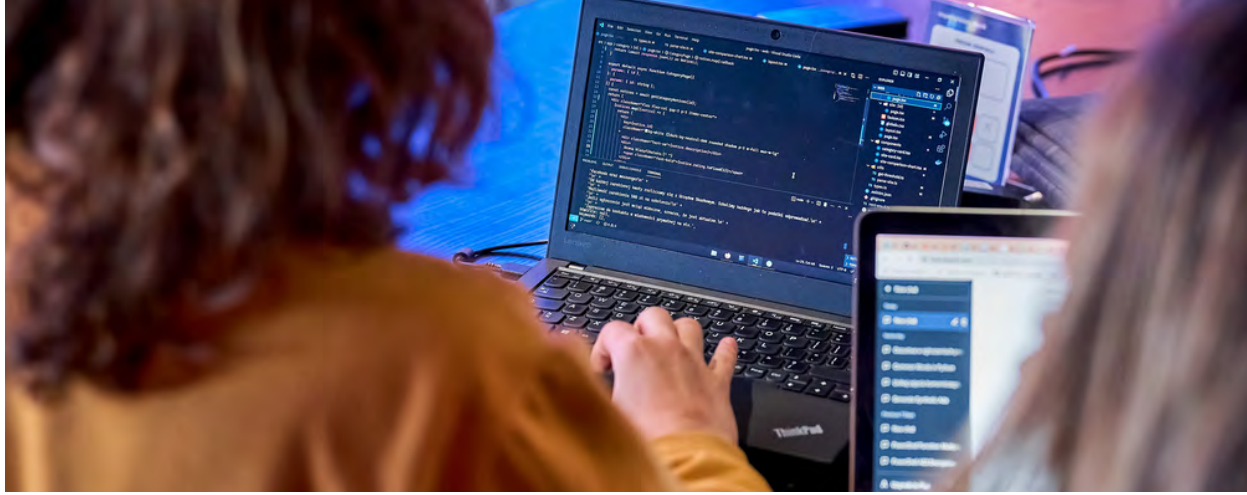
Wyjątkowe pomysły i ogromna pasja. Tak było na hackathonie UKNF!

Wydarzenie nie tylko spotkało się z ogromnym zainteresowaniem, ale przede wszystkim przyczyniło się do rozwoju innowacyjnego mechanizmów w branży fintech.

Zdjęcia z hackathonu Supervision_hack 2023 oraz więcej informacji można znaleźć na oficjalnej stronie wydarzenia_TUTAJ.

Wyjątkowe pomysły i ogromna pasja. Tak było na hackathonie UKNF!

Wyjątkowe pomysły i ogromna pasja. Tak było na hackathonie UKNF!



FOT. PROIDEA (17)


/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

CYBERATAKI ZAGROŻENIEM DLA BRANŻY MARKETINGU I PUBLIC RELATIONS

Redakcja
SECURITY MAGAZINE

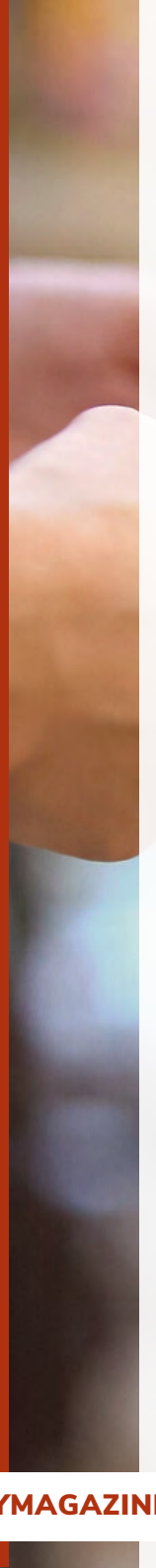
Mimo iż agencje marketingowe i PR-owe mogą nie być pierwszymi instytucjami, które kojarzymy z cyberatakami, stają one w obliczu podobnych zagrożeń co ich klienci. Jakie wyzwania związane z cyberbezpieczeństwem napotykają marketerzy i specjaliści PR, i jakie mają o nim pojęcie?

DLACZEGO CYBERPRZESTĘPCY ATAKUJĄ AGENCJE?

Choć na pierwszy rzut oka może się tak nie wydawać, agencje marketingowe i PR-owe są tak samo narażone na ataki cyberprzestępców, jak inne firmy. I to z różnych powodów. Niekiedy z tych samych, co w przypadku pozostałych organizacji, np. z chęci zdobycia pieniędzy (najczęściej poprzez szantaż lub kradzież środków) czy danych tych konkretnych firm.

To jednak nie jedyne powody. Wystarczy zacząć od samych danych. Agencje PR-owe i marketingowe przechowują nierzadko cenne informacje dotyczące ich klientów. Mowa tutaj np. o finansach czy planowanych wydatkach, inwestycjach, startujących kampaniach, nowych produktach, współpracy z influencerami, nadchodzących eventach itd. Pozyskanie takich danych może być dla cyberprzestępców niezwykle cenne. Mogą oni w ten sposób zaburzyć funkcjonowanie danej firmy albo sprzedać rzeczone informacje nieuczciwej konkurencji.

Przykładowo, z powodu kradzieży danych Sony Pictures Entertainment (w tym przypadku nie chodzi o agencję czy dział marketingu), kilka produkcji japońskiego giganta zostało odwołanych. A to dlatego, że wśród skradzionych informacji znalazły się m.in. scenariusze filmów.



Warto podkreślić, że przez to, iż obecny charakter agencji marketingowych i PR-owych mocno się zdigitalizował, siłą rzeczy łatwiej uderzać w takie organizacje. Dziś digital marketing i PR nierzadko grają pierwsze skrzypce. A wszystko, co przygotowują agencje, jest przechowywane online. To kuszący kąsek dla cyberprzestępców.

JAK CYBERPRZESTĘPCY ZAGRAŻAJĄ AGENCJOM?

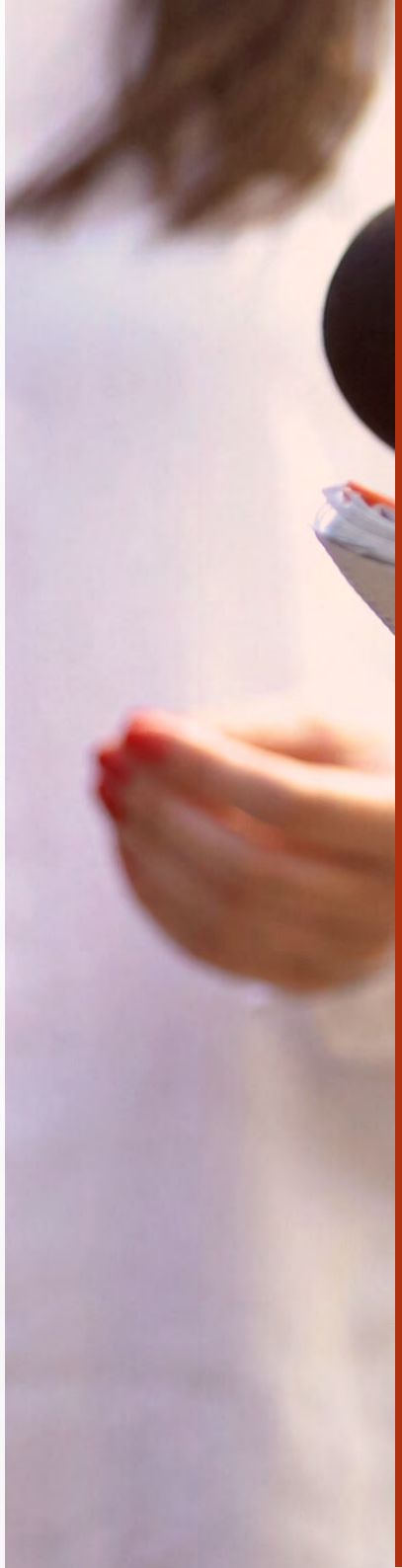
Cyberprzestępcy atakują również agencje PR-owe i marketingowe, aby zwyczajnie zaszkodzić wizerunkowi samym podmiotom, a także ich klientom. Zakłócenie działań takiej organizacji ma wpływ tak na jej reputację, jak i kontrahenta. Doprowadzić do dezinformacji, czy nawet zaszantażować agencję lub jej bezpośredniego klienta. A to wszystko wpływa nie tylko na komunikację, ale i na biznes marki.

Agencje marketingowe i PR-owe są też celem ze względu na... politykę. Czy to dosłowną, czy firmową (zarówno samej agencji, jak i klientów). Cyberprzestępcy, którzy nie zgadzają się z konkretnymi aspektami marki klienta, mogą zaatakować też agencje.

Cyberataki czasem mają też zaburzać działanie kampanii marketingowych i wizerunkowych. W tym celu cyberprzestępcy najczęściej wykorzystują np. złośliwe boty, które klikają reklamy, zwiększając ich koszty czy obciążają serwery stron internetowych, wywołując sztuczny ruch. Na celownikach są też systemy CMS czy CRM.

NAJGŁOŚNIEJSZE CYBERATAKI NA AGENCJE

Cybernaruszenia dotyczące agencji nie przechodzą tak wielkim echem, jak te wymierzone w inne przedsiębiorstwa. Kiedy spojrzymy na listy największych czy najgłośniejszych cyberataków na świecie, na próżno szukać tam tych wymierzonych w agencje.



Nie oznacza to jednak, że takie nie mają miejsca. Agencje nie dzielą się podobnymi informacjami, bo tego rodzaju szczegółowe dane o atakach hakerskich są często chronione ze względu na ich wrażliwość i prywatność klientów.

To jednak nie znaczy, że agencje marketingowe nie są narażone na cyberataki. Tak jak każda inna firma posiadająca wartościowe cyfrowe aktywa i dane, agencje marketingowe są celem dla cyberprzestępców. Różne formy ataków obejmują phishing, ransomware, ataki DDoS, włamanie do baz danych.

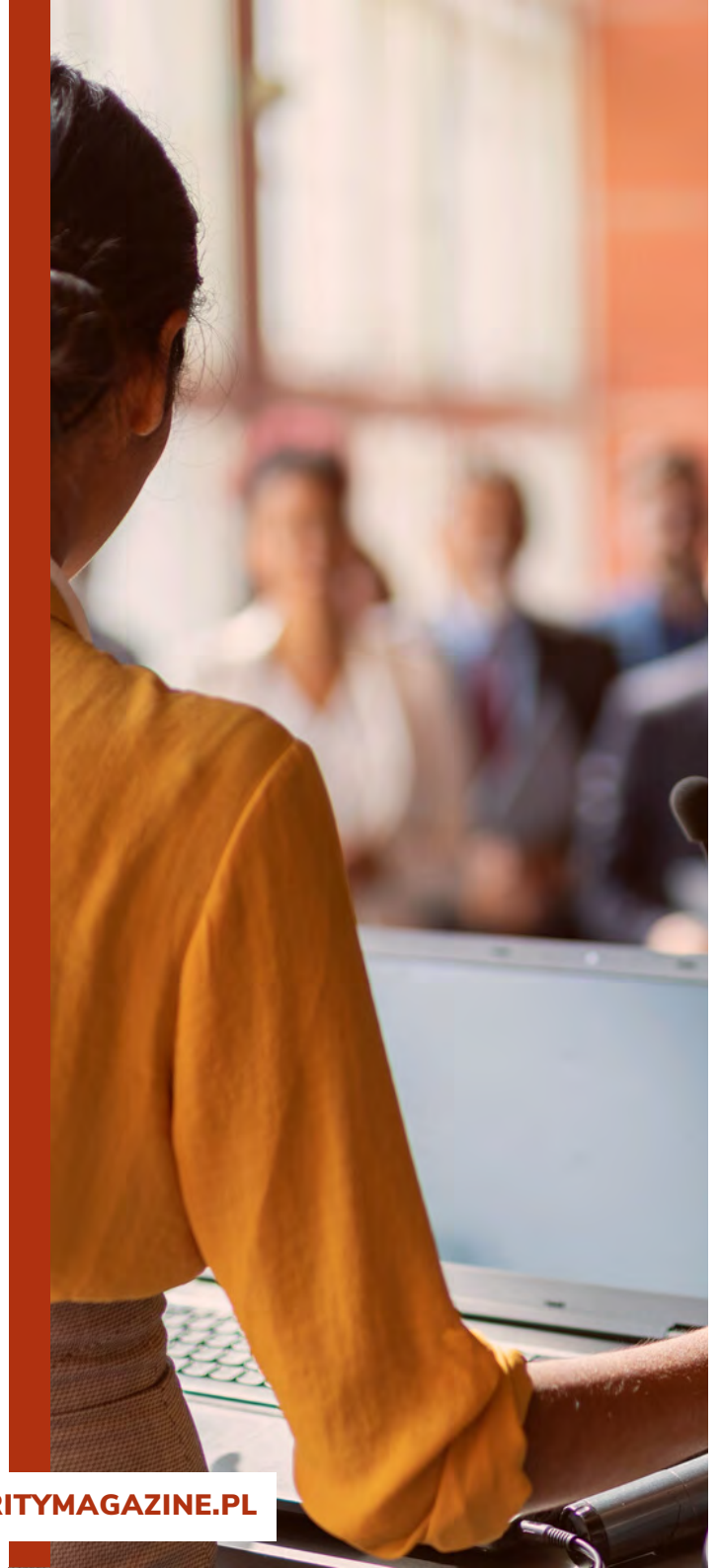
Przykładowo, firmy marketingowe często są celem ataków phishingowych, gdzie cyberprzestępca udaje, że jest pewną osobą lub firmą, aby skłonić pracowników do ujawnienia wrażliwych informacji, takich jak dane logowania, które mogą następnie być wykorzystane do nieautoryzowanego dostępu do systemów.

Przekonała się o tym np. firma WPP, która zrzesza takie agencje jak JWT, MediaCom czy Young & Rubicam. W 2017 roku poinformowała, że doświadczyła cyberataku.

Z tego powodu podmioty agencji nie miały dostępu do swoich urządzeń. Portal The Drum wskazał, że naruszenia dotyczyły wszystkich serwerów, komputerów i laptopów z systemem Windows. Wszystkie te urządzenia musiały zostać wyłączone i odłączone do odwołania. Nietrudno sobie wyobrazić, że firma, jak i jej klienci niezwykle na tym ucierpieli. Nawet kilka godzin braku dostępu do technologii, może opóźnić deadline'y o wiele dni czy tygodni.

Urządzenia te zostały zablokowane przez cyberprzestępców, którzy zażądali okupu w Bitcoinach. Jak się okazało – do cyberataku wykorzystano oprogramowanie ransomware znane jako WannaCry, które w latach 10. XXI wieku świeciło niechlubne tryumfy. Rok po naruszeniu CEO WPP przyznał, że koszt cyberataku wyniósł 15 mln dolarów, z czego ubezpieczenie pokrywało 10 mln dolarów. Oznacza to stratę aż 5 mln dolarów.

W 2019 roku agencja zajmująca się marketingiem influencerów, GetHero, przyznała, że doszło do kradzieży poufnych informacji, które posiadała. Na podstawie wpisu w internecie, opublikowanego przez sprawcę cyberataku, wynikało, że ma dostęp



do faktur oraz prywatnych dokumentów należących do dwóch sieci partnerskich, GetHero oraz Gamellon. W przypadku Gamellonu nie stwierdzono jednak żadnego wycieku danych.

Autor wpisu groził kierownictwu agencji, że jeżeli nie otrzyma okupu w wysokości 50 tysięcy złotych, będzie stopniowo publikował umowy zawarte z influencerami. Wśród ujawnionych umów znalazły się te z Young Multim (dotycząca muzycznego występu w jednym z klubów w Katowicach) oraz Frizem (dotycząca działań promocyjnych na YouTube). Ponadto, upubliczniono dokumenty związane ze współpracą z markami takimi jak Monte i Durex.

3 stycznia 2022 roku domeny Grupy iCEA, jednej z czołowych polskich agencji specjalizujących się w SEO i SXO, padły ofiarą ataków DDoS. Ataki te polegały na zajęciu wszystkich dostępnych i wolnych zasobów, by uniemożliwić funkcjonowanie całej usługi, w tym strony internetowej czy skrzynki poczty elektronicznej. Była to największa seria ataków DDoS na domeny Grupy iCEA, a co za tym idzie, na agencję SEO w Polsce.

Dzięki szybkiemu działaniu zespołów bezpieczeństwa i nadzoru sieci firmy Adminotaur, udało się zapobiec paraliżowi usług dla klientów Grupy iCEA. Firma podkreśliła w swoim komunikacie, że działanie kluczowych systemów nie było zagrożone w wyniku ataków.

PR-OWCY PRZYGOTOWANI NA CYBERZAGROŻENIA?

Ze względu na coraz bardziej online'owy charakter agencji PR i mar-

ketingowych, widać pewien progres – zwłaszcza po raporcie „Postrzeganie cyberbezpieczeństwa przez specjalistów ds. public relations w Polsce", przygotowanym przez Polską Agencję Prasową i Instytut Rozwoju Społeczeństwa Informacyjnego.

Według tego raportu, większość respondentów - specjalistów ds. public relations - zna takie pojęcia jak hacking (100%), phishing, pharming (98,3%), malware (87,4%), sniffing (73,1%), ransomware (63,9%) czy DoS/DDoS (54,6%). Co więcej – 88,2% z nich zarzeka się, że chroni swoje dane w internecie i te przechowywane zarówno na służbowym, jak i prywatnym komputerze.

A w jaki sposób? Większość wymienia zachowywanie ostrożności przy wchodzeniu w nieznane linki (96,2%), niekorzystanie z publicznych sieci WiFi (80%), stosowanie programów antywirusowych (80%), dwustopniowego logowania (72,4%), nieprzechowywania danych dostępowych i haseł na komputerze (54,3%), regularne zmienianie haseł (34,3%) czy monitorowanie informacji zbieranych przez strony internetowe (28,6%). Co więcej – zdaniem 88% PR-owców, potrafią oni rozpoznać maile z zagrożeniem. Z kolei 57% uważa, że potrafi samodzielnie chronić swoje dane. Mimo to i tak zdarzają się wpadki czy problemy.

PR-OWCY TRACĄ WAŻNE DANE?

Na pytanie, czy zdarzyło się Panu/i utracić ważne dane 13,4% PR-owców odpowiedziało, że tak. To co prawda niewiele, ale biorąc pod uwagę charakter pracy takich osób, może być szczególnie niebezpieczne. Zarówno dla ich agencji i klientów. Problemem jest jednak to, że ponad 1/3 wszystkich agencji PR-owych nie informuje na bieżąco pracowników o cyberzagrożeniach i nie instruuje ich jak się zabezpieczyć (mowa tutaj o 38,7%).

Dodatkowo – 57,1% PR-owców nie uczestniczyło w żadnych szkoleniach w zakresie cyberbezpieczeństwa. I jak wskazuje zdecydowana większość ekspertów – wiedzę czerpią z internetu (89,1%) i social mediów (47,9%). A jak dobrze wiemy – tam nie zawsze wiedza jest rzetelna i aktualna.

Zdaniem 38,7% PR-owców firmy w ich branży nie są wystarczająco dobrze chronione przed cyberatakami. Z kolei aż 40,3% respondentów odpowiedziało, że trudno powiedzieć, czy branża PR-owa jest bezpieczna w tym zakresie. Widać to też po tym, że jedynie dla 53% ekspertów w firmie, w której pracują, panuje ścisłe wytyczne odnośnie do cyberbezpieczeństwa. Mimo to PR-owcy zauważają, że cyberzagrożenia rosną. Aż 89% z nich wskazało, że na przestrzeni lat dostrzega stale rosnące zagrożenia w sieci. 68% często widzi wpisy, których autorami są boty. Z kolei 63% zawsze przy wykonywaniu czynności w sieci ma świadomość cyberzagrożeń.

PR-OWCY SŁABO CHRONIĄ WAŻNE PLIKI

Wspomniany raport PAP i IRSI ujawnia jeszcze coś ważnego. Choć z pozoru wielu PR-owców deklaruje wiedzę w kontekście cyberbezpieczeństwa, czy twierdzi, że umie chronić dane, to jednocześnie bardzo rzadko wysyłają pliki w bezpieczny sposób.

Przykładowo, aż 39% ekspertów nigdy nie hasłuje wysyłanego pliku, podając dostęp innym kanałem komunikacji. A 29% robi to wyjątkowo rzadko. To samo tyczy się hasłowania pliku i wysyłania go w odrębnym mailu. Tutaj nigdy nie stosuje tego 45% PR-owców, a 29% robi to rzadko. I to pomimo tego, że mają oni świadomość, jak łatwo można przechwycić tego typu pliki (zwłaszcza wysyłane np. poprzez WeTransfer) czy maile.

A ponadto nawet pomimo takich sytuacji, jak te z WPP czy GetHero uważają, że eksperci ds. PR-u są najmniej narażoną na cyberataki grupą. Nawet mniej niż np. dzieci i młodzież. To absurdalne zważywszy np. na dane Reboot Digital Marketing Agency, która w raporcie „Protecting the People" wskazała, że aż 20% osób pracujących w branży marketingu, PR-u i HR-u są celami wszystkich cyberataków w firmach. Biorąc pod uwagę ważną rolę tych sektorów (bo odpowiadających za wizerunek, komunikację i nierza-

dko pozyskiwanie oraz przechowywanie danych klientów) ta zuchwałość jest co najmniej nie na miejscu.

CMO NIE SĄ ZAANGAŻOWANI W CYBERBEZPIECZEŃSTWO?

CMO to dyrektor marketingu. Często jedna z najważniejszych osób w danej firmie. I jak pokazuje raport Deloitte „Why CMOs should care about cyber risk" ci bardzo rzadko są zaangażowani w cyberbezpieczeństwo. I to zarówno z ich własnej „inicjatywy", jak i firm, w których pracują.
A powinno być odwrotnie.

Dyrektorzy marketingu zwykle pełnią kluczowe role w kontekście wizerunku i... marketingu danych firm. A jak już ustaliliśmy – tym prawdziwe wyzwanie rzuca cyberprzestępczość. A dość powiedzieć, że według danych Deloitte CMO prowadzą (nie osobiście, bo mają do tego zespoły, ale te raportują do nich) 77% wszystkich kampanii social mediowych. A 58% odpowiada za analizę marketingową. CMO w firmach mają olbrzymią wiedzę i gromadzą niezliczone ilości danych. A jednocześnie – często są słabym ogniwem.

A warto dodać, że zgodnie z danymi dataprivacymanager.net dla 71% CMO największym kosztem incydentów cyberbezpieczeństwa jest utrata wartości marki. Co to oznacza dla agencji PR-owych i marketingowych?

Rzetelny® Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

BEZPIECZEŃSTWO TECHNOLOGII GENERATYWNEJ AI

Bartosz Baziński
SentiOne

SentiOne, firma specjalizująca się w sztucznej inteligencji, wprowadza na rynek innowacyjne rozwiązanie bazujące na LLM. W rozmowie CEO, Bartosz Baziński wyjaśnia m.in., jak technologia generatywna AI pozwala na skrócenie procesu tworzenia chatbotów przy jednoczesnym zapewnieniu bezpieczeństwa danych.

Początkiem roku ogłosiliście, że uruchamiacie polską odpowiedź na ChatGPT. Co zdecydowało, że postanowiliście stworzyć takie narzędzie?

Bartosz Baziński: W SentiOne od 12 lat rozwijamy swoje kompetencje w zakresie AI, budujemy własne algorytmy nauczania maszynowego, trenujemy własne modele AI, łącznie zainwestowaliśmy ponad 45 milionów zł w rozwój własnej sztucznej inteligencji - bycie częścią rewolucji generatywnej AI to był dla nas naturalny krok. W grudniu na rynku pojawił się publicznie dostępny ChatGPT i od razu zaczęliśmy zastanawiać się, jak go użyć, aby jeszcze mocniej wesprzeć nasze produkty, oraz czy możemy stworzyć podobną technologię własnymi rękami.

Czym narzędzie od SentiOne różni się od tego stworzonego przez OpenAI?

B.B.: Naszym założeniem było stworzenie LLM (large language model) takiego jak ChatGPT, ale odpowiedniego dla biznesu - czyli modeli językowych, które nie mają szansy konfabulować, rozpowszechniać fake newsów albo halucynować. Dodatkowo LLM-y SentiOne mogą być hostowane na prywatnych serwerach (on-premise), tak by zapewnić bezpieczeństwo przetwarzania i przechowywania danych. W rezultacie jest to świetne dopełnienie naszej oferty chatbotowej dla klientów typu enterprise, gdyż sama

budowa bota i jego scenariuszy dialogowych została znacząco skrócona.

Jakie były główne wyzwania technologiczne związane z opracowaniem waszej generatywnej sztucznej inteligencji?

B.B.: Jednym z najważniejszych elementów budowy bota jest również zdefiniowanie mu odpowiedniej bazy wiedzy, z której pobiera informacje, które potem przekazuje klientom podczas rozmowy. W SentiOne mamy bardzo rozbudowaną funkcjonalność budowania bazy wiedzy dla bota: mogą to być informacje produktowe klienta, polityka bezpieczeństwa, regulaminy, cenniki usług itd.

Dodatkowo trzeba pamiętać, że wszystkie narzędzia oparte o AI są dobre tylko na tyle, na ile ich dane uczące. Dlatego, aby usunąć zagrożenia związane z halucynacją, wprowadzaniem w błąd lub rozsiewaniem fake newsów, należy wyczyścić dane treningowe ze wszystkich ryzykownych elementów. W SentiOne czyścimy dane treningowe z obraźliwych treści, przeuczamy modele AI tak, aby ich wiedza była stale aktualizowana oraz odświeżana. Dodatkowo testujemy aktualnie nowe funkcje takie jak “unlearning modeli AI” - tak by modele AI mogły oduczyć się złych lub niepoprawnych treści.

W jaki sposób technologia LLM pozwoliła przyspieszyć proces tworzenia nowych botów z 3 dni do 3 godzin?

B.B.: Generatywną AI można wykorzystać, by dosłownie przyspieszyć pracę. W przypadku naszych botów generatywna AI jest w stanie stworzyć automatycznie wszystkie elementy potrzebne do ich budowy: przykładowe frazy, wypowiedzi, testowe zapytania lub słowa kluczowe służące do trenowania silnika języka naturalnego. Dzięki przyspieszeniu tworzenia wszystkich elementów budowy bota, zajmuje ona o 60-90% czasu mniej niż dotychczas.

W rezultacie boty SentiOne są nadal są bardzo bezpieczne z punktu widzenia brandingu i biznesu - odpowiadają tylko na te zakresy tematyczne, które im wcześniej zdefiniowaliśmy, pobierają informacje ze wskazanych bazy wiedzy, nie wymyślają odpowiedzi, nie mają halucynacji. A jednocześnie, dzięki wsparciu generatywnej AI, odpowiadają pięknym oraz kreatywnym językiem, stają się coraz mniej robotyczne. Dzięki automatyzacji samej budowy bota, w SentiOne jesteśmy w stanie zbudować testowego / pilotażowego bota dla klienta już w ciągu kilku godzin.

Które firmy mogą skorzystać z oferty testowania nowego rozwiązania i co zyskają dzięki temu?

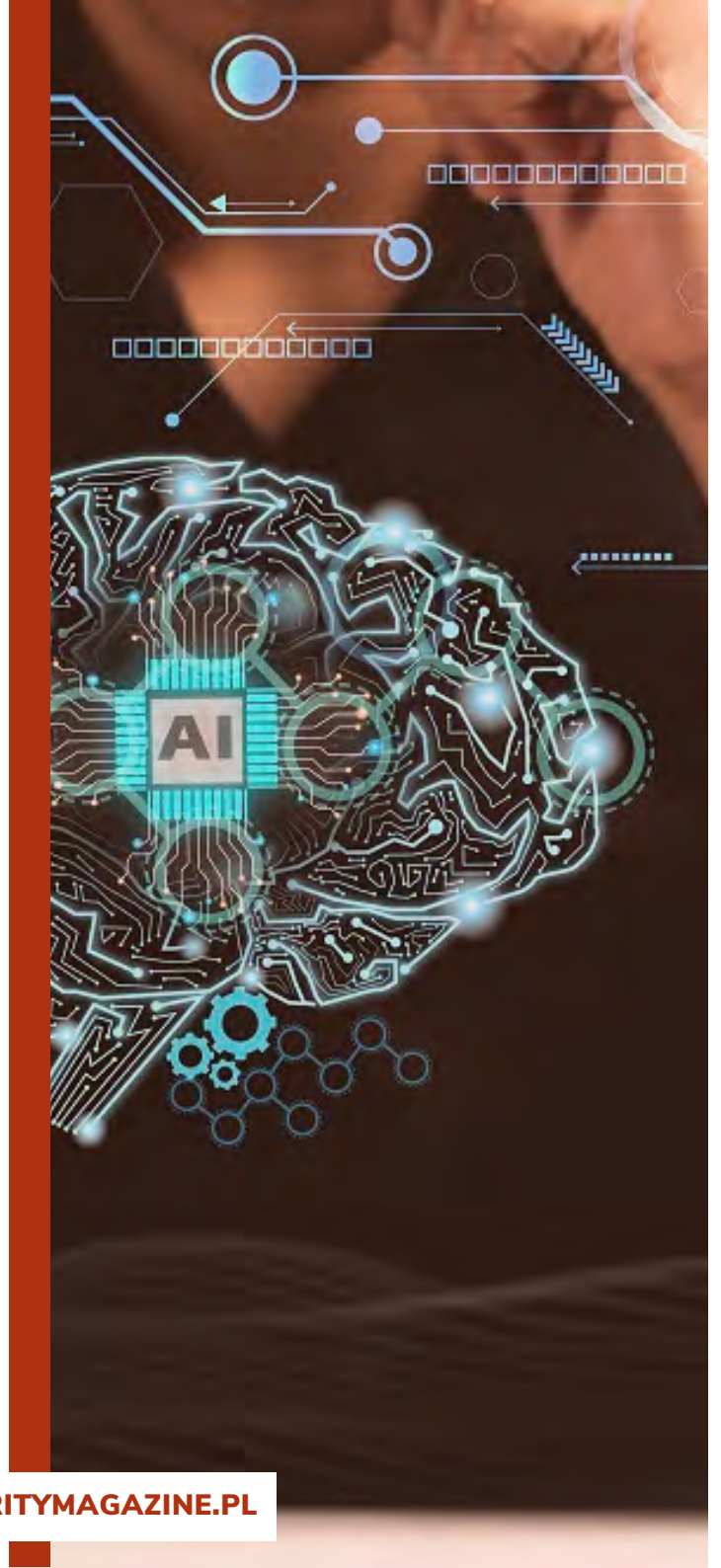
B.B.: Zapraszamy do testów wszystkie firmy, które widzą u siebie potrzebę automatyzacji procesów - obsługi klienta, wiadomości sprzedażowych, lub procesy wewnętrzne - w postaci automatycznego intranetu dla pracowników. Z wybranymi firmami zbudujemy testowe chatboty, oparte na technologii LLM. Wspólnie zbadamy skuteczność botów w pobieraniu informacji z bazy wiedzy. Przykładowo, do bazy wiedzy chatbota załadujemy kilka dokumentów na temat oferty firmy, jej polityki, cennik produktów itd., a następnie będziemy w stanie sprawdzić, na ile skutecznie bot wyciąga oraz interpretuje informacje z bazy wiedzy.

Czy mógłby Pan podać przykłady praktycznych zastosowań Waszej technologii w biznesie?

B.B.: Technologia jest bardzo młoda, w fazie beta, więc jesteśmy na etapie testowania. Niestety, produkcyjnie jeszcze żadna firma w Polsce nie używa żadnego LLM w swoich chatbotach, wedle naszej wiedzy. Ale w praktyce, modele typu LLM zrewolucjonizują wiele branży.

Jak technologia LLM radzi sobie z różnymi specyfikami branżowymi i na jakiej bazie danych jest trenowana?

B.B.: Jak widzimy na przykładzie otwarcie dostępnych LLM, takich jak tych od Open AI lub Mety, już takie generyczne modele odpowiadają imponująco. Natomiast po dostosowaniu technologii LLM do potrzeb biznesowych, przetrenowaniu na danych dziedzinowych z bankowości, na bezpośrednich danych od klienta (np. transkrypcje rozmów z call center, zapisy rozmów z Messengera i emaili) oparty na niej chatbot staje się bardzo zaawansowanym i wyuczonym konsultantem obsługi klienta i odcią-



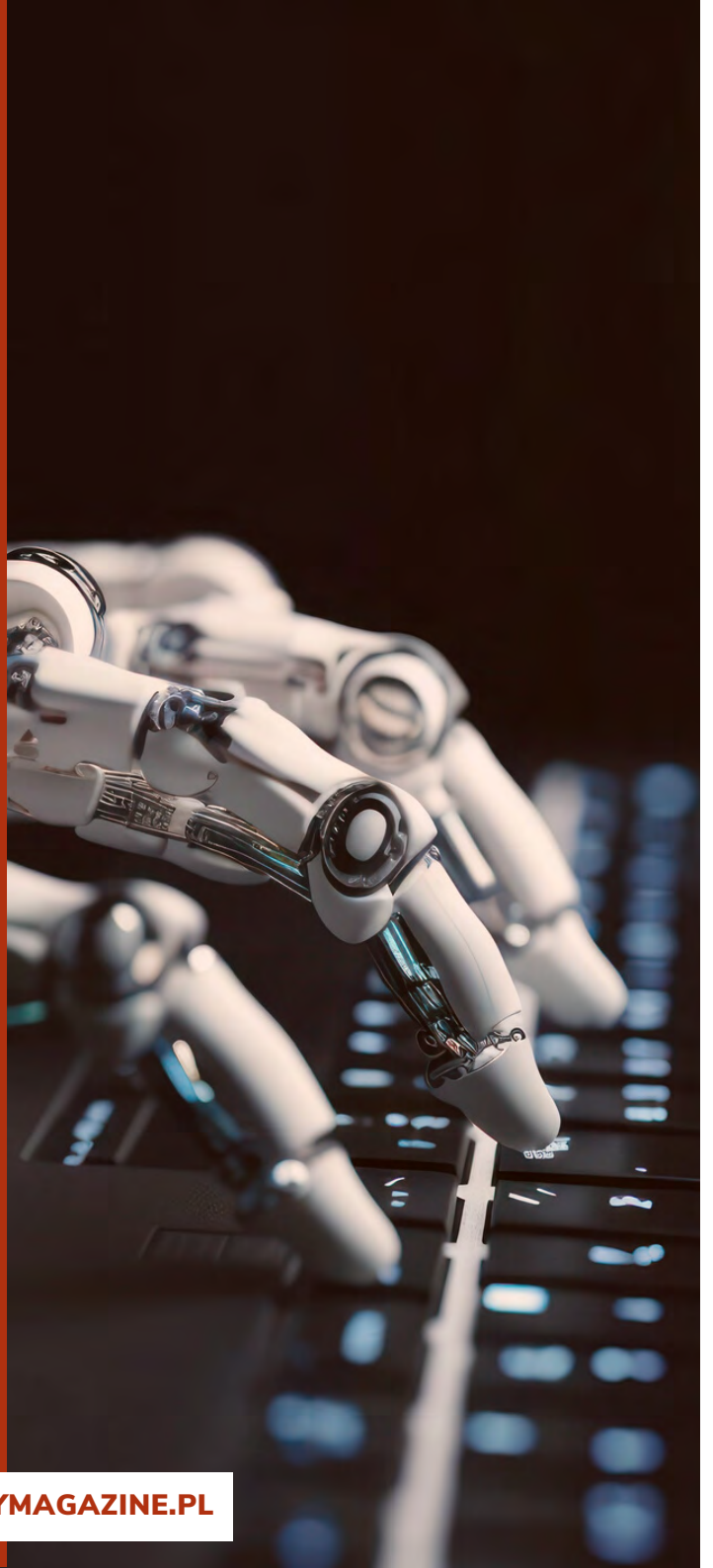
żeniem dla call center.

Jak technologia LLM radzi sobie z różnymi specyfikami branżowymi i na jakiej bazie danych jest trenowana?

B.B.: Jak widzimy na przykładzie otwarcie dostępnych LLM, takich jak tych od Open AI lub Mety, już takie generyczne modele odpowiadają imponująco. Natomiast po dostosowaniu technologii LLM do potrzeb biznesowych, przetrenowaniu na danych dziedzinowych z bankowości, na bezpośrednich danych od klienta (np. transkrypcje rozmów z call center, zapisy rozmów z Messengera i emaili) oparty na niej chatbot staje się bardzo zaawansowanym i wyuczonym konsultantem obsługi klienta i odciążeniem dla call center.

W jaki sposób technologia LLM zapewnia bezpieczeństwo danych, zwłaszcza w kontekście możliwości wdrożenia rozwiązania on-premise?

B.B.: I tutaj należy rozróżnić powszechnie dostępny i otwarty ChatGPT, który aktualnie zmaga się z dużymi problemami bezpieczeństwa. Korzystanie z zewnętrznych LLM typu OpenAI stanowi ryzyko, bo dane mogą wyciekać w niekontrolowany sposób i ciężko jest stwierdzić, co się z nimi dzieje Ostatnio HackerNews raportował, że ponad 101 tysięcy danych logowania do kont OpenAI wyciekło i znalazło się na nielegalnych platformach Dark Web między majem 2022 a czerwcem 2023.



Tak więc wdrożenia on-premise to na razie jedyny sposób na zagwarantowanie bezpieczeństwa. Przede wszystkim, wdrożenie on-premise oznacza, że wszystkie dane przetwarzane przez system LLM pozostają w sieci wewnętrznej klienta. To eliminuje ryzyko utraty danych podczas transmisji przez publiczne sieci internetowe.

Użytkownicy wysyłają do LLM dane, łącznie z danymi osobowymi. Dlatego system LLM jest zaprojektowany tak, aby bezpiecznie przechowywać wszystkie generowane dialogi, w tym logi. Technologia LLM może być wyposażona w wykrywacz halucynacji, który służy do weryfikacji generowanych numerów, adresów i innych danych. To zapewnia dodatkową warstwę ochrony przed przypadkowym lub niezamierzonym ujawnieniem poufnych informacji.

Zaawansowane mechanizmy szyfrowania stosowane w technologii LLM chronią dane w trakcie przechowywania i transmisji. Zastosowanie silnego szyfrowania zapewnia, że nawet w przypadku potencjalnego naruszenia bezpieczeństwa, dane użytkowników pozostaną niedostępne dla nieuprawnionych osób.

Technologia LLM może być w pełni zintegrowana z istniejącymi systemami bezpieczeństwa przedsiębiorstwa. To oznacza, że wszystkie funkcje związane z ochroną danych, takie jak zarządzanie tożsamością i dostępem, detekcja anomalii, czy ochrona przed zagrożeniami zewnętrznymi, mogą być nadal obsługiwane

przez sprawdzone, zaufane rozwiązania, które już są w użyciu w organizacji.

Jaki jest zakres geograficzny Waszej obecnej działalności i jakie są plany na przyszłość, zwłaszcza związane z ekspansją technologii LLM na inne rynki?

B.B.: Modele large language tworzymy po kolei na język angielski oraz polski, i na nich się skupiamy. Natomiast cały czas mamy bardzo sprawdzone i działające modele konwersacyjnej sztucznej inteligencji, oparte na silniku rozumienia języka naturalnego dla ponad 17 języków, w tym dla większości języków europejskich oraz arabskiego. Jeśli chodzi o ekspansję zagraniczną, cały czas działamy na rynku Bliskiego Wschodu w partnerstwie z największą tamtejszą firmą telekomunikacyjną - Etisalat - która daje nam dostęp do swoich klientów biznesowych na 16 rynkach. Aktywnie sprzedajemy nasze rozwiązania chatbotowe w Europie zachodniej - Niemczech, Hiszpanii, Francji i Włoszech. Dodatkowo w tym roku otworzyliśmy biuro w Londynie, zatrudniliśmy trzech sprzedawców na UK i planujemy znacząco zwiększyć swoje przychody z tego rynku.

ZAMÓW AUDYT BEZPIECZEŃSTWA

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

DOWIEDZ SIĘ WIĘCEJ!

Polityka® Bezpieczeństwa

SECURITYMAGAZINE.PL

BACKUP I KOPIE ZAPASOWE, CYBER-BEZPIECZEŃSTWO I MONITORING WEWNĘTRZNY

Redakcja
SECURITY MAGAZINE

Bezpieczeństwo, jak i cyberbezpieczeństwo w firmach są niezwykle ważne. Twoja organizacja powinna dbać o infrastrukturę tak cyfrową, jak i fizyczną. Zobacz, jak trzy różne startupy pomogą Ci usprawnić bezpieczeństwo w firmie.

BEZPIECZEŃSTWO IT

Perceptus to startup, który zajmuje się cyberbezpieczeństwem i zarządzaniem sieciami IT od 2008 r. Organizacja specjalizuje się w integracji systemów oraz dostarczaniu oprogramowania antywirusowego i narzędzi ochrony danych dla przedsiębiorstw. Głównym celem działalności startupu jest tworzenie przyjaznego i bezpiecznego środowiska informatycznego dla klientów biznesowych oraz instytucjonalnych.

Startup oferuje kompleksową analizę potrzeb klientów. Eksperci Perceptus opracowują rekomendacje dotyczące konfiguracji urządzeń i oprogramowania, zwiększając skuteczność mechanizmów zabezpieczających już na etapie wdrażania nowych rozwiązań.

Ponadto startup dostarcza też oprogramowanie antywirusowe dla firm. To ma zapewniać ochronę przed wirusami, ransomware i malware. W ofercie Perceptus nie zabrakło też wdrażania systemu backupu danych, zarówno lokalnie, jak i w chmurze, aby zapewnić bezpieczeństwo danych w sytuacji awarii lub utraty sprzętu.

Organizacja specjalizuje się również w dziedzinie cyberbezpieczeństwa i oferuje urządzenia takie jak UTM (Unified Threat Management) oraz NG Firewall, np. Stormshield. Działają one jako systemy zapobiegania włamaniom, filtrowania treści stron internetowych oraz ochrona przed spamem.

Perceptus pomaga też wdrażać oprogramowanie DLP (Data Loss Prevention), takie jak Safetica czy DeviceLock, które chroni przed wyciekami danych oraz utratą informacji. Oczywiście – możliwości, jakie zapewnia startup jest znacznie więcej. W skrócie - organizacja ta zajmuje się kompleksowym cyberbezpieczeństwem.

BACKUP I PRZYWRACANIE DANYCH PO AWARII

Xopero to startup, który powstał w 2009 r. i wywodzi się z Gorzowa Wielkopolskiego. Organizacja oferuje kompleksowy backup danych, obejmujący środowiska fizyczne, wirtualne, aplikacje SaaS oraz ekosystem DevOps. Klienci startupu to głównie sektory SMB i enterprise.

W ofercie Xopero znajdziemy m.in. proste w użyciu narzędzie do tworzenia kopii zapasowych laptopów i stacji roboczych opartych na systemach Windows, Mac czy Linux.

Startup ponadto podkreśla, że działa ono tak samo, niezależnie od tego, czy mamy do czynienia z jednym urządzeniem, czy nawet z milionem.

Xopero pomaga także w kwestii pełnego zabezpieczenia środowiska VMware, obejmującego zarówno vCenter, jak i niezależne hosty ESXi. A także rozwiązanie do tworzenia kopii zapasowych z wbudowanym mechanizmem Disaster Recovery, zapewniające ochronę dla środowisk DevOps.

Startup umożliwia również automatyczne tworzenie kopii zapasowych pakietu Office 365 – Exchange, Outlook oraz OneDrive. A także możliwość przechowywania kopii lokalnie lub w chmurze Xopero.

Dodatkowo w przypadku backupu klienci mogą wybrać między predefiniowanym planem a ustawieniem własnego, aby przyspieszyć wykonywanie kopii zapasowych czy zredukować zużycie magazynu danych.

Wśród swoich klientów Xopero T-Mobile, Orange, North Food, Subway, Roleski i wiele innych. Dodatkowo firma jest także członkiem The Linx Foundation czy Cloud NAtive Computing Foundation.

MONITOROWANIE I NAWIGACJA WEWNĄTRZ BUDYNKÓW

IndoorNavi z Gdańska z kolei pomaga w kontekście bezpieczeństwa wnętrza budynków. Oprogramowanie oferowane przez startup umożliwia zbieranie danych i analizę architektury oraz przestrzeni, w której poruszają się użytkownicy.

Jak to działa? Technologia oparta jest na specjalistycznym sprzęcie oraz dedykowanym oprogramowaniu. Do siatkowania budynku instalowane są kotwy, które umożliwiają gromadzenie danych. Bezprzewodowe tagi przesyłają informacje o pozycji i zdarzeniach do centralnego serwera. Na podstawie lokalizacji użytkowników są udostępniane informacje, takie jak optymalne trasy podróży, naruszenia dostępu czy przypadkowe zdarzenia.

Administratorzy wykorzystują historyczne i bieżące dane o położeniu urządzeń w celu optymalizacji procesów. IndoorNavi umożliwia integrację istniejących elementów systemu. Zachowując tym samym korzyści związane ze starszymi rozwiązaniami, przy jednoczesnym dostępie do najnowocześniejszego systemu lokalizacji czasu rzeczywistego.

Rozwiązanie IndoorNavi jest dostępne na różnych platformach i w różnych środowiskach. Startup skupia się na zapewnieniu niezawodnej obsługi mobilnej i narzędzi potrzebnych do tworzenia aplikacji mobilnych dla pracowników klienta.

Startup chwali się, że dzięki zastosowaniu IndoorNavi można zminimalizować ryzyko wypadków poprzez 80% redukcję nieautoryzowanego dostępu do stref niebezpiecznych.

Optymalizacja wykorzystania powierzchni użytkowej miałaby z kolei przynieść poprawę efektywności o 20%.

Dzięki dokładności lokalizacji personelu na poziomie 10 centymetrów można zwiększyć bezpieczeństwo w obszarach niebezpiecznych i zmniejszyć zagrożenie dla zdrowia.

To jednak nie wszystko, bo IndoorNavi twierdzi też, że obniżenie kosztów i poprawa efektywności jest możliwa dzięki zmniejszeniu zużycia sprzętu potrzebnego do wykonywania zadań o 30%. Z kolei dzięki zwiększeniu obszaru bezpieczeństwa o 45% można skrócić czas reakcji na potencjalne zagrożenia dla gości i pracowników.

Wszystko to ma być możliwe dzięki wykorzystaniu bigdata i aplikacji serwerowej IndoorNavi. Głównymi klientami startupu są firmy, które wdrażają rozwiązania z zakresu przemysłu 4.0.

To, oczywiście, nie wszystkie startupy pomagające w kontekście bezpieczeństwa w firmie i cyberbezpieczeństwa. Na rynku jest całe mnóstwo takich rozwiązań. Wszystko zależy od tego, jak ważne są dla Ciebie i Twojej firmy te aspekty i na kogo się zdecydujesz.

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

PIERWSZA POMOC DLA PRACOWNIKÓW ZDAL-NYCH: OCHRONA DANYCH W DOBIE CYFRYZACJI

Damian Żłobicki
WłączWizję

Bezpieczeństwo naszych pracowników jest bezpieczeństwem naszej firmy. Idąc tym samym tropem, powinniśmy bronić danych naszych pracowników w podobny sposób, w jaki chcemy ochraniać dane należące do naszego przedsiębiorstwa.

ZMIANA PREFERENCJI

Rok 2020 zrewolucjonizował globalny rynek pracy. Podczas rozprzestrzeniania się koronawirusa, któremu towarzyszyły liczne lockdowny, sankcje, regulacje oraz wiele miesięcy przymusowej zdalnej pracy i edukacji, wśród pracowników postępowała ewolucja. I choć, zgodnie z ogłoszeniem WHO, od 5 maja pandemia zostaje uznana za zakończoną, na stałe zmianie uległy ludzkie preferencje dotyczące stylów i środowiska pracy.

Dziś czymś całkowicie powszechnym i pożądanym przez zatrudnionych jest możliwość podjęcia pracy zdalnej. O ile niektórzy giganci mogą pozwolić sobie na zatrudnianie pracowników z całego świata, oferując im pracę całkowicie zdalną na preferencyjnych warunkach, to niektóre sektory są tej możliwości pozbawione, ze względu na chociażby politykę biurową. Popularniejszym rozwiązaniem okazuje się być praca hybrydowa.

Tryb mieszany cechuje się pewnymi udogodnieniami dla obydwu stron machiny: pracodawcy i pracowników. Ze względu na rotację personelu, firma może pozwolić sobie na wprowadzenie hot desków (wolnych miejsc w przestrzeniach co-workingowych, w których obowiązuje zasada „kto pierwszy ten lepszy"). To wygodne rozwiązanie - jeśli pracownicy pracują pół tygodnia w biurze, można w ten sposób zredukować połowę biurek.

Dzięki redukcji stanowisk pracy, firmy mogą ograniczyć wydatki na energię, czy wynajem nieruchomości (mogą się przenieść np. do mniejszych biur). Zaoszczędzając w ten sposób, są także w stanie oferować dogodniejsze warunki swoim pracownikom.

REWOLUCJA CYFROWA

Zmieniły się nasze tendencje do trybu pracy, owszem, ale zmienił się też świat.

Obecnie jesteśmy w procesie totalnej rewolucji cyfrowej. Doświadczamy tego, patrząc jak appki powstałe na bazie chatu GPT, są w stanie wygrywać konkursy zdjęciowe, a także: generować wielogodzinne treści wideo, czy tworzyć projekcję cyfrową kogokolwiek gdziekolwiek.

Mimo wszystko, minie trochę czasu, zanim nasi pracownicy będą generować swoje cyfrowe klony podczas wideorozmów, choć z perspektywy aktualnego postępu technologicznego - taki trik nie jest niczym zaskakującym. Jeśli współpracujemy w środowisku kreatywnym, powinniśmy mieć się na baczności!

Sztuczna inteligencja (ang. artificial intelligence, AI) jest istotnie jedną z pierwszoplanowych postaci aktualnych przemian. To, czy i w jakim stopniu nauczymy się wykorzystywać AI w swoim biznesie, może stanowić o „być" albo „nie być" naszej firmy w perspektywie kilku następnych lat.

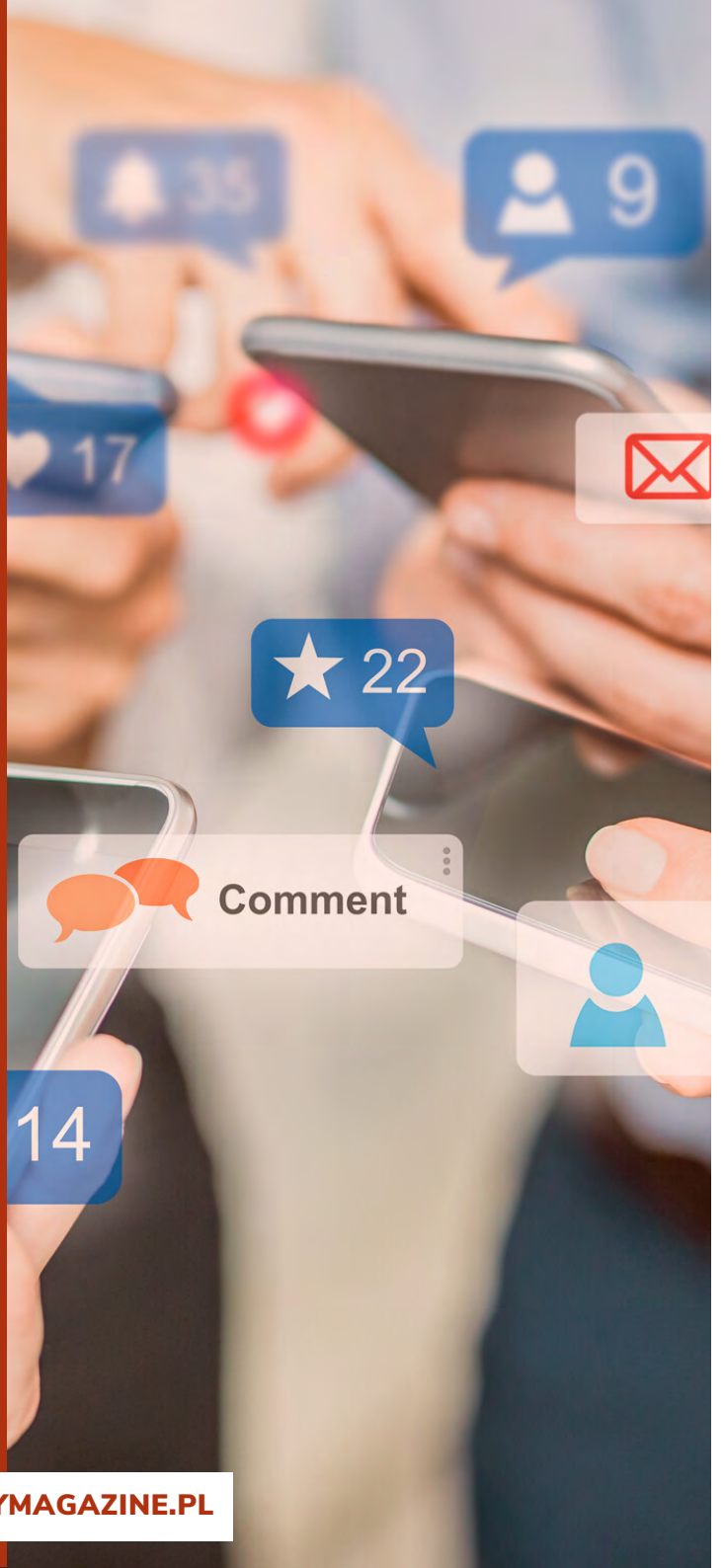
Także automatyzacja dociera do nas zewsząd.

Żyjemy w świecie 2.0, w którym technologie pozwalają na kontrolowanie każdego aspektu życia społecznego.

W Chinach w praktycznie każdym miejscu publicznym rozmieszczone są kamery biometryczne. Te śledzą i analizują ruch obywateli, a z informacjami przekazywanymi przez smartfony Chińczyków, są w stanie wyświetlać statystyki dotyczące każdego uczestnika życia społecznego z taką skutecznością, jakiej nie powstydziłby się żaden producent gier wideo.

W Białorusi natomiast czymś powszechnym jest rewizja osobista, podczas której funkcjonariusze przeglądają obywatelom Telegrama i pozostałe komunikatory. A jeśli taki obywatel należy do jakiejś opozycyjnej grupy? Jest to wystarczający powód, aby taką osobę aresztować.

Globalna inwigilacja, której zostaliśmy poddani w imię bezpieczeństwa, sprowadza nas do miejsca, w którym niezwykle ważne staje się świadome podejmowanie decyzji co do publikowanych przez nas treści w Internecie.



Media społecznościowe wciąż skutecznie zachęcają nas, abyśmy udostępniali swoje zdjęcia wraz ze wszystkimi metadanymi, takimi jak: lokalizacja, godzina, rodzaj i numer seryjny urządzenia, którym tworzyliśmy treści. My się tymi danymi chętnie dzielimy, nie widząc zagrożenia.

Z faktem, że społecznościówki są naszą cyfrową wizytówką, nie mogą polemizować osoby, które utraciły pracę po opublikowaniu kontrowersyjnych relacji. W Internecie możemy znaleźć liczne przykłady takich osób, a i mam takie w swoim najbliższym otoczeniu.

Moja koleżanka rozstała się z firmą, dla której realizowała usługi, po wrzuceniu humorystycznej relacji, którą stworzyła w miejscu i godzinach pracy. To, że miała konto prywatne na Instagramie, przed niczym ją nie uchroniło, zważywszy na to, że w gronie jej obserwujących był ktoś, kto zdecydował się na nią donieść.

Szczerze mówiąc, nie dziwi mnie przezorność firm w tej materii. Internet rządzi się swoimi prawami i nigdy nie wiemy, czy jakaś informacja, zdjęcie, czy film nie zaczną żyć swoim życiem. Zasada jest taka: to, co udostępniliśmy, zobaczyli już wszyscy. Stosując się do tej zasady, powinniśmy uczulać naszych pracowników, żeby nie publikowali treści, które mogłyby negatywnie wpłynąć na wizerunek firmy, a także ograniczyć ilość informacji na temat swojego życia prywatnego.

Apple i Google wiedzą, jak wyglądamy i gdzie ostatnio jedliśmy. Facebook chętnie podpowie nam, z kim ostatnio spotkaliśmy się na konferencji, jak i zasugeruje nam reklamy na podstawie rozmów, które odbyliśmy zaledwie kilka minut wcześniej.

Internet i współczesne technologie stwarzają nam ogrom możliwości rozwoju siebie, swoich biznesów i kreowania marki. Jeśli poświęcilibyśmy wystarczająco dużo energii, czasu i uwagi, moglibyśmy opanować niemal każdą umiejętność, oglądając filmy na YouTube. Czy w takim razie warto jest inwestować w szkolenia?

Warto, bo to, że mamy do czegoś dostęp, nie oznacza, że z niego korzystamy. Mamy wiedzę, jak przeciwdziałać atakom i systemy, które umożliwiają nam szybkie reagowanie w sytuacjach zagrożenia. Moje doświadczenie z sali szkoleniowej pokazuje jednak, że najbardziej zagrażającym bezpieczeństwu cyfrowemu wyzwaniem jest nieuważność użytkownika. Jeśli pracownicy nie zabezpieczają swoich kont do mediów społecznościowych, dane naszej firmy są zagrożone niezależnie od tego, czy prowadzi do nich inna droga niż do konta na Facebooku.

NARZĘDZIA PIERWSZEJ POTRZEBY

Aktualnie dysponujemy milionami poradników, jak zadbać o cyberbezpieczeństwo własne i swojej organizacji. Wpisując w wyszukiwarkę Google hasło „cybersecurity”, uzyskamy dostęp do 810 mln stron. Do lepszego zabezpieczania swoich kont możemy wykorzystać antywirusy i odpowiednie zapory. Blokady nieznanych domen i aplikacji mogą zapewnić bezpieczniejsze korzystanie z Intranetu. Gmail powiadomi nas o próbie oszustwa pod postacią wiadomości phishingowych (są to wyłudzenia w formie pilnych komunikatów, np. „Twoja przesyłka nie została w pełni opłacona, dopłać złotówkę pod linkiem”).

Bezpieczeństwo naszych pracowników jest bezpieczeństwem naszej firmy. Powinniśmy więc bronić danych naszych pracowników w podobny sposób, w jaki chcemy chronić dane należące do naszego przedsiębiorstwa.

Żeby to osiągnąć, możemy wyposażyć nasze zdalne zespoły w następujące narzędzia:

- Klucze U2F - urządzenia, które pozwalają na autoryzację logowania przez wpięcie do portu USB w laptopie lub przyłożenie NFC do smart-

fona. Jeśli określimy klucze U2F jako jedyną metodę autoryzacji, uniemożliwiamy tym samym dostania się do naszych kont i urządzeń alternatywnymi kanałami. Rynkowa cena kluczy U2F, to od 150 do 700 zł. Jeśli decydujemy się na tę formę zabezpieczeń, dobrą praktyką jest posiadanie dwóch takich kluczy: jednego z łatwym dostępem oraz drugiego ukrytego. Tym sposobem, jeśli taki klucz zgubimy, mamy wciąż możliwość zalogowania się.

- **Nakładki prywatyzujące** - folie przyklejane na ekran, które odbijają światło, dzięki czemu osoba stojąca za użytkownikiem urządzenia nie jest w stanie go podglądać. Łamanie haseł specjalnymi algorytmami jest tylko jedną z możliwości, jaką mają cyberprzestępcy. Nieco inną, wciąż skuteczną, jest podglądanie. Zazwyczaj filtry prywatyzujące zaczerniają obraz użytkownikom przy nachyleniu pod kątem 30 stopni. Co więcej, posiadają refleksy, dzięki czemu redukują szkodliwe działanie światła niebieskiego. Jest to korzyść i dla zdrowia i dla bezpieczeństwa. Rynkowa cena filtrów waha się od kilkudziesięciu złotych do czterystu złotych.

- **Zdrowy rozsądek** - zwłaszcza ten dotyczący publikacji materiałów w social mediach! Udostępniając nadmiar informacji na swój temat, wystawiamy się na ryzyko zhakowania. W tym przypadku dobrymi praktykami jest niepublikowanie treści dotyczących aktualnego miejsca pobytu (jeśli jesteśmy na wakacjach), a także ograniczanie grona odbiorców, do którego kierujemy prywatne treści. Świat się zmienia z każdym dniem. Praca zdalna i transformacja cyfrowa są wszechobecne i jest to postęp, którego nie sposób uniknąć ani zatrzymać. Musimy nauczyć siebie i swoje zespoły jak dbać o podstawy swojego cyberbezpieczeństwa. Zrobimy to, inwestując w narzędzia i odpowiednio edukując nasz personel.

Polityka® Bezpieczeństwa

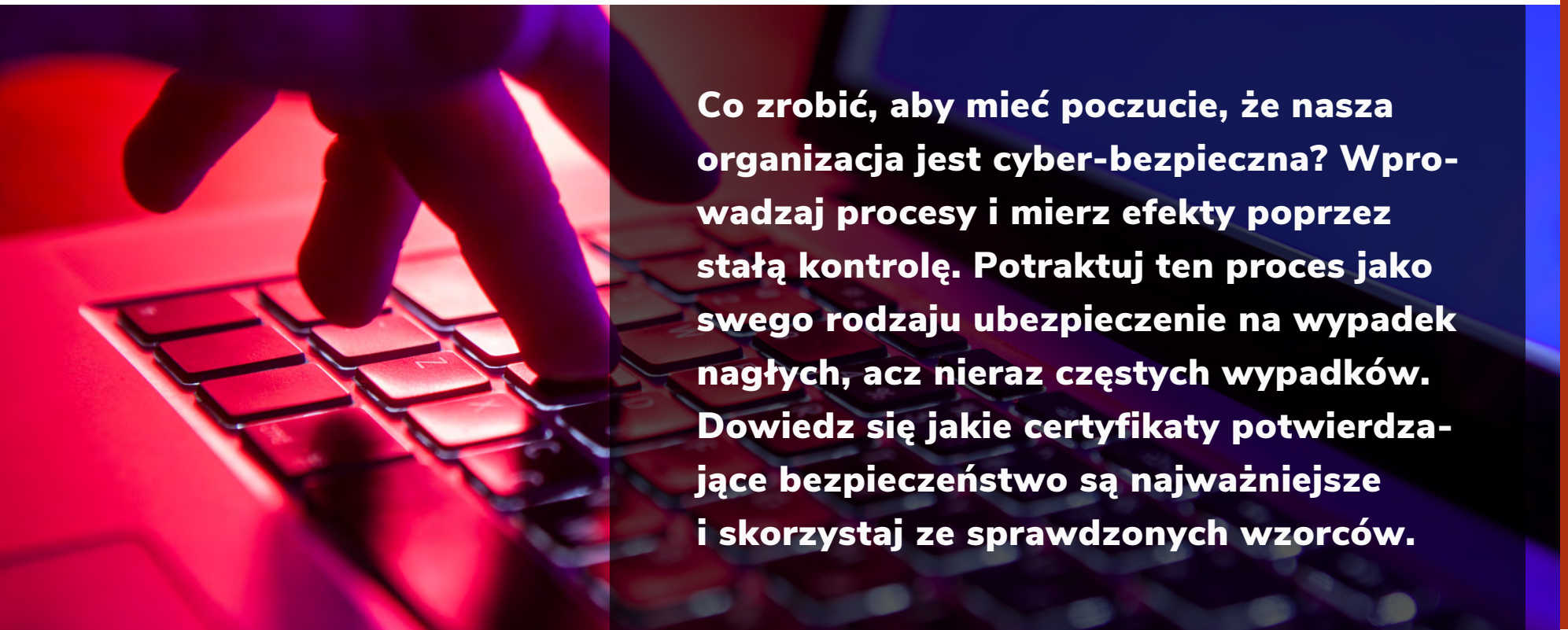
ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE

SPRAWDŹ OFERTĘ

JAK ZOSTAĆ FIRMĄ CYBER-BEZPIECZNĄ?

Mateusz Makowski
Silent Eight



Co zrobić, aby mieć poczucie, że nasza organizacja jest cyber-bezpieczna? Wprowadzaj procesy i mierz efekty poprzez stałą kontrolę. Potraktuj ten proces jako swego rodzaju ubezpieczenie na wypadek nagłych, acz nieraz częstych wypadków. Dowiedz się jakie certyfikaty potwierdzające bezpieczeństwo są najważniejsze i skorzystaj ze sprawdzonych wzorców.

Jak zostać firmą cyber-bezpieczną?

Cyberbezpieczeństwo jest praktycznie niewidocznym procesem, w którym najczęściej niepożądane sytuacje (incydenty) są zauważalne przez organizację. Odwrotnie niż przykładowo procesy produkcji, gdzie większość etapów możemy zweryfikować, zmienić czy zoptymalizować a efekty pracy są namacalne.

Dodatkowym elementem rozpraszającym uwagę jest zmienność środowiska IT – w dobie galopującej cyfryzacji, rozwiązania popularne dzisiaj, jutro będą dinozaurami na cmentarzu technologicznym. To oczywiście skrajności, ale dobrze obrazujące postęp całego sektora. Dodatkowo wielowątkowość – różnego rodzaju ataki przeprowadzone na wiele różnych sposobów, możliwości wewnętrzne i zewnętrzne przedsiębiorstwa oraz inne elementy składają się na wyzwanie jakim jest opracowanie strategii cyberbezpieczeństwa.

Aby organizacja była (cyber)bezpieczena koniecznym jest zastosowanie dużej ilości zabezpieczeń: (1) technicznych, tj. narzędzia, systemy, itp, (2) teoretycznych, czyli godziny szkoleń dla użytkowników, wdrożenia i weryfikacji procesów. Przy codziennym monitorowaniu zmiennych i wszystkich elementów układanki. Co zrobić, aby wdrożone rozwiązania nie okazały się fiaskiem? Jak skutecznie inwestować w cyberbezpieczeństwo? Jak realizować bezpieczne procesy?

Aby zrozumieć znaczenie cyberbezpieczeństwa, należy najpierw zdać sobie sprawę z zagrożeń, z jakimi mamy do czynienia w codziennym życiu.

Ataki cybernetyczne przybierają różnego rodzaju formy, takie jak kradzież danych, wyłudzanie informacji, ataki hakerskie czy złośliwe oprogramowanie. Organizacje, bez względu na ich rozmiar i branżę, są podatne na wspomniane zagrożenia. Wiele organizacji przechowuje swoje wrażliwe dane, takie jak informacje klientów, dane finansowe czy tajemnice handlowe, które są niezwykle atrakcyjne dla cyberprzestępców. Ataki na infrastrukturę krytyczną organizacji mogą prowadzić do przerwania działalności, utraty dochodów i poważnych szkód dla reputacji firmy. Dlatego konieczne jest podjęcie działań w celu ochrony systemów i danych.

NA CO WARTO ZWRÓCIĆ UWAGĘ?

Inwestowanie w cyberbezpieczeństwo to nie tylko zakup, ale również wdrożenie odpowiednich narzędzi, technologii, ale również to kompleksowy proces, który obejmuje świadomość pracowników, polityki bezpieczeństwa, zarządzanie ryzykiem oraz ciągłe monitorowanie. Kluczowym elementem jest edukacja załogi, ponieważ to oni są pierwszą linią obrony przed atakami. Szkolenia z zakresu świadomości pomagają pracownikom rozpoznawać zagrożenia, takie jak phishing czy złośliwe załączniki oraz podejmować odpowiednie środki ostrożności czy raportować anomalie.

Jednak proces nie kończy się na użytkowniku i konieczne jest zainwestowanie w narzędzia, które mają wspierać procesy w wykrywaniu, blokowaniu i monitorowaniu zdarzeń niepożądanych w całej infrastrukturze, procesach oraz środowisku organizacji. Ponadto, konieczne jest wdrażanie polityk bezpieczeństwa, które określają zakres funkcjonowania firmy, procedury i zasady korzystania z technologii w miejscu pracy.

Regularne audyty bezpieczeństwa pomagają identyfikować luki i słabe punkty, które mogą zostać wykorzystane przez nieuprawnione osoby. Kluczowe jest również tworzenie kopii zapasowych danych, aby móc szybko przywrócić systemy w przypadku ataku lub awarii. Ostatecznie równie ważnym elementem jest wykorzystywanie dobrych praktyk rynkowych oraz standardów bezpieczeństwa, takich jak ISO 27001, CIS Benchmarki oraz NIST. Te standardy stanowią wytyczne i ramy odnoszące się do różnych aspektów bezpieczeństwa

informacji i infrastruktury technologicznej. Wszystkie powyższe rozważania to dopiero wstęp do dalszych działań jakie organizacja musi podjąć, aby być bezpieczną.

Warto zastanowić się na tym, co uznajemy za skuteczną inwestycję oraz czym ona sama jest? Drugi element jest dużo łatwiejszy do oceny – inwestycja w cyberbezpieczeństwo to po prostu wdrożenie nowej lub dodatkowej technologii czy przeszkolenie użytkowników w organizacji. Z drugiej strony na ile takie podejście jest skuteczne wymaga głębszego zastanowienia.

Przyjmijmy dwa scenariusze dla naszego rozważania:

1) zmniejszenie liczby wykrywanych incydentów lub ich całkowity brak;

2) zwiększenie liczby pojawiających się incydentów (wzrost wykrywania).

Oba założenia są zarazem poprawne i błędne, a my musimy znaleźć na to złoty środek. Pierwszy scenariusz generuje w nas poczucie bezpieczeństwa oraz potencjalnie może wskazywać błędy w planowaniu czy samym wdrożeniu, gdyż nie ma takiej możliwości, aby zdarzenia niepożądane nie występowały w firmie. Co za tym idzie – zagrożenie istnieje tylko jeszcze nie wiemy jakie.

Drugie zaś generuje masę dodatkowej, nikomu niepotrzebnej pracy, gdzie nie skupiamy się na szcze-gółach i istnieje ryzyko przeoczenia katastrofalnego w skutkach zdarzenia.

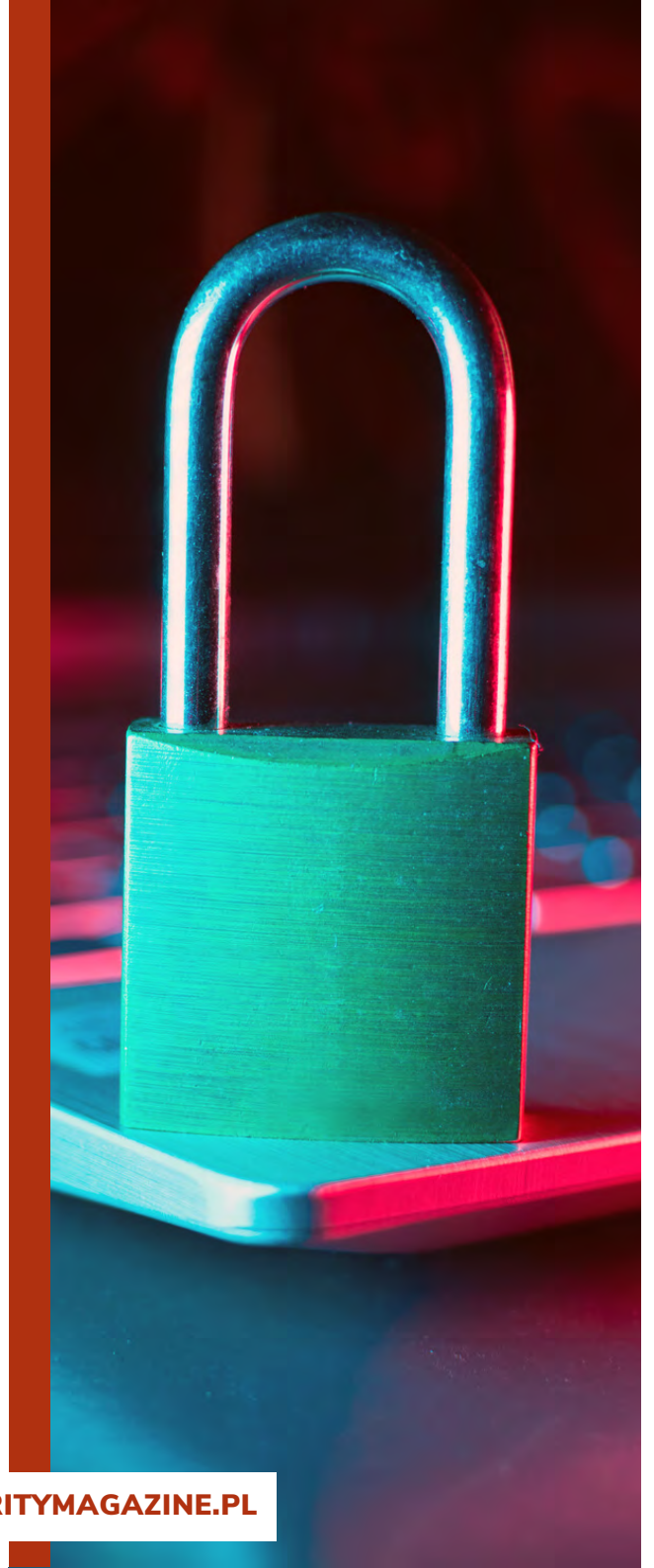
KRYTERIA SUKCESU

Każda organizacja, niezależnie od jej wielkości, musi opracować swoją własną ścieżkę rozwoju poziomu cyberbezpieczeństwa i na jej bazie wykreować mierzalne kryteria sukcesu. Z pomocą przybywa wtedy możliwość przeprowadzenie analizy ryzyka środowiska wewnętrznego i zewnętrznego – warto zwrócić uwagę, ile mamy własnych systemów (wdrażanych w naszym wewnętrznym środowisku) a ile kupujemy od dostawców (np. rozwiązania chmurowe czy SaaSowe).

Na własne środowisko mamy realny wpływ i to od nas zależy jak ono jest bezpieczne, dzięki czemu bezpieczeństwo jest w mierzalne. Chmurowe lub odmiejscowione rozwiązania są bardzo często niezależne od wewnętrznych służb IT zatrudnionych w organizacji, przez co mamy mniejszy wpływ na cyberbezpieczeństwo – np. zarządzamy tylko systemem operacyjnym, a od poziomu wirtualizatora zarządza dostawca. Co przekłada się na możliwości lub ich brak w kontekście rozwoju procesów cyberbezpieczeństwa w organizacji.

CYBERBEZPIECZEŃSTWO JAKO PROCES

Jednak samo wdrożenie odpowiednich zabezpieczeń i procedur nie wystarcza. Cyberbezpieczeństwo to proces ciągły i dynamiczny. Zagrożenia ewoluują, a cyberprzestępcy stale szukają nowych sposobów



ataku. Dlatego niezbędne jest ciągłe monitorowanie i aktualizacja systemów zabezpieczeń.

Regularne testy penetracyjne i analiza ryzyka pozwalają identyfikować słabe punkty i podejmować odpowiednie działania w celu ich naprawy. Dlatego pierwotnie inwestycja w cyberbezpieczeństwo może się wydawać się kosztowna, zwłaszcza dla mniejszych organizacji o ograniczonym budżecie. Jednak koszty związane z atakiem hackerskim, utratą danych, przerwą w działalności czy szkodami dla reputacji mogą być znacznie wyższe. Wiele firm, które padły ofiarą ataku, boryka się z poważnymi konsekwencjami, które mogą prowadzić do ich upadku. Inwestycja w cyberbezpieczeństwo to zatem rodzaj „ubezpieczenia", które minimalizuje ryzyko i chroni naszą działalność.

Podsumowując, inwestycja w cyberbezpieczeństwo to „niewidzialne ubezpieczenie" naszego biznesu. Odpowiednie środki ochrony, edukacja pracowników i ciągłe monitorowanie są kluczowe w dzisiejszym dynamicznym środowisku cybernetycznym. Koszty związane z inwestycją w cyberbezpieczeństwo są niewątpliwie uzasadnione, biorąc pod uwagę potencjalne skutki ataków. Zapewnienie bezpieczeństwa osób oraz mienia w erze cyfrowej to nie tylko obowiązek, ale również kluczowy czynnik sukcesu dla każdej organizacji a wszelkie rozważania to dopiero wierzchołek góry lodowej i często uproszczenie tematu, który dopiero zgłębiony pozwala rozwiać wszelkie wątpliwości i daje odpowiedź czy wystarczy naszej organizacji akceptacja ryzyka czy musimy poczynić nakłady na cyberbezpieczeństwo.

FIRMA NA WAKACJACH A CYBERBEZPIECZEŃSTWO

Redakcja
SECURITY MAGAZINE

Latem, kiedy biura świecą pustkami, a pracownicy korzystają z urlopów, firmy stają się nieoczekiwanie bardziej wrażliwe na cyfrowe zagrożenia. Sezon ten obfituje w szczególne ryzyka dla bezpieczeństwa danych. Jak można z wyprzedzeniem przygotować solidne mechanizmy obronne, aby skutecznie niwelować ryzyko ataków?

Lato jest czasem, kiedy zazwyczaj wiele firm jest mniej aktywnych ze względu na urlopy pracowników. To, co może wydawać się świetnym okresem na odprężenie oraz relaks, może jednak stać się także tym, w którym firmy stają się bardziej podatne na różnego rodzaju cyberzagrożenia. Z powodu mniejszej liczby pracowników i tym samym zmniejszonej czujności, cyberprzestępcy często wykorzystują ten czas na przeprowadzanie swoich ataków.

ZROZUMIENIE LETNICH ZAGROŻEŃ

Wakacje to typowy okres, kiedy wielu pracowników decyduje się na urlopy. Jest to czas, kiedy ludzie często wybierają się na dłuższe wakacje z rodziną, chcąc skorzystać z dobrych warunków pogodowych.

Dla firm, to może oznaczać pewne zmiany w codziennej pracy i operacjach:

- **zmniejsza się aktywność biznesowa.** Ponieważ wielu pracowników korzysta z urlopu, mogą pojawić się wyzwania w utrzymaniu normalnego tempa pracy. Niektóre projekty mogą być chwilowo zawieszone lub spowolnione, a procesy decyzyjne mogą być opóźnione z powodu braku niektórych kluczowych pracowników.
- **mniej inicjatyw biznesowych.** Ze względu na obniżoną wydajność, firmy mogą zdecydować się na zmniejszenie liczby nowych inicjatyw biznesowych. Może to być także czas na przemyślenie i planowanie przyszłych działań, które można zacząć realizować po zakończeniu wakacji.
- **zmiana dynamiki pracy.** Z mniejszą liczbą pracowników na pokładzie, ci, którzy pozostają, mogą mieć więcej obowiązków. Może to również oznaczać, że niektórzy pracownicy będą musieli zastępować swoich kolegów.
- **przygotowanie na okres powakacyjny.** Wakacje mogą również być dla firm okresem przygotowań do intensywniejszego okresu po. To może obejmować planowanie nowych projektów, strategii marketingowych, szkoleń pracowników.

- **modernizacja i konserwacja.** Sezon może być też wykorzystany na przeprowadzenie niezbędnych prac konserwacyjnych, modernizacyjnych, aktualizację oprogramowania, które są trudniejsze do wykonania, gdy większość zespołu jest obecna działalność firmy jest na pełnych obrotach.

Cyberprzestępcy doskonale wiedzą o tych wyzwaniach i wykorzystują moment, by zrealizować swój cel ukierunkowany właśnie na nieco “osłabioną” firmę. Wiedzą, że latem w firmach często jest mniej personelu i być może zastępują ich pracownicy tymczasowi. To sprawia, że łatwiej jest wprowadzać choćby różne techniki socjotechniczne. Zresztą... to nie muszą być nawet skomplikowane techniki, bo cyberprzestępca zwykle w tym czasie używa, prostych sposobów ataku, bo wie, że lato sprzyja większemu rozkojarzeniu, co może prowadzić do zaniedbań w codziennych obowiązkach. Jest świadom tego, że zarówno pracownicy, jak i kierownictwo mogą być mniej skoncentrowani, gdy myślą o nadchodzących urlopach lub relaksujących planach weekendowych. Ten stan rozluźnienia i nieuwagi otwiera drzwi dla potencjalnych zagrożeń, tym bardziej, że i moment reakcji na incydent może być znacznie wydłużony, co w konsekwencji daje cyberprzestępcy więcej czasu na działanie.

Kampanie phishingowe, ataki Business E-mail Compromission - wszystko to może być wykorzystane do uzyskania dostępu do systemów firmy. Ponadto, letnie miesiące to czas, kiedy pracownicy często korzystają z połączeń Wi-Fi i chmur, co również może prowadzić do zagrożeń.

RODZAJE ATAKÓW POPULARNYCH LATEM

Francuska firma zajmująca się cyberbezpieczeństwem, Tehtris, podała, że 30% firm odnotowało szczególny wzrost liczby ataków podczas wakacji, weekendów i wakacji.

Najczęstsze cyberprzestępstwa to:

- ransomware (20%)
- inne kradzieże tożsamości (43%),
- w tym fałszywe oszustwa prezesów (42%)
- i fałszywe oszustwa klientów (35%).

Obserwowane taktyki obejmują:

- **Phishing** pozostaje skutecznym atakiem dla cyberprzestępców. Wykorzystują brak czujności ofiar. Będą próbowali zaskoczyć pracowników, którzy nie są czujni, oszukując ich fałszywymi e-mailami. Zrelaksowany czy rozkojarzony pracownik straci czujność i kliknie w link.

- **Spoofing** jest jedną z metod wybieranych przez przestępcę. Jest to atak, w którym osoba podszywa się pod kogoś innego, fałszując jego dane. Np. slamming to odmiana phishingu polegająca na odzyskiwaniu nazw domen w celu zwiększenia opłat za zarządzanie. Tu warto zachować czujność, jeśli otrzymujemy oferty podróży i powiadomienia od linii lotniczych. Upewnijmy się, że witryna jest legalna. To samo dotyczy reklam - należy sprawdzać, gdzie nas prowadzą i czy sama ich treść nie jest zbyt przekoloryzowana.
- **Ransomware** jest niezwykle popularny w tym okresie. Tego lata możemy być świadkami jeszcze większej liczby podwójnych, potrójnych, a nawet poczwórnych wymuszeń.
- **Naruszenia danych.** Odnotowuje się znaczny wzrost liczby ataków e-mailowych w celu kradzieży poufnych danych.

ORGANIZACJA PRACY W WAKACJE

Organizacja pracy latem jest kluczowa dla utrzymania produktywności i bezpieczeństwa firmy. Firmy muszą przyjąć proaktywne podejście w zarządzaniu swoją pracą również w tym czasie, kiedy na pokładzie jest mniej pracowników, a ich koncentracja może być niższa i mniej odporna choćby na socjotechniki, w tym phishing.

Zapewnienie odpowiedniej ilości personelu zajmującego się bezpieczeństwem

Kiedy wielu pracowników jest na urlopach, istotne jest, aby dział bezpieczeństwa miał mimo wszystko zapewnioną odpowiednią liczbę personelu. Może to oznaczać zatrudnienie pracowników tymczasowych lub reorganizację zespołów, tak aby byli w stanie monitorować i odpowiadać na potencjalne zagrożenia. Również szkolenie dodatkowych członków zespołu w za-

kresie podstawowych procedur bezpieczeństwa może być korzystne, aby mogli oni wesprzeć dział IT w razie potrzeby.

Przygotowanie pracowników na zwiększone ryzyko ataków

Wzrost świadomości pracowników na temat cyberzagrożeń to krok w kierunku minimalizacji ryzyka. Regularne szkolenia dotyczące najlepszych praktyk w zakresie cyberbezpieczeństwa są niezbędne. Ważne jest, aby pracownicy byli świadomi technik, takich jak phishing, i wiedzieli, jak się przed nimi bronić. Można także przeprowadzać symulacje ataków, aby pracownicy mogli zrozumieć, jak działają cyberprzestępcy i jak można się przed nimi chronić. Warto o tym pomyśleć jeszcze przed wakacjami.

Wprowadzenie dodatkowych środków bezpieczeństwa dla pracowników pracujących zdalnie

Latem więcej pracowników może pracować zdalnie, korzystając z publicznych sieci Wi-Fi, co zwiększa ryzyko cyberataków. Wprowadzenie dodatkowych środków bezpieczeństwa, takich jak VPN, autoryzacja wieloskładnikowa i zasady bezpiecznego korzystania z sieci, jest niezbędne dla ochrony danych firmy.

Zrozumienie, jak odpowiednio zarządzać danymi i informacjami latem

Zarządzanie danymi i informacjami staje się bardziej skomplikowane z powodu zmniejszonej liczby pracowników. Wprowadzenie jasnych procedur dotyczących przechowywania, udostępniania i zabez-

pieczania danych jest kluczowe. Obejmuje to regularne tworzenie kopii zapasowych, restrykcyjne zarządzanie dostępem do danych i monitorowanie nieautoryzowanego dostępu.

Optymalizacja procesów i zarządzanie zasobami

Efektywne zarządzanie zasobami i optymalizacja procesów biznesowych są niezbędne, zwłaszcza latem. W tych miesiącach mogą wystąpić różnice w dostępności personelu, a także zmiany w popycie na produkty lub usługi. Dlatego ważne jest, aby firmy były elastyczne i potrafiły dostosować się do tych okoliczności.

Zautomatyzowanie rutynowych zadań

Automatyzacja może odgrywać kluczową rolę w poprawie efektywności organizacji, szczególnie gdy personel jest ograniczony. Przez zautomatyzowanie prostych i powtarzalnych zadań, pracownicy mogą skupić się na bardziej skomplikowanych i wartościowych zadaniach. Przykładem może być zastosowanie narzędzi automatyzujących procesy takie jak fakturacja, zarządzanie zamówieniami, czy raportowanie.

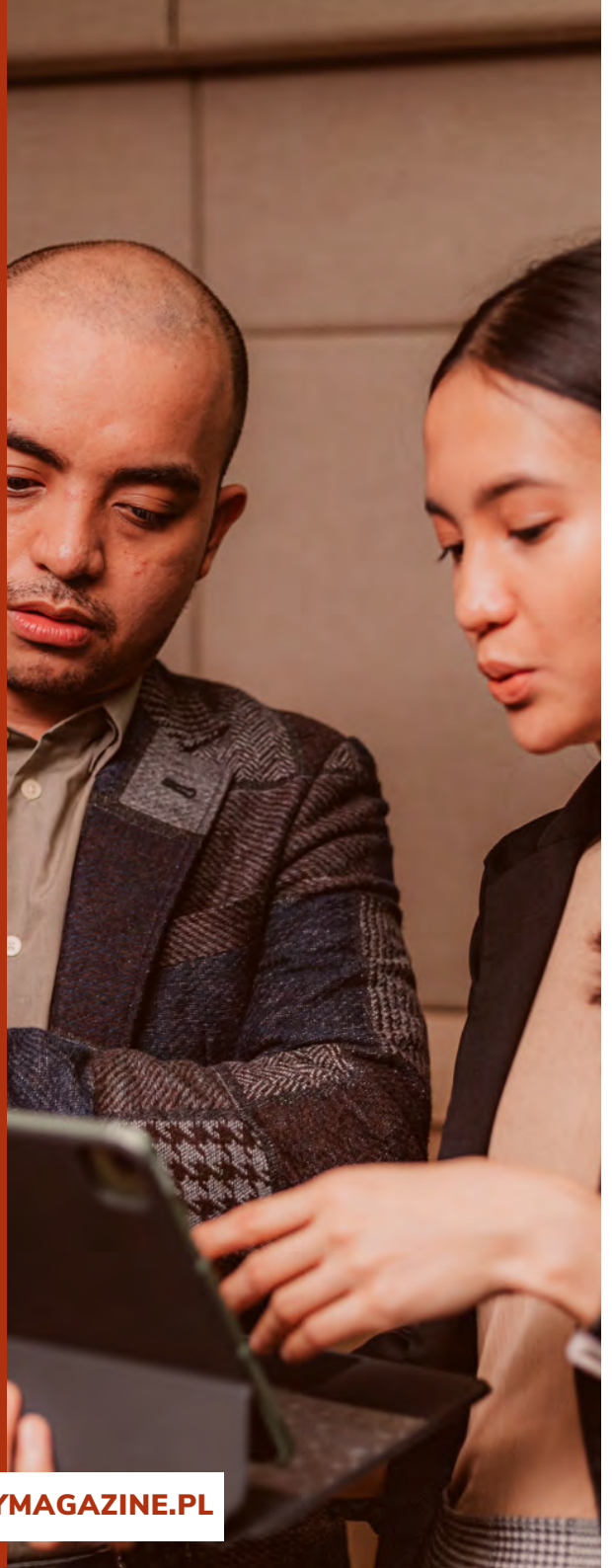
Elastyczność w planowaniu

Planowanie pracy w wakacje powinno być bardziej elastyczne. Może to obejmować rotację pracowników, dzielenie się obowiązkami, czy wprowadzenie elastycznych godzin pracy.

Organizacja pracy w wakacje jest wyzwaniem, które wymaga strategicznego podejścia. Zapewnienie odpowiedniej ilości personelu, wprowadzenie dodatkowych środków bezpieczeństwa, czy chociażby efektywne zarządzanie zasobami i czasem, wsparcie dla pracowników i przygotowanie na wzmożoną aktywność po wakacjach są kluczowymi elementami wspierającymi firmę w czasie wakacji.

TECHNOLOGIA W SŁUŻBIE BEZPIECZEŃSTWA

Organizacja pracy to nie wszystko, co zapewni bezpieczeństwo firmie. Z pomocą przychodzi technologia, która stanowi kluczowy filar współczesnych strategii zabezpieczających przed różnorodnymi zagrożeniami. Obejmuje ona szeroką gamę narzędzi i rozwiązań, które pomagają w ochronie danych, zapewnieniu fizycznego bezpieczeństwa, jak i ochronie przed cyberatakami. Jest kilka obszarów, w których technologia odgrywa kluczową rolę w zabezpieczaniu przedsiębiorstw.



Wykorzystanie technologii do monitorowania bezpieczeństwa

Pierwszym krokiem w zapewnieniu bezpieczeństwa danych firmy jest ciągłe monitorowanie systemów IT w poszukiwaniu potencjalnych zagrożeń. Latem, kiedy często brakuje kadry, konieczne jest wykorzystanie technologii, która nie wymaga ciągłej interwencji człowieka.

Systemy wykrywania i ochrony przed intruzem

To systemy, które monitorują ruch sieciowy, aby wykrywać i zapobiegać nieautoryzowanym próbom dostępu. Są szczególnie przydatne właśnie latem, kiedy hakerzy są bardziej aktywni.

Narzędzia SIEM (Security Information and Event Management)

Kolekcjonują i analizują logi oraz inne dane z różnych źródeł, pozwalając na szybką identyfikację i reakcję na podejrzane działania.

Automatyzacja procesów bezpieczeństwa

Automatyzacja jest kluczem do utrzymania wysokiego poziomu bezpieczeństwa, zwłaszcza gdy personel jest ograniczony.

Skanery podatności

Automatyczne skanery podatności używane do regularnego monitorowania systemów w poszukiwaniu luk, które mogą być wykorzystane przez cyberprzestępców.

Orkiestracja i automatyzacja reakcji na incydenty (SOAR)

Integruje różne narzędzia bezpieczeństwa i umożliwia automatyczne uruchamianie procesów reakcji na określone rodzaje zagrożeń.

Zarządzanie dostępem i uwierzytelnianie
W wakacje pracownicy mogą częściej korzystać ze zdalnego dostępu do systemów firmy.

Wieloskładnikowe uwierzytelnianie (MFA)
Wdrożenie MFA, w którym użytkownik musi dostarczyć więcej niż jedną formę weryfikacji, aby uzyskać dostęp, jest kluczowe.

Zarządzanie tożsamością i dostępem (IAM)
Pomaga kontrolować, kto ma dostęp do jakich zasobów, i zapewnia, że dostęp jest przyznawany odpowiednio.

Szkolenia i edukacja pracowników
Edukacja pracowników na temat najlepszych praktyk w zakresie cyberbezpieczeństwa jest niezbędna. Regularne szkolenia i przypomnienia o zagrożeniach, takich jak phishing, mogą być bardzo ważne w budowaniu kultury bezpieczeństwa wśród pracowników. W wakacje, kiedy pracownicy mogą korzystać z publicznych sieci Wi-Fi podczas podróży, ważne jest, aby byli świadomi potencjalnych ryzyk oraz wiedzieli, jak się przed nimi chronić.

Programy świadomości bezpieczeństwa
Firmy mogą też wdrażać programy, które pomagają w edukacji pracowników na temat zagrożeń i strategii minimalizacji ryzyka. Mogą to być webinaria, prezentacje czy nawet gry edukacyjne skupiające się na cyberbezpieczeństwie.

Symulacje ataków phishingowych
Regularne przeprowadzanie symulowanych ataków phishingowych może pomóc w ocenie, jak dobrze pracownicy rozpoznają i reagują na próby oszustwa, i jednocześnie stanowi doskonałe szkolenie.

Tworzenie planów awaryjnych
W przypadku naruszenia bezpieczeństwa, konieczne jest szybkie działanie, aby zminimalizować szkody. Kiedy personel może być ograniczony, ważne jest, aby firmy miały dobrze przygotowane plany awaryjne.

Plan reakcji na incydenty
Jest to formalny dokument, który określa, jak organizacja ma reagować na różne rodzaje incydentów bezpieczeństwa. Powinien zawierać procedury, które będą stosowane w odpowiedzi na potencjalne zagrożenia, i powinien być regularnie testowany i aktualizowany.

Kopie zapasowe
Regularne tworzenie kopii zapasowych danych o-

systemów to kluczowy element planu awaryjnego. To pozwala na szybkie przywrócenie usług w przypadku ataku ransomware lub innych form utraty danych.

Ustalanie priorytetów i odpowiednie reagowanie na zagrożenia

Nie wszystkie zagrożenia są takie same i nie wszystkie wymagają natychmiastowej reakcji.

Systemy zarządzania ryzykiem

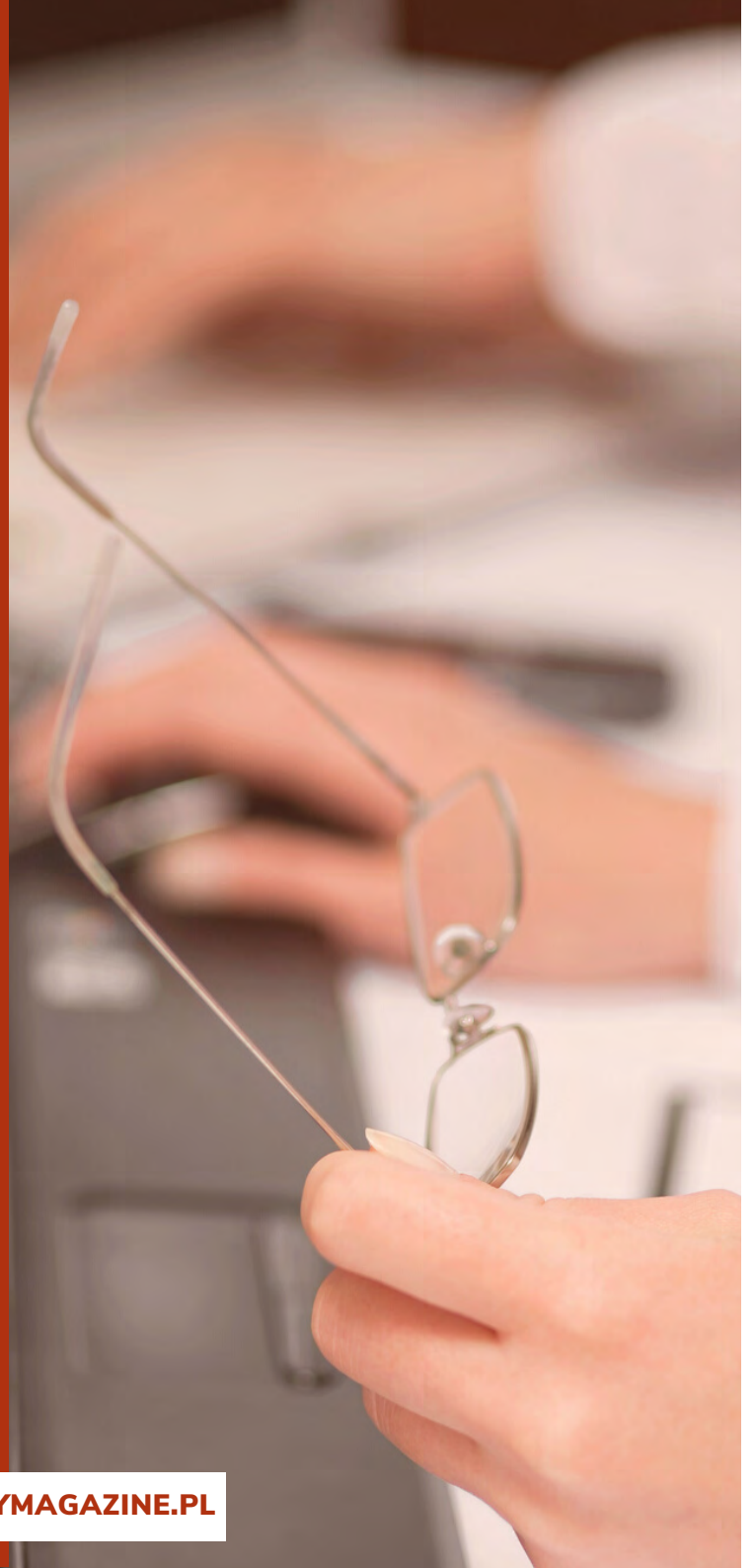
Wdrożenie systemu zarządzania ryzykiem, który pozwala na ocenę i priorytetyzację zagrożeń, jest kluczowe w zarządzaniu zasobami bezpieczeństwa.

Zespoły reakcji na incydenty (IRT)

Formowanie specjalnych zespołów, które skupiają się na reagowaniu na incydenty, może pomóc w szybkim i skutecznym radzeniu sobie z problemami, gdy one się pojawią.

- Przygotowanie firm do wakacji pod względem bezpieczeństwa jest niezwykle istotne, choć, niestety, zaniedbywane w wielu przypadkach. Kluczowa jest tu edukacja pracowników. Kiedy pracownicy wyjeżdżają na urlopy, często korzystają z mniej bezpiecznych, prywatnych lub ogólnie dostępnych, niezabezpieczonych połączeń internetowych, co może stanowić ryzyko dla danych firmy. Warto zainwestować w regularne szkolenia i symulacje, aby upewnić się, że pracownicy są świadomi zagrożeń oraz wiedzą, jak postępować w różnych sytuacjach, zwłaszcza ci, którzy korzystają z coraz popularniejszego workation - powiedział **Rafał Stępniewski, prezes Rzetelnej Grupy, redaktor naczelny "Security Magazine" i serwisu politykabezpieczenstwa.pl.**

Zaznaczył, że w wakacje, kiedy kadra zarządzająca i kluczowi pracownicy mogą być nieobecni, niezwykle ważne jest, aby posiadać solidny plan reakcji na incydenty.



- Mogę poradzić firmom, aby nie tylko opracowały takie plany, ale również przeprowadzały regularne ćwiczenia, które pomogą zrozumieć, jak działać w przypadku rzeczywistego naruszenia bezpieczeństwa - dodał Rafał Stępniewski.

- Jestem również orędownikiem stosowania systemów zarządzania ryzykiem oraz tworzenia zespołów reakcji na incydenty. Zarządzanie ry-zykiem pozwala firmom zrozumieć, na jakie zagrożenia powinny zwrócić szczególną uwagę, i pozwala efektywnie alokować zasoby w celu ich zwalczania. Z kolei zespoły reakcji na incydenty są niezbędne do szybkiego i skutecznego reagowania w sytuacji kryzysowej. Jeśli zbyt wielu pracowników jest w danym momencie poza firmą, warto rozważyć współpracę z firmami specjalizującymi się w bezpieczeństwie, choćby przy zarządzaniu bezpieczeństwem stacji roboczych, laptopów, urządzeń mobilnych czy wdrożeniu systemu kopii zapasowych z mechanizmem odzyskiwania, a także zabezpieczeń przed wyciekiem danych z urządzeń. Bezpieczeństwo to przecież nie tylko odpowiedzialność działu IT, ale całej organizacji. Pamiętajmy, że bezpieczeństwo to proces, nie jednorazowy projekt. Wymaga ciągłej uwagi, inwestycji i zaangażowania na wszystkich szcze-blach organizacji - podsumował **redaktor naczelny miesięcznika “Security Magazine” i serwisu politykabezpieczenstwa.pl.**

Monika Świetlińska

EKSPERCI WYDANIA

BARTOSZ BAZIŃSKI
CEO
SentiOne

Programista, przedsiębiorca, pasjonat wdrażania innowacyjnych technologii do świata biznesu. Od 2011 roku kieruje rozwojem narzędzia do monitoringu internetu i automatyzacji obsługi klienta - SentiOne.

DAMIAN ŻŁOBICKI
Trener, andragog
Włącz Wizję

Właściciel firmy szkoleniowej „Włącz Wizję”, w ramach której wspiera firmy w dokonywaniu transformacji cyfrowej przy pomocy zaawansowanych szkoleń z wykorzystaniem technologii VR, AR i silnika Unreal Engine. Wspiera organizacje i firmy w wykorzystywaniu współczesnych technologii w edukacji oraz biznesie, szkoli i występuje medialnie

MATEUSZ MAKOWSKI
Head of Security
Silent Eight

Związany od 2013 roku z branżą bezpieczeństwa informacji. Specjalizuje się we wdrażaniu systemów zarządzania, budowaniu świadomości użytkowników i zarządzaniu ryzykiem w sektorach bankowości, ochrony zdrowia, telekomunikacji. Występował na konferencjach, m.in. Konwent Ochrony Danych Osobowych i What The H@ck.

RAFAŁ STĘPNIEWSKI
CEO
Rzetelna Grupa s. z o.o.

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

SECURITYMAGAZINE.PL

ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ

Wydanie 2/2022
POBIERZ

Wydanie 3/2022
POBIERZ

Wydanie 4/2022
POBIERZ

Wydanie 5/2022
POBIERZ

Wydanie 6/2022
POBIERZ

Wydanie 7/2022
POBIERZ

Wydanie 8/2022
POBIERZ

Wydanie 9/2022
POBIERZ

Wydanie 1(10)/2023
POBIERZ

Wydanie 2(11)/2023
POBIERZ

Wydanie 3(12)/2023
POBIERZ

Wydanie 4(13)/2023
POBIERZ

Wydanie 5(14)/2023
POBIERZ

Wydanie 6(15)/2023
POBIERZ

WYDAWCA

Wydawca:

Rzetelna Grupa sp. z o.o.

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

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

Redaktor Naczelny: Rafał Stępniewski

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

Współpraca i kontakt: redakcja@securitymagazine.pl

SECURITYMAGAZINE.PL