5(14)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

Jak ochronić wizerunek firmy po cyberataku?

Regulacje rozwiążą etyczne i prawne problemy związane z AI?

Cyberbezpieczeństwo w abonamencie

Rola metadanych w przechowywaniu plików

Ochrona nie powinna być jednorazowym zadaniem

SPIS TREŚCI

Security News	4
Cybersecurity: Jaki był I kwartał 2023? Co przyniosą kolejne miesiące?	7
Cyberbezpieczeństwo w abonamencie – szansa dla MŚP	15
Jak działać, by ochronić wizerunek firmy po cyberataku?	22
Zintegrowany system ochrony klasy PSIM w infrastrukturze krytycznej	30
„Splątanie generatywne”. Regulacje rozwiążą etyczne i prawne problemy związane z AI?	37
Cyberbezpieczeństwo jako element ochrony wizerunku firmy	45
Rozwój nowych technologii a prywatność	52
Wizerunek firmy zaczyna się na etapie skutecznej prewencji	60
48% maili to spam. Co to oznacza dla biznesu?	67
Rola metadanych w przechowywaniu plików	75
Wirtualny agent, rozpoznawanie głosu i ochrona przed oszustwami reklamowymi	83
Sztuczna inteligencja a ochrona informacji	88
Ochrona nie powinna być jednorazowym zadaniem	95
Eksperci wydania	101

UWAGA! PISMO "SECURITY MAGAZINE" JEST CHRONIONE PRAWEM AUTORSKIM I PRASOWYM. **ZABRANIA SIĘ** WYCINANIA, PRZETWARZANIA I PUBLIKOWANIA FRAGMENTÓW TEKSTOWYCH ORAZ GRAFICZNYCH MAGAZYNU DYSTRYBUOWANYCH W INTERNECIE JAKO ODRĘBNE MATERIAŁY. **SZCZEGÓŁY STR. 114.**

SZANOWNI PAŃSTWO,

cyberbezpieczeństwo podstawą wizerunku każdej firmy oraz prawne aspekty korzystania ze sztucznej inteligencji — to dwa przewodnie tematy tego wydania.

W obu przypadkach mamy do czynienia z zagadnieniami, które mają kluczowe znaczenie dla funkcjonowania współczesnych organizacji. W dobie nieustannego rozwoju technologii oraz coraz większego związania z siecią, potrzeba adekwatnej ochrony i świadomości ryzyka staje się priorytetem.

W tym wydaniu podejmujemy próbę zrozumienia, jak odpowiednie zabezpieczenia cyfrowe i zarządzanie ryzykiem mogą przyczynić się do poprawy wizerunku firmy oraz do jej pozycjonowania na rynku. Z drugiej strony, razem z naszymi ekspertami badamy kwestie prawne dotyczące sztucznej inteligencji, które mogą mieć wpływ na działalność przedsiębiorstw oraz na życie codzienne.

Odpowiednie przygotowanie i zrozumienie tych aspektów może być kluczowe dla sukcesu Państwa firmy, dlatego w tym wydaniu mamy dla Was eksperckie analizy, praktyczne porady oraz najnowsze informacje ze świata technologii i bezpieczeństwa.

Serdecznie polecam lekturę tego wydania i zachęcam do współpracy!

Rafał Stępniewski

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

PINAPPALL: REWOLUCJA PŁATNOŚCI

Polski fintech PinAppAll stworzył rewolucyjną aplikację z pomocą technologii IBM, przekształcając smartfony w terminale płatnicze. Aplikacja działa na IBM Cloud oraz wykorzystuje klucze szyfrowania IBM związane z komputerami kwantowymi. To bezpieczne i praktyczne rozwiązanie odpowiada na rosnące zapotrzebowanie na płatności cyfrowe. PinAppAll jako pierwszy polski fintech zdobył certyfikat PCI DSS z szyfratorami HSM w chmurze, wspierany przez IBM.

NOWY KOMUNIKATOR DLA CYBERWOJSKA

Eksperci DKWOC wprowadzili Merkury 2.0 - nowy komunikator dla żołnierzy oraz pracowników resortu obrony narodowej. Bezpieczna wymiana informacji jawnych zastępuje komercyjne narzędzia komunikacji, ograniczając ich użycie. System instalowany na urządzeniach służbowych.

TESTY E-NOTATNIKA DLA POLICJI

Policja musi wciąż doskonalić metody działania oraz wykorzystywać nowe narzędzia i technologie, by wypełniać stawiane przed nią oczekiwania społeczne w zakresie zapewnienia bezpieczeństwa. Dlatego w Komendzie Głównej Policji podjęto prace koncepcyjne i programistyczne wynikiem, których jest opracowanie nowego narzędzia rewolucjonizujące dotychczasowy sposób gromadzenia i przetwarzania informacji dedykowanych głównie policjantom realizującym zadania „na ulicy". Rozpoczęto pilotaż pierwszego z trzech modułów systemu informatycznego e-Notatnik.

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

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

Redakcja "Security Magazine"

PATRONAT
SECURITY MAGAZINE

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.

DRUGA EDYCJA
CYBERTEK TECH FESTIVAL

DOŁĄCZ DO NAS
I 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

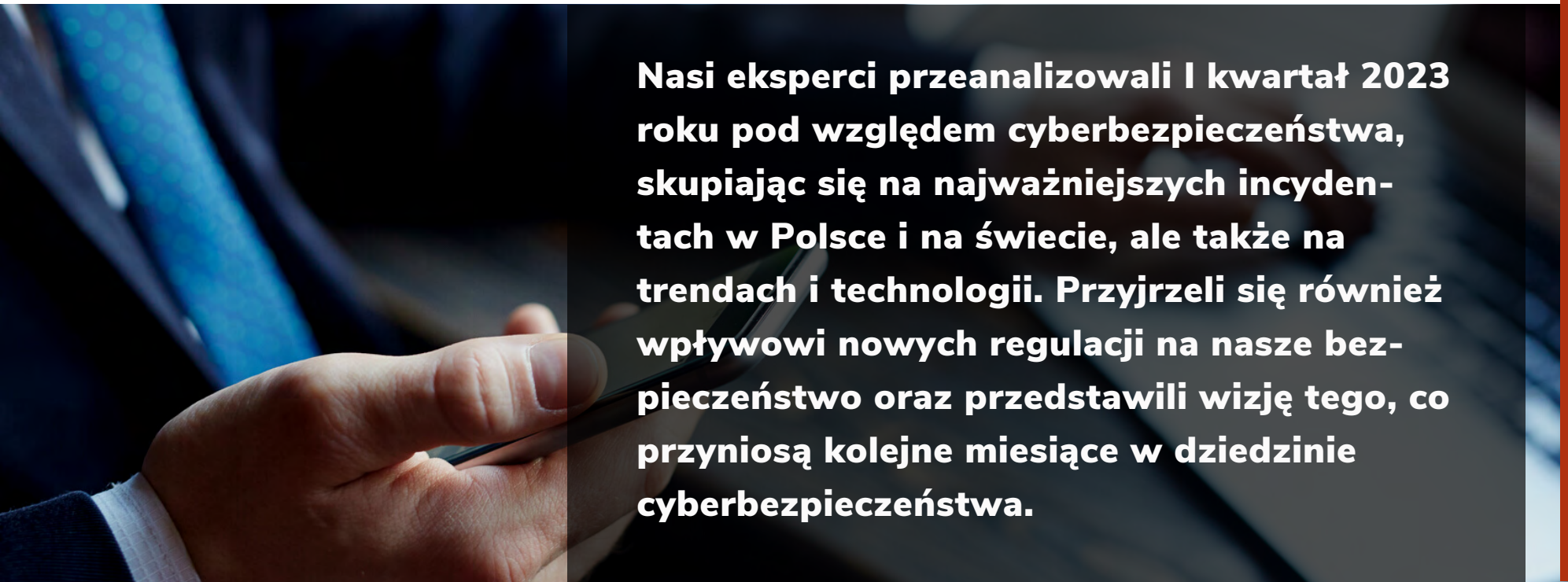
10% ZNIŻKI DLA NASZYCH CZYTELNIKÓW

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

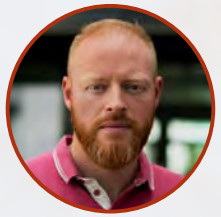
Szczegóły s. 5

CYBERSECURITY: JAKI BYŁ I KWARTAŁ 2023? CO PRZYNIOSĄ KOLEJNE MIESIĄCE?

Redakcja
SECURITY MAGAZINE



Nasi eksperci przeanalizowali I kwartał 2023 roku pod względem cyberbezpieczeństwa, skupiając się na najważniejszych incydentach w Polsce i na świecie, ale także na trendach i technologii. Przyjrzeli się również wpływowi nowych regulacji na nasze bezpieczeństwo oraz przedstawili wizję tego, co przyniosą kolejne miesiące w dziedzinie cyberbezpieczeństwa.



Marcin Biały
Advisory Architect, Grandmetric

INCYDENTY ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM W POLSCE I NA ŚWIECIE

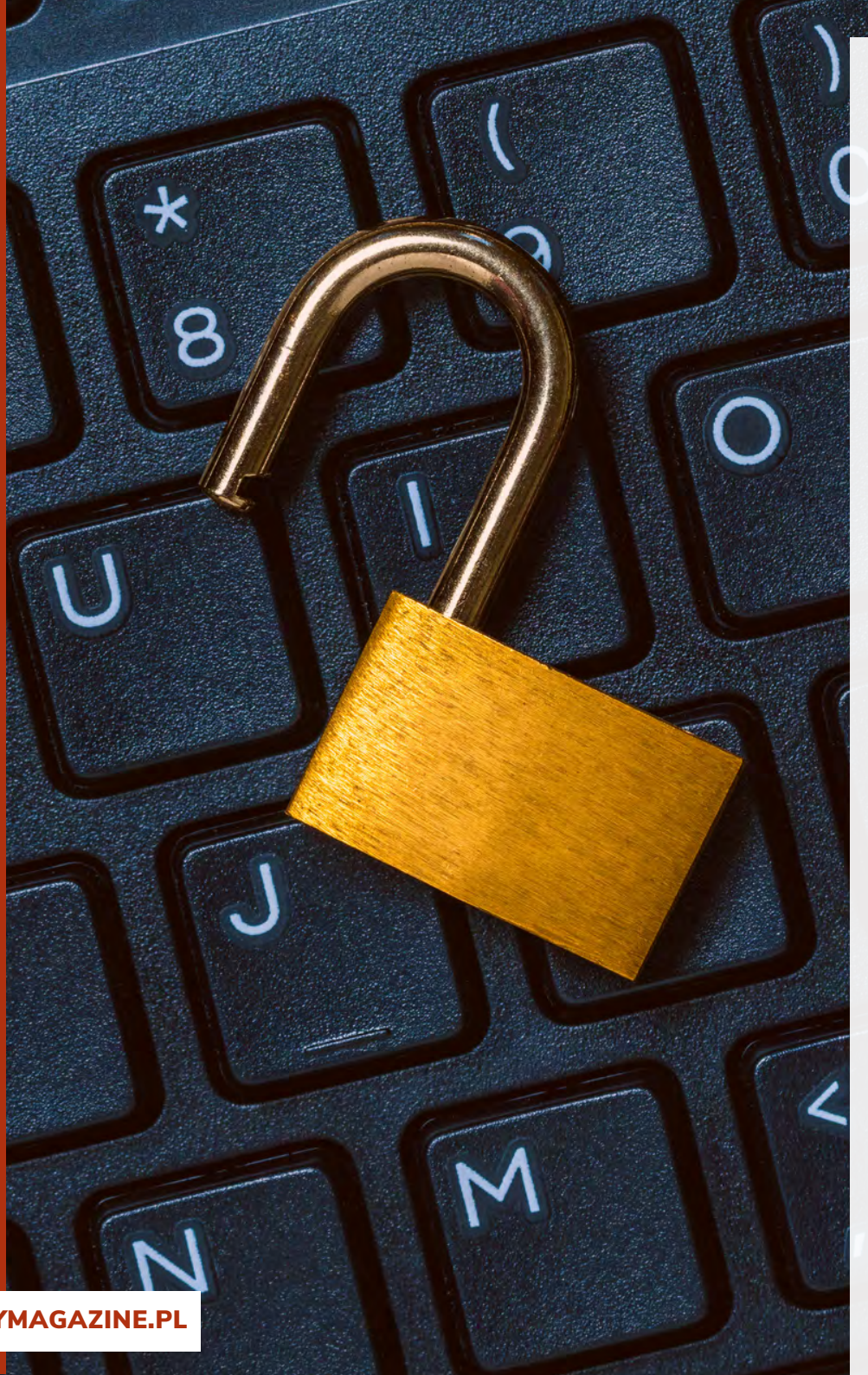
Z głośniejszych incydentów ostatnich miesięcy można przywołać choćby wykradzenie danych osobowych pacjentów i ich dokumentacji medycznej z placówki medycznej w Otwocku. Głośnym echem na świecie odbiły się z kolei incydenty z branży motoryzacyjnej. Hakerzy wykorzystali podatności portalu dealerskiego Kia połączonego z platformą Kia Connect, co pozwoliło im zdalnie uruchomić, otwierać samochody oraz uzyskać dostęp do kamer wewnętrznych. Z kolei z Ferrari padło ofiarą ataku ransomware, w wyniku którego wyciekły dane osobowe klientów.

TRENDY I TECHNOLOGIE

W obszarze najnowszych trendów w dziedzinie cyberbezpieczeństwa można przywołać zastosowanie głośnego narzędzia ChatGPT do pisania kodu malware przez osoby niezwiązane na co dzień z programowaniem. Mimo, że oficjalnie OpenAI twierdzi, że nie dostarcza szkodliwych rozwiązań, odpowiednio spreparowane polecenia pozwalają na stworzenie złośliwego kodu w kilkanaście minut.

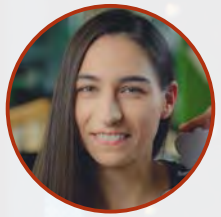
PRAWO A CYBERBEZPIECZEŃSTWO

Pod koniec ubiegłego roku wprowadzono nowelizację dyrektywy NIS, która definiuje kategorie podmiotów kluczowych i ważnych. Najważniejsze regulacje NIS2 nakładają na te podmioty obowiązek wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz zgłaszanie poważnych incydentów odpowiednim organom. Wprowadzono także obowiązek szkolenia kadry kierowniczej, a także konieczność powiadamiania odbiorców usług o poważnych incydentach i uczestnictwo w mechanizmach wymiany informacji.



PERSPEKTYWY NA KOLEJNE MIESIĄCE

W dobie coraz bardziej powszechnego dostępu do narzędzi wykorzystujących silniki AI, należy spodziewać się przyspieszenia pojawiających się różnorodnych i nowych ataków cybernetycznych. Należy także zwrócić uwagę na możliwości, które dają usługi typu Ransomware as a Service lub DDoS as a Service, czyli komercyjne wykorzystywanie usług stworzonych do prowadzenia ataków cybernetycznych.



Aleksandra Kornecka
inżynier ds. cyberbezpieczeństwa

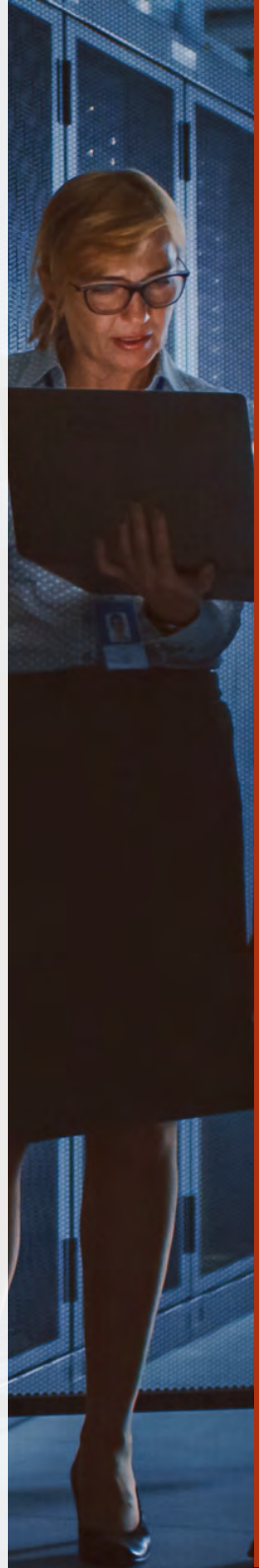
INCYDENTY ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM W POLSCE I NA ŚWIECIE

Gdybym miała wymienić jak najbardziej ogólne zagrożenia, jakie widzę to z pewnością będą to możliwości sztucznej inteligencji, jej banalnie prostą dostępność dla każdego (zwłaszcza ostatnio) oraz wykorzystanie jej do oszustw, phishingu i siania niepokojów społecznych oraz wpływania na ekonomię oraz politykę. Cyberwojna rozgrywa się w małych aktach codziennie przy nas i zajmuje coraz większe obszary, stając się jednocześnie coraz bardziej subtelna i trudna do wychwycenia. Mam tu na myśli oczywiście wizerunki deepfakes, tworzenie treści pisanych jak i mówionych głosem znajomej osoby, która nigdy tych słów sama nie wypowiedziała itp. Przeciętny użytkownik Internetu będzie miał wielkie trudności by to wszystko zawsze rozpoznać i nie dać się złapać. Dlatego tak ważna jest proaktywna postawa poszukiwania wiedzy i rzetelnych informacji, niepoddawanie się pośpiechowi (“Kliknąłem, bo nie zobaczyłem dokładnie a spieszyłem się..”), ogólna uważność i czujność co się dzieje w naszych urządzeniach i jak używamy technologii.

TRENDY I TECHNOLOGIE

Nieco przerażająca jest łatwość dostępu do malware’u - sztuczna inteligencja jest w stanie napisać dla nas kod/program do wyłudzania haseł, stworzyć bardzo sprytny mail phishingowy albo podać nam pomysły na oszustwa. To jest poziom dostępu do informacji dla osób o złych zamiarach, jakiego nigdy chyba jeszcze ludzkość nie miała.

Do tego można dodać pojęcie prywatności danych oraz kontroli nad ich przetwarzaniem. Jeśli sami wrzucamy poufne informacje w niepowołane miejsca, to sami wystawiamy się na problemy jak potencjalne wycieki. Firma zarządzająca popular-



nym czatem ze sztuczną inteligencją też jest po prostu firmą, w której pracują ludzie, którzy mogą paść ofiarą wycieku danych, ataku hakerskiego bądź wykradzenia danych przez fizyczne zdobycie dostępu do nich.

Oczywiście, jest też mnóstwo dobrych stron sztucznej inteligencji. Można poprosić ją o wyszukanie podatności bezpieczeństwa w próbce kodu albo zadawać jej pytania odnośnie bezpieczeństwa i uczyć się dzięki temu jak o nie dbać w różnych przypadkach.

Z perspektywy inżyniera ds. cyberbezpieczeństwa zatrważające jest obserwować, ile firm ulega wyciekom w ostatnim czasie, również takich z finansowymi możliwościami dobrego zabezpieczania się. To rodzi przypuszczenie, że miliony mniejszych firm nie inwestują zbyt wiele lub nic w bezpieczeństwo, co nie napawa optymizmem.

Rafał Stępniewski
prezes zarządu Rzetelna Grupa sp. z o.o.

INCYDENTY ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM W POLSCE I NA ŚWIECIE

Każdego miesiąca informowano o incydentach, naruszeniach, potężnych atakach. Oświadczenia jednak nie są praktyką powszechną - o wielu zdarzeniach nie dowiemy się choć z pewnością miały miejsce.

Styczeń to m.in. miesiąc, w którym firma NortonLifeLock zajmująca się oprogramowaniem antywirusowym i ochroną przed kradzieżą tożsamości potwierdziła, że stała się celem cyberprzestępców. Użyli oni danych uwierzytelniających zakupionych w Dark Necie, próbując zalogować się na konta klientów Norton. Luty minął np. pod znakiem naruszenia danych moskiewskiej firmy Elevel i wycieku 1,1 TB danych osobowych.

W sumie znaleziono 7 milionów wpisów danych z ostatnich dwóch lat, w tym nazwiska klientów, numery telefonów, adresy e-mail i adresy dostawy. w marcu doszło do głośnego cyberataku na Ferrari, Skylink, Alliance Healthcare.

W Polsce wciąż zwiększa się liczba ataków na polski sektor użyteczności publicznej oraz bankowo-finansowy, który jest drugą najczęściej atakowaną branżą w kraju. Mówimy tu o kilku tysiącach w skali tygodnia!

TRENDY I TECHNOLOGIE

Nie będę tu oryginalny, mówiąc o sztucznej inteligencji czy uczeniu maszynowym. Rozwój tych technologii umożliwia tworzenie coraz bardziej zaawansowanych systemów wykrywania i reagowania na ataki w czasie rzeczywistym. Wzrost popularności Internetu Rzeczy (IoT) oraz technologii 5G zwiększa jednak atakowalność systemów, co stawia wyższe wymagania wobec bezpieczeństwa.

PRAWO A CYBERBEZPIECZEŃSTWO

Sporo mówi się o dyrektywie NIS2. Znacznie mniej o dyrektywie CER, która zapewnia ramy pomagające organizacjom łagodzić szereg zagrożeń związanych z cyberbezpieczeństwem. Obejmuje zagrożenia naturalne, ataki terrorystyczne i zagrożenia wewnętrzne. CER dotyczy 11 sektorów, które zostały uznane za krytyczne, w tym bankowość, infrastruktura cyfrowa, energia, infrastruktura rynku finansowego czy opieka zdrowotna. Jej wymagania stanowią, że objęte nią podmioty muszą przygotować się na zakłócające incydenty, wdrażając środki w celu ochrony przed nimi, reagowania na nie i odzyskiwania po nich. Organizacje objęte zakresem dyrektywy będą musiały przeprowadzać ocenę ryzyka co najmniej raz na cztery lata celem zidentyfikowania organizacji świadczących kluczowe usługi. Muszą również wdrożyć środki zapewniające ich odporność i powiadamiać właściwe organy o incydentach zakłócających.

PERSPEKTYWY NA KOLEJNE MIESIĄCE

W kolejnych miesiącach można oczekiwać, niestety, dalszych ataków na infrastrukturę krytyczną oraz rosnącego zagrożenia ze strony cyberprzestępczości. Firmy i rządy powinny zatem intensywnie inwestować w cyberbezpieczeństwo oraz edukować społeczeństwo na temat zagrożeń i praktyk bezpiecznego korzystania z technologii. Ponadto, współpraca międzynarodowa będzie kluczowa w wymianie wiedzy i doświadczeń w walce z globalnymi zagrożeniami cybernetycznymi.

PATRONAT
SECURITY MAGAZINE

CYBER.GOV

BEZPIECZEŃSTWO IT W SEKTORZE PUBLICZNYM

POZNAJ SZCZEGÓŁY

W dobie cyfryzacji i rosnącej liczby zagrożeń cybernetycznych, sektor publiczny musi nieustannie podnosić swoje kompetencje w zakresie bezpieczeństwa IT. Z myślą o tym, Evention organizuje już dziewiątą edycję konferencji CyberGov, która odbędzie się pod hasłem "Bezpieczeństwo IT w sektorze publicznym".

Konferencja odbędzie się w Hotelu Sound Garden w Warszawie 18 maja w godzinach 9.00 — 16.30, a także 19 maja w godzinach 9.00 -15.00 jako warsztaty online i on-site.

Dla instytucji publicznych

Planowana liczba uczestników wynosi ponad 300 osób, które będą miały okazję wymienić się doświadczeniami, poznać najnowsze rozwiązania technologiczne oraz nawiązać kontakty z innymi ekspertami związanych z bezpieczeństwem IT.

Bloki tematyczne

Konferencja będzie składać się z kilku bloków tematycznych, które pozwolą uczestnikom na zgłębienie najważniejszych aspektów związanych z bezpieczeństwem IT w sektorze publicznym.

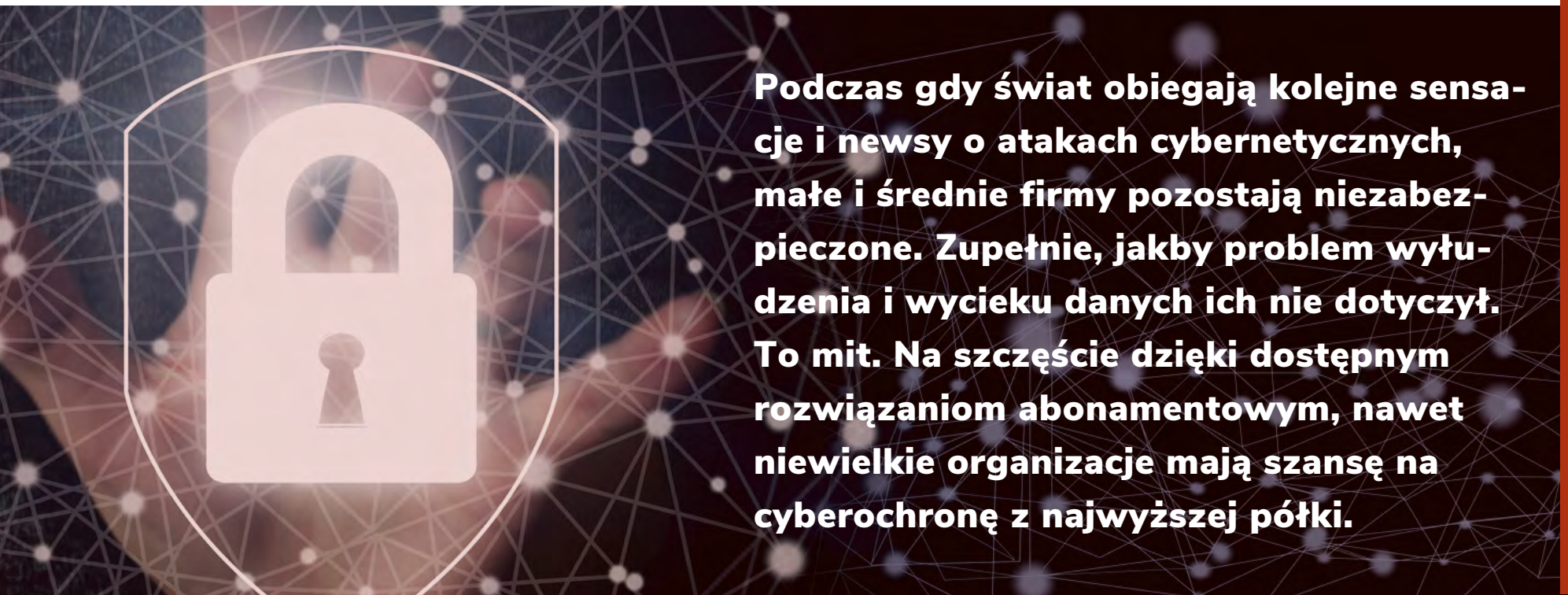
W ramach konferencji odbędą się również warsztaty, podczas których uczestnicy będą mieli okazję uczestniczyć w praktycznych ćwiczeniach związanych z tematyką bezpieczeństwa IT. Warsztaty te będą prowadzone przez doświadczonych ekspertów z branży oraz przedstawicieli sektora publicznego. Wydarzenie będzie doskonałą okazją do nawiązania kontaktów oraz wymiany doświadczeń z innymi uczestnikami zajmującymi się bezpieczeństwem IT w sektorze publicznym.

Zachęcamy do rejestracji na 9. edycję konferencji CyberGov. Wydarzenie może przyczynić się do podniesienia świadomości na temat cyberzagrożeń oraz umożliwi uczestnikom zgromadzenie wiedzy niezbędnej do skutecznej ochrony instytucji publicznych.

CYBERBEZPIECZEŃSTWO W ABONAMENCIE. SZANSA DLA MŚP

Jakub Fabiś
Grandmetric

FINALISTA KONKURSU "ARTYKUŁ ROKU"



Podczas gdy świat obiegają kolejne sensacje i newsy o atakach cybernetycznych, małe i średnie firmy pozostają niezabezpieczone. Zupełnie, jakby problem wyłudzenia i wycieku danych ich nie dotyczył. To mit. Na szczęście dzięki dostępnym rozwiązaniom abonamentowym, nawet niewielkie organizacje mają szansę na cyberochronę z najwyższej półki.

CYBERBEZPIECZEŃSTWO JEST DROGIE?

Nie da się ukryć, że największą obawą MŚP związaną z zabezpieczaniem firmy są wysokie koszty. Tymczasem cyberbezpieczeństwo jest jak dobre ubezpieczenie. Ubezpieczamy samochody od kradzieży, mieszkanie od zalania czy pożaru, a wielokrotnie cenniejsze dane firmy zostawiamy same sobie? Jeśli podliczymy ryzyko biznesowe i prawne związane z wyciekiem danych czy atakiem ransomware, szybko okaże się, że koszt wdrożenia systemów cyberochrony jest nawet kilkaset razy niższy. I tak jak w przypadku ubezpieczenia, ochronę przez cyberzagrożeniami można (i powinno się) dobrać do specyfiki firmy. Mimo to, jak podaje Sophos, aż ¼ polskich firm nie ma żadnego budżetu na cyberbezpieczeństwo.

Na korzyść zabezpieczeń przemawia też chmurowy (abonamentowy) model rozliczeń, oferowany przez coraz szersze grono dostawców.

Co zyskujesz wdrażając cyberochronę w modelu abonamentowym?

- **Ograniczasz koszty.** Chmurowe zabezpieczenia od topowych producentów kosztują tyle, co kawa na mieście.
- **Chronisz firmę i pracowników** dzięki jednej, stałej, miesięcznej opłacie.
- **Instalujesz dodatkowe zabezpieczenia** bez względu na to, z jakiego dostawcy sprzętu IT korzystasz.
- Wybierając rozwiązanie od znanego producenta, **masz pewność, że spełnia ono wszystkie wymogi prawne.** Dodatkowo, korzystając ze sprawdzonej i zaufanej ścieżki dystrybucyjnej, masz pewność, że nie będzie problemów z licencjonowaniem i supportem.
- Większość rozwiązań **możesz przetestować za darmo**, a autoryzowani resellerzy tacy jak Grandmetric, oferują dłuższy okres próbny niż sam producent.

CZY ISTNIEJE JEDNA RECEPTA NA ZABEZPIECZANIE FIRM?

Obszarów, które możemy chronić rozmaitymi narzędziami i systemami bezpieczeństwa jest coraz więcej. Kiedyś to były tylko komputery w intranecie, następnie wszelkie urządzenia sieciowe np. drukar-

ki, w końcu cała gama urządzeń i aplikacji, na których pracujemy w siedzibie firmy i poza nią.

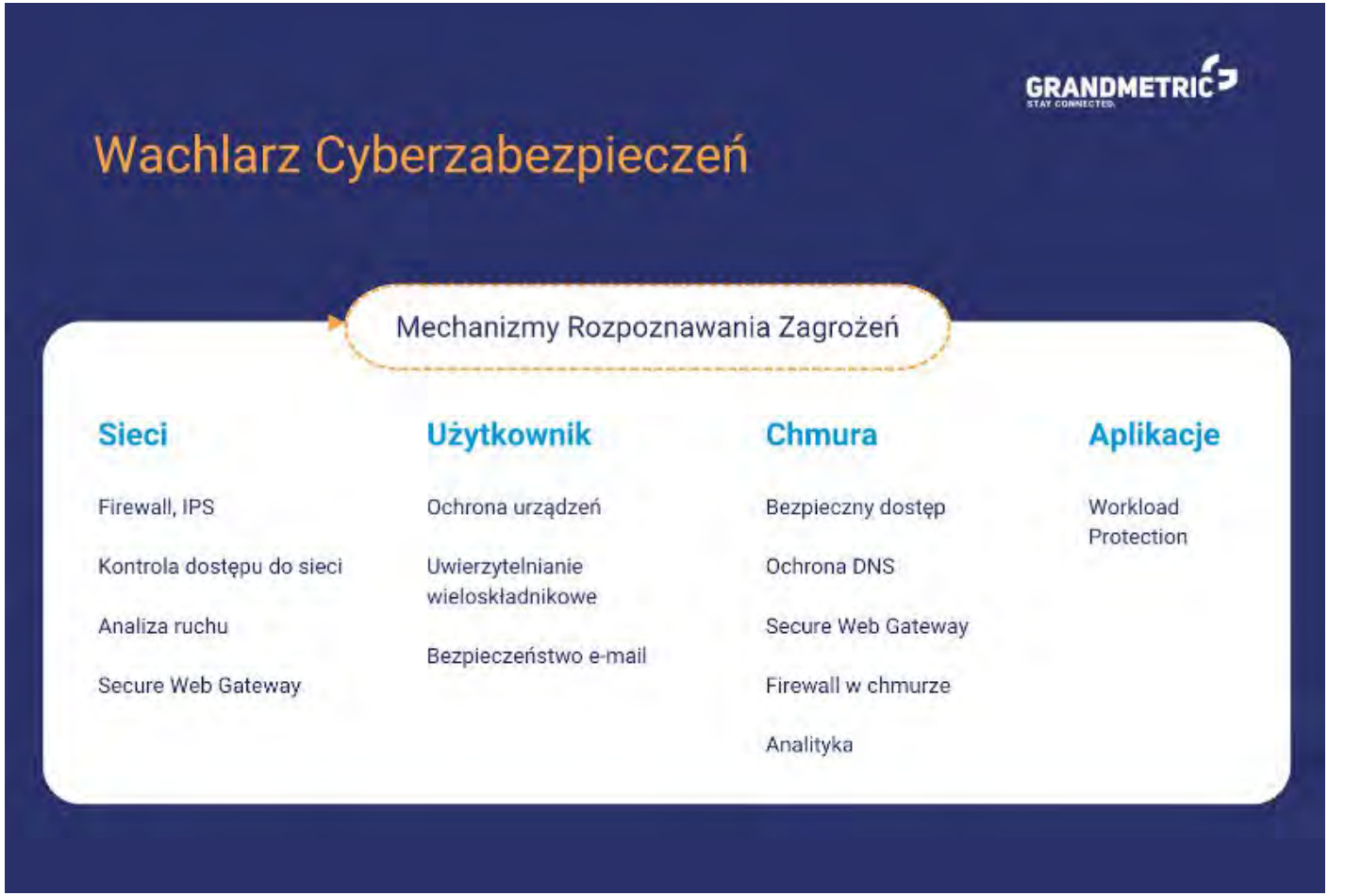
Rozwój infrastruktury mobilnej, a co za tym idzie, zwiększenie elastyczności pracy, wymaga od firm podążania za użytkownikiem, gdziekolwiek ten się znajduje. zy to oznacza, że należy zabezpieczać wszystko, od razu i na wszystkie sposoby?

Niekoniecznie. Najważniejsze, żeby robić to mądrze, uszczelniając kolejno najbardziej newralgiczne obszary.

OD CZEGO ZACZĄĆ ZABEZPIECZANIE MAŁEJ FIRMY?

Zabezpiecz hasła managerem

Idealna alternatywa dla niebezpiecznych, ale wciąż



stosowanych haseł “na żółtych karteczkach”, rozsianych po biurze.

Aplikacja do bezpiecznego przechowywania haseł to absolutna podstawa. W ten sposób możesz nie tylko wymóc korzystanie z bardzo silnych haseł, ale również zagwarantować, że nikt nie wykorzysta tego samego hasła więcej niż raz. Popularne managery pozwalają też bezpiecznie udostępniać hasła w ramach firmy.

Dodaj czynnik uwierzytelniający

Jeśli pracownicy logują się do firmowych systemów czy korzystają z firmowych komputerów poza siedzibą firmy, zapewnij im bezpieczne, szyfrowane połączenie. Może to być VPN, do którego będą musieli się logować, klucz typu YubiKey, który będą musieli ze sobą nosić, czy zwykła aplikacja typu Duo, w której wystarczy potwierdzić tożsamość jednym kliknięciem czy poprzez FaceID, bez konieczności podawania jakichkolwiek haseł.

Ubezpiecz DNS

O ile VPN czy MFA pozwolą Ci bezpiecznie nawiązać połączenie, brakuje im mechanizmów zabezpieczających przed niebezpiecznymi stronami. Tu w sukurs przychodzą rozwiązania, zapewniające filtrowanie dostępu do zasobów internetowych na poziomie usługi DNS. Jednym z nich jest Umbrella.

Jak to działa? W ramach subskrypcji otrzymujemy dostęp do zaawansowanych mechanizmów, które oznaczają strony zainfekowane malware lub stwarzające zagrożenia innego typu. Umbrella dokładnie

sprawdzi, czy pod docelowym adresem IP znajduje się legalna czy fałszywa strona www. W tym drugim przypadku, zablokuje połączenie i uchroni Twoją firmę przed wyłudzeniem danych.

Co ważne, Umbrella działa bez względu na to, z jakich modeli urządzeń sieciowych korzystasz, oraz chroni użytkowników nie tylko w sieci firmowej, ale również poza nią. Na bieżąco otrzymuje też informacje o nowych zagrożeniach, pochodzące od największej grupy badawczej Threat Intelligence na świecie.

Zadbaj o porządny firewall

Do tego, że firewall powinien być na wyposażeniu każdej firmy, raczej nie trzeba przekonywać. Trochę gorzej wygląda kwestia jego konfiguracji. Jak podaje Gartner, w 2023r. 99% naruszeń zabezpieczeń firewalli będzie związane z błędami w konfiguracji, a nie z ograniczeniami samych firewalli. Dlatego czas zadbać o profesjonalne zabezpieczenie brzegu sieci. Dobra wieść jest taka, że można to też zrobić w abonamencie, bez instalowania dodatkowych urządzeń.

ABONAMENT NA SPOKOJNY SEN

Rozwiązania abonamentowe to szansa dla mniejszych firm, żeby skorzystać z cyberochrony na światowym poziomie. To, co dotychczas było dostępne dla największych graczy, można już w wygodny sposób wdrożyć w sektorze MŚP, czyli tam, gdzie powstaje ponad 72% polskiego PKB a zatrudnienie znajduje 67,8% pracowników sektora prywatnego.

Jak zabezpieczyć się dzięki rozwiązaniom chmurowym?

1. **Chroń pracowników** przed zmyślnymi (i niewybrednymi) atakami typu phishing - rozwiązanie Umbrella, w zależności od skali firmy, można wdrożyć już w cenie kawy.
2. **Zainwestuj w firewall** - opcji jest wiele, również software'owych, bez konieczności kupowania urządzenia na własność. Pomożemy dobrać odpowiednią ochronę w adekwatnym budżecie.
3. Każde **logowanie zabezpiecz podwójnie**, lecz w sposób nieuciążliwy dla pracowników - sięgnij po rozwiązania MFA (uwierzytelnianie wieloskładnikowe) typu Duo.
4. W planie minimum – **zainstaluj managera haseł** i przeszkol pracowników ze współczesnych cyberzagrożeń. To też możesz zrobić z Grandmetric.

Oczywiście, rozwiązania subskrypcyjne dają znacznie większe możliwości ochrony (nie tylko małych i średnich podmiotów).

W ofertach światowej klasy producentów znajdziemy też systemy AMP (Advanced Malware Protection), XDR (Extended Detection and Response), UTD (Unified Threat Detection), Secure Workload (mikrosegmentacja w modelu Zero-Trust) i wiele innych. Możliwości jest wiele, wszystko zależy od tego, co naprawdę jest potrzebne danej organizacji. Inżynierowie Grandmetric na co dzień pomagają odpowiadać na to pytanie. Skontaktuj się po bezpłatną konsultację.

PATRONAT
SECURITY MAGAZINE

CONFIDENCE 2023

KONFERENCJA W KRAKOWIE

Pełna agenda wydarzenia oraz bilety

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

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

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

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

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

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

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

JAK DZIAŁAĆ, BY OCHRONIĆ WIZERUNEK FIRMY PO CYBERATAKU?

Magdalena Grochala
Ekspertka ds. komunikacji i PR

Cyberatak to nie tylko problem technologiczny i finansowy, ale też wizerunkowy. Firma, która straciła dane klientów czy pracowników, będzie mierzyć się ze spadkiem zaufania i koniecznością uspokojenia nastrojów swoich interesariuszy. Pomoże jej w tym odpowiednia i szybko podjęta komunikacja. Jak ją prowadzić, by była skuteczna?

Kluczem do uspokojenia sytuacji jest otwartość i rzetelne informowanie o tym, co się stało i co firma robi, by zminimalizować skutki naruszenia. Kogo i jak informować?

Warto pamiętać, że cyberatak dotyka wielu grup osób związanych z przedsiębiorstwem. Każda z nich ma inne potrzeby, każdą będzie interesował inny aspekt cyberataku. Dodatkowo – zazwyczaj grupy te mają też różne oczekiwania dotyczące sposobu kontaktu z nimi. Nie wystarczy zatem zamieścić informacji o ataku na stronie WWW. Więcej – nie wystarczy nawet notka wysłana do mediów. Komunikacja w tak kryzysowej sytuacji musi obejmować wszystkie dostępne firmie kanały przekazywania informacji, musi bowiem dotrzeć do wszystkich poszkodowanych osób.

W sytuacji idealnej firmy są przygotowane do komunikacji w czasie cyberataku, zanim on jeszcze nastąpi. W swoich strategiach PR mają zdefiniowane działania, które należy podjąć w takiej sytuacji.

Wtedy pierwszym krokiem w czasie cyberataku jest wdrożenie takiego planu. Sprawa komplikuje się jednak, gdy go nie ma. Ale i wtedy przedsiębiorstwo może skutecznie zadbać o swój wizerunek. Jak to zrobić?

PRZYGOTUJ I WPROWADŹ W ŻYCIE PLAN DZIAŁAŃ KOMUNIKACYJNYCH

Powołaj zespół kryzysowy

W przypadku cyberataku najważniejsze jest współdziałanie wielu różnych działów firmy. Komunikacja nie jest tylko i wyłącznie sprawą PR-u, ale także specjalistów ds. IT i bezpieczeństwa, prawników, zarządu, działów HR. Planowanie wszelkich działań trzeba zacząć od zdefiniowania, kogo dotyka przeprowadzony atak, i wybrania do zespołu kryzysowego osób, które pomogą w komunikacji z tymi grupami. Oczywiście absolutnie konieczne jest wsparcie działu IT, bo przekazywane wiadomości muszą być konkretne i jasno wyjaśniać zaistniały problem.

Wyznacz osobę odpowiedzialną za kontakty z mediami

Media mogą być w czasie cyberataku sprzymierzeńcem firmy – pomagają bowiem docierać z informacjami do szerokiego grona odbiorców, prostować nieprawdziwe wiadomości. Oczywiście, aby tak było, kontakt z nimi musi

być szybki, sprawny, a sama komunikacja szczera. Szczególną rolę w tym procesie odgrywa rzecznik prasowy lub inna osoba wyznaczona do współdziałania z dziennikarzami. Dlatego trzeba ją jak najszybciej wyznaczyć i umożliwić mediom sprawny kontakt z nią.

Zdefiniuj grupy osób, z którymi będziesz się komunikować

Komunikacja w czasie starcia z cyberprzestępcami nie ogranicza się do przekazywania informacji mediom. Cyberatak dotyka często bardzo wielu różnych grup. Zazwyczaj są to klienci, ale też pracownicy, inwestorzy, partnerzy biznesowi. Zespół kryzysowy musi więc określić, jakie to są grupy i w jaki sposób należy się z nimi skutecznie komunikować.

Wybierz kanały kontaktów

Firma ma zazwyczaj kilka różnych kanałów komunikacji z interesariuszami. Po cyberataku trzeba przede wszystkim ustalić, które z tych kanałów są w ogóle dostępne (na skutek działań cyberprzestępców może bowiem na przykład przestać działać służbowa poczta elektroniczna czy strona internetowa) i zadecydować, czy i w jaki sposób używać ich w komunikacji.

Przygotuj i roześlij odpowiednie informacje

Dzięki współpracy z ekspertami z różnych działów można szybko przygotować pierwsze informacje dla różnych zainteresowanych grup, które wyjaśnią, co się stało, kto i w jakim zakresie ucierpiał, co mogą zrobić osoby poszkodowane oraz jakie kroki naprawcze zostaną podjęte przez przedsiębiorstwo.

DBAJ O JAKOŚĆ PRZEKAZYWANYCH TREŚCI

Współpracuj z działem IT i ze specjalistami do spraw bezpieczeństwa

Cyberbezpieczeństwo jest trudnym tematem, a naruszenie bezpieczeństwa po-

ważną sytuacją, dlatego we wszystkich działaniach komunikacyjnych wyjątkową rolę odgrywa współpraca z działem IT, który najlepiej zna sytuację i może wyjaśnić techniczne aspekty problemu. Oczywiście dział PR powinien zadbać o to, by specjalistyczne komunikaty były jasne i w miarę możliwości prosto sformułowane. Dzięki temu firma będzie informować opinię publiczną w sposób rzetelny i zrozumiały.

Bądź szczery

Ukrywanie cyberataku to błąd, który może wiele kosztować. Tym bardziej że w dobie social mediów naprawdę trudno jest coś ukryć i o wycieku danych czy o niedziałającej usłudze prędzej czy później zaczną mówić w sieci klienci czy pracownicy firmy. Priorytetem powinno być więc jak najszybsze poinformowanie opinii publicznej o problemie. Jednak w tej komunikacji firma musi postawić na szczerość. Unikanie odpowiedzialności, zatajanie faktów, niedomówienia narażą ją na kryzys wizerunkowy i odpływ klientów.

Mów o tym, na co masz dowody

Komunikacja nie może wyprzedzać faktów. Jeśli firma nie ma pewności, czy problem z działaniem infrastruktury rzeczywiście wynika z cyberataku, i nie wie, czy jakiekolwiek dane ucierpiały – nie powinna sugerować tego w komunikatach przekazywanych opinii publicznej (usprawiedliwiając, na przykład, dużą awarię domniemaniami o możliwym cyberataku).

Pamiętaj o spójności komunikatów

O cyberataku należy mówić z odpowiednią powagą. Niezależnie od kanału komunikacji. Jeżeli firma korzysta z różnych mediów (strona www, Facebook, Instagram), jej przekazy w tych miejscach muszą mieć podobny ton oraz treści, nawet jeśli na co dzień któryś z tych kanałów jest wykorzystywany do przekazywania wiadomości o żartobliwym charakterze.

BĄDŹ OSTROŻNY W PODEJMOWANIU DZIAŁAŃ

Współpracuj z działem prawnym i z IT

Mówiąc o cyberataku, firma musi być bardzo ostrożna. Atak wiąże się także z koniecznością zgłoszenia do UODO, zatem to, co firma przekazuje w dokumentach do urzędu, i komunikaty w mediach czy social mediach muszą być spójne.

Dodatkowo podając zbyt wiele danych na temat infrastruktury firmy, można ją narazić na kolejne ataki cyberprzestępców. Dlatego tak ważne jest konsultowanie przygotowanych treści z prawnikami i specjalistami ds. bezpieczeństwa.

INFORMUJ I UDZIELAJ POMOCY POSZKODOWANYM

Przeproś i opowiedz o konsekwencjach

Cyberatak, w wyniku którego wyciekły dane, oznacza niepokój po stronie klientów czy pracowników. Zadaniem firmy jest więc nie tylko poinformowanie ich o naruszeniu, a także przeproszenie za zaistniałą sytuację, ale również wyjaśnienie, co ten wyciek oznacza, jakie może mieć konsekwencje dla zainteresowanych oraz jakie kroki mają teraz podjąć, by zminimalizować skutki naruszenia.

Przygotuj materiały informacyjne

Pomocne mogą być także dodatkowe materiały informacyjne – np. dostępna na www lista najczęściej zadawanych pytań i odpowiedzi na nie lub krótki poradnik wyjaśniający, co mogą zrobić osoby, których dane wyciekły.

KOMUNIKUJ REGULARNIE, ALE DO CZASU

Informuj o postępach działań naprawczych

Cyberatak oznacza spadek zaufania do firmy. Dlatego komunikacja nie może zakończyć się na poinformowaniu o problemie. Przedsiębiorstwo powinno też mówić o tym, jakie działania naprawcze podjęło, by nie dopuścić do podobnych zdarzeń w przyszłości. Wszystko po to, by pokazać, że traktuje sprawę poważnie i że robi wszystko, bo zwiększyć bezpieczeństwo danych firmy, jej pracowników i klientów.

Wyznacz moment, w którym zakończysz komunikację

Jednak ciągłe przypominanie o ataku również nie jest wskazane. Regularną komunikację należy zakończyć, gdy problem zostanie opanowany. Natomiast jeśli w późniejszym okresie firma podejmie ważne działania poprawiające jej bezpieczeństwo, może o tym, oczywiście, poinformować klientów i kontrahentów.

Czy w ogóle jest sens przejmować się na zapas cyberatakiem? Kilka minut przed napisaniem tego zdania otrzymałam wiadomość od jednej z firm kurierskich o możliwym wycieku

danych (w tym moich danych) u jego dostawcy usług SMS-owych. Ile takich wiadomości dos-tajecie? A ich liczba będzie rosła.

Każdy może paść ofiarą cyberataku. Nawet najlepiej zabezpieczona firma. Jednak dzięki dobrej współpracy różnych działów przedsiębiorstwa i szczerej, otwartej komunikacji z mediami, klientami, pracownikami i partnerami może zminimalizować negatywny wpływ ataku na swój wizerunek. Warto się zawczasu do tego przygotować.

PATRONAT
SECURITY MAGAZINE

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

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

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

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

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

4) **Znajdź skuteczne narzędzia walki z cyberatakami. Stwórz skuteczny plan reakcji na incydenty w cyberprzestrzeni.** 2 dni konferencji to p formatów szkoleniowych, w tym warsztaty i wykłady techniczne, oraz prezentacja start'upów oraz scale'upów z pionierskimi rozwiązaniami.

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

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

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

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

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

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

ZAREJESTRUJ SIĘ

Bilet standard 20% taniej z kodem SecMag20ST

ZINTEGROWANY SYSTEM OCHRONY KLASY PSIM W INFRASTRUKTURZE KRYTYCZNEJ

Tobiasz Bąkowski
C&C Partners

Elektrownie konwencjonalne, gazowe, wiatrowe, wodne, farmy fotowoltaiczne – w tych strategicznych obiektach wymagane są systemy najwyższej jakości, które w niezawodny sposób podnoszą efektywność procesów produkcyjnych, zapewniają bezpieczeństwo, umożliwią szybką reakcję w sytuacjach awaryjnych i dostarczą jednoznaczne dane do oceny sytuacji o zdarzeniu lub zagrożeniu. Każde wdrożenie musi być dopasowane do warunków charakterystycznych dla tej branży.

Zintegrowany system ochrony klasy PSIM w infrastrukturze krytycznej

Zdajemy sobie sprawę, że dobrze działająca infrastruktura techniczna ma wpływ na bezpieczeństwo i zapewnienie odpowiedniego standardu życia. Elementy infrastruktury niezbędne do minimalnego funkcjonowania gospodarki i państwa określa się mianem infrastruktury krytycznej, którym bez wątpienia jest energetyczna infrastruktura krytyczna. Aby podnieść bezpieczeństwo oraz niezawodność obiektów energetycznych, C&C Partners na bazie wieloletniego doświadczenia przygotowało dedykowane, modułowe rozwiązanie, biorąc pod uwagę obowiązujące przepisy, specyficzne warunki oraz wymagania klientów.

TECHNIKA VS. CZŁOWIEK

Rozwój techniki sprawia, że systemy informatyczne integrujące łączność i zarządzanie danymi, połączone z procederami zapewniają efektywniejszy nadzór nad bezpieczeństwem obiektów, niż człowiek pozbawiony tych narzędzi . Potwierdzają to wdrożone na całym świecie rozwiązania WinGuard - oprogramowania klasy PSIM+.

W pewnych założeniach systemy zarządzania bezpieczeństwem obiektów klasy PSIM+ (Physical Security Information Management) nie miały wyręczać stacjonarnych pracowników ochrony, lecz ich wspierać. Jednak lata rozwoju i ciągłego poszerzania funkcjonalności doprowadziły do sytuacji, w której systemy zintegrowane w praktyce zapewniają obiektom skuteczny monitoring i realizację założeń procesowych przez jednego operatora zdalnie, bez konieczności dozorowania wszystkich obiektów przez osobę na miejscu.

Producenci zintegrowanych systemów bezpieczeństwa klasy PSIM+ rozwijają wyjściowe założenia i wciąż udoskonalają swoje rozwiązania, wprowadzając sztuczną inteligencję (AI) do systemów zarządzania kryzysowego oraz wsparcia pracy operatora. Celem takiego działania jest coraz wyższy poziom bezpieczeństwa obiektów.

OBNIŻENIE KOSZTÓW ZARZĄDZANIA OBIEKTAMI

Skuteczniejsza ochrona jest możliwa obecnie przez centralizację zarządzania informacjami pozyskiwanymi ze wszystkich systemów zabezpieczeń technicznych zainstalowanych na chronionych obiektach. Nowoczesna technologia monitoringu wizyjnego z funkcją analizy oraz automatycznej detekcji niepożądanych zdarzeń, podwyższa skuteczność zdalnej ochrony obiektu i zarazem umożliwia natychmiastową reakcję ze strony operatorów systemu, pracujących w trybie 24/7/365.

Możliwość ograniczenia kosztów ochrony, których zdecydowaną większość pochłaniała dotychczas stała obecność w obiektach wyspecjalizowanych pracowników ochrony, jest odbierana jako duża zaleta systemu klasy PSIM+.

ELASTYCZNE NARZĘDZIE

Sam system WinGuard jest oprogramowaniem służącym do zarządzania procesem bezpieczeń-

stwa. Dzięki technologicznej otwartości, cechuje się zdolnością integrowania dotychczas użytkowanych w danym obiekcie technologii bezpieczeństwa, a także systemów przemysłowych, automatyki budynkowej czy komunikacji w jeden system bezpieczeństwa.

PROCES INWESTYCYJNY

System WinGuard jest rozwiązaniem nie powiązanym z żadnym producentem sprzętu, co umożliwia jego bardzo szybkie wdrożenie w istniejącej infrastrukturze serwerowej. PSIM to aplikacja skalowana, co oznacza, że system może się rozwijać zgodnie z możliwościami budżetowymi jednostki.

ZAPEWNIENIE NAJWYŻSZYCH STANDARDÓW BEZPIECZEŃSTWA POŻAROWEGO

Większą efektywność działania, a więc i wyższy poziom bezpieczeństwa pożarowego obiektu gwarantuje integracja wszystkich systemów ochrony przeciwpożarowej, niezależnie od producenta. Taką możliwość gwarantuje certyfikowany system integrujący urządzenia przeciwpożarowe (SIUP) CC WINGUARD. Należy mieć na uwadze, że system detekcyjny odpowiedzialny za ekspresowe wykrycie ognia, stanowi autonomiczną część układu systemu bezpieczeństwa pożarowego obiektu.

CERTYFIKOWANY SIUP

W momencie zagrożenia pożarowego kierujący akcją ratowniczo-gaśniczą, dzięki integratorowi urządzeń przeciwpożarowych CC WINGUARD, może podjąć odpowiednie kroki według procedur bezpieczeństwa (scenariusza pożarowego) zdefiniowanych dla całego chronionego obiektu.

Wizualizacja i możliwość sterowania systemami przeciwpożarowymi z wykorzystaniem integratora CC WINGUARD poprawia bezpieczeństwo obiektu o-raz pozwala na pracę nawet przy utracie zasilania podstawowego. Potwierdzanie bądź kasowanie alarmów pożarowych, sterowanie klapami pożarowymi, modyfikacje scenariusza pożarowego zgodnie z wytycznymi kierującego akcją ewakuacyjną to tylko niektóre z działań możliwych do przeprowadzenia w sposób szybki i sprawny z poziomu stacji operatorskiej.

Pełen zakres funkcjonalności integracji urządzeń przeciwpożarowych mogą zapewnić jedynie systemy certyfikowane, mające świadectwo dopuszczenia CNBOP-PIB.

PEŁNA GAMA MOŻLIWOŚCI

System integrujący urządzenia przeciwpożarowe (SIUP) CC WINGUARD jest kopalnią możliwości i korzyści na wszystkich etapach inwestycji i użytkowania obiektu – zarówno podczas projektowania, jak i w trakcie eksploatacji systemów przeciwpożarowych. Projektant ma w końcu możliwość zrealizowania koncepcji działania systemów ppoż., które do tej pory mogły być wyłącznie pomysłem. Wszystkie prace związane z wdrożeniem i późniejszą konserwacją systemu mogą zostać samodzielnie wykonane przez instalatora. W efekcie operator zyska komfort pracy dzięki intuicyjności rozwiązania. Inwestor z kolei będzie cieszył się najwyższym poziomem bezpieczeństwa, osiągając jednocześnie kompromis z wymarzoną architekturą wnętrza swojego obiektu.

PODSUMOWANIE

System PSIM WinGuard bez wątpienia jest rozwią-

zaniem przyszłościowym, z którego zarządzający obiektami rozproszonymi korzystają na całym świecie. Możliwość przeniesienia procedur obowiązujących w danym obiekcie, czy kompleksie obiektów, w tym ochrony przeciwpożarowej do elektronicznego świata IT jest ogromnym autem zarówno dla inwestorów, jaki i dla osób obsługujących system.

PATRONAT
SECURITY MAGAZINE

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

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

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

Pogłębisz swoją wiedzę w obszarach takich jak:

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

KOGO SPOTKASZ NA KONFERENCJI?

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

ZAREJESTRUJ SIĘ TUTAJ!

incidentbusters.pl

„SPLĄTANIE GENERATYWNE”. REGULACJE ROZWIĄŻĄ ETYCZNE I PRAWNE PROBLEMY ZWIĄZANE Z AI?

Anna Szymańska
Kancelaria Prawna Media Law

Oficjalnie termin „splątanie generatywne” nie istnieje, ale za to trafnie definiuje zjawiska, które wywołane przez generatywne modele sztucznej inteligencji rewolucyjnie zmieniają nasze życie w każdej niemal dziedzinie.

Wzajemne oddziaływanie na siebie i przenikanie się tego co prawdziwe, z tym co trudno ocenić pod względem prawdy lub fałszu, przy jednoczesnym kolosalnym wpływie sztucznej inteligencji na rozwój technologiczny, skłania do dokonania pierwszych poważnych podsumowań.

Zacznijmy od podstawowego pytania. Czym jest sztuczna inteligencja?

Przejście do świata, w którym sztuczna inteligencja, czyli systemy zbudowane na uczeniu maszynowym i głębokim przetwarzaniu danych są zdolne do rozumienia na ludzkim poziomie, konwersacji, mają nadludzkie moce asymilacji danych i są zdolne do samodzielnego rozpoznawania wzorców jest już faktem.

Można oczekiwać, że w dalszej perspektywie będzie miało to wpływ na to, jak będziemy pracować, organizować biznes i definiować rolę człowieka w codziennej korelacji z maszyną.

Rozwój technologii na niespotykaną dotąd skalę nie pozostawia wątpliwości, że należy nadać mu ramy prawne.

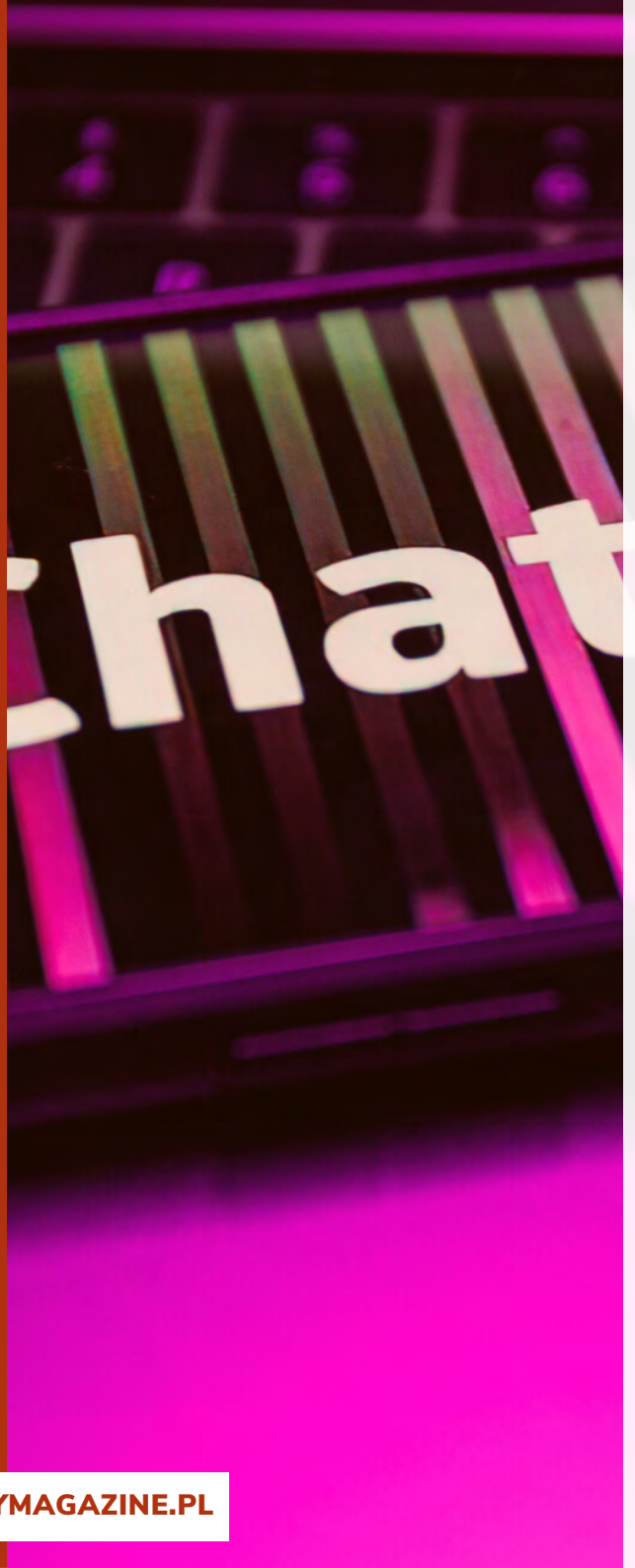
CZY PRAWNA DEFINICJA POMOŻE?

Przyjęcie przez unijnego ustawodawcę ostatecznej prawnej definicji sztucznej inteligencji będzie momentem przełomowym dla uregulowania tego zjawiska. Z pomocą przychodzi unijny projekt rozporządzenia o sztucznej inteligencji - Artificial Intelligence Act (AI Act).

Według rozporządzenia sztuczna inteligencja to *„system oparty na maszynie, który jest zaprojektowany do działania na różnych poziomach autonomii i który może, w przypadku jawnych lub dorozumianych celów, generować dane wyjściowe, takie jak prognozy, zalecenia lub decyzje mające wpływ na środowiska fizyczne lub wirtualne"*.

Po pierwszych analizach tej definicji nasuwają się wątpliwości co do kwalifikacji rozwiązań technologicznych jako AI. Nieprecyzyjna i zbyt szeroka definicja sztucznej inteligencji może powodować problemy interpretacyjnie co do uznania danego rozwiązania za AI i poddania go regulacji.

Rozwój AI ma szansę pozytywnie wpłynąć na



gospodarki, rynki i rozwój technologii na całym świecie. Dlatego należy uważać, żeby „twarde" regulacje nie zablokowały rozwoju innowacyjności jak i samej technologii. Potrzebne jest także wypracowanie zbioru zasad AI (te są proponowane w AI Act), które dadzą podstawę do rozwiązania już istniejących problemów związanych z korzystaniem ze sztucznej inteligencji.

ETYKA, CZYLI SZACUNEK DO WARTOŚCI

Sformułowanie problemów etycznych związanych ze sztuczną inteligencją pomoże unijnemu ustawodawcy na wypracowanie właściwych przepisów wyznaczających kierunki korzystania z AI.

Istotnym problemem jest trudność oceny, czy to co zostało wygenerowane przez AI jest prawdą. I to na poziomie trenowania AI, jak i generowania tekstów przez użytkowników. Ostatnie badania pokazują, że wygenerowany tekst przez ChatGPT nie musi zawierać prawdziwych informacji. Jak pisze na swoim blogu Stephen Wolfram – brytyjski naukowiec, matematyk i założyciel wyszukiwarki Wolfram Alfa - AI nie potrafi weryfikować informacji. Produkuje je na podstawie wprowadzonych do niej danych. Chociaż naukowcy zajmujący się sztuczną inteligencją potrafią wyjaśnić mechanikę działania systemów AI, nie są w stanie powiedzieć, co tak naprawdę się w nich dzieje. Jeśli treść nie jest prawdziwa, może spowodować szkodę, naruszyć dobra osobiste lub renomę firmy poprzez publikację nieprawdziwych informacji.

Nieetyczne jest przypisanie sobie przez człowieka autorstwa tekstu w całości wygenerowanego przez ChatGPT lub grafik wygenerowanych przez Midjourney.

Dynamicznie zwiększająca się ilość treści w Internecie, których nie można obiektywnie zweryfikować poprzez pryzmat tego jak zostały stworzone, wprowadza chaos i niepewność. Nie wiemy już, co jest prawdą.

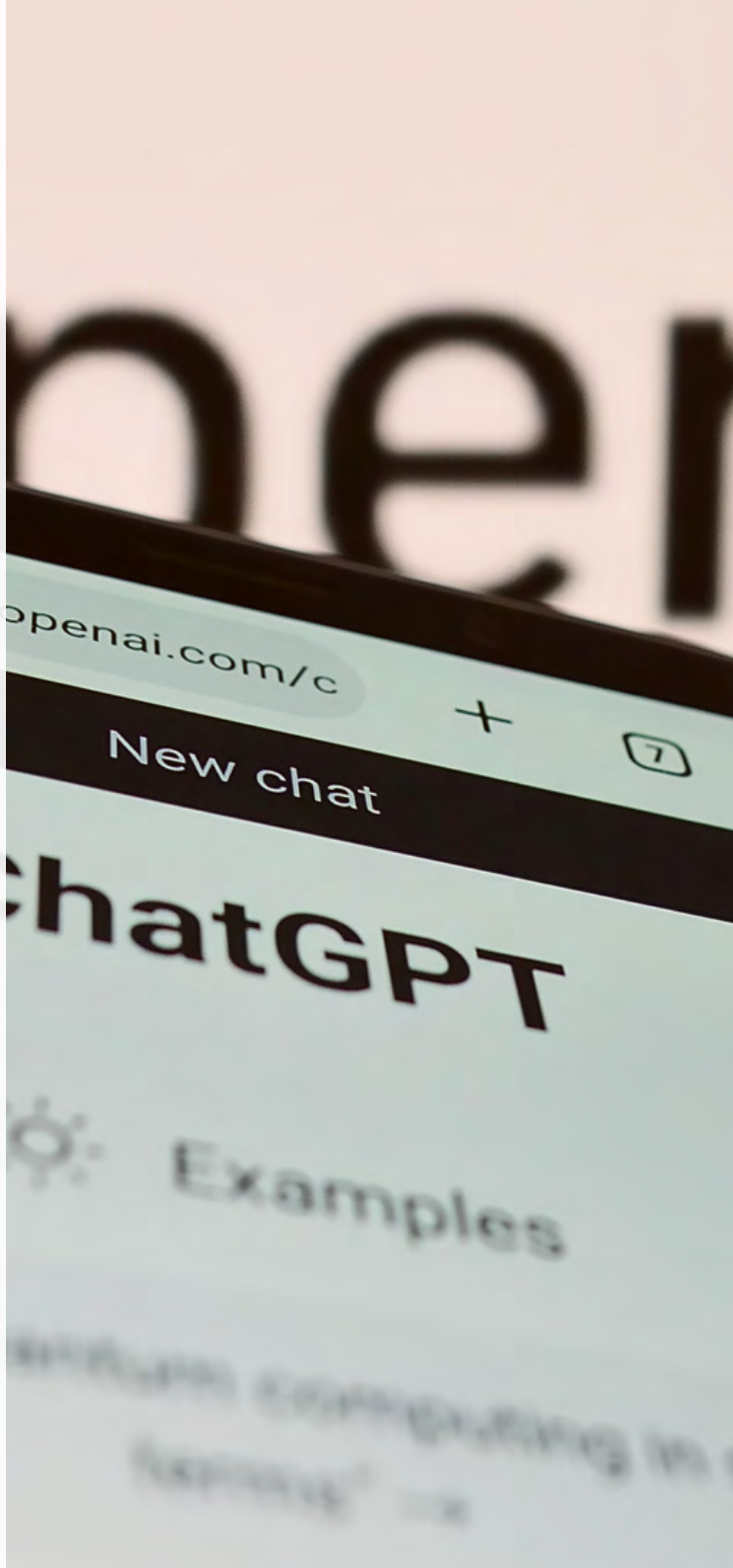
Bezrefleksyjne korzystanie z AI to nadużywanie wartości etycznych, co widać już w interakcjach społecznych, procesach naukowych i dydaktycznych oraz w biznesie.

PRAWA AUTORSKIE NARUSZONE PRZEZ TRENOWANIE AI?

Po pierwszej euforii jednych lub sceptycyzmie innych w związku z pojawieniem się narzędzi sztucznej inteligencji na niespotykaną dotąd skalę, przyszła kolej na definiowanie problemów prawnych, które są wyzwaniem dla prawników na całym świecie.

Pojawiło się pytanie czy trenowanie modeli sztucznej inteligencji narusza prawa autorskie? Czy producenci modeli Stability AI (UK) i Stable Diffusion, Midjourney i DeviantArt (USA) mogli pozyskiwać dane, treści i obrazy z internetu w celu trenowania swoich modeli?

Tu z odpowiedzią przyjdą wyroki sądów w USA i Wielkiej Brytanii w sprawach, które toczą się przeciwko tym producentom. Sądy będą musiały odpowiedzieć na szereg pytań takich jak: czy trenowanie modeli AI odbywa się na zasadzie amerykańskiego fair use, czyli dozwolonego użytku korzystania z utworów? Czy pobieranie i wykorzystanie tzw. „latent images" (ukrytych obrazów) w celu trenowania AI jest bezprawnym opracowaniem i zwielokrotnieniem utworów chronionych prawem autorskim?



Czy AI tworzy utwory zależne w odniesieniu do utworów użytych do trenowania AI? Czy użytkownik AI może stworzyć za pomocą narzędzia AI plagiaty cudzych prac i przez to naruszyć ich prawa autorskie? Czy producenci AI naruszają regulaminy serwisów internetowych i umów?

Na gruncie europejskim Dyrektywa o prawie autorskim na jednolitym rynku cyfrowym (prace nad implementacją Dyrektywy do polskiej ustawy o prawie autorskim i prawach pokrewnych już trwają) niesie zmiany, wprowadzając nowe przepisy dla uczenia maszynowego.

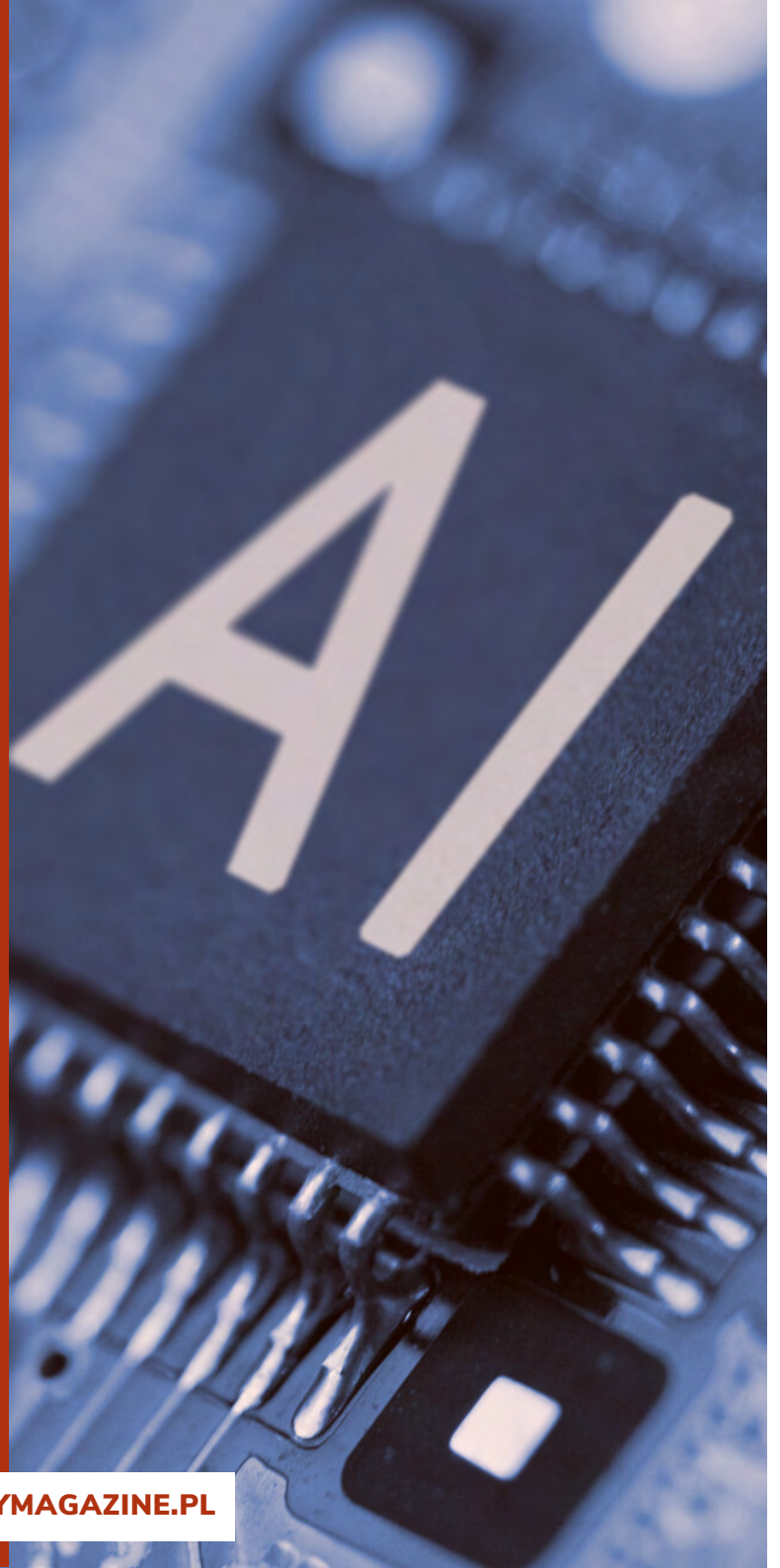
CZY WYNIKI AI MOGĄ BYĆ CHRONIONE PRAWEM AUTORSKIM?

Nie wszyscy zdają sobie sprawę, że korzystając z ChatGPT, jednocześnie trenują ten model poprzez formułowanie pytań. Szczególnie powinny uważać firmy, które chronią swoje know-how oraz prawa autorskie, które służą rozwojowi biznesu i zawierają dane będące tajemnicą przedsiębiorstwa. Dane wprowadzone w formie pytań zadawanych chatbotowi nie są chronione, tracimy nad nimi kontrolę.

Problemem jest także sam wynik wygenerowany przez ChatGPT. Należy pamiętać o tym, że zgodnie z regulacjami TSUE oraz orzeczeniami sądów na całym świecie, twórcą utworu może być tylko człowiek, nie maszyna. Wynika z tego, że tekst lub grafika wygenerowane przez AI nie są chronione prawami autorskimi. To z kolei prowadzi do wniosku, że nie można takich praw przenieść na inne osoby lub udzielić licencji. Każdy także może wykorzystać i skopiować wygenerowany tekst bez zarzutu naruszenia prawa autorskiego.

Urząd ds. praw autorskich w USA - US Copyright Office - wydał oficjalne wytyczne w sprawie uznania praw autorskich do utworów zawierających elementy stworzone przez AI. Czytamy, że ochronie podlegają tylko oryginalne, kreatywne, intelektualne wybory twórcze autora. Należy przy tym badać, czy dzieło jest autorstwa człowieka, a AI jest jedynie narzędziem pomocniczym, czy też „tradycyjne elementy” dzieła (literacki, artystyczny, muzyczny lub elementy selekcji, aranżacji etc.) zostały wymyślone i wykonane przez maszynę.

W przypadku prac zawierających materiał wy-



generowany przez AI należy rozważyć, czy wkłady AI są wynikiem jedynie „mechanicznej reprodukcji czy rezultatem własnej oryginalnej koncepcji myślowej autora, której nadał on widoczną formę.

Jeśli „tradycyjne elementy” autorskie dzieła zostały wygenerowane przez maszynę, dzieło nie jest autorstwa człowieka. Jednak w przypadkach, gdy człowiek może wybrać lub zaaranżować materiał wygenerowany przez sztuczną inteligencję w wystarczająco kreatywny sposób, takie dzieło jako całość będzie stanowiło oryginalne dzieło autorskie.

Ma to ogromne w skutkach znaczenie dla firm, dla których prawa własności intelektualnej są istotną częścią biznesu, czyli dla większości firm i branż działających w środowisku cyfrowym.

CZY AI ACT ROZWIĄŻE PROBLEM?

AI Act to pierwszy akt prawny regulujący korzystanie ze sztucznej inteligencji w Unii Europejskiej. Określa zharmonizowane zasady stosowania sztucznej inteligencji zgodnie z unijnymi wartościami, a ich celem ma być zapewnienie bezpieczeństwa użytkownikom i przejrzystość działania modeli AI, przy zachowaniu możliwości rozwoju innowacji.

Uregulowanie rynków technologicznych ma nastąpić poprzez różnicowanie wysokości ryzyka, jakie niesie ze sobą sztuczna inteligencja.

Tym samym odpowiedzialność za działanie sztucznej inteligencji wysokiego ryzyka obciąży dostawców AI, którzy będą musieli zapewnić narzędzia do weryfikacji zakazanych praktyk.

AI Act przewiduje także obowiązek wdrożenia systemów kontroli zarządzania ryzykiem, kontroli danych i cyberbezpieczeństwa, tak żeby możliwa była ocena oddziaływania rozwiązań sztucznej inteligencji na człowieka.

Zapewnienie przejrzystości działania AI przez dostawców technologii i podstaw do oceny prawdziwości informacji generowanych przez AI jest dobrymi kierunkiem, chociaż budzi wątpliwość co do skuteczności jego wyegzekwowania.

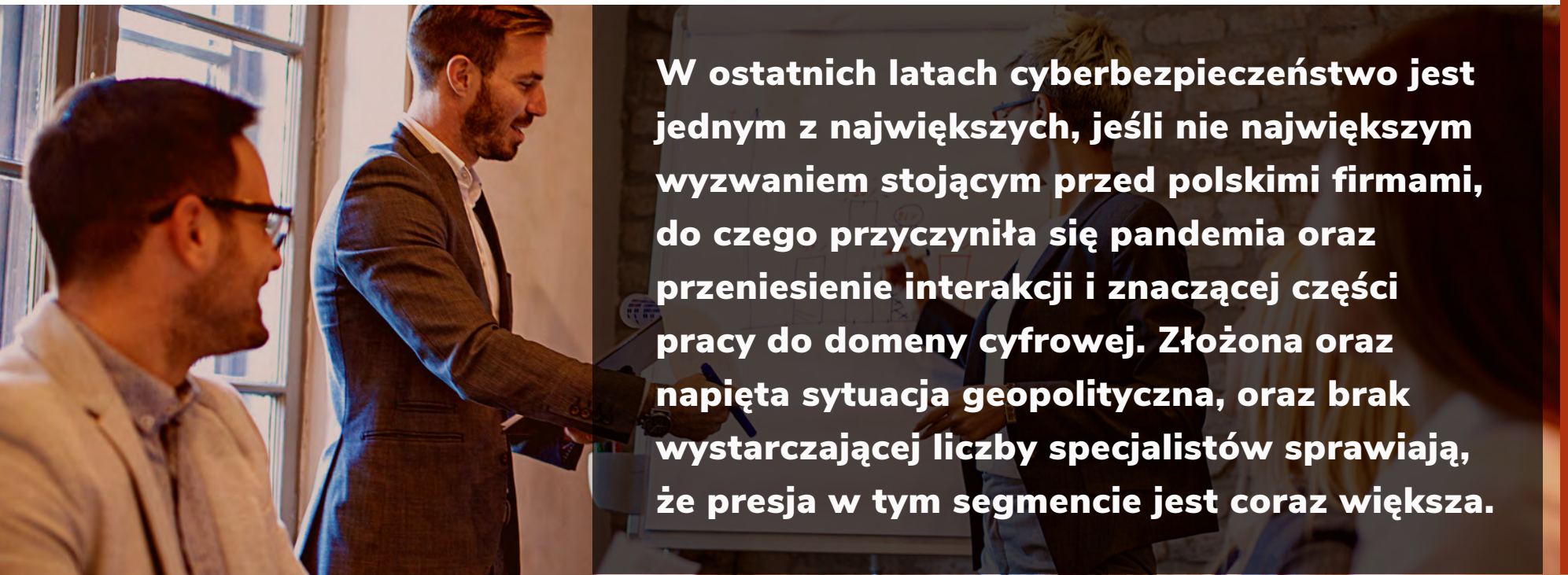
Do nowych przepisów AI Act będą musiały się dostosować wszystkie firmy i organizacje wykorzystujące rozwiązania AI.

Nie ma wątpliwości, że regulacje działania sztucznej inteligencji są pilnie potrzebne. Perspektywa szybkości i łatwości tworzenia tekstów, obrazów, treści multimedialnych jest atrakcyjna, ale też niebezpieczna. Szczególnie ważne jest zaprojektowanie skutecznych przepisów dotyczących odpowiedzialności za działania AI, bo prawo tylko wtedy ma sens, kiedy jest możliwe do wyegzekwowania. Już teraz warto uczyć się o potencjale korzystania z AI i prawnych możliwościach modelowania rozwiązań opartych o AI w biznesie, bo chociaż jest jeszcze wiele niewiadomych to technologie są przyszłością. To jest podróż w jedną stronę. Od sztucznej inteligencji nie ma odwrotu.

/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

CYBERBEZPIECZEŃSTWO JAKO ELEMENT OCHRONY WIZERUNKU FIRMY

Dariusz Mrugowski
ENGAVE S.A.



W ostatnich latach cyberbezpieczeństwo jest jednym z największych, jeśli nie największym wyzwaniem stojącym przed polskimi firmami, do czego przyczyniła się pandemia oraz przeniesienie interakcji i znaczącej części pracy do domeny cyfrowej. Złożona oraz napięta sytuacja geopolityczna, oraz brak wystarczającej liczby specjalistów sprawiają, że presja w tym segmencie jest coraz większa.

LICZBA CYBERATAKÓW WCIĄŻ ROŚNIE

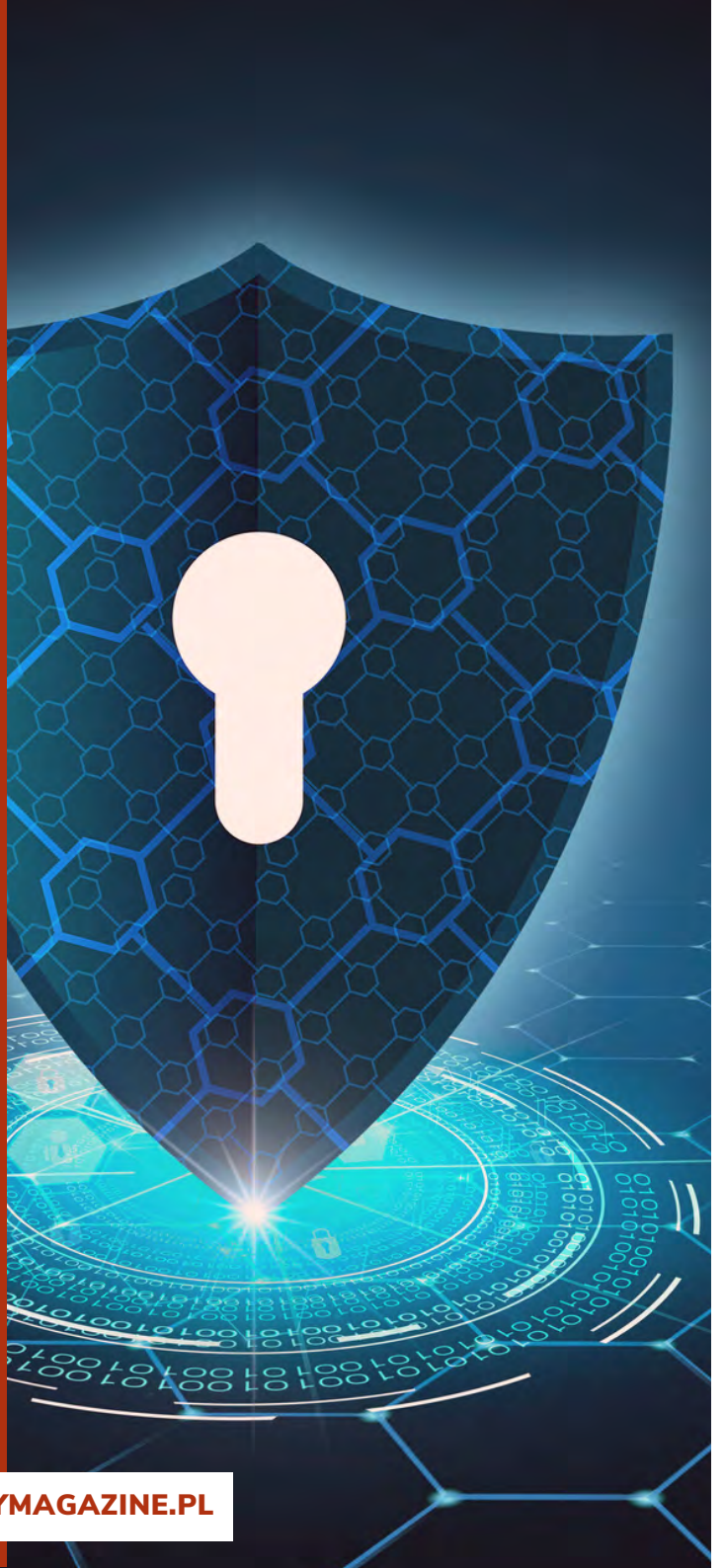
Sukces digitalizacji został natychmiast dostrzeżony i wykorzystany przez cyberprzestępców, którzy dostosowali pod jej kątem swoje sposoby działania. Zagrożenia w sieci są realne i mogą mieć bardzo poważne konsekwencje dla renomy firmy oraz zaufania klientów.

Cyberbezpieczeństwo jest niezwykle istotne dla wizerunku firmy, ponieważ liczba cyberataków na przedsiębiorstwa rośnie z roku na rok. Jak KPMG wskazuje w swoim raporcie „Barometr cyberbezpieczeństwa" za 2022 r. aż 1/3 przedsiębiorstw działających w Polsce, odnotowała wzrost intensywności cyberataków na swoje systemy.

Największym ograniczeniem dla wielu firm w zakresie uzyskania odpowiedniego poziomu zabezpieczeń jest brak wystarczających budżetów, co według raportu, deklaruje aż 57% przedsiębiorstw. Dużym ograniczeniem dla blisko połowy organizacji są również trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników. CERT Polska natomiast zarejestrował w 2021 r. łącznie 29 483 unikalnych incydentów cyberbezpieczeństwa, co wskazuje na wzrost obsłużonych incydentów o 182 proc. w porównaniu do roku 2020.

NIEWŁAŚCIWE ZARZĄDZANIE FIRMĄ?

Skutki cyberataków mogą być bardzo poważne i w krótkim czasie wpłynąć na reputację firmy. Incydenty związane z naruszeniem bezpieczeństwa danych, takie jak wycieki informacji o klientach, czy cyberprzestępstwa finansowe, często kojarzą się z brakiem dbałości o bezpieczeństwo i niewłaściwym zarządzaniem firmą. Takie zdarzenia przekładają się na utratę zaufania klientów i inwestorów, a także na spadek sprzedaży i wartości rynkowej firmy.



Przykłady słynnych incydentów, takich jak atak na Sony Pictures Entertainment, czy wyciek danych u dostawcy menadżera haseł Last pass, pokazują, jak negatywny wpływ na wizerunek firmy mogą mieć cyberataki.

W wyniku incydentów, firmy te musiały zmagać się z utratą zaufania klientów i spadkiem wartości rynkowej. Ponadto zgodnie z badaniami, aż 66% klientów decyduje się na rezygnację z usług firmy, która padła ofiarą cyberataków, co oznacza znaczące straty finansowe dla przedsiębiorstwa.

KLUCZOWY ELEMENT STRATEGII FIRMY

Dlatego właśnie cyberbezpieczeństwo powinno być kluczowym elementem strategii biznesowej i wizerunkowej każdej firmy bez względu na branżę. Skuteczne działania w zakresie cyberbezpieczeństwa nie tylko pomogą uniknąć strat finansowych i reputacyjnych, ale także zbudować pozytywny wizerunek przedsiębiorstwa jako jednostki odpowiedzialnej oraz dbającej o bezpieczeństwo swoich klientów, jak również ich danych powierzonych firmie.

W celu zbudowania wizerunku firmy odpornego na cyberzagrożenia, należy przede wszystkim przeprowadzić wnikliwą analizę ryzyka, polegającą na zidentyfikowaniu zagrożeń oraz potencjalnych słabych punktów w systemach informatycznych i procesach biznesowych firmy. Taką analizę znacznie ułatwia posiadanie dokładnie zmapowanych procesów funkcjonujących w przedsiębiorstwie.

Na tej podstawie można opracować plan działań, które pomogą zminimalizować ryzyko wystąpienia incydentów związanych z bezpieczeństwem informacji.

Kolejnym krokiem jest wdrożenie odpowiednich rozwiązań technologicznych, takich jak oprogramowanie antywirusowe, zabezpieczenia sieciowe, czy systemy monitorujące ruch w sieci. Należy również pamiętać o regularnym aktualizowaniu oprogramowania i wdrażaniu nowych wersji zabezpieczeń, które pomogą zminimalizować ryzyko wystąpienia luk w bezpieczeństwie. Ważnym elementem budowania wizerunku firmy odpornego na cyberzagrożenia jest cykliczne szkolenie wspierane budowaniem świadomości z zakresu bezpieczeństwa informacji u pracowników.

Wszyscy pracownicy powinni mieć świadomość zagrożeń w sieci oraz wiedzieć, jak postępować w przypadku podejrzenia ataku. Warto również przeprowadzać regularne testy penetracyjne, które pomogą zidentyfikować ewentualne słabości systemów oraz ocenić skuteczność działań w zakresie bezpieczeństwa.

Oprócz działań technicznych i szkoleń, warto zwrócić uwagę na komunikację z klientami i inwestorami. Informowanie o podejmowanych działaniach w zakresie cyberbezpieczeństwa oraz reakcji na incydenty może zbudować pozytywny wizerunek firmy jako odpowiedzialnej i troszczącej się o bezpieczeństwo swoich interesariuszy.

PROCEDURY

Dlatego należy mieć gotowe procedury, które pozwolą na szybką i skuteczną reakcję na ewentualne incydenty oraz na skuteczną komunikację z klientami i inwestorami. W przypadku wystąpienia incydentu, reakcja firmy jest kluczowa dla jej wizerunku.

W pierwszej kolejności należy podjąć natychmiastowe działania mające na celu zminimalizowanie szkód i przywrócenie systemów do poprawnego działania. Należy również poinformować odpowiednie służby, takie jak policja czy prokuratura, w przypadku podejrzenia przestępstwa. Ważne jest również szybkie powiadomienie klientów i inwestorów o incydencie oraz o podjętych działaniach mających na celu ochronę ich danych.

Dobre praktyki w tym zakresie obejmują przygotowanie gotowych procedur reagowania na incydenty oraz prowadzenie regularnych ćwiczeń symulujących różnego rodzaju ataki. Warto pamiętać, że nie tylko sama reakcja na incydent ma znaczenie, ale również sposób, w jaki jest ona komunikowana. Należy unikać ukrywania informacji, które mogą być istotne dla klientów lub inwestorów oraz działać w sposób transparentny i rzetelny. W ten sposób można zminimalizować negatywny wpływ incydentu na wizerunek firmy oraz zbudować zaufanie do jej działań w zakresie cyberbezpieczeństwa.

Ostatecznie, warto pamiętać, że budowanie wizerunku firmy odpornego na cyberzagrożenia to proces ciągły i wymagający stałego monitorowania oraz aktualizacji działań zabezpieczających. Działania w zakresie cyberbezpieczeństwa powinny być integralną częścią strategii biznesowej każdej firmy, a ich skuteczność powinna być regularnie oceniana i mierzona. W dzisiejszych czasach firmy, które nie inwestują w cyberbezpieczeństwo, narażają się na poważne ryzyko i mogą być postrzegane jako nieodpowiedzialne wobec swoich klientów i partnerów biznesowych.

BRAK FUNDUSZY? JAK TO ROZWIĄZAĆ?

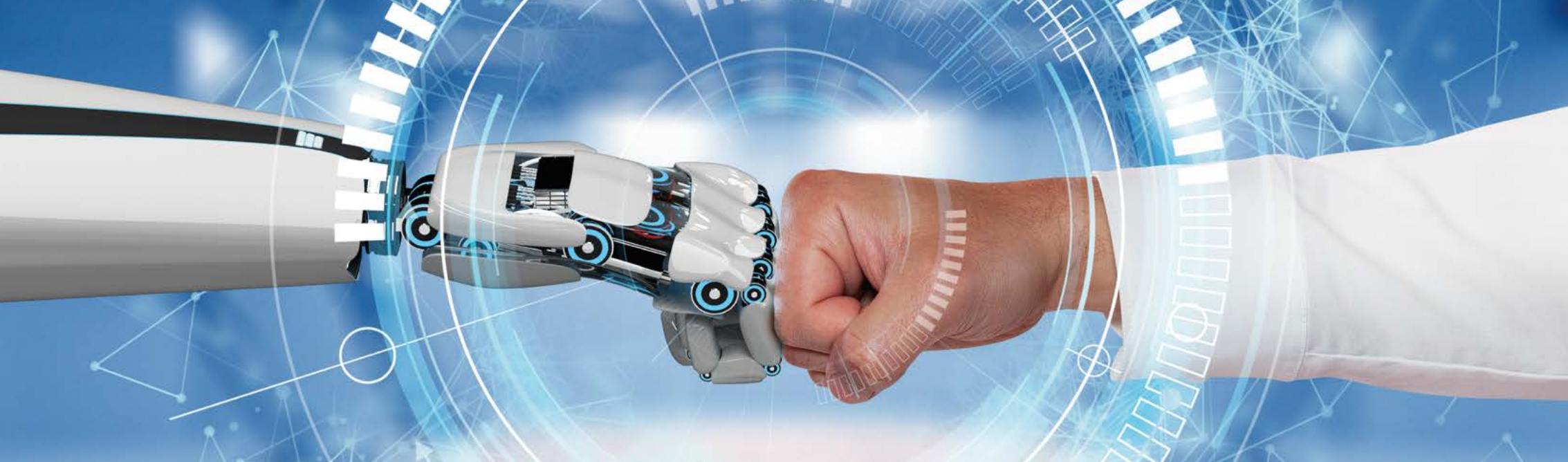
Cyberbezpieczeństwo staje się coraz ważniejsze dla firm, ponieważ cyberzagrożenia stają się coraz bardziej powszechne i zaawansowane. Zabezpieczenie danych, ochrona przed atakami oraz szybka reakcja na incydenty to kluczowe elementy, które mogą pomóc w ochronie wizerunku firmy.

Jednakże nie wszystkie firmy mogą pozwolić sobie na stworzenie wewnętrznych struktur cyberbezpieczeństwa, zatrudnienie wykwalifikowanych specjalistów oraz zakup niezbędnych narzędzi monitorujących zagrożenia w czasie rzeczywistym.

Ratunkiem w takiej sytuacji jest skorzystanie z outsourcingu usług w tym zakresie, co pozwoli na utrzymanie odpowiedniego poziomu bezpieczeństwa w stosunku do ponoszonych kosztów. Wiele doświadczonych firm jest w stanie reagować o wiele szybciej niż etatowi pracownicy firmy zaatakowanej – zwłaszcza, jeśli jest to niewielka firma, w której nie ma możliwości utrzymania w całodobowej gotowości działu IT lub stworzenia własnego SOC (Security Operations Center).

Cyberbezpieczeństwo jest, więc niezbędnym elementem ochrony wizerunku firmy i powinno być integralną częścią strategii biznesowej w każdej organizacji. Inwestycje w cyberbezpieczeństwo i regularne szkolenia pracowników to klucz do sukcesu.

Doświadczenia wielu firm pokazują, że dobrze przygotowane przedsiębiorstwa są postrzegane przez swoich klientów jako godne zaufania. Niezależnie jak zaawansowany poziom zabezpieczeń technologicznych ma firma, zawsze kluczową rolę odgrywa człowiek i jego czujność, dlatego też nie można oszczędzać na kształtowaniu pozytywnych postaw.



engave

Razem zbudujemy
TWOJĄ FIRMĘ
jutra

Sprawdź

APLIKACJE I SYSTEMY DLA BIZNESU | USŁUGI DLA IT | DORADZTWO BIZNESOWE

#PlayTechTogether

ROZWÓJ NOWYCH TECHNOLOGII A PRYWATNOŚĆ

Magdalena Celeban
ODO Szkolenia

Prywatność w świecie cyfrowym to złożona kwestia, która zyskała na znaczeniu wraz z rozwojem nowych technologii. Czym szybszy rozwój nowych technologii, tym więcej zadajemy sobie pytań dotyczących naszej prywatności, czy jeszcze coś takiego istnieje? Na ile chcemy wierzyć, że jeszcze zarządzamy lub mamy ułudę wpływu na nasze życie i podejmowane decyzje.

Nadszedł czas, aby zacząć zastanawiać się nad pojęciem „prywatności", które ewaluuje z roku na rok obserwując powstawanie nowych metod i narzędzi kontroli.

Chciałabym zaznaczyć, że jestem zwolenniczką nowoczesnych technologii, rozwoju, AI oraz wszystkiego co będzie w najbliższym czasie, (a nie potrafimy jeszcze tego nazwać), wszelkie nowe wynalazki, technologie mają za zadanie wspierać oraz pomagać człowiekowi, i w tym miejscu nie sposób nie wspomnieć, o Nikoli Tesli, który był uważany za szaleńca ze względu na innowacyjność swoich wynalazków, którymi wyprzedzał swoje czasy. Obecnie większość z jego patentów zostaje wykorzystywana w motoryzacji, jak i wielu innych dziedzinach, nie zdajemy sobie jednak z tego sprawy, nie zastanawiamy się nad tym.

Podobnie było z żarówkami traktowanymi jeszcze na początku ubiegłego wieku w wielu miejscach jako „wynalazek diabła" - któż z nas wyobraża sobie nie korzystanie z żarówek i prądu? Chyba już nikt. Podobnie jest z telefonami, które obecnie są dla nas codziennym przedmiotem, bez którego nie wyobrażamy sobie życia, bez względu na wiek. Młodsze pokolenie zadaje nam pytanie: „jak żyliście bez telefonów komórkowych?", a w szczególności bez internetu. Tak żyliśmy, i to całkiem dobrze, w innym świecie technologicznym. Tak szybki rozwój technologii wiąże się zarówno z wieloma możliwościami, jak również zagrożeniami.

PRYWATNOŚĆ

Czym jest prywatność? Na ile mamy jeszcze wpływ na anonimowość? Brak prywatności jest trudniejszy dla pokolenia X (urodzeni w latach 1965-1979), pokolenie które żyło w czasach, gdy głównym doświadczeniem pokoleniowym była dla nich przemiana ustrojowa w Polsce. Obecnie są to ludzie w wieku 40+, którzy są przywiązani do tradycyjnych kontaktów międzyludzkich i komunikacji twarzą

w twarz. To od tego pokolenia najczęściej słyszymy słowa: „za moich czasów”, ale tych czasów już nie ma, są inne, z nowymi technologiami oraz wielkimi możliwościami.

Pokolenie Y (urodzeni w latach 1980-1996), których ukształtował już Google oraz gry wideo podchodzą do pojęcia prywatności w sposób bardziej elastyczny. Wierzą, że są kowalami swojego życia - to oni decydują, kto i co o nich będzie wiedział, często, niestety, właśnie oni są tym pokoleniem, które najbardziej jest zagrożone na utratę prywatności w sieci. Pokolenie X, które często wycofuje się z kontaktów w sieci, nie ufa do końca nowym technologiom, posiadając pamięć z dawnego ustroju politycznego, gdzie kontrola obywatela była głównym zadaniem wielu organów, w zderzeniu z pokoleniem Y zachowuje większą czujność. Młodsze pokolenie bardzo często nie posiada takich umiejętności i wiedzy, jak pokolenie Z, a w ich opinii są bezpieczni, nie lubią prosić o pomoc.

Pokolenie Z (urodzeni po 1995 roku), które zawsze najbardziej mnie interesuje ze względu na życie w świecie cyfrowym praktycznie od początku swojego życia, w mojej opinii, nie odczuwa prywatności jako nadrzędnej wartości.

Inaczej definiuje, czego innego wymaga. Bardzo często zdaje sobie sprawę z jej braku. Pokolenie, które często jest nazywane pokoleniem C od angielskich słów connect, communicate, change. Młodzi ludzie zanurzeni w świecie internetu. Dzieci urodzone po 2010 roku bardzo często nazywane są „tubylcami cyfrowymi”.

Każde z tych pokoleń będzie miało inną definicję prywatności. Nie ma w tym nic złego, wręcz przeciwnie, odmienne czasy wymagają różnego podejścia do pojęć.

GROMADZENIE DANYCH

Dzięki powszechnemu użyciu smartfonów, mediów społecznościowych i innych technologii cyfrowych, firmy i rządy mogą zbierać ogromne ilości danych o osobach, mieszkańcach i obywatelach. Dane te mogą obejmować informacje osobiste, historię przeglądania, dane dotyczące lokalizacji i inne.

W dzisiejszych czasach coraz więcej firm, organizacji jak również instytucji gromadzi dane osobowe o swoich klientach i pracownikach również w celach uzasadnionego interesu administratora, marketingu. Dane te mogą zawierać zarówno dane zwykłe takie jak: imię, nazwisko, adres zamieszkania, ale również

dane dotyczące preferencji zakupowych, aktywności na stronach, a nawet dane szczególnej kategorii jak stan zdrowia, przynależności związkowe i polityczne.

Gromadzenie danych osobowych jest ważne dla wielu firm oraz organizacji, a czasami wręcz jest warunkiem istnienia na rynku, ponieważ zbieranie i analizowanie danych umożliwia im lepsze zrozumienie swoich klientów, dostosowanie swoich usług i ofert handlowych do ich potrzeb, a co za tym idzie zwiększenie zysków. Nie możemy jednak zapominać, że gromadzenie takich danych niesie bardzo często za sobą ryzyko związane z zagrożeniem prywatności, a nawet bezpieczeństwa tych osób.

PRZEPISY PRAWA DOTYCZĄCE PRYWATNOŚCI

W związku z powyższym wiele krajów wprowadziło przepisy dotyczące ochrony danych osobowych, takie jak ogólne rozporządzenie o ochronie danych osobowych (RODO) w Unii Europejskiej czy ustawy o ochronie danych osobowych. Przepisy te nakładają na firmy i organizacje dodatkowe obowiązki z zakresu bezpieczeństwa, mają za zadanie regulować sposób, w jaki firmy mogą gromadzić i wykorzystywać dane osobowe, a także mogą nadawać osobom fizycznym pewne prawa dotyczące ich własnych danych osobowych.

W prawie krajowym również kwestia bezpieczeństwa jest uwzględniana w prawodawstwie. Przykładem mogą być ostat-

nie zmiany w kodeksie pracy, które chyba pierwszy raz od 2018 r. ukazały nam jak obecnie bezpieczeństwo, ochrona danych osobowych jest ściśle powiązana z innymi aktami prawnymi. Co niektórzy zwracali nawet uwagę na fakt, że przy zmianach w kodeksie pracy dotyczących pracy zdalnej więcej zmian dotyczy zapewnienia bezpieczeństwa niż wdrożenia wytycznych pracy zdalnej.

MONITORING A PRYWATNOŚĆ

Monitorowanie jest ważnym narzędziem w wielu dziedzinach, takich jak bezpieczeństwo publiczne, monitorowanie procesów przemysłowych czy nadzór nad pracownikami w miejscu pracy.

W ostatnim czasie często podnosi się temat wykorzystywanie danych osobowych do innych celów niż są pozyskiwane, najczęściej mówimy tu o moni-

toringu zarówno wizyjnym, jak i pracowniczym. Najgorętsze dyskusje, to te oczywiście oparte na art. 6 pkt. 1 lit. f RODO dotyczące uzasadnionego interesu Administratora w przypadku monitoringu wizyjnego, który ma za zadanie zapewnienie bezpieczeństwa. W wielu przypadkach monitoring będzie musiał być uregulowany prawnie, w przypadku zainstalowania monitoringu w zakładach produkcyjnych jesteśmy zobowiązani do opracowania szczegółowego regulaminu monitoringu, jak również poinformowania wszystkich pracowników w ustalonym przez ustawodawcę terminie o planowanym nagrywaniu.

Niestety, przez wielu z nas monitoring wizyjny jest spostrzegany jako kontrola, podobnie jak monitoring pracowniczy, który jest negatywnie oceniany przez pracowników. Kontrola pracownika, to, niestety, w opinii związków zawodowych, jak również i zainteresowanych - brak zaufania wobec pracownika. Bardzo często pracodawcy, aby nie utracić pozytywnego wizerunku firmy rezygnują z kontroli poczty pracownika, jego kontaktów. Wciąż w naszym społeczeństwie bazuje stwierdzenie, że pracownik na pewno chce nas oszukać, i stąd różne formy monitoringu. W wielu przypadkach wymagana jest zgoda osób do przetwarzania wizerunku w celu ochrony prywatności.

Podobnie jak w przypadku gromadzenia danych osobowych, należy stosować zasadę minimalizacji danych, czyli gromadzić te dane na tyle, które są niezbędne do osiągnięcia określonych celów. Wiele monitorów nagrywających działa w oparciu o sieci komputerowe, co oznacza, że są one podatne na ataki cybernetyczne. Dlatego ważne jest, aby zabezpieczyć sieć przed atakami, stosując odpowiednie oprogramowanie i urządzenia, jak firewall, antywirusy itp. Stosowanie zasad bezpieczeństwa pozwoli na zapewnienie bezpieczeństwa monitoringu oraz ochrony prywatności i wolności jednostek.

NOWE TECHNOLOGIE A PRYWATNOŚĆ

Wraz z rozwojem nowych technologii i internetu, prywatność staje się coraz istotniejszą kwestią dla każdego z użytkowników. Co się z tym wiąże, pojawiają się także nowe zagrożenia i wyzwania związane z prywatnością w erze cyfrowej. Nowe technologie umożliwiają zbieranie oraz przetwarzanie i udostępnianie ogromnej ilości danych osobowych, co zwiększa ryzyko naruszenia prywatności użytkowników. W przypadku nowych technologii, takich jak sztuczna inteligencja, biometria czy internet rzeczy, pojawiają się dodatkowe wyzwania związane z prywatnością.

Ochrona prywatności staje się coraz ważniejsza w kontekście nowych technologii, a użytkownicy powinni mieć świadomość, jakie dane są zbierane i jak są przetwarzane.

Podsumowując, nowe technologie stwarzają wiele wyzwań związanych z prywatnością, ale jednocześnie umożliwiają rozwój innowacyjnych rozwiązań.

PODSUMOWANIE

W ostatnim czasie rosną obawy dotyczące nadzoru rządowego, szczególnie w kontekście bezpieczeństwa narodowego. Niektóre rządy zostały skrytykowane za wykorzystywanie technologii cyfrowych do monitorowania swoich obywateli bez odpowiedniego nadzoru lub przejrzystości.

Prywatność w świecie cyfrowym jest złożonym i rozwijającym się zagadnieniem. Ważne j est, aby być na bieżąco z najnowszymi osiągnięciami w zakresie prawa i technologii ochrony prywatności oraz podejmować kroki w celu ochrony własnej prywatności w internecie.

ODO

WDROŻENIA | AUDYTY | SZKOLENIA

„ODO SZKOLENIA“

BERKA JOSELEWICZA 15/11
42- 202 CZĘSTOCHOWA

600 299 249

BIURO@ODOSZKOLENIA.PL

SPECJALIZACJE

RODO

SZKOLENIA

AUDYTY

WDROŻENIA

Specjaliści RODO – zarówno w zakresie usług doradczych, jak i wdrożeniowych.

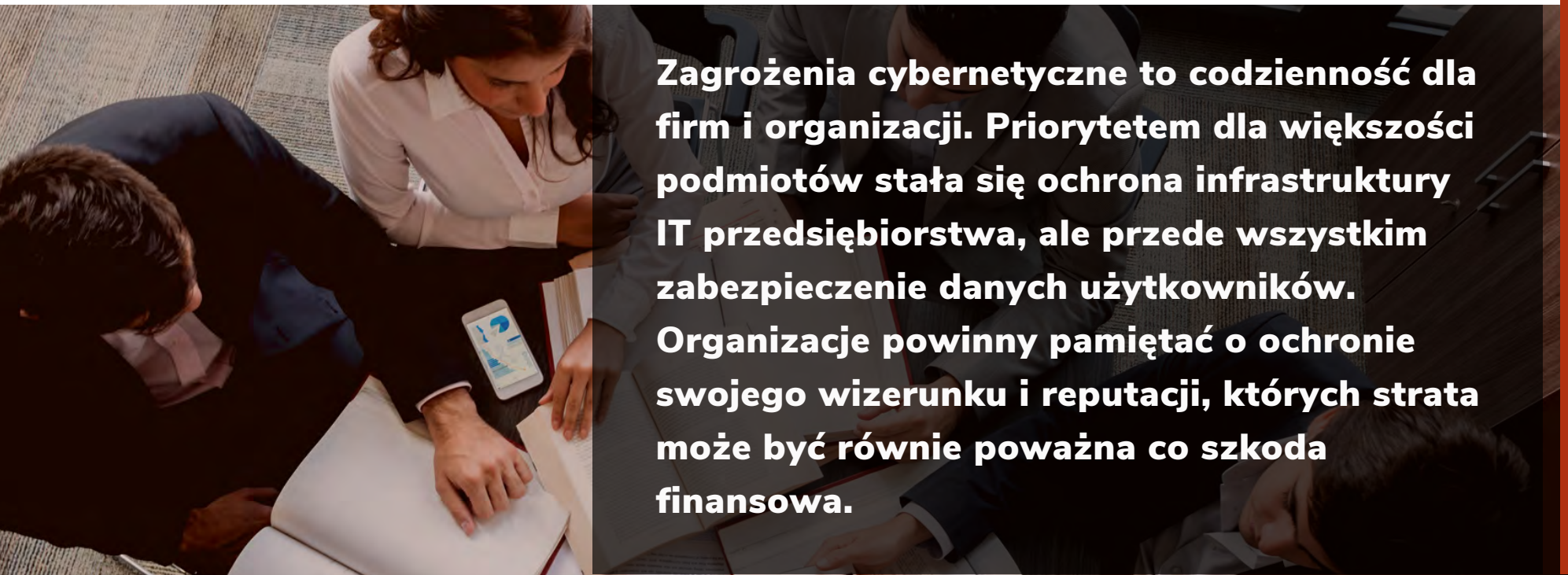
Z naszych dedykowanych usług, jak i szkoleń specjalistycznych korzystają przedstawiciele niemal każdej branży, jak również sektora publicznego. Wspieramy firmy i Instytucje w procesach rozwojowych, dlatego oferta naszych szkoleń jest rozbudowana oraz przystosowywana do wymagań i rozwoju biznesu naszych Klientów. ODO Szkolenia to specjaliści, eksperci, praktycy, świetni szkoleniowcy – oferujemy najwyższej jakości konsultacje, szkolenia, audyty.

Działamy na terenia całej Polski.

Uczestniczymy w grupach roboczych, należymy do branżowych Stowarzyszeń Inspektorów Ochrony Danych (SABI), szkolimy studentów. Nasi eksperci pełnią funkcje IOD.

WIZERUNEK FIRMY ZACZYNA SIĘ NA ETAPIE SKUTECZNEJ PREWENCJI

Tomasz Bill
thebill, Alfa Lingua



Zagrożenia cybernetyczne to codzienność dla firm i organizacji. Priorytetem dla większości podmiotów stała się ochrona infrastruktury IT przedsiębiorstwa, ale przede wszystkim zabezpieczenie danych użytkowników. Organizacje powinny pamiętać o ochronie swojego wizerunku i reputacji, których strata może być równie poważna co szkoda finansowa.

Wizerunek firmy zaczyna się na etapie skutecznej prewencji

W obliczu coraz częstszych i intensywniejszych ataków cybernetycznych ochrona firmowej infrastruktury IT i danych stała się priorytetem w codziennym funkcjonowaniu wielu przedsiębiorstw. Niemniej jednak, samo zabezpieczenie przed cyberzagrożeniami to tylko jedna strona medalu. Firmy powinny również pamiętać o ochronie swojego wizerunku i reputacji, których uszczerbek może być bardzo poważny i nieść ze sobą skutki finansowe.

JAK DBAĆ O WIZERUNEK FIRMY PW DOBIE CYBERZAGROŻEŃ?

Idealnego rozwiązania nie ma. Do znalezienia najlepszej metody dla własnej organizacji czy firmy są zintegrowane działania zapobiegawcze. Te z kolei wynikają z kultury organizacyjnej przedsiębiorstwa. Jeśli firma jest świadoma swojej pozycji i potencjalnych cyberzagrożeń powinna stawiać na edukację pracowników oraz klientów.

Przygotowanie scenariusza postępowania na wypadek kryzysu to konieczność dla firmy. Niestety nadal wiele organizacji, w kontekście świadomego budowania wizerunku, nie dba o etap stricte „przygotowawczy", bagatelizując zagrożenie aż do momentu jego wystąpienia.

Co taki scenariusz powinien uwzględniać? Poza aspe-

ktami technicznymi (np. w formie backupu danych) powinny być przygotowane również kwestie związane z komunikacją. W przypadku wycieku danych czy ataku hakerów, firma powinna szybko poinformować o tym klientów i partnerów biznesowych.

REGULARNE SZKOLENIA PRACOWNIKÓW ORGANIZACJI

Duża liczba ataków cybernetycznych zaczyna się od nieostrożnego zachowania pracownika, np. poprzez kliknięcie w podejrzany link lub udostępnienie swojego hasła. Dlatego ważnym jest, aby regularne zapewniać szkolenia pracowników w zakresie świadomości cyberbezpieczeństwa. Powinny one obejmować przede wszystkim edukację na temat metod ataku, sposobów rozpoznawania zagrożeń oraz procedur postępowania w przypadku podejrzenia incydentu.

MONITOROWANIE MEDIÓW SPOŁECZNOŚCIOWYCH

W erze internetu i mediów społecznościowych negatywna opinia o firmie może szybko się rozprzestrzenić, co z kolei może wyrządzić poważną szkodę. Dlatego potrzeba regularnego monitorowania wzmianek na temat organizacji w sieci i reagowania na ewentualne nieprawdziwe informacje czy komentarze. Warto mieć przygotowany plan działania w przypadku naruszenia prywatności lub ataku hakerskiego na profil firmy w mediach społecznościowych. Na rynku istnieje wiele narzędzi, które dysponują monitorowaniem wzmianek o firmach w social mediach.

TRANSPARENTNE DZIAŁANIA TO PODSTAWA

W obliczu zdarzeń cybernetycznych należy koniecznie działać transparentnie i na bieżąco udzielać szczegółowych informacji co do sytuacji. Pod żadnym pozorem nie można ukrywać faktu ataku, czy chociażby skali szkody. W praktyce może to tylko pogorszyć sytuację kryzysową. Ważne, aby klienci oraz partnerzy biznesowi wiedzieli, jaki jest status sytuacji.

DOPASOWANY STRATCOM NIEZALEŻNIE OD SYTUACJI GEOPOLITYCZNEJ

Czym jest stratcom? To proces zarządzania strategiczną komunikacją w wypadku kryzysu, w którego centrum znajdzie się nasza firma lub organizacja. Celem jest zminimalizowanie szkód dla firmy lub organizacji w sytuacjach kryzysowych, takich jak wypadki, skandale, lub właśnie ataki cybernetyczne.

Scenariusz postępowania na wypadek kryzysu, o którym mówiłem wcześniej, pozwoli zminimalizować takie szkody. Strategia komunikacyjna powinna być centralnie skoordynowana i dopasowana do potrzeb sytuacji kryzysowej. Informacje powinny być przekazywane w sposób klarowny, spójny, a komunikaty dostosowane do odbiorców.

PR-OWY DAMAGE CONTROL

To zbiór procedur, który tak naprawdę każdy podmiot powinien wdrożyć i na bieżąco aktualizować na wypadek zagrożenia wizerunku firmy. Najważniejsze to działać szybko, zdecydowanie, a przede wszystkim skutecznie.

W przypadku strategicznego zarządzania kryzysowego istotne są następujące elementy:

- **Szybka reakcja**. W przypadku kryzysowej sytuacji ważne jest, aby firma działała szybko i niezwłocznie odpowiedziała na krytykę.
- **Zebranie wszystkich niezbędnych informacji.** Jeszcze przed podjęciem jakichkolwiek działań firma powinna dokładnie zbadać sytuację i dowiedzieć się, co się stało.
- **Odpowiedź na zarzuty.** Organizacja powinna odpowiedzieć na zarzuty profesjonalnie i rzeczowo, bez oskarżeń i krytyki.
- **Propozycje rozwiązań.** Przedstawienie planu na rzecz poszukiwania rozwiązania może obejmować publiczne przeprosiny, obietnice naprawienia sytuacji lub wprowadzenie nowych procedur.
- **Transparentność.** Udzielając informacji i odpowiadając na pytania mediów oraz klientów, można uniknąć nieporozumień i dalszej krytyki.

ZAUFANIE DO EKSPERTÓW W BRANŻY

Na przykładzie firmy Nomios przedstawię, jak skutecznie dbać o wizerunek firmy w obliczu wszechobecnych zagrożeń w przestrzeni cybernetycznej. Firma Nomios jest wiodącym dostawcą usług w zakresie cyberbezpieczeństwa i sieci. Zespoły Nomios, obecne w siedmiu krajach w Europie, odpowiadają za projekty i zabezpieczenia infrastruktur cyfrowych.

Nomios kładzie nacisk na wartość edukacyjną. Misją firmy jest dzielenie się wiedzą z klientami oraz społecznością skupioną wokół świadomego korzystania z przestrzeni cyfrowej. Zamysł firmy jest prosty – dzielić się wartościowymi treściami edukacyjnymi, które w dobie wielu zagrożeń cybernetycznych mogą okazać się bezcenne w procesie rozwijania firmy czy organizacji. Stąd ogromna regularność w kwestii organizacji wydarzeń branżowych, mających na celu podnoszenie świadomości zagrożeń, ale i przedstawiania gotowych rozwiązań.

Dlatego eksperci sugerują, by regularnie przeprowadzać audyty cyfrowych zabezpieczeń swojej firmy czy organizacji.

Obecnie na rynku istnieje wiele firm, które się w tym specjalizują, a wartość takiej inwestycji może okazać się wprost bezcenna dla wizerunku.

Motto firmy "Secure and connected" z pewnością znajdziemy w celach statutowych najrozmaitszych organizacji, które też stawiają na rozwój w oparciu o świadomość zagrożeń i ryzyka związanego z obecnością i działaniami w sieci.

Bezpieczeństwo i łączność są w dzisiejszym świecie niezbędne dla wzmocnienia pozycji firm oraz organizacji i służą do jeszcze skuteczniejszego przekazywania zmieniających świat idei.

Wspierając rozwój Nomios, przekonałem się, że to właśnie ludzie są czynnikiem decydującym o sukcesie lub porażce w dziedzinie bezpieczeństwa i łączności, a mała pomyłka potrafi przerodzić się w wyzwanie wizerunkowe ogromnej skali. Podejście do technologii skoncentrowane na człowieku jest niezbędne, bo to od niego wszystko się zaczyna.

PODSUMOWANIE

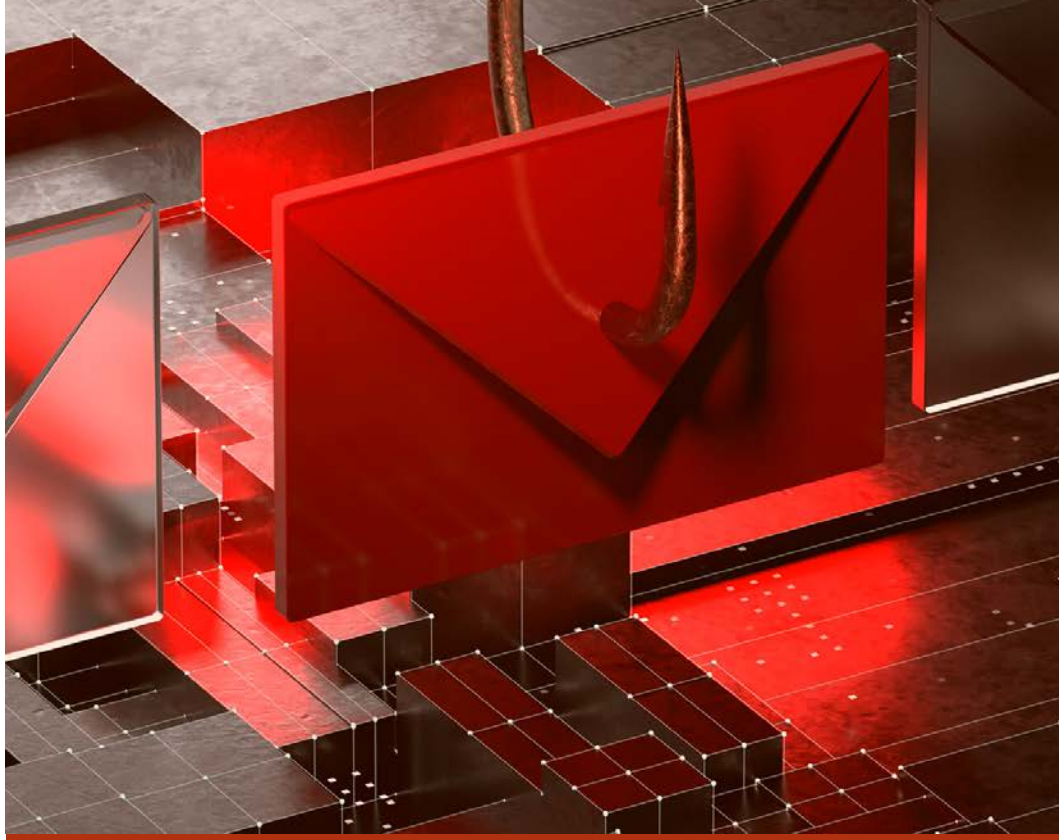
Co firma powinna zrobić, by zminimalizować ryzyko i dbać o swoją reputację w przypadku zagrożeń cybernetycznych:

- **Zabezpieczenie swojej infrastruktury.** Istotne jest, żeby firma zainwestowała w narzędzia i rozwiązania, które zabezpieczą infrastrukturę przed atakami cybernetycznymi. Należy regularnie aktualizować oprogramowanie, instalować antywirusy, firewalle i używać silnych haseł. Warto też rozważyć skorzystanie z usług zewnętrznych Security Operations Center, aby przy niższym nakładzie czasu i pieniędzy stale monitorować swoją sieć.
- **Szkolenia dla pracowników.** Pracownicy firmy powinni być odpowiednio przeszkoleni w zakresie bezpieczeństwa cybernetycznego, aby uniknąć potencjalnych zagrożeń. Należy edukować pracowników w zakresie identyfikowania ataków phishingowych, wykrywania złośliwego oprogramowania oraz innych zagrożeń.
- **Plan reagowania na zagrożenia.** Firma powinna posiadać plan reagowania na zagrożenia, który obejmuje procedury postępowania w przypadku ataku cybernetycznego. Plan ten powinien być regularnie aktualizowany i testowany, aby skutecznie i zdecydowanie reagować na wypadek zdarzenia.
- **Regularna kontrola bezpieczeństwa.** Zgodnie z zaleceniami Nomios, firma powinna regularnie przeprowadzać audyty i kontrole bezpieczeństwa, aby wykryć ewentualne luki w systemie i zabezpieczyć je przed potencjalnymi atakami.
- **Otwartość i transparentność.** W przypadku incydentu związanego z bezpieczeństwem cybernetycznym, firma powinna być otwarta i transparentna w swoich działaniach. Należy informować klientów, partnerów biznesowych i inwestorów o sytuacji i podejmowanych krokach.

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

48% MAILI TO SPAM. CO TO OZNACZA DLA BIZNESU?

Redakcja
SECURITY MAGAZINE



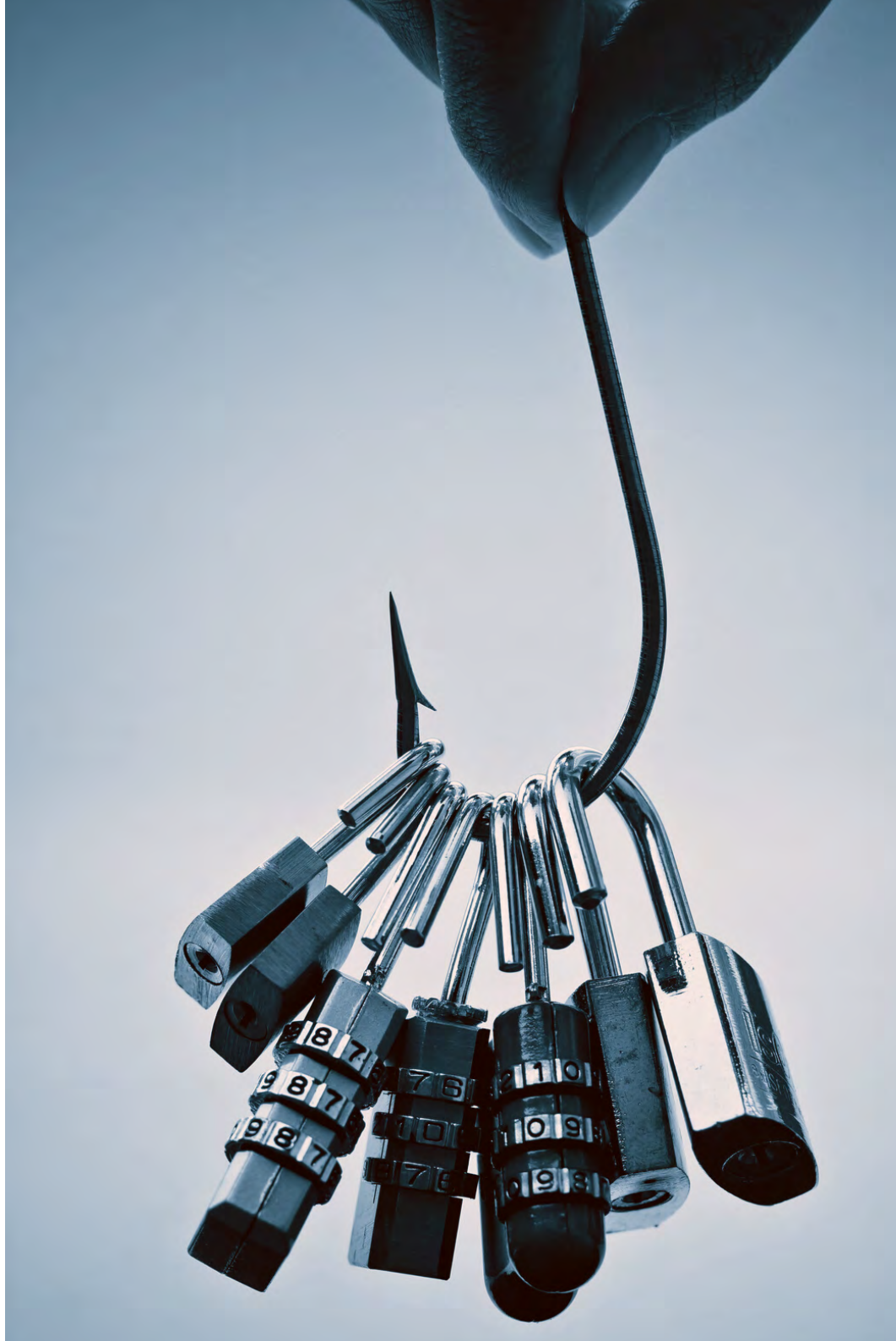
Aż 48% maili wysłanych w 2022 roku były spamem. W tym samym okresie 83% brytyjskich firm, które padły ofiarą cyberataku wskazały że był to phishing. Jak najpopularniejsza metoda cyberoszustwa rozprzestrzenia się w sieci i co to oznacza dla biznesu?

PHISHING KRÓLUJE, A NIE UMIERA

Nie ma drugiej tak popularnej metody cyberataku, co phishing. Dziennie wysyłanych jest 3,4 miliarda fałszywych wiadomości e-mail na całym świecie. Jak twierdzą badacze cyberbezpieczeństwa, aż 48% maili w samym tylko 2022 roku były spamem. W tym samym czasie 83% brytyjskich organizacji, które odnotowały cyberatak na swoją firmę, wskazało, że był to phishing. Również w 2021 roku do najpopularniejszych metod cyberoszustwa w Azji należała właśnie ta metoda.

Ponadto 92% przedsiębiorstw w Australii padło choć raz ofiarą phishingu. Jeszcze w 2021 roku było to „zaledwie" 39%. Czyli mamy tu wzrost na poziomie aż 53 punktów proc.

I pomimo ciągłego ulepszania filtrów antyspamowych, ciągle trudno jest wyeliminować to zjawisko. Dość powiedzieć, że Google blokuje dziennie aż 100 milionów fałszywych wiadomości e-mail. Jednak na 3,4 miliarda (oczywiście – nie wszystkie wysyłane są przez Gmail) to zaledwie kropla w morzu potrzeb. Szacuje się, że średni koszt naruszenia danych w organizacji wynosi 4 miliony dolarów. A jeden tzw. whaling attack może kosztować firmę nawet 47 milionów dolarów.



Najgorsze w tym wszystkim jest to, że phishing dotyczy każdego. Niezależnie od tego, czy jest się firmą, czy zwykłym użytkownikiem internetu – prędzej czy później zetkniemy się z phishingiem. I w dużej mierze to od nas zależy, czy nie damy się zwieźć. W samym tylko 2021 r. ponad 323 tys. internautów padło ofiarą phishingu (tzn. stracili dane lub pieniądze przez cyberprzestępców). A należy dodać, że aż 62% wszystkich cyberataków ma miejsce dzięki wykradzeniu danych pozyskanych w wyniku phishingu lub ataków typu brute-force.

Był a to połowa wszystkich ofiar cyberataków w tamtym okresie. Ponadto aż 92% organizacji zgłosiło, że przynajmniej jeden ich firmowy mail został naruszony. A 93% doświadczyło wycieku danych z powodu nieostrożności. Tak wielką „moc" ma phishing. A co zmienia się w tej kwestii na przestrzeni lat?

CYBERPRZESTĘPCY CHĘTNIE PODSZYWAJĄ SIĘ POD MARKI

Phishing jest metodą równie starą co internet. Pierwsze oszustwa tego typu szacuje się na lata 90 XX wieku. Czyli w okresie, kiedy sieć zaczęła się znacząco popularyzować na globalnej Północy. Jednak to po prostu scyfryzowanie oszustwa starego jak świat. Prawdopodobnie od początku istnienia naszego gatunku mieliśmy do czynienia z osobami, które podszywały się pod innych ludzi czy organizacje.

Phishing stał się tak popularny, bo zwyczajnie jest prosty. W zasadzie nie wymaga tak du-żych umiejętności, jak klasyczne hakowanie. Wykorzystuje się tu głównie socjotechniki, czasem również złośliwe oprogramowania typu ransomware. Nierzadko jednak cyberprzestępcy posiłkujący się tą metodą, nie są żadnymi hakerami, a zwyczajnie – oszustami.

Badacze cyberbezpieczeństwa sprawdzili, pod jakie marki cyberoszuści podszywają się najchętniej. I okazuje się, że w I kwartale 2022 roku najczęściej cyberprzestępcy starali się przekonać swoje ofiary, że te korespondują z LinkedInem (52%). Na 2. miejscu znalazło się DHL (14%), na 3. Google (7%), na 4. miejscu ex aequo Microsoft i FedEx (po 6%). Oczywiście – to w kwestii marek globalnych. W poszczególnych krajach sytuacja może wyglądać nieco inaczej. W Polsce np. cyberoszuści chętnie podszywają się pod marketplace'y takie jak OLX.

Co ważne – cyberprzestępcy chętnie podszywają się też pod marki osobiste. Najczęściej pod CEO (22% wszystkich fałszywych wiadomości wysyłanych do pracowników) danej firmy. Dzięki temu łatwo wzbudzają zaufanie pracowników.

LINKEDIN ULUBIONĄ PLATFORMĄ CYBEROSZUSTÓW

Platforma należąca do Microsoftu – LinkedIn – ma globalnie ponad 800 milionów użytkowników i działa w 200 krajach. Jest to też zresztą medium społecznościowe, na którym ludzie chętnie wymieniają się swoimi danymi czy informacjami ze względów biznesowych. I jak się okazuje – LinkedIn stał się ulubioną platformą dla cyberoszustów.

Nie tylko najczęściej się pod nią podszywają, ale też maile wysyłane rzekomo pod szyldem LinkedIna mają największą otwieralność – na poziomie aż 42%. Na 2. miejscu uplasował się Facebook z 20%, a na 3. Twitter z 9%. Dlaczego tak się dzieje? Jak wspomniałem – LinkedIn jest medium społecznościowym wykorzystywanym w biznesie i karierze. W niektórych firmach czy branżach to wręcz narzędzie pracy.

Użytkownicy tej platformy poszukują na niej pracy, zleceń, potencjalnych kandydatów itd. Innymi słowy – raj dla wszelkiej maści oszustów. Niedawno zresztą firma Mandiant wydała obszerny raport, w którym opisuje proceder phishingowy na LinkedInie.

Cyberprzestępcy podszywali się pod rekruterów, zdobywali zaufanie użytkowników, później przenosili komunikację na WhatsApp, gdzie wysyłali złośliwe oprogramowanie. Co ciekawe – na tym komunikato-

rze najczęściej wysyłane są phishingowe wiadomości tekstowe – aż 90%. Na 2. miejscu znalazł się Telegram z zaledwie 5,04%.

Oszuści uderzali głównie w firmy w Europie oraz Stanach Zjednoczonych. Głównie w branżę mediową i cyberbezpieczeństwa. Może nawet któryś z Twoich obecnych pracowników zetknął się z „ofertą od konkurencji”? Albo nawet padł ofiarą takiego oszustwa. Choć LinkedIn stara się z tym walczyć i ukrócić proceder, to nie ma lekko.

¼ PHISHINGOWYCH MAILI POCHODZI Z ROSJI

Za wspomnianą wcześniej kampanią phishingową na LinkedInie stoi najprawdopodobniej północnokoreańska grupa hakerów znana jako UNC2970, którą utożsamia się też z UNC577 znaną jako Temp.Hermit. I faktycznie północni Koreańczycy specjalizują się w atakach hakerskich i phishingowych na organizacje z globalnej Północy. Jednak jak pokazują dane – za największą liczbą maili phishingowych stoją... Rosjanie.

Aż ¼ (24,77%) tego typu wiadomości ma być wysyłana właśnie przez nich. Oczywiście – niekoniecznie tak musi być. W jednym z artykułów w "Security Magazine" opisywaliśmy, jak chińscy hakerzy często, aby zmylić tropy, zapisują kod w cyrylicy. I tu podobnie – niektóre grupy z innych krajów mogą podszywać się pod Rosjan. Zwłaszcza te organizacje oraz cyberprzestępcy z byłego ZSRR.

Na 2. miejscu pod względem liczby wysyłanych maili phishingowych co ciekawe stoją Niemcy (14,12%), a na 3. Stany Zjednoczone (10,46%). Chiny znalazły się dopiero na 4. miejscu (8,73%), a na 5. Niderlandy (Holandia, 4,75%).

ATAKI PHISHINGOWE, KTÓRE PRZYNIOSŁY NAJWIĘKSZE STRATY

Może wydawać się, że najprostszymi celami dla cyberoszustów są zwykli użytkownicy internetu czy firmy z sektora MMŚP. Przeważnie takie osoby nie mają szczególnej wiedzy o cyberbezpieczeństwie, a wspomniane organizacje nie posiadają w zespołach stałych ekspertów czy departamentów. Jednak ofiarami cyberoszustów równie często padają duże spółki. Przykładowo sieć hoteli Marriott straciła dane nawet 5,2 miliona swoich gości zaledwie w ciągu 3 lat. A to

wszystko z powodu cyberataków. Z kolei Google i Facebook w latach 2013–2015 straciły nawet 100 milionów dolarów z powodu kampanii phishingowych.

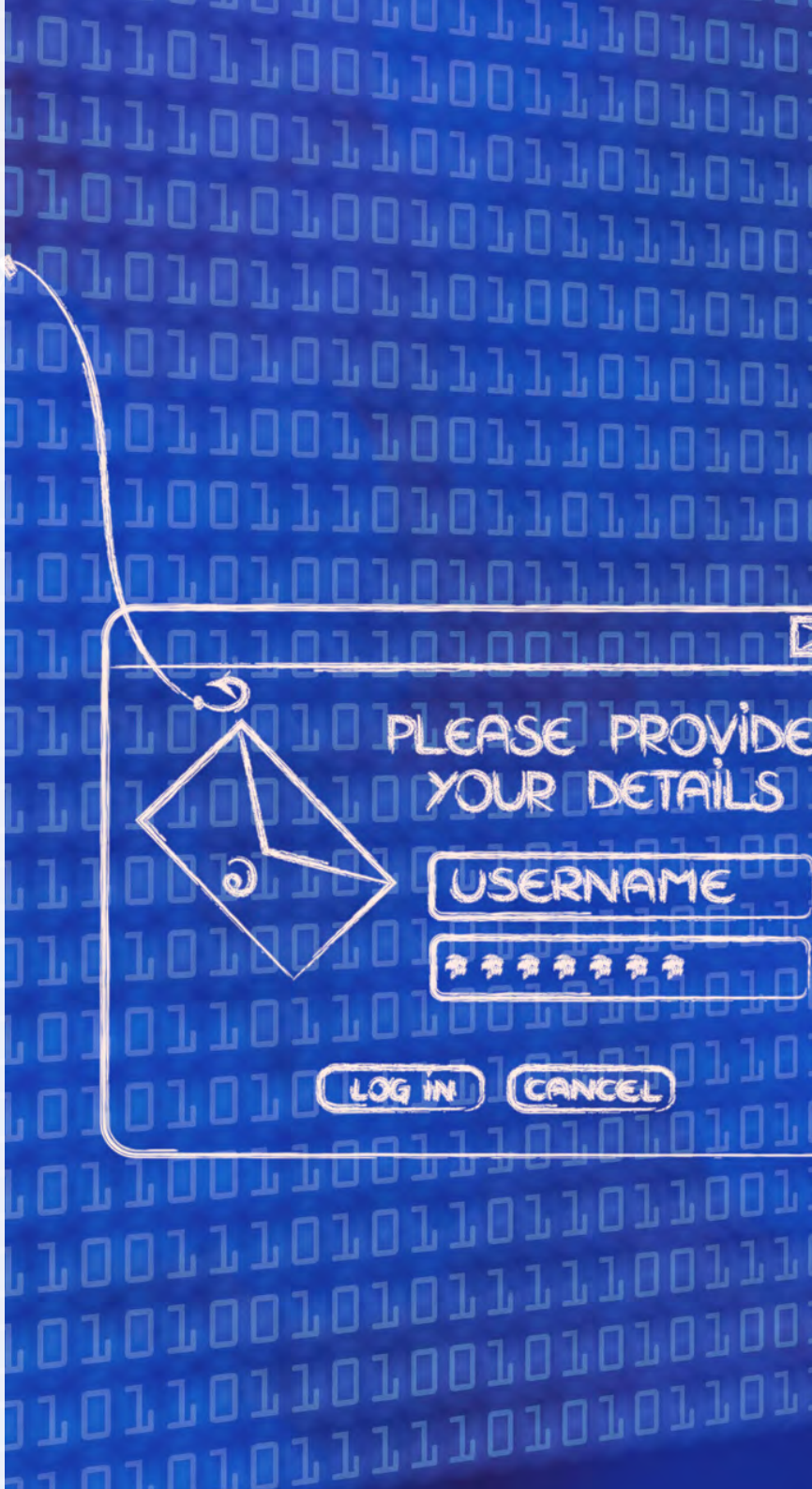
Od (udanych) ataków phishingowych nie są wolne nawet banki. Crelan Bank w Belgii z powodu oszustwa stracił 75,8 miliona dolarów. Cyberprzestępca podszył się wówczas pod jednego z dyrektorów.

PONAD 76% CYBERATAKÓW W POLSCE TO PHISHING

Co się zaś tyczy naszego kraju to według danych NASK w 2021 roku 76,57% wszystkich zgłoszonych incydentów związanych z cyberprzestępczością stanowił phishing. Oznacza to wzrost o prawie 200% w kontekście tego typu zdarzeń w stosunku do 2020 roku. Najbardziej narażoną branżą w Polsce na tego typu próby oszustwa są usługi, handel i przemysł.

Choć Polska nie znajduje się na czele krajów, w których dochodzi do ataków phishingowych (w przeciwieństwie np. do Stanów Zjednoczonych czy Niderlandów), to liczba tych incydentów stale rośnie. I to o zatrważające liczby.

W samym tylko 2020 roku liczba incydentów związanych z cyberprzestępczością wyniosła ponad 29 tys. A mówimy tu o wykrytych przypadkach. Dlatego CERT i rząd ostrzegają przed natężeniem występowania takich ataków zwykłych użytkowników, jak i firmy. Tym bardziej że cyberprzestępcy stają się coraz bardziej wyrafinowani.



Przykładowo, według badań 61% internautów, nie było w stanie odróżnić prawdziwej strony Amazona od tej podrobionej.

A to coraz częstsza metoda phishingowa. Tzn. tworzenie fałszywych landing page'y, które do złudzenia przypominają rzeczywiste witryny.
W ten sposób oszuści podszywają się np. pod marketplace'y, bramki płatności, banki i innych usługodawców. I często dbają o nawet drobne szczegóły – takie jak chociażby certyfikaty SSL (aż 50% stron wyłudzających dane je posiada).

PHISHING TO JUŻ PROCEDER ZORGANIZOWANY

Na początku artykułu wspominałem, że do phishingu nie trzeba mieć szczególnych umiejętności hakerskich. Nie trzeba nawet mieć kompetencji programistycznych. Często wystarczają socjotechniki. Jednak phishing ze względu na swoją popularność jest wspierany przez różne grupy cyberprzestępcze. Jak wskazuje Microsoft – w sieci znajdziemy wiele grup czy nawet zestawy narzędzi, które pomniejsi przestępcy wykorzystują do phishingu. Mowa tutaj m.in. o zestawie DEV-1101. Ów zestaw można „wypożyczyć" czy „wykupić" od twórcy i używać do kampanii phishingowych.

To zupełnie tak jakby skorzystać z gotowych narzędzi od firm zajmujących się e-mail marketingiem, aby dokonać wysyłki wiadomości. Działa to na podobnej zasadzie – w tym przypadku jednak mamy gotowy produkt, który stworzy dla nas fałszywy landing page. Skorzystać z narzędzia możemy, uiszczając od 300 do 1000 dolarów miesięcznie.

Co ciekawe – eksperci z Microsoftu, tj. zespół Microsoft Threat Intelligence śledzi cyberprzestępcę, który odpowiada za opracowanie DEV-1101. Big-techy podobnie jak organy ścigania starają się wyeliminować takie zagrożenia, ponieważ tracą przez nie pieniądze a nierzadko - reputację.

Przed phishingiem nie ma ucieczki. I prawdopodobnie długo nie będzie. Przez kolejne lata pozostanie on najpopularniejszą metodą cyberataków na świecie. I zwyczajnie – trzeba będzie być coraz uważniejszym.

Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

ROLA METADANYCH W PRZE-CHOWYWANIU PLIKÓW

Paweł Kaczmarzyk
Serwis komputerowy Kaleron

W początkach cyfrowych nośników danych informacje były zapisywane wprost w adresacji fizycznej. Rodziło to szereg niedogodności, gdyż trzeba było wiedzieć, gdzie te informacje się znajdują, by można było je odnaleźć przy odczycie, a także uważać, by ich przypadkiem nie zastąpić inną zawartością. Było to o tyle istotne, że do jednego nośnika mogło mieć dostęp wiele osób i błąd w komunikacji między tymi osobami mógł skutkować zniszczeniem danych.

PARTYCJE

Rozwiązaniem problemu było zorganizowanie danych w przyjaznej dla użytkownika strukturze logicznej. Pierwszym krokiem w zarządzaniu strukturą logiczną dysków (lub ich zespołów widzianych jako jedna całość – macierzy RAID) jest ich podział na logicznie wydzielone części – partycje. Podział dysku na partycje opisuje tablica partycji znajdująca się w pierwszym sektorze dysku - głównym sektorze rozruchowym (MBR – Master Boot Record). Tablica ta pozwala na utworzenie maksymalnie czterech partycji.

Cztery partycje nie zawsze wystarczają. Dlatego pojawił się podział na partycje podstawowe (opisywane w MBRze wprost) i partycje rozszerzone, na których mogą być tworzone woluminy logiczne. Po założeniu od 1 do 3 partycji podstawowych można utworzyć partycję rozszerzoną, którą można później dzielić na praktycznie nieograniczoną liczbę woluminów logicznych.

Partycja rozszerzona zaczyna się od struktury logicznej zwanej Secondary MBR, zawierającej kolejną tablicę partycji. W tej tablicy umieszczamy rekord opisujący wolumin logiczny oraz kolejną partycję rozszerzoną obejmującą obszar do końca dysku, która znów zaczyna się od Secondary MBRu. I tak aż do wyczerpania miejsca na dysku.

Innym rozwiązaniem problemu jest użycie tablicy GPT (GUID Partition Table, przy czym GUID oznacza Globally Unique Identifier – identyfikator unikatowy globalnie). Wbrew szeroko rozpowszechnionemu przekonaniu, GPT nie zastępuje MBRu, a stanowi jego rozszerzenie. MBR wciąż znajduje się w pierwszym sektorze dysku, wciąż zawiera tablicę partycji, jednak w tej tablicy opisuje tylko jedną partycję z kodem typu 0xEE, obejmującą całą dostępną przestrzeń adresową. Jest to zabezpieczenie na wypadek podłączenia dysku pod systemem nieobsługującym GPT. Dzięki temu wpisowi taki system będzie wiedział, że dysk nie jest pusty i że coś się na nim znajduje.

W kolejnym sektorze znajduje się nagłówek tablicy GPT, a dalej – 32 sektory tablicy pozwalającej na opisanie 128 partycji. Liczba dostępnych partycji może być zwiększona w przyszłości przez zwiększenie rozmiaru tablicy.

Kopia tablicy GPT znajduje się na końcu dysku, co ułatwia odzyskiwanie danych w przypadku uszkodzenia początkowych sektorów dysku.

Tablica GPT rozwiązuje jeszcze jeden problem. Dzięki 64- bitowemu adresowaniu pozwala na obsługę partycji na dyskach większych od 2 TB. Wystarczy pomnożyć maksymalną liczbę 32-bitową 0xFFFFFFFF przez rozmiar sektora 0x200 [B], by przekonać się, dlaczego posługująca się 32-bitowymi adresami tablica partycji z MBRu może adresować maksymalnie 2 TB – 1 sektor.

SYSTEMY PLIKÓW

Dane stanowiące spójną, zorganizowaną całość tworzą plik, który może być traktowany, jako obiekt jednostkowy zarówno przez użytkownika, jak i przez system operacyjny. Jednak dysk nie rozumie tego, czym jest plik. Wciąż jedynie może odczytać lub zapisać dowolne sektory zgodnie z otrzymanym żądaniem, a więc musi istnieć coś, co wskaże dyskowi właściwe sektory, gdy wybieramy określony plik.

Tym czymś są systemy plików. Pozwalają one użytkownikowi zapomnieć o adresacji sektorowej przechowując informację o położeniu plików. Struktury systemu plików zwane metadanymi opisują także nazwy plików, ich położenie w strukturze logicznej katalogów (zwanych też folderami), uprawnienia dostępu, różne parametry czasu (np. utworzenia, modyfikacji pliku) oraz inne atrybuty.

Systemy plików zwykle nie posługują się adresacją sektorową, ale większymi wewnętrznymi jednostkami, zwanymi, w zależności od nomenklatury przyjętej w danym systemie, klastrami lub blokami. W systemach plików środowiska uniksowo – linuksowego występują też grupy łączące wiele bloków oraz fragmenty, mogące być

częścią bloków. W praktyce fragmentów od dawna nie używa się do adresowania danych i w parametrach ich rozmiar określa się jako równy rozmiarowi bloku.

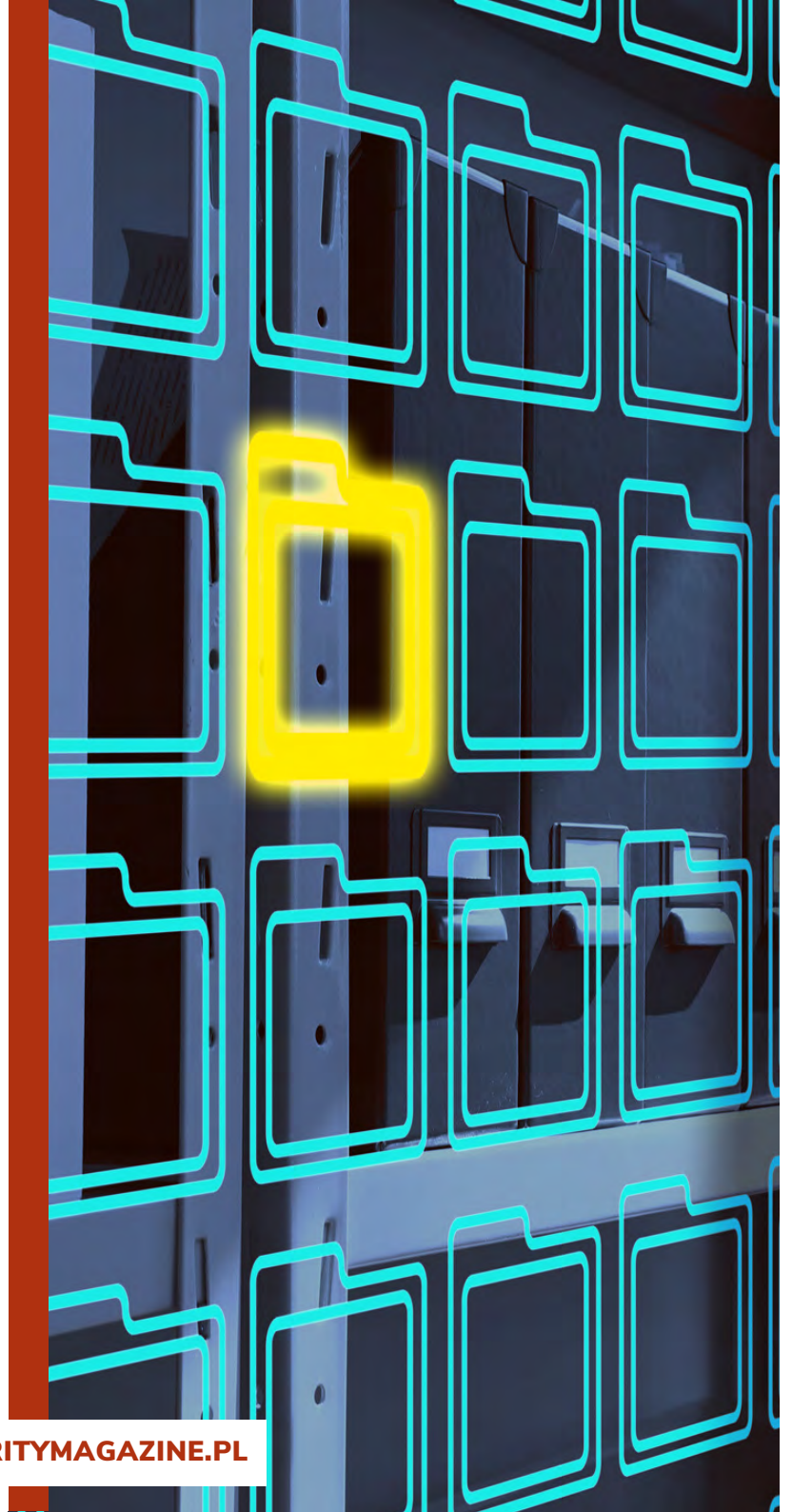
Oczywiście różne systemy plików różnią się między sobą i niekoniecznie muszą obsługiwać te same atrybuty plików. Np. stosunkowo proste systemy plików z rodziny FAT nie pozwalają na identyfikację właściciela pliku oraz nadawania plikom praw dostępu, a pierwsza wersja FAT12 nie pozwalała na tworzenie struktury katalogów. Był tylko jeden katalog główny, w którym umieszczano wszystkie pliki.

W większości systemów plików jednak występuje możliwość tworzenia struktury katalogów, a za przyporządkowanie pliku do danego katalogu odpowiada umieszczenie opisu tego pliku w konkretnym katalogu (w większości systemów plików) lub umieszczenie informacji odwołującej się do danego katalogu w opisie pliku. Drugi z tych wariantów jest wykorzystywany w systemie plików NTFS, gdzie o przynależności pliku do konkretnego katalogu decyduje informacja w rekordzie MFT opisującym ten plik.

Przenoszenie pliku z katalogu jest operacją na metadanych. Plik zostaje fizycznie w tym samym miejscu, w którym był. Przenoszony lub zmieniany jest jedynie jego opis. Do tego samego pliku metadane systemu plików mogą się odwoływać wielokrotnie wskazując wprost położenie na partycji (dowiązanie twarde) lub wskazując nazwę i ścieżkę dostępu (dowiązanie symboliczne).

Innym istotnym zadaniem systemów plików jest określanie zajętego (zaalokowanego w strukturach logicznych) i wolnego miejsca na partycji. System plików wiedząc o tym, że dany obszar partycji jest zajęty przez plik, nie pozwoli na jego nadpisanie kolejnymi informacjami.

W przypadku dużych partycji dobrze jest mieć możliwość szybkiego ustalenia, gdzie jest wolne miejsce, w którym można umieścić nowy plik bez konieczności analizy wszystkich metadanych. Pomocne w tym są wykorzystywane przez wiele systemów plików bitmapy – struktury opisujące klastry partycji w ten sposób, że każdemu z nich odpowiada jeden bit. Zwykle bity opisujące zajęte klastry przyjmują wartość 1, a wolne – 0. Bitmapy są też niezwykle przydatne przy wykonywaniu kopii posektorowych, gdyż pozwalają ograniczyć



czas i ryzyko ich wykonywania dzięki możliwości ominięcia wolnych obszarów.

PLIKI

Plik jest czymś odrębnym od jego opisu, który może się zmieniać niezależnie od zawartości. Tak się dzieje, kiedy, na przykład, zmieniamy nazwę pliku. Zmiana nazwy zdjęcia kotka z „kot.jpg” na „pies.jpg” nie spowoduje żadnych zmian w treści zdjęcia. Tak samo zmiana rozszerzenia (ostatniego członu nazwy pliku po kropce) używanego do określenia typu pliku nie spowoduje, że typ pliku się zmieni.

Zmiana nazwy na „kot.pdf” nie przekonwertuje zdjęcia do pdfu, próba otwarcia tego pliku w programie Acrobat Reader lub innym programie do odczytu pdfów zakończy się komunikatem o nieprawidłowym formacie pliku. Ale jeśli wymusimy otwarcie tego pliku przez dowolną przeglądarkę grafiki, zdjęcie otworzy się nam poprawnie, pomimo zmienionego rozszerzenia.

Niekiedy pliki mogą w swej wewnętrznej strukturze skrywać niespodzianki. Zmień rozszerzenie pliku .docx, .xlsx lub .pptx na .zip i spróbuj rozpakować. Co jest w środku? Dlaczego takie coś jest możliwe? I dlaczego tym razem program nie zwrócił komunikatu o nieprawidłowym formacie pliku?

Pliki też mają swoją wewnętrzną strukturę.

Większość typów plików zaczyna się od określonej sygnatury i właśnie po tej sygnaturze programy mogą sprawdzić, czy mają do czynienia z obsługiwanym przez nie typem pliku. Sygnatury są też wykorzystywane do wyszukiwania plików przez programy odzyskujące dane. W przypadkach rozległych uszkodzeń metadanych systemu plików to może być jedyna droga, by odzyskać cokolwiek.

Pliki odzyskiwane na podstawie sygnatur mają nazwy generowane przez program. Zwykle jest to numer sektora, w którym znajduje się sygnatura i skorelowane z nią rozszerzenie. Rozmiar odzyskiwanych plików może się istotnie różnić od pierwotnego rozmiaru odzyskiwanych plików. Niektóre typy plików, np. ,pdf, mają sygnatury końca pliku, ale większość plików ich nie ma.

Dlatego program często nie potrafi znaleźć końca pliku i umieszcza w nim wszystkie sektory aż do napotkania kolejnej sygnatury lub do końca nośnika.

Pliki odzyskiwane po sygnaturach często są uszkodzone.

Dzieje się tak zwłaszcza w przypadku, gdy pliki były pofragmentowane. Uszkodzenie lub utrata metadanych nie pozwala na odnalezienie i ułożenie we właściwej kolejności wszystkich klastrów zawierających ten plik. Dlatego program w takiej sytuacji odnajduje jedynie pierwszy fragment pliku, niekiedy zanieczyszczony fragmentami innych plików.

Innym powodem pojawienia się w wynikach uszkodzonych plików są pozostałości starych plików, które zostały usunięte w strukturach logicznych, ale pozostały fizycznie na dysku. Często takie pliki ulegają uszkodzeniu przez częściowe nadpisanie, gdyż miejsce, które zajmują z punktu widzenia struktur logicznych jest miejscem wolnym. Możliwe jest też pojawienie się fałszywych wyników, kiedy w odpowiednim miejscu znajduje się wartość przypadkowo zbieżna z określoną sygnaturą.

Niektóre typy plików nie mają żadnych sygnatur ani elementów tworzących wewnętrzną strukturę.

Przeważnie dotyczy to plików tekstowych, takich, jak pliki .txt, czy skrypty Pythona. W przypadku takich plików o tym, że są one plikami tego, a nie innego rodzaju w 100 % odpowiada opis w metadanych odnoszący się do wskazanego w tym opisie miejsca na partycji.

Odzyskiwanie takich plików po sygnaturach nie jest możliwe, ale można próbować ich szukać wpisując w wyszukiwarkę hex-edytora ciągi znaków, jakich się w tych plikach spodziewamy. Przeważnie są to pliki łatwo czytelne w ASCII i na tyle małe, że po odnalezieniu zadanego ciągu znaków możemy manualnie zidentyfikować i wykopiować potrzebne sektory.

Rzetelny® Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ

SECURITYMAGAZINE.PL

WIRTUALNY AGENT, ROZPOZNAWANIE GŁOSU I OCHRONA PRZED OSZUSTWAMI REKLAMOWYMI

Redakcja
SECURITY MAGAZINE

W internecie istnieje mnóstwo zagrożeń – w tym także dla firm. Dlatego coraz lepiej rozwijają się startupy z branży cyberbezpieczeństwa. Dowiedz się, jak te innowacyjne spółki mogą pomóc Twojemu przedsiębiorstwu.

ROZPOZNAWANIE GŁOSU

Istnieje wiele form uwierzytelniania, które pozwalają np. logować się do ważnych dla przedsiębiorstwa kont. Jednym z takich sposobów jest wykorzystanie danych biometrycznych. Są to np. odciski palców czy skany twarzy, ale też, chociażby rozpoznawanie głosu. Na polskim rynku funkcjonuje startup **Voice PIN**, który umożliwia uwierzytelnianie głosowe dla dowolnej aplikacji.

Spółka chwali się, że dzięki ich technologii czas weryfikacji użytkownika jest znacznie krótszy. Startup pomaga np. w zwalczaniu nadużyć i oszustw finansowych, poprzez weryfikację głosową klienta dzwoniącego na infolinię czy prowadzącego wideorozmowę. Dzięki zastosowaniu sztucznej inteligencji VoicePIN od razu odkrywa, czy osoba jest tą, za którą się podaje.

Technologia opiera się na analizie charakterystycznych wzorców zawartych w każdym ludzkim głosie, których w teorii nie da się odtworzyć czy naśladować. W praktyce zastosowanie sztucznej inteligencji, która porozumiewa się głosem innej osoby, pewnie może pomóc. Jednak, aby było to skuteczne – taki voicebot musiałby bazować na dużej ilości próbek. Choć startup twierdzi, że ich rozwiązanie potrafi wykryć, czy próbka jest oryginalna, czy też może jest to nagranie.

Co w przypadku przeziębienia czy innej infekcji, która wpływa na brzmienie naszego głosu? VoicePIN wskazuje, że ich AI też sobie z tym radzi. Szuka ono bowiem pewnych matematycznych wzorców, a nie brzmienia samego głosu.

Co ciekawe, spółka dostarcza też rozwiązania z zakresu analityki predykcyjnej głosu, czyli przewiduje zachowania klientów i tworzy profile użytkowników na podstawie ich brzmienia. Dodatkowo VoicePIN oferuje też voicebota, który porozumiewa się z klientami dzwoniącymi na infolinię.

Z usług startupu miały skorzystać m.in. ING Bank Śląski, Ministerstwo Finansów, Orange, Alior Bank, Tauron czy PZU.

OCHRONA PRZED OSZUSTWAMI REKLAMOWYMI

Szacuje się, że ok. 40–60% ruchu w internecie to boty. Niektóre z nich są złośliwe i przykładowo fałszują ruch na stronach czy liczbę wyświetleń reklam displayowych, przez co zaburzają wyniki kampanii adsowych. Konsekwencja? Tracisz pie-

niądze. Niezależnie od tego, czy jesteś wydawcą, czy zleciłeś kampanię reklamową.

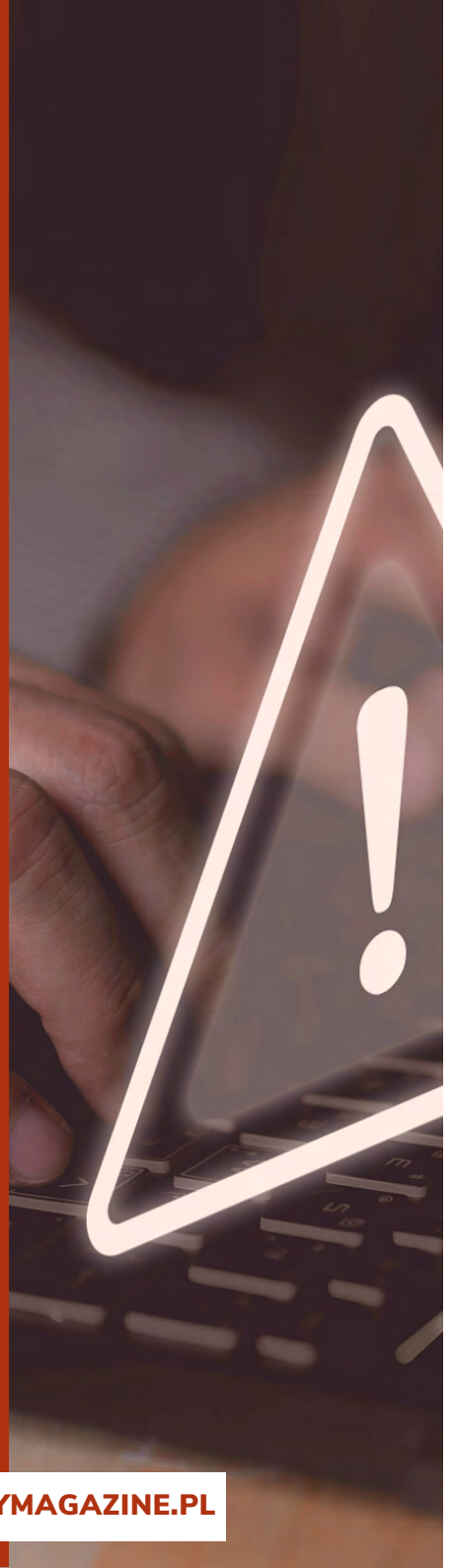
Istnieją jednak startupy, które dostarczają rozwiązania pozwalające niejako walczyć z tym problemem. Jednym z nich jest Travatar, który służy do analizy wykrywania nieprawidłowych kliknięć oraz botów w kontekście kampanii marketingowych. Spółka twierdzi, że dzięki skutecznej analizie jesteś w stanie zaoszczędzić pieniądze.

Dlaczego? Bo będziesz mógł wybierać miejsca, w których faktycznie przede wszystkim jest ruch ludzki. Dodatkowo Travatar pozwala na blokowanie możliwości klikania reklam przez konkurencję.

Technologia, którą stosuje startup działa na podstawie biometrii behawioralnej, czyli wykrywającej ludzkie zachowania. Ponadto używany jest system czerwonych flag, który oznacza podejrzane akcje. Nad wszystkim czuwa sztuczna sieć neuronowa zdolna do przetwarzania języka naturalnego. Jest to szczególnie przydatne w trakcie prowadzenia kampanii marketingowych, aby nie przepalać budżetów.

WIRTUALNY AGENT CYBERBEZPIECZEŃSTWA

Firmy z sektora MMŚP nierzadko nie mają funduszy na



dedykowany zespół ds. cyberbezpieczeństwa albo nawet korzystanie z usług firm, które zajmują się tym na co dzień. Jednak każde przedsiębiorstwo wymaga ochrony. Zważywszy na to, jak rośnie cyberprzestępczość na całym świecie i jak globalnym jest wyzwaniem.

W przeciwieństwie do tradycyjnej przestępczości – sprawca incydentu może znajdować się na drugiej stronie półkuli ziemskiej, a przez to wykrycie go czy doprowadzenie przed oblicze sprawiedliwości może być dla lokalnych służb niemożliwe. Z pomocą dla organizacji, które nie mają dużych budżetów na cyberbezpieczeństwo. przychodzi 1strike.

Jest to platforma SaaS, która korzysta z nowych sposobów na zabezpieczenie swojego systemu przed atakami hakerów. Wykorzystują one sztuczną inteligencję, chmurę oraz specjalną metodę o nazwie „Breach & Attack", aby przewidywać i zapobiegać cyberprzestępstwom. Za pomocą tego rozwiązania, firma może zasymulować zachowanie hakerów i wykrywać potencjalne naruszenia.

Dzięki rozwiązaniu startupu łatwo dowiesz się, jakie są słabe strony Twojej firmy w kontekście infrastruktury cyberbezpieczeństwa. Jesteś też w stanie zmniejszyć ryzyko i wykryć oraz wyeliminować luki w systemach IT. Dodatkowo monitorować ekspozycję zewnętrzną.

Co więcej – platforma pozwala też na testowanie bramek poczty e-mail. Dzięki temu możesz chronić swoją organizację przed phishingiem i wiadomościami zawierającymi złośliwe oprogramowanie.

To, oczywiście, nie wszystkie startupy, które dostarczają rozwiązań z zakresu cyberbezpieczeństwa. Takich spółek na rynku jest znacznie więcej. Pamiętaj jednak, że nawet najlepsze zabezpieczenia nie zdadzą się na nic, jeśli Twój zespół lub Ty sam nie jesteście odpowiednio wyedukowani w zakresie cyberbezpieczeństwa. Dlatego w pierwszej kolejności powinieneś poszerzać swoją wiedzę w tym aspekcie.

35 TYSIĘCY

TYLE POBRAŃ KWIETNIOWEGO WYDANIA

"SECURITY MAGAZINE"

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

NAPISZ DO NAS

REDAKCJA@SECURITYMAGAZINE.PL

SZTUCZNA INTELIGENCJA A OCHRONA INFORMACJI

Mateusz Jakubik
iSecure Sp. z o.o.

W dzisiejszym świecie, gdzie sztuczna inteligencja (AI) zdobywa coraz większe uznanie jako kluczowy element przemysłu, biznesu i życia codziennego, konieczne jest zrozumienie jej wpływu na ochronę informacji. Chociaż AI przyczynia się do wielu korzyści, takich jak automatyzacja procesów, lepsza analiza danych czy wyższa efetywność, nie można ignorować istotnych wyzwań związanych z ochroną danych i prywatności.

W artykule przedstawimy najważniejsze kwestie dotyczące ochrony informacji w kontekście stosowania sztucznej inteligencji, zwracając uwagę na potencjalne zagrożenia, jak i możliwości zastosowania AI w celu wzmocnienia bezpieczeństwa danych. Omówimy również, jak odpowiednie praktyki oraz regulacje mogą pomóc w zarządzaniu ryzykiem oraz w ochronie prywatności i bezpieczeństwa informacji w środowisku zdominowanym przez technologie AI.

INFORMACJA W XXI WIEKU

Informacja to zorganizowane, użyteczne dane, które przedstawiają wiedzę i mają wartość dla jednostek, organizacji czy społeczeństwa. Informacje mogą występować w różnych formach, takich jak tekst, obrazy, dźwięki czy multimedia i są przetwarzane, przechowywane oraz wymieniane za pomocą różnych technologii i systemów komunikacji.

Informacje pełnią kluczowe funkcje w procesach podejmowania decyzji, planowania, komunikacji oraz zarządzania w każdej organizacji, niezależnie od jej wielkości czy rodzaju działalności.

- **Podstawa podejmowania decyzji:** Informacje dostarczają niezbędnych danych i wiedzy, które pozwalają menedżerom i pracownikom podejmować świadome, oparte na faktach decyzje. Bez odpowiednich informacji organizacje mogą nie być w stanie podejmować skutecznych decyzji ani osiągać celów biznesowych.
- **Komunikacja:** Informacje są niezbędne do skutecznej komunikacji wewnątrz organizacji i z klientami, partnerami czy dostawcami. Wymiana informacji umożliwia koordynację działań, zrozumienie potrzeb i oczekiwań interesariuszy oraz dostosowywanie się do zmieniających się warunków rynkowych.
- **Tworzenie wiedzy:** Informacje stanowią podstawę dla tworzenia wiedzy, która z kolei przekłada się na konkurencyjność organizacji. Przetwarzanie, analiza i interpretacja informacji pozwala na identyfikację trendów, odkrywanie wzorców czy generowanie innowacji.
- **Optymalizacja procesów:** Dostęp do odpowiednich informacji pozwala organizacjom analizować i oceniać efektywność swoich procesów, co może prowadzić do ich usprawnienia, zwiększenia wydajności i oszczędności kosztów.
- **Zarządzanie ryzykiem:** Informacje są kluczowe dla identyfikacji, monitorowania i zarządzania ryzykiem, które może wpływać na działalność organizacji.

Dzięki odpowiedniej analizie informacji, organizacje mogą lepiej zrozumieć i kontrolować różne zagrożenia oraz podejmować odpowiednie działania prewencyjne i zaradcze.

KATEGORYZACJA INFORMACJI

Kategoryzacja informacji, znana również jako klasyfikacja informacji, to proces organizowania i przypisywania kategorii lub etykiet do informacji w celu lepszego zarządzania nimi, ochrony i kontrolowania dostępu. Kategoryzacja informacji pomaga organizacjom zrozumieć, jakie dane są najcenniejsze, najbardziej wrażliwe, co pozwala na podjęcie odpowiednich działań w celu ich ochrony.

Proces kategoryzacji informacji jest ważny z perspektywy doboru środków bezpieczeństwa z kilku powodów:

- **Ochrona wrażliwych danych:** Kategoryzacja informacji pozwala na identyfikację i oznaczenie danych wrażliwych, (dane osobowe, informacje finansowe, tajemnice handlowe). Wiedza, które informacje są najbardziej wrażliwe, pozwala firmom skupić się na zabezpieczaniu ich przed nieautoryzowanym dostępem, modyfikacją czy utratą.
- **Zgodność z przepisami:** Wiele organizacji musi przestrzegać przepisów dotyczących ochrony danych, takich jak ogólne rozporządzenie o ochronie danych (RODO) w UE. Kategoryzacja informacji pomaga w spełnieniu wymogów prawnych poprzez odpowiednie zabezpieczenie i zarządzanie danymi, które podlegają szczególnym regulacjom.

- **Efektywność kosztowa:** Kategoryzacja informacji pozwala organizacjom na optymalne wykorzystanie zasobów i nakładów finansowych na ochronę danych. Inwestowanie w odpowiednie środki bezpieczeństwa dla różnych kategorii informacji umożliwia skupienie się na zabezpieczaniu najcenniejszych danych, co może prowadzić do oszczędności kosztów.
- **Zarządzanie dostępem:** Kategoryzacja informacji ułatwia kontrolowanie dostępu do danych. W oparciu o kategorie informacji, organizacje mogą definiować polityki dostępu oraz przyznawać uprawnienia użytkownikom w zależności od ich roli czy poziomu odpowiedzialności. Dzięki temu ogranicza się ryzyko nieautoryzowanego dostępu do wrażliwych danych.
- **Świadomość organizacyjna:** Kategoryzacja informacji zwiększa świadomość pracowników na temat wartości i wrażliwości danych, na których pracują. Pozwala to na lepsze zrozumienie konieczności ochrony informacji i zachowanie odpowiednich praktyk bezpieczeństwa.

W związku z tym, kategoryzacja informacji odgrywa kluczową rolę w doborze środków bezpieczeństwa i zarządzaniu ryzykiem w organizacjach. Pomaga w ochronie najbardziej wrażliwych danych, spełnieniu wymogów prawnych, optymalizacji kosztów, zarządzaniu dostępem i zwiększeniu świadomości organizacyjnej na temat bezpieczeństwa informacji.

Wprowadzenie efektywnego systemu kategoryzacji informacji umożliwia organizacjom skuteczniejsze zarządzanie danymi oraz lepszą ochronę przed zagrożeniami związanymi z utratą, kradzieżą czy naruszeniem prywatności.

Aby osiągnąć te cele, organizacje powinny opracować i wdrożyć politykę klasyfikacji informacji, która określa cele, metody, kategorie i odpowiedzialności związane z tym procesem. Ważne jest również szkolenie pracowników w zakresie zasad klasyfikacji informacji oraz regularne monitorowanie i aktualizowanie systemu kategoryzacji, aby dostosować go do zmieniających się potrzeb organizacji oraz warunków rynkowych.

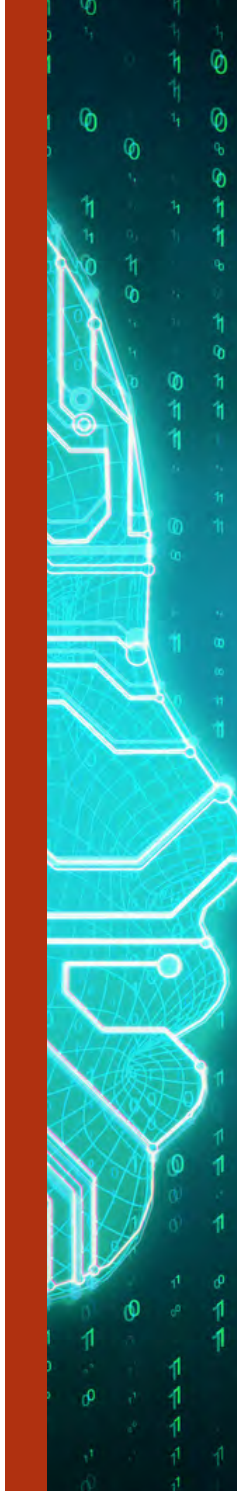
METODY WYKORZYSTANIA AI DO OCHRONY INFORMACJI

Sztuczna inteligencja (AI) może znacząco przyczynić się do ochrony informacji w organizacji poprzez zastosowanie zaawansowanych technologii i algorytmów, które usprawniają i wzmacniają procesy

związane z bezpieczeństwem danych.

Oto kilka sposobów, jak AI może pomóc chronić informacje:

- **Wykrywanie anomalii i zagrożeń:** może analizować duże ilości danych oraz wzorce zachowań użytkowników w celu identyfikacji nieprawidłowości, które mogą wskazywać na naruszenie bezpieczeństwa. Systemy oparte na AI są w stanie uczyć się i adaptować do zmieniających się zagrożeń, co pozwala na szybsze wykrywanie i reagowanie na incydenty.
- **Ochrona przed atakami typu phishing:** może być wykorzystana do analizowania treści wiadomości e-mail i innych form komunikacji w poszukiwaniu prób phishingowych. Dzięki uczeniu maszynowemu, systemy te są coraz skuteczniejsze w rozpoznawaniu prób wyłudzenia danych osobowych czy poufnych informacji.
- **Zarządzanie tożsamością i dostępem:** może wspomagać procesy uwierzytelniania i autoryzacji, ułatwiając zarządzanie dostępem do wrażliwych informacji. Systemy oparte na AI mogą stosować zaawansowane metody uwierzytelniania, takie jak rozpoznawanie twarzy czy analiza zachowania użytkownika, aby zwiększyć poziom ochrony.
- **Ochrona przed malware i ransomware:** może pomóc w wykrywaniu i blokowaniu złośliwego oprogramowania oraz ataków ransomware.



Systemy oparte na uczeniu maszynowym są w stanie analizować wzorce aktywności oraz zachowania plików w celu identyfikacji potencjalnych zagrożeń, zanim zdążą one wyrządzić szkody.

- **Automatyzacja i optymalizacja procesów bezpieczeństwa:** AI może pomóc w automatyzacji wielu zadań związanych z bezpieczeństwem informacji, takich jak monitorowanie logów, zarządzanie patchami czy analiza konfiguracji. Dzięki temu organizacje mogą lepiej alokować zasoby i skupić się na bardziej strategicznych aspektach ochrony danych.
- **Reagowanie na incydenty:** może wspierać działania związane z reagowaniem na incydenty bezpieczeństwa, przyspieszając proces identyfikacji, analizy i rozwiązania problemów. AI może również pomóc w opracowywaniu strategii zarządzania ryzykiem i planów reagowania na incydenty, co pozwala na lepsze przygotowanie organizacji na ewentualne zagrożenia.

Trzeba jednak pamiętać, że choć AI może znacznie przyczynić się do ochrony informacji, samo zastosowanie sztucznej inteligencji nie jest wystarczające. Optymalne rezultaty można osiągnąć, łącząc zaawansowane technologie AI z dobrze opracowanymi strategiami bezpieczeństwa, właściwym zarządzaniem ryzykiem oraz odpowiedzialnością i świadomością pracowników.

Wdrażając AI w celu ochrony informacji, organizacje powinny również dbać o bezpieczeństwo samych systemów AI, tak aby chronić je przed potencjalnymi atakami i wykorzystaniem przez osoby trzecie. Należy wdrożyć odpowiednie środki bezpieczeństwa, takie jak szyfrowanie danych, kontrola dostępu czy monitorowanie aktywności, w celu zabezpieczenia technologii AI i zapewnienia skutecznej ochrony informacji.

W rezultacie, sztuczna inteligencja może stać się potężnym narzędziem wspierającym ochronę informacji w organizacjach, pod warunkiem właściwego zastosowania, zarządzania i zabezpieczenia. AI może nie tylko zwiększyć efektywność i skuteczność istniejących praktyk bezpieczeństwa, ale także umożliwić organizacjom lepsze dostosowanie się do dynamicznie zmieniających się zagrożeń i wyzwań w dziedzinie ochrony danych.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC

SPRAWDŹ JAK

Polityka® Bezpieczeństwa

OCHRONA NIE POWINNA BYĆ JEDNORAZOWYM ZADANIEM

Łukasz Korecki
Daktela Polska

Cyberbezpieczeństwo powinno być traktowane jako integralna część strategii biznesowej każdej firmy, bez względu na branżę, w której działa. Wraz z rozwojem technologii i rosnącą złożonością sieci informatycznych, firmy stają się bardziej narażone na ataki cybernetyczne, a ich systemy informatyczne mogą być zagrożone różnymi rodzajami szkodliwego oprogramowania, hakerami czy phishingiem.

Ochrona przed zagrożeniami cybernetycznymi nie powinna być traktowana jako jednorazowe zadanie, ale jako ciągły proces, który wymaga ciągłego monitorowania, aktualizowania i doskonalenia.

Skutki cyberprzestępców mogą być poważne. Pamiętacie atak phishingowy na Emmanuela Macrona? W 2016 roku hakerzy wysyłali e-maile wyglądające jak oficjalna korespondencja, a w rzeczywistości zawierały złośliwe oprogramowanie. Próbowali tym wpłynąć na wyniki wyborów, a w dodatku uzyskali dostęp do kont bankowych prezydenta.

BEZPIECZEŃSTWO NAJWIĘKSZĄ WARTOŚCIĄ

Działania cyberprzestępców mają coraz większy wpływ na działalność firm, a ich skutki mogą być bardzo poważne. Mogą to być nie tylko straty finansowe, ale także wpływać negatywnie na wizerunek firmy. Ważne jest zatem dobre oprogramowanie, które nie tylko jest odpowiednio aktualizowane, ale także posiada support techniczny 24/7 - szczególnie w firmach wysokiego zaufania (banki, szpitale). Każda jednak firma powinna dbać o bezpieczeństwo poprzez edukację swoich pracowników, regularne audyty i skanowanie systemów zabezpieczających.

Oprogramowanie Daktela Contact Center jest jednym z najważniejszych narzędzi, które może pomóc w utrzymaniu bezpieczeństwa firmy. Dane w CRM są odpowiednio przetrzymywane i udostępniane tylko wybranym pracownikom, co zabezpiecza dane przed niepowołanym dostępem, a także kontroluje przepływ informacji wewnątrz firmy. Bieżący monitoring natomiast umożliwia szybkie reakcje na incydenty, a także na indentyfikację zagrożeń. Na przykład, telefonujących oszustów, podszywających się pod pracowników banku.

Daktela łączy ze sobą wszystkie kanały komunikacyjne w jednej platformie i pozwala na systemowy monitoring obsługi klienta - również dzięki wsparciu AI Agenta (sztucznej inteligencji). Każdy pracownik rozpoczynający zmianę loguje się na swoje indywidualne konto i odbiera połączenia lub inne próby kontaktu od klientów za pośrednictem platformy, według stworzonego wcześniej routingu. Wszystkie rozmowy mogą być nagrywane i kontrolowane

przez superwizora. Dane do klienta są udostępniane tylko tym pracownikom, które mają przydzielony dostęp. Dostępne statystki i raporty w dokładny sposób podsumowują jakość obsługi, a także pomagają w wykryciu niepożądanych aktywności.

SZTUCZNA INTELIGENCJA WSPARCIEM W UTRZYMANIU BEZPIECZEŃSTWA

Sztuczna inteligencja dodatkowo może wesprzeć firmę w cyberbezpieczeństwie poprzez utrzymywanie na posterunku AI Agenta monitorującego system, kiedy pracownicy są na przerwie, albo poza godzinami pracy. System zatem jest monitorowany 24 godziny na dobę, 7 dni w tygodniu. Jeśli AI Agent wykryje nieprawidłowości lub zagrożenia, niezwłocznie zawiadamia o tym odpowiednie osoby w firmie. To nie tylko pomaga w bezpiecznym prowadzeniu biznesu, ale także oszczędza pieniądze!

AI Agent jest w stanie wykrywać nie tylko standardowe zagrożenia, ale także te, które są bardziej zaawansowane i skomplikowane. Wykorzystując algorytmy uczenia maszynowego, AI Agent może analizować i przewidywać zachowanie użytkowników oraz wykrywać podejrzane aktywności. Firma może uniknąć nie tylko kradzieży danych, ale także prób dostępu do systemu przez osoby niepowołane.

Sztuczna inteligencja w contact center nie tylko zwiększa bezpieczeństwo, ale także pozwala na skuteczniejszą identyfikację i rozwiązywanie problemów. AI Agent może automatycznie identyfikować i klasyfikować zapytania klientów, przyporządkowując je do odpowiednich kategorii. Pracownicy contact center mogą szybciej i skuteczniej odpowiadać na pytania klientów, co przekłada się na wyższą jakość obsługi.

RODO A AI

Ochrona danych osobowych stała się w ostatnich latach jednym z najważniejszych aspektów funkcjonowania firm. Wprowadzenie rozporządzenia RODO (ang. General Data Protection Regulation) w maju 2018 roku sprawiło, że przedsiębiorstwa musiały dopasować swoje działania do rygorystycznych wymagań dotyczących przetwarzania danych osobowych.

W przypadku firm, które korzystają z oprogramowania Contact Center, ochrona danych jest szczególnie istotna. Przecież pracownicy w ramach swojej pracy często mają dostęp do wrażliwych danych klientów, takich jak numery telefonów, adresy email czy dane osobowe.

Właśnie z myślą o zapewnieniu wysokiego poziomu bezpieczeństwa, sztuczna inteligencja może wesprzeć firmę w ochronie danych. Jednym z przykładów jest anonimizacja danych. Sztuczna inteligencja może być wykorzystana do automatycznego usuwania wszelkich informacji, które umożliwiają identyfikację konkretnego klienta. W ten sposób firma może zachować pełną zgodność z RODO, a jednocześnie zapewnić ochronę prywatności swoim klientom.

INFORMUJ KLIENTÓW

Informowanie klientów o działaniach firmy na rzecz ochrony ich prywatności i bezpieczeństwa danych jest bardzo ważne.

Firma powinna umieścić na stronie internetowej zapis o polityce prywatności, która wyjaśnia, jakie dane są zbierane, w jaki sposób są przetwarzane i chronione.

W przypadku naruszenia bezpieczeństwa danych, klientów należy o tym powiadomić szybko i skutecznie. Ważne jest, aby w takim powiadomieniu zawrzeć informacje na temat naruszenia, jakie dane były zagrożone oraz jakie kroki podejmuje firma, aby zminimalizować ryzyko dla klientów. Firmy mogą również korzystać z mediów społecznościowych lub newsletterów, aby przekazywać informacje na temat działań związanych z cyberbezpieczeństwem.

Informacje powinny były jasne, przystępne oraz zrozumiałe dla klientów. Warto też zapewnić klientom możliwość kontaktu z firmą w przypadku pytań lub wątpliwości.

CHROŃ SIĘ!

Ścisła kontrola jakości, analiza zachowań klientów, czy zwiększenie ochrony danych wzmacnia bezpieczeństwo w firmie, a co za tym idzie, dobre oceny konsumentów.

Bezpieczeństwo powinno być podstawową wartością - to właśnie dzięki niej klienci nie boją się korzystać z usług.

Hakerzy często szukają słabych punktów w systemach firmy, aby uzyskać nieuprawniony dostęp do danych lub sieci. Mogą kraść poufne informacje, zmieniać lub uszkadzać pliki, blokować dostęp do zasobów, a nawet żądać okupu w zamian za ich odblokowanie!

Coraz więcej firm prowadzi główną sprzedaż online (szczególnie po pandemii). Ważne jest, abyśmy byli świadomi ryzyka, jakie niesie ze sobą korzystanie z internetu, i abyśmy podejmowali odpowiednie kroki w celu zminimalizowania szansy na atak hakerski i osłabienie wizerunku firmy.
Powodzenia!

DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

EKSPERCI WYDANIA

MARCIN BIAŁY
Advisory Architect
Grandmetric

Prowadził projekty transformacji IT w bankowości, sektorze produkcyjnym oraz publicznym. Dziś, wraz z zespołem konsultantów Grandmetric, doradza inżynierom i managerom IT, jak zwiększyć niezawodność i bezpieczeństwo systemów IT.

MAGDALENA CELEBAN
Właściciel
ODO Szkolenia

Wykładowca, szkoleniowiec, praktyk z zakresu ochrony danych osobowych. Pełni funkcję inspektora ochrony danych zarówno w podmiotach publicznych, jak również w sektorze prywatnym. Z wieloletnim doświadczeniem z zakresu bezpieczeństwa przetwarzania danych osobowych.

DARIUSZ MRUGOWSKI
Head of Product Development
ENGAVE S.A.

Ekspert ds. bezpieczeństwa obiektów przemysłowych oraz zarządzania projektami, posiadający ponad 10-letnie doświadczenie w zarządzaniu projektami inwestycyjnymi o łącznej wartości 60+ mln PLN netto.

TOBIASZ BĄKOWSKI
Kierownik działu marketingu
C&C Partners

Od początku pracy w firmie C&C Partners związany z systemami bezpieczeństwa. Pracę zaczynał jako osoba wdrażająca systemy, następnie pracował na stanowisku kierownika ds. serwisu, a w latach 2018 - 2021 pełnił funkcję kierownika ds. produktu. Obecnie kieruje działem marketingu. Zdobytą wiedzą i doświadczeniem chętnie dzieli się z innymi.

EKSPERCI WYDANIA

ANNA SZYMAŃSKA
CEO
Media Law Kancelaria Prawna

Radczyni prawna, ekspertka prawa własności intelektualnej, prawa nowych technologii, nieuczciwej konkurencji i znaków towarowych. Wspiera największe polskie i międzynarodowe firmy w każdej branży, projektując strategie biznesowe w zakresie ochrony i zarządzania prawami własności intelektualnej. Chroni prawa autorskie, znaki towarowe i know-how.

MAGDALENA GROCHALA
Ekspertka ds. komunikacji i PR

Ekspertka w zakresie komunikacji i Public Relations, wykładowczyni, trenerka, autorka branżowych artykułów, współautorka badań. Z PR związana od 2006 roku. Tworzy i realizuje strategie komunikacji dla dojrzałych firm i wchodzących na rynek start-upów. Specjalizuje się w tematyce nowych technologii, ze szczególnym naciskiem na cyberbezpieczeństwo.

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.

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

EKSPERCI WYDANIA

JAKUB FABIŚ
Head of Sales
Grandmetric

Od 13 lat na styku biznesu i technologii, aktywnie wspiera klientów w doborze najlepszych rozwiązań entrerprise i security. Kładzie nacisk na zrozumienie potrzeb i celów kadry zarządzającej i działów technicznych. Brał udział w fazie przygotowawczej projektów audytów bezpieczeństwa u kluczowych klientów Grandmetric.

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.

MATEUSZ JAKUBIK
Oficer Bezpieczeństwa Informacji
iSecure Sp. z o.o.

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

TOMASZ BILL
CEO
thebill oraz Alfa Lingua

Zajmuje się projektowaniem języka komunikacji. Szkoli ze storytellingu jako narzędzia do budowania marek. Właściciel firmy szkoleniowej thebill., założyciel agencji językowej Alfa Lingua, która zajmuje się kursami językowymi, tłumaczeniami i transkreacjami materiałów marketingowych.

EKSPERCI WYDANIA

ŁUKASZ KORECKI
Country Manager
Daktela Polska

Menedżer z ponad 20-letnim doświadczeniem w branży IT, telekomunikacji, call/contact center, współpracujący z największymi markami we wszystkich kategoriach IT w partnerach bezpośrednich i kanałowych. Dynamiczny, zorientowany na wyniki lider, posiadający głęboką wiedzę i doświadczenie w IT i sprzedaży, w tym aspekty technologiczne, biznesowe i operacyjne.

KATALOG FIRM

engave

ENGAVE S.A.

ul. Czarodzieja 16
03-116 Warszawa, Polska

Dane kontaktowe

+48 22 863 13 90
biuro@engave.pl

www

Specjalizacje

chmura | backup | aplikacje | procesy | cyberbezpieczeństwo | outsourcing | szkolenia | integracja | digitalizacja | serwis | testy | architektura

Technologia zmieniła sposób konkurowania w biznesie i nie ma już miejsca dla firm, które nie są gotowe na cyfrową przemianę.

Jednak wiemy, że dla wielu przedsiębiorstw jest to cały czas zbyt trudne zadanie. Dlatego nie tylko oferujemy nasze wsparcie i pomoc w przeprowadzeniu Twojej firmy przez proces cyfrowej zmiany w sposób, który zagwarantuje ci bezpieczeństwo na najwyższym poziomie.

Jako lider w dziedzinie cyberbezpieczeństwa, oferujemy zakres usług i rozwiązań, które pomagają chronić przed zagrożeniami związanymi z atakami cybernetycznymi. Wspieramy naszych klientów w ochronie danych osobowych, systemów transakcyjnych oraz infrastruktury IT.

Dzięki naszemu doświadczeniu i wiedzy, pomogliśmy wielu klientom z różnych branż. Są to między innymi: ZUS, NFZ, Wody Polskie, Hubix, Man Truck & Bus.

Nasze rozwiązania obejmują backup as a service (BaaS), archiwizację, a także rozwiązania z zakresu disaster recovery. Nasze usługi backupu i archiwizacji umożliwiają klientom utworzenie kopii zapasowych danych w czasie rzeczywistym i archiwizację wiadomości e-mail.

W przypadku wystąpienia sytuacji awaryjnej, nasze rozwiązania disaster recovery pomagają przywrócić systemy i dane do stanu sprzed awarii. To oznacza minimalizację strat wynikających z niedostępności danych lub systemów.

Jeśli szukasz rozwiązania, które pomaga w zapewnieniu bezpieczeństwa Twojej firmy, skontaktuj się z nami już dziś!

Jesteśmy gotowi pomóc w rozwiązaniu najtrudniejszych problemów, z jakimi możesz się spotkać.

KATALOG FIRM

THE BILL

tomaszbill.pl

Dane kontaktowe

+48 531 074 525

hello@tomaszbil.pl

Specjalizacje

- szkolenia dla firm
- szkolenia tematyczne
- PR
- storytelling
- strategia marki
- języki obce
- employer branding
- scenariusze
- komunikacja
- copywriting premium
- branding
- naming

Agencja kreatywna thebill. to nie tylko silna marka osobista, ale przede wszystkim firma, której podstawą działalności są szkolenia kreatywne dla firm i osób fizycznych oraz storytelling jako skuteczne narzędzie do budowania marek, wspierania sprzedaży czy w formie rozwijania kompetencji miękkich.

Założyciel i CEO firmy, Tomasz Bill, swoje autorskie warsztaty oraz szkolenia prowadzi na takich uczelniach jak SWPS, Uniwersytet Warszawski czy AGH w Krakowie.

Obecnie skupia się na rozwijaniu projektu mentoringowego dedykowanego freelancerom oraz markom, które stawiają na rozwijanie kompetencji przyszłości wśród swoich pracowników.

Wraz ze swoją drugą firmą - agencją językową **Alfa Lingua** - jest sponsorem drużyny waterpolowej AZS UW Waterpolo, wspierając jej rozwój w strukturach marketingowych oraz wizerunkowych.

Dlaczego warto skorzystać z firmy thebill.?

- Pewna inwestycja w rozwój osobisty z naciskiem na kompetencje przyszłości w zakresie marketingu, sprzedaży i rozwijania własnej firmy,
- Szkolenia prowadzone są w jednym z 3 języków: polskim, angielskim oraz niemieckim,
- Wyjątkowe doświadczenie szkolenia, które łączy w sobie wartości merytoryczne oraz unikalny performance, co stanowi dodatkową wartość dla pracowników,
- Sprawna komunikacja i wybitna obsługa klientów,
- Niespotykana kreatywność oraz lekkość w projektowaniu języka marek,
- Konkurencyjne ceny w stosunku do ogromnej wartości dla uczestników szkoleń.

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

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

Wszelkie prawa zastrzeżone.

Współpraca i kontakt: redakcja@securitymagazine.pl

Publikacja w całości jak i każdy jej fragment nie mogą być powielane ani rozpowszechniane w żadnej formie i w żaden sposób bez uprzedniego pisemnego zezwolenia Rzetelna Grupa sp. z o.o. z siedzibą w Warszawie. Wszelkie znaki towarowe, nazwy własne, logotypy oraz znaki graficzne i inne treści są chronione prawem autorskim.

Redakcja ma prawo do korekty i edycji nadesłanych materiałów celem dostosowani ich do wymagań pisma.

SECURITYMAGAZINE.PL