



1(10)/2023

SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

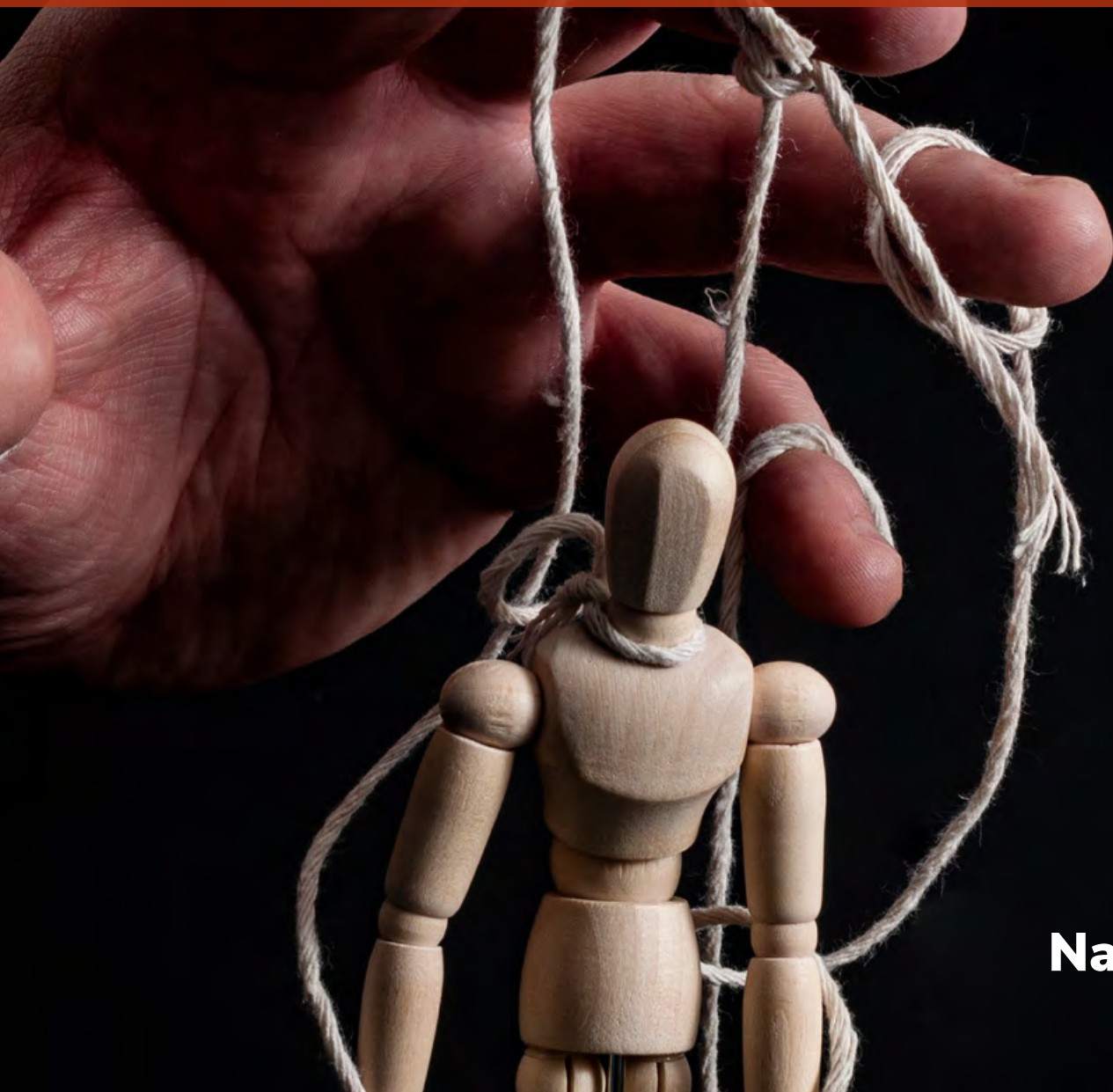
ChatGPT: Eksperci ostrzegają przed zagrożeniami

Dlaczego
socjotechnika działa?

Kradzież tożsamości
w cyberprzestrzeni

Bezpieczeństwo
w łańcuchu dostaw

Najczęstsze błędy samodzielnego
odzyskiwania danych



SPIS TREŚCI

Postępowanie wyjaśniające w przedsiębiorstwie	4
Dlaczego socjotechniki działają?	11
Fakty i mity na temat pracy w CBZC	19
Kradzież tożsamości w cyberprzestrzeni. Ochrona danych	24
„ABC cyberbezpieczeństwa”. Od tego możesz zacząć ochronę w sieci	30
Najczęstsze błędy samodzielnego odzyskiwania danych	32
PATRONAT: Jak podnieść bezpieczeństwo na kolei?	39
Bezpieczeństwo w łańcuchu dostaw	47
Ostrzeżenia przed okupami, backup i identyfikacja tożsamości	57
12 błędów związanych z wdrożeniem systemu dla sygnalistów	61
ChatGPT: Ekspert ostrzega przed zagrożeniami	74
Czy pracodawca może dysponować wizerunkiem pracownika?	90
Prognozy na 2023 w cyberbezpieczeństwie	96
Ekspert wydania	108

SZANOWNI PAŃSTWO,

witamy w 2023 roku, który może okazać się przełomowy pod względem postrzegania bezpieczeństwa, ochrony i profilaktyki związanej z obroną przed atakami, a szczególnie cyberatakami. Pojawienie się końcem 2022 roku modelu językowego ChatGPT udowadnia, w jak błyskawicznym tempie zmieniać się może wirtualna rzeczywistość, która ma wpływ na to, jak funkcjonujemy poza światem online, zarówno zawodowo, jak i prywatnie.

Dlatego tak ważne jest, byśmy byli świadomi zagrożeń, których - jak pokazują prognozy - będzie w tym roku coraz więcej. Oddajemy w Wasze ręce 10 wydanie "Security Magazine", licząc, że to tu znajdziecie odpowiedzi na pytania związane z szeroko rozumianym bezpieczeństwem.

Rafał
Ślepniowski



**Z kodem promocyjnym
SECURITYMAGAZINE10**

otrzymasz 10% zniżki.

Promocja trwa do 30 stycznia!

Do zobaczenia na jednym w swoim rodzaju wydarzeniu poświęconym bezpieczeństwu twardej infrastruktury!

Szczegóły na str. 105

ZAPISZ SIĘ NA
NEWSLETTER
BY NIE PRZEOCZYĆ
KOLEJNEGO WYDANIA

SECURITY MAGAZINE
Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy



ZAPISZ SIĘ

NEWSLETTER



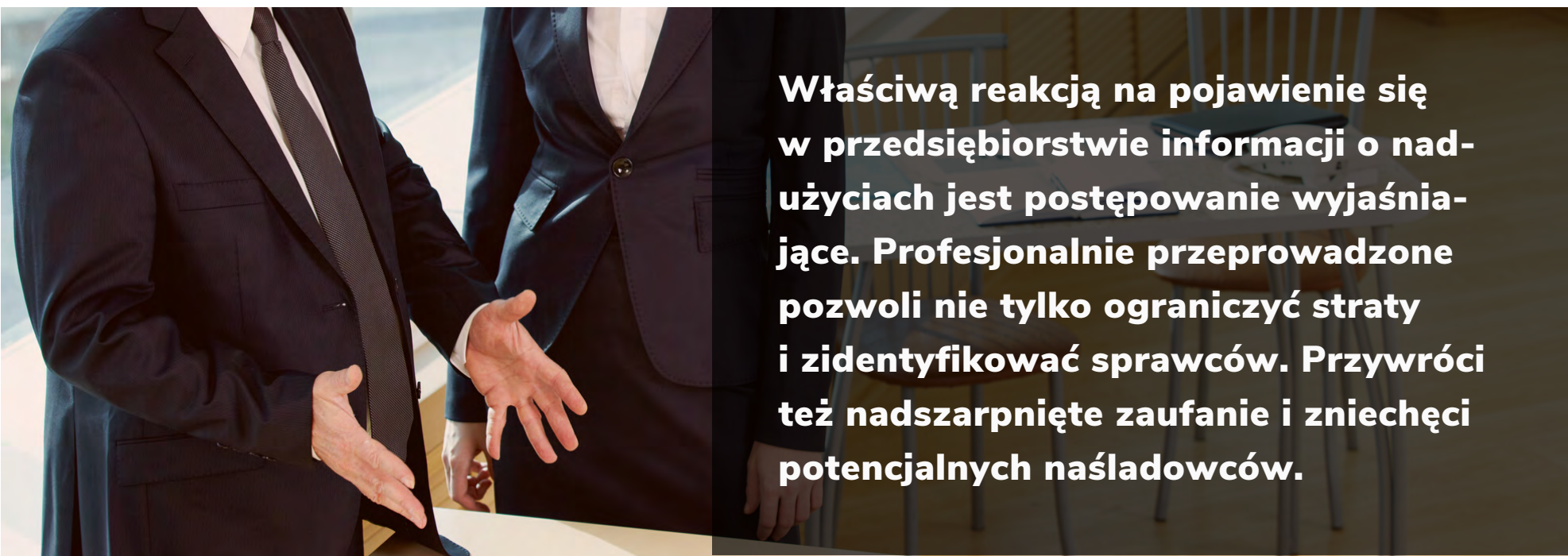
YOUR EMAIL HERE

SUBSCRIBE

POSTĘPOWANIE WYJAŚNIAJĄCE W PRZEDSIĘBIORSTWIE



Rafał Lachowicz



Właściwą reakcją na pojawienie się w przedsiębiorstwie informacji o nadużyciach jest postępowanie wyjaśniające. Profesjonalnie przeprowadzone pozwoli nie tylko ograniczyć straty i zidentyfikować sprawców. Przywróci też nadszarpnięte zaufanie i zniechęci potencjalnych naśladowców.

Informacja o nadużyciach, do jakich może dochodzić w przedsiębiorstwie, to zawsze zła informacja. Jeśli wiadomości w niej zawarte potwierdzą się, będzie to oznaczać, że zawiodły wewnętrzne mechanizmy kontrolne, a wśród współpracowników znajdują się osoby nieuczciwe, z premedytacją działające na szkodę przedsiębiorstwa. Brak dowodów na prawdziwość zawartych w informacji oskarżeń zawsze pozostawia pewien margines niepewności co do tego, czy sprawa na pewno została wyjaśniona należycie. Zignorowanie jej może natomiast wiązać się z tragicznymi w skutkach konsekwencjami - finansowymi, prawnymi i wizerunkowymi. Zrozumiałe jest zatem, że pojawienie się informacji o tym, że w przedsiębiorstwie może dochodzić do nadużyć, wywołuje mnóstwo emocji wśród wszystkich osób zaangażowanych, a jej wyjaśnienie to delikatny i skomplikowany proces.

PRZYJMOWANIE INFORMACJI O NADUŻYCIACH

To, że jest to informacja zła, nie oznacza jednak, że źle się stało, że się pojawiła. Stałoby się naprawdę źle, gdyby do nadużyć w przedsiębiorstwie dochodziło, a informacje o nich nigdy nie dotarły do osób odpowiedzialnych za bezpieczeństwo. Dlatego, mimo dyskomfortu wiążącego się z koniecznością wyjaśnienia opisywanych w nich spraw, warto zapewnić dobrze funkcjonujący system zgłaszania informacji o nadużyciach. Tym bardziej, że - jak wynika z badań PriceWaterHouseCoopers, opublikowanych w raporcie pod nazwą "Kto i jak okrada polskie firmy. 8 edycja badania przestępczości gospodarczej w Polsce" - aż 45% wszystkich zidentyfikowanych nadużyć wykryto właśnie dzięki takim informacjom. Jest to jednocześnie najskuteczniejszy



obecnie sposób wykrywania i zapobiegania nadużyciom w przedsiębiorstwach. Nie jest to jedyny powód.

Obowiązek ustanowienia wewnętrznych kanałów zgłaszania informacji o nadużyciach wynika z przepisów obowiązującej od ponad roku Dyrektywy w sprawie ochrony osób zgłaszających naruszenia prawa Unii. Co prawda, brak jest dotąd aktów krajowych, które implementowałyby zapisy dyrektywy do polskiego systemu prawnego, nie oznacza to jednak, że zapisy te w Polsce nie obowiązują. A wymagają one nie tylko zapewnienia mechanizmów umożliwiających przyjmowanie zgłoszeń, ale też opracowania procedur reagowania na nie i polityki chroniącej osoby zgłaszające przed odwetem.

KANAŁY ZGŁASZANIA INFORMACJI

Narzędzi umożliwiających przekazywanie informacji o nadużyciach jest wiele. Może to być dedykowana skrzynka e-mailowa, specjalna infolinia telefoniczna lub formularz online. Wybór narzędzia powinien uwzględniać możliwości finansowe przedsiębiorstwa, poziom jego zaawansowania technologicznego, strukturę organizacyjną oraz specyfikę działalności.

By wybrane narzędzie było skuteczne, powinno być ono ogólnodostępne oraz zapewniające pełną anonimowość i bezpieczeństwo osobie zgłaszającej. Wiedza o możliwości zgłoszenia podejrzenia nadużycia za jego pomocą musi być powszechna wśród wszystkich pracowników, a każde zgłaszane podejrzenie weryfikowane. Tylko wtedy będzie spełniać przypisaną mu rolę.

CZEGO NIE ROBIĆ

Informacji o możliwości wystąpienia nadużycia przede wszystkim nie należy ignorować. Wyjaśnienie zawartych w informacji zarzutów wiąże się z nakładami pracy i kosztów, a dodatkowo może dotyczyć osób lubianych lub wpływowych, zatem chęć jej zignorowania jest reakcją naturalną. Ignorując napływające sygnały, osoby decyzyjne pozabawiają się jednak kluczowych informacji o sytuacji w przedsiębiorstwie. Pozostawienie sprawy samej sobie dodatkowo zniechęca osoby chcące podzielić się ważną z punktu widzenia interesu przedsiębiorstwa wiedzą i rozzuchwala sprawców, utwierdzając ich w przekonaniu o bezkarności. A kiedy sprawa wyjdzie na wierzch, a wychodzi zawsze, trudno będzie wyjaśnić opinii publicznej lub - co gorsza - prokuraturze, powody rezygnacji z podjęcia działań wyjaśniających.

Także nakłady związane z ratowaniem nadszarpniętego wizerunku i ewentualnymi procesami sądowymi znacznie przewyższą te, jakie należało przeznaczyć na wcześniejsze wyjaśnienie sprawy.

Błędem jest też natychmiastowa konfrontacja z podejrzanym, wynikająca z chęci szybkiego wyjaśnienia sprawy. Jest mało prawdopodobne, by ktoś się w sytuacji takiej konfrontacji przyznał. Bardziej prawdopodobne jest natomiast to, że – poznając zakres zarzutów – podejrzany zacznie mataczyć i zacierać ślady swojej działalności. Dodatkowo szybkie ujawnienie treści otrzymanej informacji uniemożliwi przeprowadzenie działań niejawnych, bez których wyjaśnienie zarzutów może być niemożliwe.

Chęć działania może również zachęcać do bezzwłocznego zwolnienia podejrzanego, jeszcze przed próbą wyjaśnienia zarzutów. To z kolei nie tylko utrudni dalsze prowadzenie dochodzenia (osoba zwolniona – zwłaszcza niesłusznie – nie zechce współpracować), ale może również narazić przedsiębiorstwo na kosztowne postępowania sądowe i odszkodowania.

BYĆ PRZYGOTOWANYM

By zatem uniknąć błędów i chaotycznych działań, do otrzymania informacji o możliwości wystąpienia nadużycia, warto przygotować się z wyprzedzeniem.

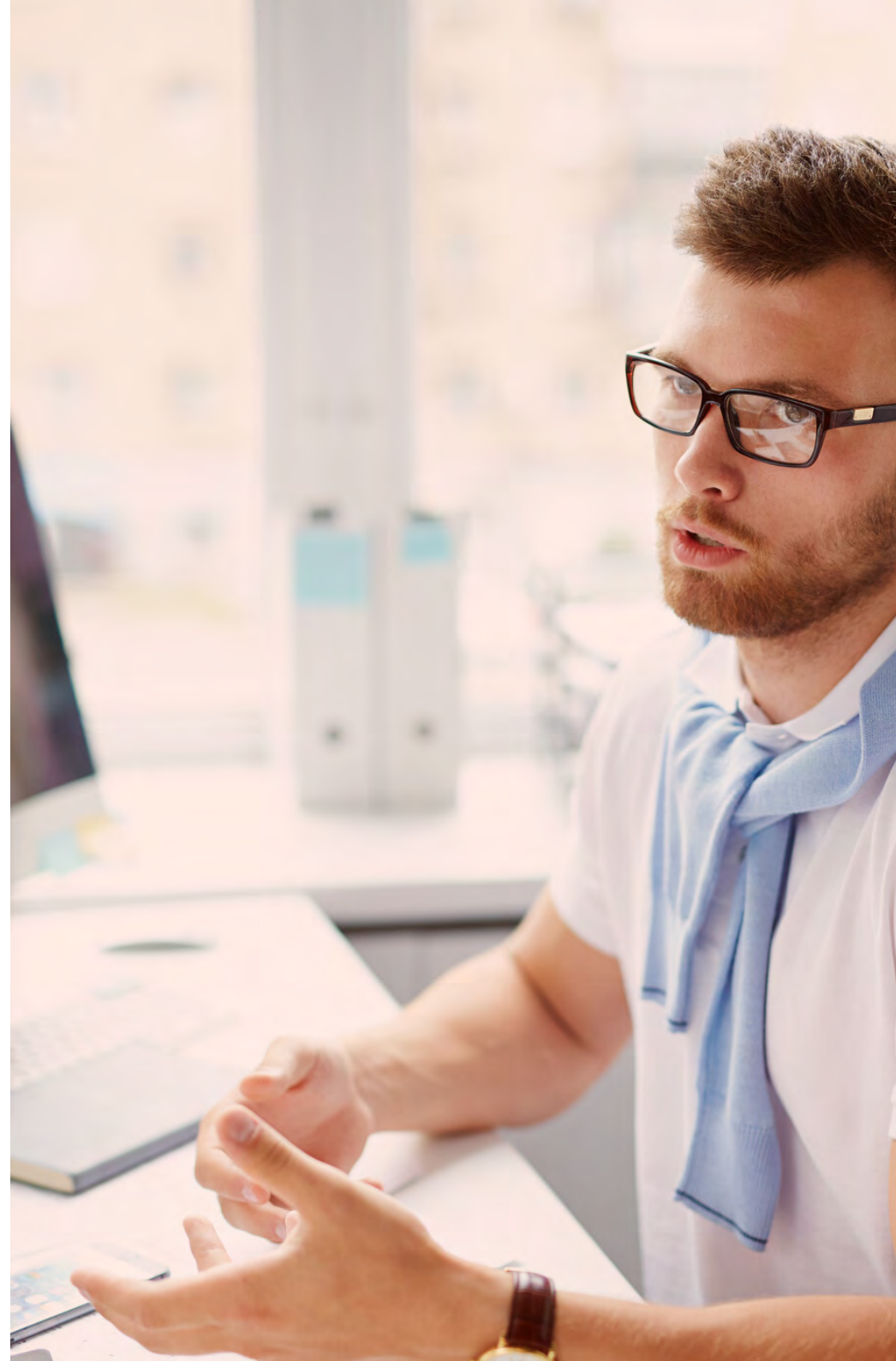
Niezbędne jest opracowanie i wdrożenie procedur, które precyzyjnie określą schemat działań, jakie należy wykonać w przypadku pojawienia się informacji oraz wskażą osoby odpowiedzialne za wyjaśnienie zarzutów w niej zawartych. Procedury powinny zapewnić spójność działań i przedstawiać ścieżki postępowania w zależności od tego, jakich obszarów i których osób zarzuty dotyczą.

POSTĘPOWANIE WYJAŚNIAJĄCE

Nie każda pojawiająca się informacja wymaga przeprowadzenia postępowania wyjaśniającego. Część zgłaszanych zarzutów jest po prostu nieweryfikowalna, część wyraźnie wskazuje na złą wolę zgłaszającego, część opisuje zachowania, które – nawet jeśli zostałyby potwierdzone – nie świadczą o wystąpieniu nadużycia. Większość informacji wymaga jednak przeprowadzenia jakichś czynności wyjaśniających. Postępowanie wyjaśniające zawsze powinno składać się z dwóch osobnych, wyraźnie wyodrębnionych etapów – części niejawnej i części jawnej.

Pierwszy etap to wszelkie działania, jakie należy wykonać przed poinformowaniem osób podejrzanych o pojawieniu się zarzutów. Na tym etapie należy zebrać dowody – będą nimi wszelkie informacje i dostępna dokumentacja niezbędna do wyjaśnienia sprawy.

Dowodów należy szukać tam, gdzie są one dostępne - czyli



w działach księgowych i finansowych (faktury, płatności), działach informatycznych (skrzynka służbowa, zawartość komputera), magazynach (stany magazynowe), działach zamówień (dokumentacje przetargowe, umowy), wszelkich prowadzonych w przedsiębiorstwie bazach danych, rejestrach logowań czy ewidencjach wydatków. Charakter działań oraz typ dowodów determinowane są treścią zarzutów.

Podczas gromadzenia dowodów należy pamiętać, by ich źródła były legalne, a osoba, która je pozyskuje, była do tego uprawniona – dotyczy to przede wszystkim zawartości komputera służbowego oraz treści skrzynki pocztowej.

Dowody zebrane w sposób niewłaściwy mogą stać się bezużyteczne, a gromadzenie informacji przez osoby nieuprawnione może wystawić przedsiębiorstwo na ryzyko procesów dotyczących naruszenia poufności danych osobowych oraz łamania tajemnicy korespondencji.

Działania w części niejawnej prowadzić powinny tylko te osoby, których udział jest konieczny. Ich liczba, przez wzgląd na poufny charakter działań, powinna zostać ograniczona do minimum.

Dopiero po zdobyciu niezbędnych informacji i dokumentów, i tylko wtedy, można przejść do drugiego etapu postępowania: części jawnej. Etap ten to przede wszystkim szczegółowa analiza zebranych informacji przy udziale osób niedopuszczonych wcześniej do sprawy, konsultacje z działem prawnym oraz - finalnie - konfrontowanie osób podejrzanych z posiadanymi dowodami. Należy przy tym pamiętać, by niczego nie zakładać z góry i nie formułować pochopnych osądów. Niezbędne jest przy tym zachowanie sceptycyzmu i umiarkowanej dawki podejrzliwości, a także przygotowanie się na różne, czasami zaskakujące, scenariusze.

WARTOŚĆ DODANA

Prawidłowo przeprowadzone postępowanie powstrzyma osoby nieuczciwe i pozwoli odzyskać generowane przez nie straty. Zdobyta w jego trakcie wiedza może przyczynić się do wzmocnienia odporności przedsiębiorstwa w przyszłości - usprawnienia wadliwie funkcjonujących procesów i uszczelnienia systemu. Samo postępowanie - wraz ze stanowczymi działaniami podejmowanymi w jego następstwie - wykaże natomiast determinację kadry zarządzającej w walce z nieprawidłowościami i przywróci nadszarpnięte w wyniku informacji o nadużyciu zaufanie.



Rzetelny[®]
Regulamin

DYREKTYWA OMNIBUS

DOSTOSUJ Z NAMI SWÓJ SKLEP
DO NOWYCH PRZEPISÓW

SPRAWDZAM OFERTĘ



DLACZEGO SOCJOTECHNIKI DZIAŁAJĄ?



Łukasz Remisiewicz
Instytut Socjologii
Uniwersytetu Gdańskiego



Media uwielbiają historie wielkich oszustw, szczególnie wówczas, gdy oszuści zastosowali właśnie jakiś nowy, wymyślny sposób na oszukanie swoich ofiar. Gdy mechanizm zostanie już opisany, publiczności towarzyszy często uczucie, że ofiary okazały się naiwne i niemądre. Śmiech towarzyszy osobom z publiczności dopóty, dopóki socjotechnik nie znajdzie klucza pasującego do ich własnego umysłu. W tym artykule chciałbym przyrzec się nie tyle rodzajom inżynierii społecznej, ale przyczynom, które sprawiają, że ona w ogóle działa.

WYKORZYSTANIE NATURALNYCH SŁABOŚCI LUDZKIEGO MÓZGU

Odpowiedź na pytanie o to, dlaczego socjotechnika bywa skuteczna musi najpierw odwołać się do mechanizmów kognitywnych, które wykorzystują twórcy oszustw. Są oni często bardzo bystrzymi obserwatorami i analitykami ludzkich rozumowań.

Zacznijmy od tego, że nasze działania podejmujemy z różnym poziomem refleksyjności: niekiedy zastanawiamy się nad przyczynami, skutkami i procedurami tego, co robimy, ale częściej, przy rutynowych działaniach, wolimy włączyć tak zwany tryb domyślny, który często przyspiesza nasze działanie, ale ogranicza zdolność kontroli nad nimi. Można wyróżnić kilka podstawowych mechanizmów wykorzystywanych w tym kontekście przez socjotechników.

Pierwszym z nich jest rozpraszanie uwagi, co ma doprowadzić do ograniczenia refleksyjności. Przykładowo w popularnych schematach wyłudzeń pieniędzy przedstawiona jest często angażująca historia, która w założeniu w całości powinna owładnąć osobą okradaną.

Na przykład, złodzieje udający na portalach randkowych amerykańskich żołnierzy, rzekomo pragnących spotkać się z poznaną w internecie kobietą, starają się przekonująco i emocjonalnie opisać swoje problemy, które wymagają opłacenia ich przelotu do Polski, zapłacenia kar czy sfinansowania kosztownej operacji. „Zajęcie” umysłu historią ma na celu wyłączenie mechanizmów kontroli u strony oszukiwanej.

Nasza refleksyjność może być uspiona, jeśli jakieś działania są podejmowane przez osoby, których nie podejrzewamy o nieuczciwość. Na przykład oszuści na portalach aukcyjnych mogą tworzyć „pacynki” – fejkowe konta, które budują reputację sprzedawcy, mającego w zamiarze oszukanie prawdziwych klientów. Ci, kierując się pozytywnymi opiniami, wystawieni są na ryzyko kradzieży. Techniką wykorzystującą podobny mechanizm jest **astroturfing** – przedstawianie pewnych zaplanowanych działań konkretnej jednostki, jako spontanicznych i oddolnych działań grup. Skoro „zwykli ludzie” organizują się i czegoś żądają, przyłączenie się do nich lub poparcie jest bardziej prawdopodobne, niż wówczas, gdy mamy do czynienia z zaplanowaną akcją, której sztuczną konstrukcję łatwo

dostrzegamy.

Socjotechnicy mogą także wykorzystywać albo wpierać poczucie winy: gdy samemu zrobi się coś nie do końca uczciwego, trudno jest podejmować kroki przeciwko oszustowi.

Powszechnie znaną sztuczką jest tzw. **nigeryjskie oszustwo**. Ofiara otrzymuje maila, że oto ktoś (np. zarządca wielkiego spadku) oferuje jej olbrzymią sumę pieniędzy, ale oczywiście żeby ją otrzymać należy wpłacić zaliczkę. Osoby oszukane często nie zgłaszały tego faktu na policję, ponieważ orientowały się, że cała sprawa miałaby charakter prania brudnych pieniędzy, a zatem wnioskowały, że bezpieczniej jest milczeć o stracie swoich środków.

Podobny mechanizm indukowania winy próbowali zastosować oszuści rozsyłający wiadomości zawierające żądania zapłacenia pewnej (niezbyt wygórowanej) sumy pieniędzy pod groźbą upublicznienia kompromitujących zdjęć z kamery internetowej, na których rzekomo widać ofiary oglądające filmy pornograficzne. Choć, oczywiście, takich zdjęć wcale nie było, to sposób ten w pierwszym okresie jego funkcjonowania okazał się dość skuteczny, ponieważ niektóre z okradzionych ofiar faktycznie korzystały wcześniej z pornografii, nie chciały by ktokolwiek się o tym dowiedział, a poza tym suma nie wydawała się im na tyle astronomiczna, by ryzykować kompromitację. Dzięki „racjonalnej kalkulacji” na podstawie tych czynników, decydowały się zapłacić.

Nasza refleksyjność może być zaburzona także pod presją czasu. Jak pokazują liczne badania psychologiczne, gdy mamy podjąć szybką decyzję, wykorzystujemy nieco inne zasoby niż wówczas, gdy możemy się nad nią w spokoju zastanowić.



Presja czasu sprawia, że nasz umysł poszukuje prostszych schematów, by analizować otaczającą rzeczywistość, co w złożonym kontekście często jednak prowadzi do błędów. Niewątpliwie sytuacje, w których ktoś oczekuje od nas potwierdzenia lub podpisu dokumentu, którego nie jesteśmy w stanie w zadanym czasie dokładnie przeczytać, powinniśmy traktować jako alarmujące.

SOCJOTECHNIKA I ZAUFANIE

Perspektywa ewolucjonistyczna wydaje się interesująca, by wyjaśnić pewną szczególną

przyczynę ulegania socjotechnice: naszą ufność. Mózgi homo sapiens kształtowały się około 120 tys. lat temu i od tej pory praktycznie się nie zmieniły. Oznacza to, że naturalnie jesteśmy najbardziej przystosowani do rozwiązywania problemów, które napotykali nasi przodkowie na terenach afrykańskiej sawanny.

Gdy nasze mózgi kształtowały się, zaufanie było konieczne do przetrwania – ktoś, kto opanował daną umiejętność, mógł ją przekazać dalej; ktoś, kto dowiedział się, gdzie można upolować zwierzynę, prowadził tam resztę gromady.



Z ciągłym wzrostem złożoności świata i rozwojem technologii zaufanie tylko zyskuje na znaczeniu. Nie znamy się na wszystkim, a nawet gdyby tak było, to przecież nie mamy czasu, by weryfikować wszystkich danych: jeśli oddajemy samochód do naprawy oczekujemy, że specjalista zdiagnozuje i naprawi usterkę.

Jeśli zamawiamy w restauracji jedzenie, przyjmujemy, że jest przyrządzone przynajmniej na tyle dobrze, byśmy się nie otruli. Jeśli dzwoni do nas sympatyczny pracownik banku, prosząc o podanie hasła do konta.... No właśnie, wtedy zaczynają się problemy.

Nasz mózg naturalnie przystosowany jest do ufności i oszuści wykorzystują różne powiązane mechanizmy z tym związane. Oszustwa polegające na wyciąganiu istotnych informacji dotyczących danych prywatnych lub haseł często wykorzystują zaufanie w powiązaniu z domyślnym trybem naszego rozumowania.

Wspomniany atak metodą „na bankiera” ma przekonać osobę po drugiej stronie słuchawki, że „ekspert” ma ważny powód, by otrzymać hasło do naszego konta, a ponieważ wie lepiej,

co robić – nie należy wątpić w jego słowa.

Wrażeniu temu sprzyjać może profesjonalny język kojarzony z instytucjami bankowymi i pewność siebie. Wielu nieudolnych oszustów odpadało już na tym etapie – nawet zwykli, nieprzeszkoleni ludzie czuli, że za telefonem stoi jakieś matactwo, gdy słyszeli, że osoba, z którą rozmawiają płcze się, a w jej słowach pobrzmiwa rosyjski akcent.

Z kolei znany amerykański hacker Kevin Mitnick był mistrzem w tego rodzaju zagrywkach. W książce „Sztuka podstępu” o znamienym podtytule „Łamałem ludzi, nie hasła” przedstawia wiele przykładów dotyczących tego, jak jego spryt i umiejętność natychmiastowego rozwiewania wątpliwości osób, z którymi rozmawiał, pozwolił mu na uzyskiwanie informacji, które z pewnością nie były dla niego przeznaczone.

Jedna z jego rozmówczyń była przekonana, że rozmawia ze swoim współpracownikiem mimo, że nie mieli nawet podobnych głosów. Plan się powiódł, bo Mitnick potrafił zmienić numer telefonu, z którego dzwonił, a tym ra-



zem sprawił, że jego ofierze wyświetlił się numer wspomnianego współpracownika. Mając tę podstawową, kotwiczącą legitymację dla swojej tożsamości, zmianę głosu wystarczyło wytłumaczyć chorobą gardła.

Zaufanie jednak można zdobywać także bez kontaktu – znaną metodą kradzieży wrażliwych danych i istotnych informacji jest podrabianie stron internetowych serwisów, których klienci podają takie dane w ten sposób, by do złudzenia przypominały oryginalne. Wykorzystuje to mechanizm domyślnego trybu działania: przesyłając „zatrutą” reklamę serwisu zachęca się klienta do kliknięcia w nią, po czym ten – zwabiony nieodróżnialnym wyglądem serwisu robi to, co zwykle, czyli loguje się lub podaje wymagane informacje.

ROLA WIEDZY

Opisane wyżej mechanizmy działały, ale na szczęście działają coraz rzadziej. Co za to odpowiada? Poziom zaufania nie jest stały, a czynnikiem sprzyjającym zmianom jest wiedza. Liczne badania dowodzą, że nie ma lepszego środka, by zapobiegać oszustwom, jak informowanie potencjalnie zagrożonych grup o tym, jakie metody aktualnie stosowane są przez oszustów. Przeciętni ludzie, a w szczególności starsi, niezapoznani w wystarczającym stopniu z nowoczesnymi technologiami, nie tylko nie wiedzą, co powinno uruchomić ich czujność, ale tak-

że często nie mają świadomości, w jaki sposób ich dane mogą zostać wykorzystane.

Gdy posiadamy wiedzę w jakimś temacie, istnieje bardzo małe prawdopodobieństwo, że zadziała na nas oszustwo, które ten temat wykorzystuje. Na przykład, badania pod kierownictwem Stephana Lea z Uniwersytetu Exeter pokazały, że osoby, które same grały czasami na loterii, są o wiele mniej podatne na zawierzenie oszukańczym informacjom o „wielkiej wygranej”. Podobnie osoby, które posiadają wiedzę o udziałach i akcjach są mało podatne na scam inwestycyjny.

Jak można sądzić, poznanie przyczyn, mechanizmów i czynników wspierających podatność na bycie ofiarą socjotechniki jest niezwykle istotne dla osób projektujących architekturę zabezpieczeń.

Choć wiele mechanizmów czysto technicznych ma niebagatelne znaczenie, to mogą one efektywniej współdziałać wtedy, gdy wiedza o zagrożeniach wśród potencjalnych ofiar będzie jeszcze większa.



PATRONAT

SECURITY MAGAZINE

POLSECURE 2023

MIĘDZYNARODOWE TARGI 25-27 KWIETNIA



Debiut wystawy poświęconej bezpieczeństwu publicznemu gwarantowanemu przez służby mundurowe był niezwykle udany. Kolejna edycja **Międzynarodowych Targów POLSECURE** odbędzie się w Targach Kielce w kwietniu 2023 roku.

Międzynarodowe Targi to efekt współpracy Targów Kielce z Komendą Główną Policji. Specjalistyczne wydarzenia wymaga merytorycznego i taktycznego wsparcia. W projekt zaangażowane są: Komenda Główna Policji, Komenda Główna Straży Granicznej, Państwowa Straż Pożarna, Służba Więzienna, Służba Ochrony Państwa, Agencja Bezpieczeństwa Wewnętrznego, Komisja Nadzoru Finansowego, Główny Inspektor Transportu Drogowego, Lotnicze Pogotowie Ratunkowe, Narodowe Centrum Badań i Rozwoju, a także Rządowe Centrum Bezpieczeństwa.

W pierwszej edycji wystawy uczestniczyło blisko 100 wystawców. Partnerem Strategicznym Targów POLSECURE była firma WB Group, jeden z największych polskich koncernów, specjalizujący się w projektowaniu i produkcji rozwiązań w sektorze obronnym i cywilnym.

POLSECURE 23 pod Honorowym Patronatem Ministra Spraw Wewnętrznych i Administracji, po raz kolejny będzie w pełni poświęcone bezpieczeństwu publicznemu. Wydarzenie będzie doskonałą okazją do zaprezentowania oferty firm specjalizujących się w produkcji wyposażenia specjalnego, środków ochrony osobistej, sprzętu ratowniczego, oprogramowania służącego łączności, dowodzeniu czy kontroli, ale także do wymiany doświadczeń i rozmów o potrzebach służb mundurowych.

Obok ekspozycji kluczowym elementem wydarzenia będzie Międzynarodowa **Konferencja Policyjna** organizowana przez Komendę Główną Policji. Podczas drugiej edycji Targów spotkanie koncentrowało się będzie na trzech głównych tematach: cyberbezpieczeństwo, laboratorium kryminalistyczne oraz logistyka.

FAKTY I MITY NA TEMAT PRACY W CENTRALNYM BIURZE ZWALCZANIA CYBERPRZESTĘPCZOŚCI



Marcin Zagórski

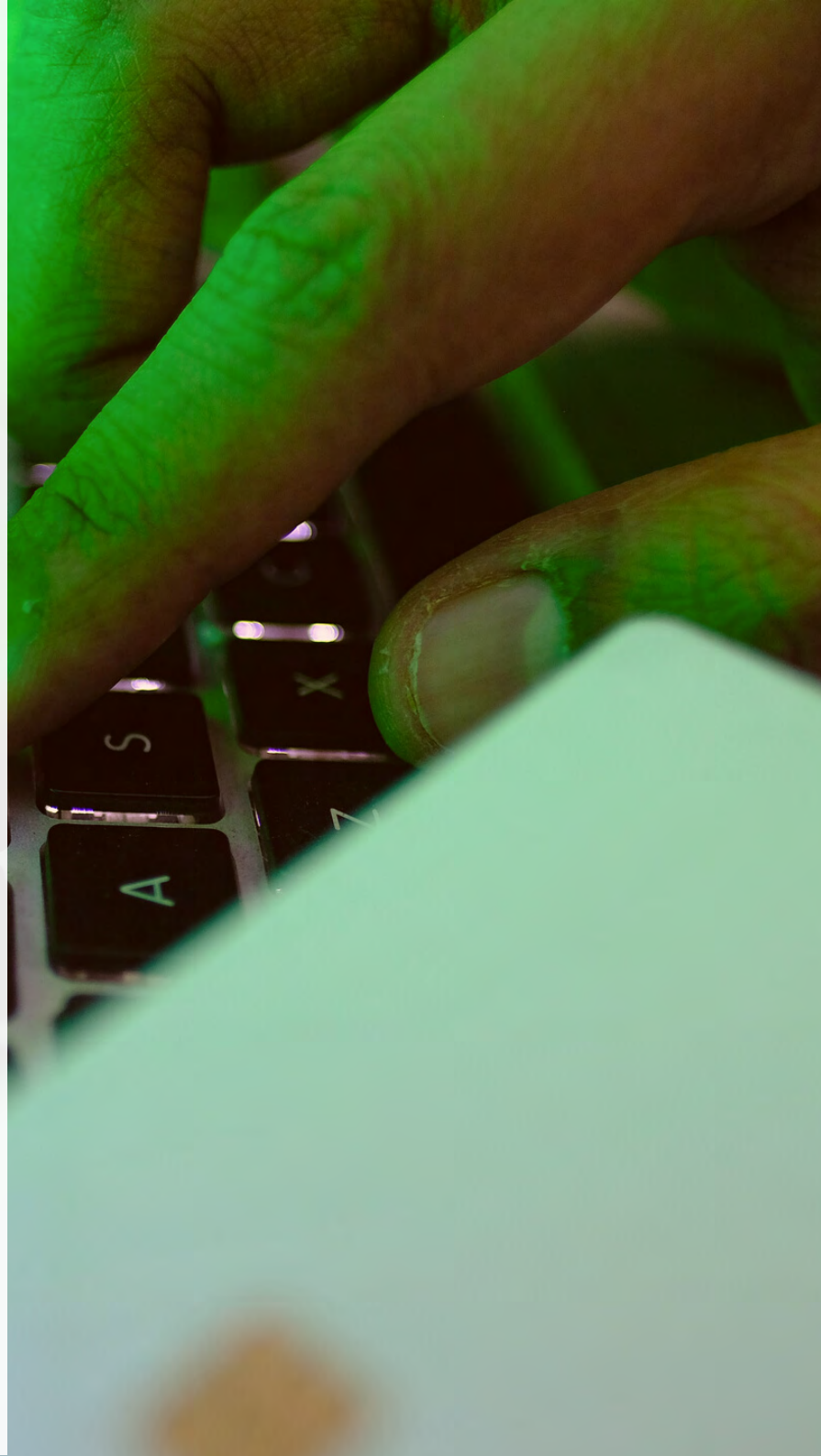
Centralne Biuro Zwalczania Cyberprzestępczości

Cyberbezpieczeństwo i zagrożenia, jakie wiążą się z tym zagadnieniem, są aktualnie największym wyzwaniem dla wielu służb, których zadania koncentrują się na zapewnieniu bezpieczeństwa w tym obszarze. Jedną z takich służb z całą pewnością jest Policja.

Rokrocznie zauważalny jest wzrost udziału cyberprzestępstw do wszystkich przestępstw i taki trend przewidywany jest na nadchodzące lata nie tylko w naszym kraju, lecz również w Europie i na świecie.

W odpowiedzi na to zjawisko, pod koniec 2021 roku Komendant Główny Policji gen. insp. Jarosław Szymczyk powołał insp. Adama Cieślaka na stanowisko pełnomocnika Komendanta Głównego Policji do przygotowania rozwiązań organizacyjnych i prawnych związanych z planowanym utworzeniem Centralnego Biura Zwalczania Cyberprzestępczości. Biura, które ma być odpowiedzią na pojawiające się coraz to nowe zagrożenia w cyberprzestrzeni i rosnącą skalę cyberprzestępstw.

Centralne Biuro Zwalczania Cyberprzestępczości swoje funkcjonowanie rozpoczęło 12 stycznia 2022 roku. Od tego momentu rozpoczął się trwający kilka miesięcy proces formowania struktur i doboru kadr. 12 lipca minionego roku CBZC formalnie „wchłonęło” dotychczasowe wydziały ds. zwalczania cyberprzestępczości w komendach wojewódzkich policji oraz Komendzie Stołecznej Policji,



a także Biuro ds. Zwalczania Cyberprzestępczości Komendy Głównej Policji wraz z większością prowadzonych w tych komórkach postępowań.

1800 ETATÓW DO 2025 ROKU

Rozwój CBZC, przewidziany jest na najbliższe kilka lat, kiedy to struktura biura w 2025 roku, ma wynieść nawet 1800 etatów. Po wstępnym procesie doboru funkcjonariuszy do CBZC, którzy dotychczas pełnili służbę w innych jednostkach policji, 3 listopada 2022 ruszyła pierwsza rekrutacja przewidziana dla osób niebędących funkcjonariuszami policji.

Od tego też dnia, ruszyła kampania informacyjna, której celem jest dotarcie do jak najszerszego grona kandydatów do służby w Policji w Centralnym Biurze Zwalczania Cyberprzestępczości.

Kandydatom, którzy zdecydują się wstąpić do CBZC oferujemy uczestnictwo w profesjonalnym oraz nowoczesnym systemie szkoleń w Polsce i za granicą z zakresu nowoczesnych technologii i informatyki śledczej. Służbę w CBZC będzie można pełnić we wszystkich miastach wojewódzkich w kraju, gdzie utworzone zostały wydziały i zarządy podległe Komendantowi Biura.

Poszukujemy osób, które dysponują wiedzą z zakresu nowoczesnych technologii, informatyki, programowania, które chciałyby zrobić coś dobrego, zwalczając przestępczość internetową, chciałyby ochronić innych przed zagrożeniami i stanąć po dobrej stronie sieci.

Proces rekrutacji został szczegółowo opracowany oraz zamieszczony na naszej stronie www.wzkladce.rekrutacja.



WYNAGRODZENIE POLICJANTA

Jeśli chodzi o podstawowe wynagrodzenie policjanta, to jest to suma kilku składników: wynagrodzenia zasadniczego, które zależy od grupy zaszergowania, dodatku stażowego, a także dodatków służbowego/funkcyjnego oraz dodatku za stopień. Aktualna wysokość wynagrodzenia zamieszczana jest na policyjnych stronach internetowych. Dla policjantów pełniących służbę w CBZC na stanowiskach związanych z bezpośrednim rozpoznawaniem i zwalczaniem przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobieganiem tym przestępstwom, a także wykrywaniem i ściganiem sprawców tych przestępstw, oferujemy specjalne świadczenie. Świadczenie to wynosi od 70 do 130 % przeciętnego uposażenia policjantów. Na chwilę obecną dodatek ten kształtuje się na poziomie 4800 – 8800 zł brutto.

Policjantom pełniącym służbę w CBZC oferujemy możliwość podjęcia studiów podyplomowych w zakresie cyberbezpieczeństwa. Studia te kierowane są w szczególności dla funkcjonariuszy i pracowników Policji i funkcjonariuszy innych służb. Ponadto w Wyższej Szkole Policji w Szczytnie planowane jest poszerzenie oferty w zakresie dodatkowego kształcenia z tematyki cyberbezpieczeństwa i cyberzagrożeń.

-20%

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PL



NOWOROCZNY RABAT

NA WIZYTÓWKĘ FIRMY W "SECURITY MAGAZINE"

WAŻNY DO
28.02.2023



KONTAKT I SZCZEGÓŁY: REDAKCJA@SECURITYMAGAZINE.PL

KRADZIEŻ TOŻSAMOŚCI W CYBERPRZESTRZENI. OCHRONA DANYCH



Piotr Siwiec
AIQLabs



Kradzież tożsamości w Internecie to z perspektywy globalnej bardzo powszechne zjawisko. Badania wskazują, że każdego roku około 9 mln Amerykanów jest narażonych na cyberprzestępstwo. W naszym kraju dochodzi rocznie do 1,5 mln naruszenia danych. Liczba rośnie z roku na rok, niosąc za sobą różne konsekwencje.

Fałszerstwa w sieci osiągają wielu płaszczyzn. Jedne są relatywnie niegroźne, jak na przykład wykorzystanie kodu pocztowego do rozsyłania spamu. Inne natomiast mogą być bardzo poważne, uwzględniając realne straty finansowe. Jak wynika z raportu Związku Banków Polski, cyberprzestępcy wyłudniają rocznie nawet 60 mln zł.

Kradzież tożsamości, określana także fałszerstwem tożsamości lub defraudacją tożsamości, to przestępstwo opierające się na wykorzystaniu cudzych danych, jak imię, nazwisko, PESEL, adres domowy lub wizerunek, bez zgody właściciela. Ich zdobycie umożliwia przestępcy podszywanie się pod ofiarę i podejmowanie działań w jej imieniu bez jej wiedzy.

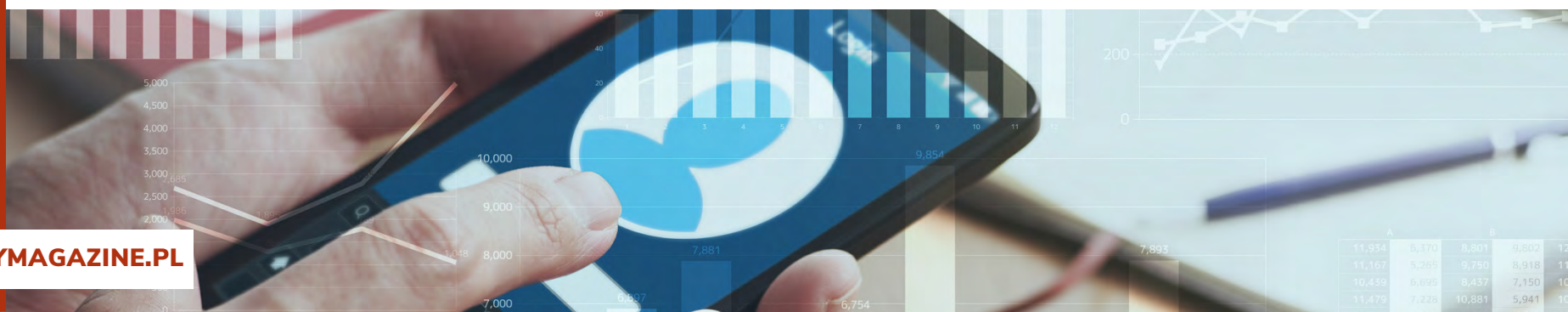
NIEPOWOŁANY DOSTĘP

Każda tożsamość ma swój unikalny charakter, także, a może nawet przede wszystkim, w Internecie.

Dokumenty oraz dane osobowe są czymś, czego nie można wypożyczyć. Powinny być one chronione przed niepowołanym dostępem. Należy mieć to na uwadze, również w trakcie obecności w sieci. Jak wynika z raportu GUS "Społeczeństwo informacyjne w Polsce", ponad 90% gospodarstw domowych ma dostęp do Internetu i z niego korzysta regularnie.

Każda z osób, bez wyjątku, zostawia w sieci swój cyfrowy ślad. Dane zbierane online służą do różnych celów – wykorzystuje się je na przykład do zapamiętywania preferencji lub tworzenia anonimowych statystyk odwiedzanych serwisów.

Wystarczy przeglądać strony www, robić zakupy w e-commerce, korzystać z poczty mailowej, mediów społecznościowych czy popularnych komunikatorów. W sieci nikt nie jest zupełnie anonimowy, co z kolei stanowi duże udogodnienie dla cyberprzestępców.



Ochrona prywatności w Internecie jest czymś, o czym należy pamiętać każdego dnia, w trakcie każdej aktywności podejmowanej online. W celu ograniczenia ryzyka narażenia się na cyberprzestępstwo, warto uruchomić czujność i ograniczyć potencjalne zagrożenie.

Mniejsza liczba publikacji na forach czy kanałach social media to mniej treści o charakterze publicznym. Kluczowym aspektem jest natomiast używanie unikalnych haseł. Warto również uruchomić dwuskładnikowe uwierzytelnianie. Równie ważnym aspektem jest czytanie polityki prywatności, korzystanie z wiarygodnych i zweryfikowanych aplikacji, a także zmiana ustawień przeglądarki na tryb prywatny lub incognito. Dzięki podjęciu wskazanych działań, można skutecznie ochronić się przed cyberatakiem. Należy jednak zwracać uwagę na wszelkie niepokojące sygnały.

Nie brakuje przypadków, w których to właśnie sam użytkownik jest „słabym ogniwem”. Trywialne hasła lub używanie podobnych ciągów autoryzacyjnych naraża go na realne niebezpieczeństwo. Każda, nawet najlepsza i wysoce zabezpieczona usługa, jest narażona na cyberatak.

Te narzędzia, które są najmocniej ufortyfikowane, mają oczywiście mniejsze szanse na to, że zostaną złamane przez hakera, lecz nigdy nie możemy mieć maksymalnej pewności. Podmioty, które obrotują danymi, muszą jednak zapewnić możliwie najwyższy poziom bezpieczeństwa. Przykładem jest inwestycja w nowoczesne i zaawansowane narzędzia, jak dane znajdujące się w zbiorach opartych o Blockchain, czyli rozwiązania kryptograficzne.

WZMOŻONA CZUJNOŚĆ

Obecnie wiele spraw można sprawnie załatwić w e-urzędzie lub placówce online. Zdalne wyrobienie nowego dowodu osobistego lub nowego meldunku już nikogo nie dziwi i stało się standardem szczególnie w czasach pandemii. Bankowość również coraz rzadziej wymaga osobistej wizyty, którą coraz skuteczniej zastępują zaawansowane aplikacje do zarządzania kontem osobistym. Nie trzeba wychodzić z domu, aby otworzyć lokatę, wziąć kredyt lub pożyczkę. Wiąże się to jednak z pewnym ryzykiem, o którym warto pamiętać, tym bardziej że wspomniane dane dotyczące rozwoju cyberprzestępstw wymagają wzmożonej czujności. Fundamentem bezpieczeństwa w Internecie jest przede wszystkim wiedza



na temat tego, jakie zachowania w sieci są ryzykowne.

Kwestie związane z cyberbezpieczeństwem dotyczą również prób wyłudzenia kredytu. Według raportu o infoDOK wydanego przez Związek Banków Polskich, w drugim kwartale 2022 roku zablokowano 1,8 tys. prób wyłudzeń kredytów na łączną kwotę 54,4 mln zł. Jednocześnie zastrzeżono ponad 37 tys. skradzionych lub zgubionych dokumentów tożsamości.

W ostatnim kwartale baza Systemu DOKUMENTY ZASTRZEŻONE wzrosła o 37 112 sztuk – to niemal dokładnie tyle samo, jak w analogicznym okresie rok temu. Statystycznie do bazy trafiało 408 sztuk dziennie.

Ograniczone do minimum formalności i możliwość zaciągnięcia pożyczki bez jakichkolwiek zaświadczeń to duże udogodnienie dla osób chcących jak najszybciej zdobyć dofinansowanie na dowolny cel.

Uproszczone procedury przyznawania pożyczek czy nawet kredytów w bankach to także pewne ułatwienie dla złodziei tożsamości.

WERYFIKACJA DANYCH

Dowód osobisty jest przydatny podczas załatwiania formalności w urzędach, ale nie tylko. Dokument ten wykorzystywany jest również w innych sytuacjach, np. podczas meldowania się w hotelu czy wypożyczania sprzętu sportowego. Zdarza się także, że oszuści podają się za pracowników banku i wysyłają maila z prośbą o aktualizację danych osobowych lub też dzwoniąc w tej sprawie do potencjalnej ofiary wyłudzenia. Inną stosowaną przez nich praktyką jest oferowanie atrakcyjnej pracy, najczęściej zdalnej na podstawie umowy o dzieło. Właśnie dlatego tak istotne jest, aby nie podawać danych osobowych osobom do tego nie upoważnionym i nie udostępniać informacji niezbędnych do zawarcia umowy o pracę, jeśli istnieją podstawy ku temu, że potencjalny pracodawca jest nieuczciwy.

METODY DZIAŁANIA

Kradzież lub zgubienie dowodu osobistego należy jak najszybciej zgłosić policji oraz w bankach i firmach pożyczkowych, w których zaciągnęliśmy zobowiązania. Poza tym należy udać się do urzędu gminy i poprosić o zaświadczenie potwierdzające utratę dokumentu tożsamości, którym będzie moż-

na posługiwać się aż do wyrobienia nowego.

Oprócz wspomnianych wyżej czynności, warto też zastrzec dowód osobisty w Internecie. Najłatwiejsze zadanie mają osoby zarejestrowane na stronie BIK – wówczas można zrobić to za pomocą jednego kliknięcia. Jest to bezpłatne dla wszystkich użytkowników.

Zdarza się, że pomimo zachowanych środków ostrożności, złodziejom udało się wykraść dane osobowe i zaciągnąć kredyt lub pożyczkę. Wówczas należy bezzwłocznie powiadomić policję oraz prokuraturę, niezależnie od tego, na jaką kwotę zaciągnięto zobowiązanie. Oczywiście, może zdarzyć się, że cała sprawa zakończy się w sądzie. Jak wówczas udowodnić, że padliśmy ofiarą oszustwa? W przypadku umów wymagających podpisu pożyczkobiorcy, można powołać biegłego grafologa, który potwierdzi, że podpis został sfalszowany. Jeśli zaś pożyczka została zaciągnięta przez Internet, można przedstawić wyciąg z konta osobistego, dzięki czemu udowodnimy, że pożyczone pieniądze nigdy nie trafiły na nasz rachunek.

Poznaj, zrozum, uchron się!

Pierwszy
taki poradnik

Ponad
100 stron



Pobierz
za darmo!

Ponad 150 haseł
i definicji

abccyberbezpieczenstwa.pl



Rzeczpospolita
Polska



OGÓLNOPOLSKA
SIEĆ EDUKACYJNA

NASK

„ABC CYBERBEZPIECZEŃSTWA”. OD TEGO MOŻESZ ZACZAĆ OCHRONĘ W SIECI



Redakcja
SECURITY MAGAZINE

we współpracy z

NASK



Być może rzuciła Ci się w oczy kampania telewizyjna NASK i KPRM, w której mowa jest o bezpłatnej wiedzy z zakresu bezpieczeństwa w internecie. Nowa publikacja opracowana przez ekspertów w ramach Ogólnopolskiej Sieci Edukacyjnej przybliży Ci kwestię cyberzagrożeń. I możesz ją mieć na swoim urządzeniu bezpłatnie.

Poradnik "ABC cyberbezpieczeństwa", bo o nim mowa, to kompendium wiedzy dla osób chcących zabezpieczyć urządzenia przed różnego rodzaju atakami i niebezpieczeństwami w sieci. Cyberbezpieczeństwo, higiena cyfrowa, profilaktyka i wsparcie - to obszary na których opiera się darmowy poradnik.

Cyberbezpieczeństwo, czyli hasła takie jak cyberstalking, fake news, FOMO, kradzież tożsamości, niebezpieczne kontakty, oszustwa internetowe, sexting, sharenting, trolling w sieci czy vishing, czyli definicje ważnych zjawisk i zagrożeń online.

Higiena cyfrowa: pigułki wiedzy, które podpowiadają, jak zadbać o równowagę online-offline i zdrowe nawyki – np. filtry kontroli rodzicielskiej, JOMO, social media sabbatical, offline challenge.

Profilaktyka: porady, jak bronić się przed zagrożeniami w sieci – definicje dotyczące np. aktualizacji, kopii zapasowych, oprogramowania antywirusowego, uwierzytelniania dwuskładnikowego i zabezpieczeń biometrycznych.

Wsparcie: hasła zawierające numery linii pomocowych i adresy punktów kontaktowych – m.in. CERT, Dyżurnet.pl, helpline, incydent bezpieczeństwa.

Zawiera on mnóstwo przydatnych informacji - autorzy przedstawiają podstawowe pojęcia z zakresu cyberbezpieczeństwa, a następnie opisują krok po kroku, jak chronić swoje urządzenia oraz to, co mają najcenniejsze - swoje dane.

Napisany przystępnym językiem, sprawia, że każdy, bez względu na wiek, zawód czy też stopień korzystania z internetowego świata, może dowiedzieć się, jak ochronić przed cyberzagrożeniami siebie oraz swoich najbliższych

- Cyfrowy świat zmienia się bardzo szybko i często trudno jest nadążyć za nowymi zjawiskami pojawiającymi się online. Często zanim zidentyfikujemy, zbadamy i opiszymy zagrożenie, pojawiają się już następne. Poradnik „ABC Cyberbezpieczeństwa” nie tylko przybliży takie zjawiska jak child grooming, FOMO, quishing, malware, scam, ale także odpowiada na podstawowe pytania, jak choćby - jak utworzyć silne hasło i dlaczego warto korzystać z uwierzytelniania dwuskładnikowego oraz zabezpieczeń biometrycznych - powiedział Wojciech Pawlak, dyrektor NASK PIB.

Poradnik możesz bezpłatnie pobrać pod linkiem: [ABC Cyberbezpieczeństwa](#).

NAJCZĘSTSZE BŁĘDY SAMODZIELNEGO ODZYSKIWANIA DANYCH



Paweł Kaczmarzyk
Serwis komputerowy Kaleron



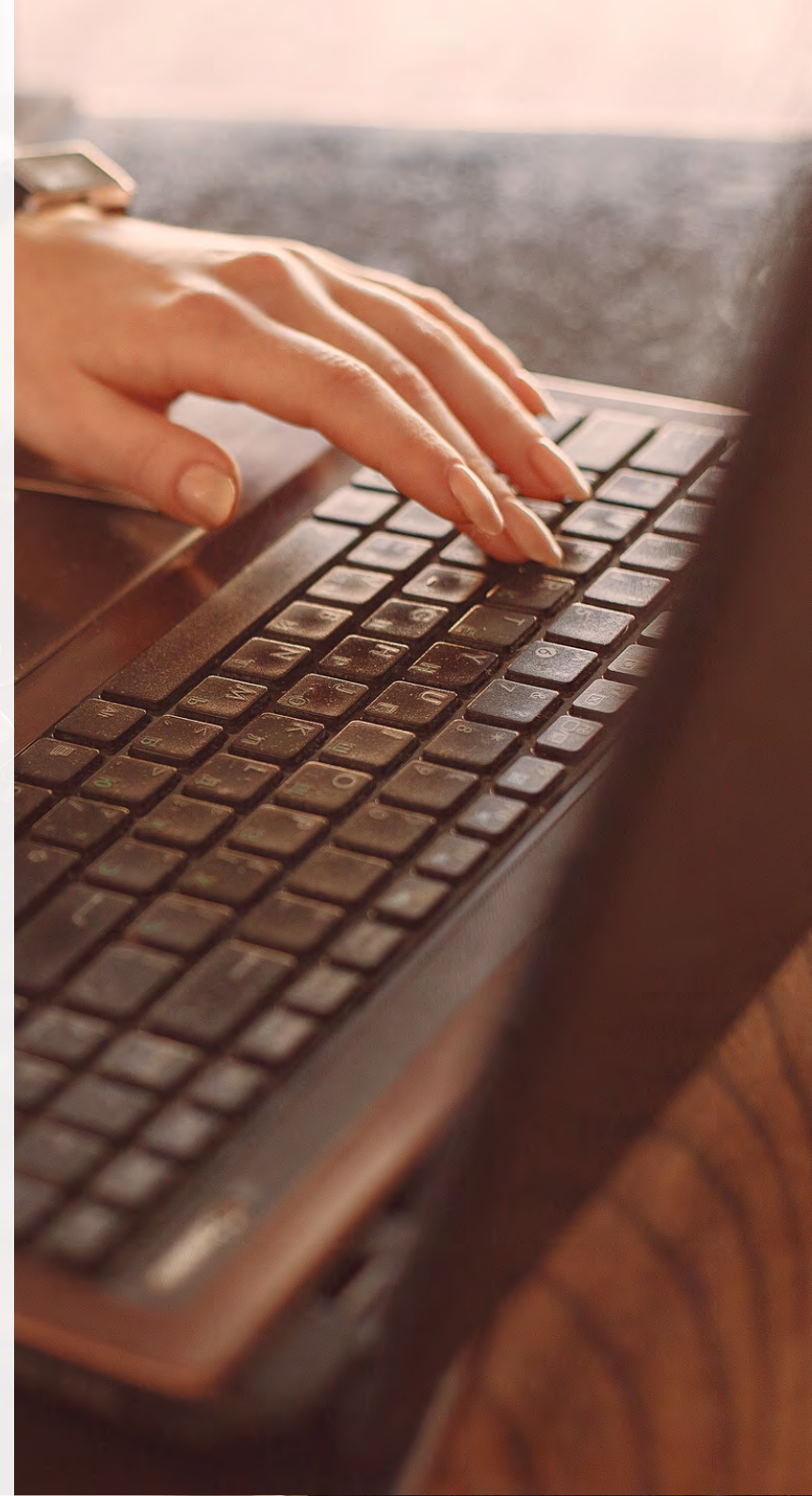
Przyczyny utraty danych często dzieli się na fizyczne i logiczne. O ile w przypadku uszkodzeń fizycznych dane są zwykle dość dobrze chronione przed nieumiejętnymi ingerencjami użytkowników, to sprawne nośniki często dają wrażenie, że problem jest łatwy i zapraszają do podjęcia samodzielnej próby jego rozwiązania. Niestety, takie próby są obciążone dużym ryzykiem popełnienia błędów skutkujących nieodwracalnymi konsekwencjami.

Fizyczne przyczyny utraty danych wynikają ze sprzętowych awarii nośników danych, takich, jak uszkodzenia elektroniczne lub mechaniczne, czy problemy oprogramowania układowego, a logiczne – związane są ze skasowaniem poszczególnych plików, sformatowaniem lub usunięciem całych partycji, rozsynchronizowaniem macierzy RAID i różnego rodzaju błędami struktur logicznych systemów plików.

KORZYSTANIE Z URZĄDZENIA, Z KTÓREGO ZOSTAŁY STRACONE DANE

Najczęściej spotykanym błędem jest praca na komputerze, z którego została utracona informacja. Sama praca systemu operacyjnego wiąże się z dokonywaniem licznych zapisów na dysku. Plik wymiany, plik hibernacji, liczne pliki tymczasowe generowane przez procesy wykonywane przez użytkownika lub automatycznie, w tle, w niekontrolowany sposób nadpisują poprzednią zawartość. Nawet jeżeli użytkownik jest w stanie się upilnować i niczego nie zapisywać na dysku, nigdy nie upilnuje systemu operacyjnego.

Jeśli do tego dojdzie, zawartość świadomie (np. programy do odzyskiwania danych) lub nieświadomie (np. aktualizacje systemu operacyjnego) pobierana z sieci, szanse na odzyskanie utraconej zawartości spadają jeszcze bardziej. Tym bardziej, że niektórzy użytkownicy nie tylko instalują oprogramowanie do odzyskiwania danych na dyskach, z których te dane zostały stracone, ale też na tych samych dyskach zapisują wyniki pracy tych programów. W ten sposób często jeden odzyskany plik uniemożliwia poprawne odzyskanie następnego.





W przypadku utraty danych należy bezwzględnie niezwłocznie wyłączyć komputer. Najlepiej przez odcięcie wszystkich źródeł zasilania (także wyjęcie baterii w przypadku laptopów). Sam proces zamykania systemu operacyjnego wiąże się z zapisywaniem na dysku wielu różnych informacji, które może i są istotne dla samego systemu, ale na pewno są daleko mniej ważne od naszych danych.

UŻYCIE CHKDSK

Chkdsk, scandisk i inne procedury sprawdzania spójności i naprawy struktur logicznych systemów plików są bardzo niebezpieczne dla danych. Te procedury są często używane w celu przywrócenia działania systemu i nie zawsze wyrządzają szkody, jednak ze względu na ryzyko, jakie ze sobą niosą, nigdy nie powinny być używane na nośnikach zawierających ważne dane. Aby lepiej zrozumieć to ryzyko, musimy sobie uświadomić podstawowy cel i zasadę działania takich procedur.

Podstawowym celem procedur weryfikujących spójność struktur logicznych systemu plików jest doprowadzenie tych struktur do takiego stanu, by partycja nadawała się do zamontowania przez system operacyjny.

Struktury logiczne są skanowane w poszukiwaniu błędów i jeśli jakieś błędy zostaną znalezione, są naprawiane. To chyba dobrze, prawda? Otóż nie. Gdyby naprawa błędów polegała na wpisaniu w odpowiednie miejsca właściwych wartości, niczego więcej byśmy nie potrzebowali.

Ale czym innym jest zidentyfikowanie błędu, a czym innym ustalenie, co w tym miejscu powinno być. Chkdsk tego nie umie, więc po prostu usuwa uszkodzone fragmenty struktur, by nie przeszkadzały przy montowaniu partycji i nie destabilizowały pracy systemu operacyjnego. Ale jakie zagrożenie dla danych niesie usunięcie uszkodzonych fragmentów struktur logicznych? Przecież skoro są uszkodzone, to chyba są bezużyteczne?

Struktury logiczne, nawet te uszkodzone, są cennym materiałem do analizy dla specjalisty naprawdę znającego się na odzyskiwaniu danych. Ułatwiają zidentyfikowanie i odnalezienie zagubionych plików. Nieraz można je naprawdę naprawić wykorzystując inne dane, wiedzę o systemach plików i używanych w nich schematach, przyjmując założenia w kategoriach prawdopodobieństwa, a niekiedy po prostu zgadując lub podstawiając do skutku prawdopodobne warianty. Zniszczenie uszkodzonych struktur bezpowrotnie uniemożliwia ich wykorzystanie. W takiej sytuacji radość z poprawnego uruchomienia systemu operacyjnego może być brutalnie przzerwana odkryciem, że bardzo ważne pliki gdzieś zniknęły.

TRIM

Konsekwencje niekontrolowanych zmian w czasie naprawy struktur logicznych systemu plików wykraczają daleko poza proste zgubienie plików w przypadku nośników obsługujących funkcję TRIM. Jest to funkcja pośrednicząca w przekazywaniu informacji o obszarach niezaalokowanych w strukturach logicznych systemu plików (wolnym miejscu na partycji) do obsługiwanego przez oprogramowanie układowe podsystemu translacji adresów logicznych na fizyczne. Szczegółowe opisanie działania tej funkcji wykracza poza ramy tego artykułu, ale na potrzeby samodzielnego odzyskiwania danych wystarczy nam informacja, że nośnik obsługujący funkcję TRIM nie musi fizycznie przechowywać danych, które nie są odpowiednio zaalokowane przez system plików.

Jeśli nośnik nie przechowuje fizycznie obszaru niezaalokowanego logicznie, w odpowiedzi na żądanie odczytania sektorów niezaadresowanych w strukturach systemu plików zwróci sektory wypełnione wartością 0x00. W praktyce oznacza to, że przeszukując dysk w poszukiwaniu utraconych danych nie będziemy mogli ich znaleźć. W przypadku dysków SSD fizyczne bloki przechowujące dane usunięte na poziomie struktur logicznych są kasowane

w czasie rzędu kilku minut odbierając i specjalistom jakiegokolwiek szanse na odzyskanie znajdujące się w nich zawartości.

Nieco lepiej sytuacja przedstawia się w przypadku dysków twardych wykorzystujących technologię zapisu gontowego (SMR), gdzie nie występuje operacja fizycznego kasowania danych i są realne szanse na odnalezienie utraconych danych pracując w adresacji fizycznej. Przynajmniej dopóki ta zawartość nie zostanie nadpisana kolejnymi danymi zapisywanymi na ten dysk. A przecież sprawdzanie spójności danych często skutkuje bardzo długimi seriami zapisów.

Ze względu na sposób działania funkcji TRIM, najlepiej jest wyłączyć ją na komputerze, którego zamierzamy użyć do odzyskiwania danych jeszcze przed podłączeniem dysku, z którego dane chcemy odzyskiwać. Komenda, jaką należy wpisać w wierszu poleceń, by wyłączyć funkcję TRIM, to: `fsutil behavior set disabledeletenotify 1`.

Szczegółowe wskazanie nośników obsługujących funkcję TRIM byłoby zbyt objętościowe i zbyt szybko by się dezaktualizowało, więc dla bezpieczeństwa lepiej przyjąć, że funkcję tę obsługują wszystkie dyski SSD (z naprawdę nielicznymi i coraz rzadziej spotykanymi wyjątkami) i dyski z technologią SMR (tu dysków nieobsługujących funkcji TRIM jest sporo więcej, ale lepiej przesadzić z nadmiarem ostrożności, niż gdyby jej zabrakło). Ze względu na projektowane rozwiązania zarządzania adresowaniem danych w dyskach z zapisem przeplutowym (IMR/HIMR), które mają szansę pojawić się na rynku w perspektywie kilku najbliższych lat, możemy się spodziewać, że także w nich pojawi się obsługa TRIM lub podobnie działającej funkcji.

SFORMATOWANIE PARTYCJI

Jednym z bardziej absurdalnych zachowań praktykowanych podczas amatorskich prób odzyskiwania danych jest tworzenie nowych lub formatowanie istniejących partycji.

Zapewne osoby dopuszczające się takich czynności liczą na to, że utworzenie nowej partycji pozwoli zobaczyć dane znajdujące się w tym miejscu wcześniej lub że formatowanie naprawi jakieś błędy. Takie czynności nierzadko zalecane są na słabych merytorycznie forach internetowych, a także wymuszane są przez niektóre programy do odzyskiwania danych napisane przez ludzi niemających o tym głębszego pojęcia.

Utworzenie nowej partycji w obszarze niezaalokowanym w tablicy partycji, gdzie znajdują się utraczone dane nie jest odtworzeniem poprzedniej partycji, ale utworzeniem w jej miejscu nowej. Niekiedy, jeśli błędy występują wyłącznie w tablicy partycji, utworzenie nowej partycji o położeniu dokładnie odpowiadającym partycji starej może być skutecznym rozwiązaniem problemu, ale jedynie w przypadku, gdy ta partycja nie zostanie sformatowana. Wtedy system dowie się o istnieniu tej partycji i będzie mógł odnaleźć we właściwym miejscu struktury starej partycji.

W przypadku sformatowania partycji zostaną utworzone nowe struktury logiczne, które nadpiszą poprzednie. Skala zniszczeń będzie uzależniona od wielu czynników, spośród których największe zna-

czenie mają rodzaj używanego systemu plików oraz nośnika danych, na jakim pracujemy. W szczególności większych szkód możemy się spodziewać na dyskach SMR i SSD.

To jedynie kilka najpopularniejszych błędów popełnianych przy próbach samodzielnego odzyskiwania danych.

Podsumowując – najważniejsze, aby wystrzegać się jakichkolwiek zapisów na nośniku, z którego straciliśmy dane i nie dopuścić do pogorszenia stanu wyjściowego.

Najrozsądniejszym rozwiązaniem jest wykonanie kopii posektorowej dysku i dalsza praca z kopią, ale kto by na to tracił czas, kiedy w Internecie można znaleźć tyle prostych instrukcji samodzielnego odzyskiwania danych?





/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**



SECURITYMAGAZINE.PL

JAK PODNIEŚĆ BEZPIECZEŃSTWO NA KOLEI? KONFERENCJA PO RAZ CZWARTY



PATRONAT
SECURITY MAGAZINE



Czy na polskiej kolei jest bezpiecznie? Jakie działania należałoby wdrożyć, aby zmniejszyć liczbę wypadków na torach? O tym debatowali już po raz czwarty uczestnicy konferencji „Bezpieczeństwo na Kolei”, organizowanej przez Polską Izbę Producentów Urządzeń i Usług na Rzecz Kolei.



W roku 2021 na polskich torach doszło do 194 zdarzeń, w wyniku których zginęły 43 osoby, a 16 zostało ciężko rannych. Statystyki nie napawają optymizmem. Od stycznia do końca listopada 2022 roku w 149 wypadkach i kolizjach poszkodowanych zostało 20 osób, zaś 38 zginęło. Co jeszcze należy zrobić, by liczba tych zdarzeń malała?

- Niezmiennie 72 % -75 % wszystkich wypadków na liniach kolejowych to wypadki z udziałem strony trzeciej, spoza systemu kolejowego – powiedział w trakcie wystąpienia Grzegorz Prusik, Dyrektor Departamentu Monitorowania i Bezpieczeństwa Urzędu Transportu Kolejowego.

Na zmniejszenie liczby zdarzeń na przejazdach kolejowych wpływ może mieć doedukowanie kierowców oraz pieszych z zakresu zasad i zachowania się w pobliżu terenów kolejowych. Jednak nie tylko użytkownicy dróg są winni tragicznym zdarzeniom na torach, co podkreślał w swoim wystąpieniu Tadeusz Ryś, Przewodniczący Państwowej Komisji Badania Wypadków Kolejowych. Jak zaznaczył, chodzi także o dobrą widoczność.

- W obrębie trójkątów widoczności nie sytuuje się obiektów ograniczających pole widzenia, w szczególności obiektów budowlanych, drzew, krzewów i innych upraw wysokopiennych, reklam, czy elementów ochrony akustycznej – podkreślał.

Bezpieczna kolej to także ta chroniona w sieci. O cyberbezpieczeństwie systemów kolejowych na przykładzie doświadczeń z wojny między Rosją a Ukrainą mówił kmdr (rez.) dr hab. Grzegorz Krasnodębski, prof. Akademii Marynarki Wojennej w Gdyni. Jednak nie tylko konflikt na wschodzie może nieść za sobą zagrożenie w cyberprzestrzeni.

Jak zaznaczył Rafał Zgorzelski, Członek Zarządu PKP S.A., Przewodniczący Rady Polityki IT Grupy PKP i PKP PLK, systemy kolejowe na ataki narażone są każdego dnia.

- Cyfryzacja procesów realizowanych przez podmioty Grupy PKP to z jednej strony wielki rozwój technologiczny i związana z nim gospodarka oparta na informacji, bowiem dochodzi tu do wykładniczo zwiększającego się apetytu na różnego typu dane umożliwiające budowanie lub utrzymanie przewagi konkurencyjnej. PKP S.A. i Grupa PKP będąc największym podmiotem w Polsce zarządzającym infrastrukturą krytyczną jest szczególnie narażona na ataki hackerskie, ale jest także szczególnie zobowiązana do dbałości o bezpieczeństwo pracowników PKP S.A., GRUPY PKP, PASAŻERÓW, przewożonych różnego typu towarów oraz majątku poszczególnych Spółek – mówił.

O wymaganiach w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa mówił Marek Pawlik, Z-ca Dyrektora Instytutu Kolejnictwa. Temat „Inteligentna architektura PSIM dla etapowej modernizacji infrastruktury kolejowej” podjął Krzysztof Rybak z firmy SAT-SYSTEM Sp. z o.o.

O wnioskach, które powinniśmy brać pod uwagę budując system cyberbezpieczeństwa mówił zaś Paweł Nogowicz, Prezes Zarządu firmy Evercom. Wystąpienia gości były wstępem do prelekcji bloku pierwszego:

CYBERBEZPIECZEŃSTWO I MONITORING

Odpowiedzią na cyberzagrożenia w branży kolejowej jest Centrum Cyberbezpieczeństwa Kolei. Mówił o nim Radosław Zawierucha, Członek Zarządu PKP Informatyka Sp. z o.o.

- Celem projektu jest utworzenie centrum kompetencyjnego, którego głównym zadaniem będzie wsparcie podmiotów podsektora kolejowego – tłumaczył Zawierucha: – Utworzenie CCK zapewni sprawną wymianę informacji o zdarzeniach i incydentach komputerowych w podsektorze kolejowym oraz wsparcie w ich obsłudze.

O wykrywaniu słabych punktów sieci teleinformatycznej IP na przykładzie czeskich kolei państwowych mówił Karol Kujawa, Solution Architect – IP & Security, z firmy Vector Solutions Sp. z o.o. O działaniach Spółki mówił zaś Prezes Janusz Kilon.



Kwestie monitorowania i ochrony dworców kolejowych podjął Michał Zagalski, Dyrektor Projektu z PKP S.A.

- W PKP S.A. funkcjonuje Centrum Bezpieczeństwa Dworców Kolejowych PKP S.A. – całodobowa komórka organizacyjna w Biurze Bezpieczeństwa PKP S.A., monitorująca zagrożenia na dworcach kolejowych i innych nieruchomościach PKP S.A. Pozyskuje ona, gromadzi, przetwarza i przekazuje informacje o zdarzeniach zaistniałych w nieruchomościach Spółki z terenu całej Polski. Pełni funkcję całodobowego punktu kontaktowego spółki PKP S.A. w systemie zarządzania kryzysowego – opisywał projekt Michał Zagalski.

WŚRÓD PRELEGENTÓW BYLI TAKŻE

- Krzysztof Wójtowicz, Head of Sales z firmy ICsec S.A., który omówił najważniejsze wyzwania cyberbezpieczeństwa dla transportu.
- Marcin Kopczyński, Naczelnik Wydziału Ochrony Informacji i Spraw Obronnych z Biura Bezpieczeństwa i Audytu PKP CAR-GO, który przedstawił rolę SOC w procesie ochrony informacji.
- Artur Ślubowski, Dyrektor Projektu, p.o. Naczelnika Wydziału Bezpieczeństwa PKP Informatyka, który przedstawił działania funkcjonującego w Spółce zespołu CERT.
- Tomasz Malej, Key Account Manager Hexagon, Intergraph Polska Sp. z o.o. przedstawił temat „HxGN Connect – koordynacja kluczem do bezpieczeństwa”.







Fot. FLC Studio Dariusz Konsek (2)

MERYTORYCZNIE

- Mamy przekonanie, że lokalny poziom bezpieczeństwa – gmina, miasto, powiat i metropolie to kluczowe obszary aktywności administracji, przede wszystkim samorządowej oraz Policji, służb i straży podejmujących codzienny wysiłek zmierzający do ograniczania zagrożeń dla mieszkańców, zapobiegania kryzysom i właściwego reagowania w przypadku identyfikacji niebezpieczeństw - zapowiadała wydarzenie Polska Izba Ochrony.

Konferencje oficjalnie otworzyli: Jacek Jaśkowiak, Prezydent Miasta Poznania oraz Generał broni oraz Dowódca Wojsk Lądowych RP w latach 2006-2009, Waldemar Skrzypczak.

Wydarzenie zgromadziło wybitnych znawców tematyki bezpieczeństwa, zarówno praktyków jak i teoretyków. Obfitowało nie tylko w wiele merytorycznych prezentacji, ale i wartościowe debaty. Jednym z istotnych paneli dyskusyjnych była rozmowa ekspertów na temat współpracy prywatnego sektora ochrony z samorządami lokalnymi.



**Organizujesz wydarzenie związane
z bezpieczeństwem w firmie
lub nowymi technologiami?**

**Sprawdź ofertę
PATRONATU
MEDIALNEGO**



Napisz do nas:

redakcja@securitymagazine.pl

BEZPIECZEŃSTWO W ŁAŃCUCHU DOSTAW



Katarzyna Bieńkowska
Silny&Salamon



Jednym z kluczowych czynników wpływających na satysfakcję klienta końcowego jest pewny łańcuch dostaw. Jak dobrze go zabezpieczyć, by podnieść bezpieczeństwo w firmie i zoptymalizować procesy produkcji, magazynowania, pakowania i dystrybucji? Kiedy wybrać inteligentne zabezpieczenia, a kiedy klasyczne?

Logistyka powinna być sprawna, zwinna i efektywna, co wyraża się poprzez odpowiednie oznaczanie i pakowanie produktów oraz precyzyjne ewidencjonowanie wysyłki towarów. Wdrażanie rozwiązań logistyki 4.0 to dziś konieczność, która łączy się z potrzebą analizy ogromnej ilości danych. Choć ich płynna i szybka interpretacja przynosi wymierne korzyści, to implementacja wymaga zaangażowania wielu zasobów. Poza inteligentnymi rozwiązaniami szerokie zastosowanie mają łatwe w użyciu i atrakcyjne cenowo plomby, które skutecznie zabezpieczają i dostarczają pewność, że towary i miejsca są chronione przed manipulacją, nieuprawnionym wejściem czy kradzieżą. Stanowią również nośnik informacji o produkcie.

Bezpieczny łańcuch dostaw

Jak zapewnić bezpieczeństwo i ciągłość informacji w całym łańcuchu dostaw?



Czy proces produkcyjny, od surowca do gotowego produktu, jest monitorowany?



Czy produkt jest prawidłowo skompletowany i oznaczony?



Czy można łatwo zinventaryzować produkty w magazynie?



Czy towar jest właściwie zamknięty i bezpieczny?

Dzięki zastosowaniu odpowiednich plomb, będziesz znał odpowiedzi na te wszystkie pytania.

DNA PRODUKTU ZAPISANE W PLOMBIE

Na pierwszym etapie łańcucha dostaw, a więc produkcji, kluczowe są informacje, takie jak: kod, numer, seria, pochodzenie, data i godzina wytworzenia. Można je zakodować w plombach RFID, klasycznych plombach z nadrukami, nadanymi kolorami, etykietami z kodami kreskowymi czy QR. Warto wiedzieć, że informacje zaszyte w fizycznych oznaczeniach wspierają procesy posprzedażowe, w tym reklamacyjne.

Z kolei podczas pakowania zastosowanie zabezpieczeń i oznaczeń zapewnia wiedzę o pochodzeniu produktów, a po zamknięciu w zbiorcze opakowania, nadawane są kolejne oznaczenia. Tu poza tradycyjnymi plastikowymi plombami, sprawdzają się plomby naklejkowe, z kodami kreskowymi, QR i plomby gwarancyjne. Do innych rozwiązań należą też etykiety bazowe umieszczane na pojemnikach wielorazowego użytku.

Wkraczając w kolejny etap łańcucha dostaw, magazynowanie, właściwe znakowanie produktów pojedynczych czy konfekcjonowanych, sprzyja szybkiej i łatwej inwentaryzacji, potwierdza też nienaruszalność towaru i zabezpiecza pojemniki.

Co ważne, plomby w magazynach umożliwiają wizualną identyfikację rozmieszczenia produktów i kontrolę dostępu do pomieszczeń lub wybranych stref.



GDY PRODUKT WYRUSZA W DROGĘ

Na ostatnim etapie łańcucha dostaw, czyli w transporcie, by zapewnić nienaruszalność ładunku, niezbędne jest monitorowanie towaru, identyfikacja i zabezpieczenie. Międzynarodowy i krajowy transport towarów narażony jest na kradzieże, a często standardowe zabezpieczenia nie są wystarczające, aby chronić produkty o wysokiej wartości, a zarazem łatwe do sprzedaży na rynku wtórnym.

Cyfryzacja zwiększa więc wydajność, produktywność i bezpieczeństwo w logistyce. Plomby elektroniczne, jak np. TrackLock 2.0 wraz z platformą online działają w koncepcji IoT, dostarczając natychmiastowo informacji o położeniu, przebiegu trasy i statusie w każdym punkcie drogi, tj. plomba otwarta, zamknięta, naruszona. Umożliwiają też przyznanie dostępu do towarów osobom upoważnionym, dzięki uzbrajaniu je na kilka sposobów: przy użyciu kart RFID, platformy web, aplikacji mobilnej, SMS, BT lub kodu PIN.

Co ważne, rozwiązanie można zintegrować z dowolnym systemem zarządzania, co jest dobrą bazą do optymalizacji procesów poprzez dostęp do statystyk i analiz w czasie rzeczywistym.

W transporcie sprawdzają się też plomby z tagami RFID, plomby kontenerowe i linkowe. Tam też często stosowane są podwójne zabezpieczenia, które pełnią funkcję identyfikacyjną i zabezpieczającą. Dodatkowo w zależności od polityki firm transportowych mogą być widoczne lub dyskretne. Inną korzyścią stosowania inteligentnych rozwiązań do zabezpieczania transportu jest zmniejszenie emisji spalin poprzez optymalizację tras na podstawie zbieranych danych.



ZABEZPIECZENIA DOBRANE DO RZECZYWISTYCH POTRZEB

Pierwszym etapem doboru zabezpieczeń powinna być analiza przedwdrożeniowa, w tym zbadanie potrzeb w zakresie bezpieczeństwa, a następnie indywidualny dobór rozwiązań. Plomby plastikowe czy metalowe są idealne do środków transportu, pomieszczeń, boksów, szaf i worków. Plomby butelkowe i linkowe są cenione przez firmy działające w branży TSL i stosowane przy kontenerach transportowych, zaś elektroniczne modele pozwalają śledzić dostawy w czasie rzeczywistym.

Z kolei firmy, które świadczą usługi pocztowe, kurierskie, bankowe czy podmioty administracji publicznej, doceniają bezpieczne saszetki i torby, umożliwiające przechowywanie i transport gotówki, dokumentów i innych wartościowych przedmiotów. Natomiast plomby naklejkowe w postaci samoprzylepnych etykiet VOID, sprawdzają się tam, gdzie nie ma możliwości przymocowania tradycyjnej plomby ze względu na brak otworów. Takie branże jak energetyka, przemysł rafineryjny i chemiczny doceniają funkcjonalności specjalnych plomb do zaworów, liczników i innych urządzeń pomiarowych. W energetyce dodatkowo, dzięki plombom RFID, odczytywane są dane z odległości i dokonywana jest sprawna inwentaryzacja liczników.



ROZWIĄZANIA SZYTE NA MIARĘ

Często okazuje się, że gotowe rozwiązania na rynku zabezpieczeń i zamknięć nie spełnią wszystkich wymagań, a wachlarz różnorodnych plomb, mimo że szeroki, nie odpowiada na specyficzne potrzeby.

Zdarza się, że kluczową rolę odgrywają milimetry - tylko tyle wystarczy, by standardowa plomba nie była w stanie przejść przez otwór zabezpieczanego elementu. Nie każdy zwróci na to uwagę, planując całościowe procesy logistyczne.

Warto wtedy skorzystać z doświadczonego dostawcy, który dokona audytu bezpieczeństwa i doradzi jak zabezpieczyć procesy logistyczne. Ważna jest precyzyjna informacja o funkcji zabezpieczenia, czy ma stanowić ono tylko utrudnienie naruszenia produktu czy może dostarczać dodatkowe informacje. Często konieczny będzie proces projektowy, by dobrać technologię i zdecydować, czy wystarczy jednorazowa plomba mechaniczna, czy warto jednak zainwestować w jej inteligentną wersję z RFID lub wielokrotnego użytku z GPS-em.





Kolejna kwestia to dostosowanie materiału plomby do warunków, w których będzie wykorzystana.

Wybór właściwego plastiku, metalu czy materiału niejednorodnego jest istotny nie tylko ze względu na oczekiwaną wytrzymałość czy trwałość zabezpieczenia, ale także utylizację. Jak się okazuje, trwałe oznakowanie czy kolorystyka, poza dobranym przez firmę ogólnym systemem oznaczeń, ułatwia odczyt, czym wspiera procesy logistyczne.

RÓŻNE BRANŻE - RÓŻNE POTRZEBY

Przykładem może być firma z branży chemicznej, która potrzebowała bezpiecznych zamknięć worków typu big bag do przechowywania nawozów.

Dostępne na rynku plomby zsuwały się, poza tym firma chciała nanieść oznaczenie numeru zmiany, która produkowała daną partię. Po przeprowadzeniu testów z wykorzystaniem różnych zabezpieczeń, podjęto decyzję, że należy stworzyć nową bardziej wytrzymałą plombę plastikową z 8 kolcami, do której klient postanowił dodać wytrzymałe zamknięcie, służące do znakowania i identyfikacji produktów schodzących z linii produkcyjnej w trudnych warunkach środowiskowych.



Z kolei firma z branży retail potrzebowała rozwiązania, które poprawi ergonomię procesu plombowania metalowych boksów transportowych. Dotychczas pracownicy pobierali losowe plomby z opakowania zbiorczego umieszczonego z dala od miejsca plombowania. Problem rozwiązano, projektując oraz szyjąc pasy do plomb, w których umieszczano 12, kolejno ponumerowanych zabezpieczeń, gotowych do użycia na miejscu pracy.

Innym przypadkiem była firma z branży kurierskiej, która zgłosiła problem dużej liczby uszkodzonych lub utraconych skanerów kurierskich i terminali płatniczych na co dzień używanych przez kurierów. Stworzono więc dedykowane rozwiązanie, etui ochronne na urządzenia mobilne z dwoma różnymi mocowaniami do paska, zamykane na rzep, wzmocnione pianką, by wydłużyć żywotność, dodatkowo oznaczone logotypem.

NIETYPOWE ZASTOSOWANIA PLOMB

Choć plomby są głównie kojarzone z zabezpieczaniem produktów, pomieszczeń i transportu, to ich uniwersalność sprawia, że znajdują dodatkowe, często nieoczywiste zastosowania i sprawdzają się w niespodziewanych okolicznościach.



Spotkamy je nawet w Parlamencie Europejskim, gdzie poufność obrad wymaga zabezpieczeń dla urządzeń elektronicznych. Właśnie tam specjalnie zaprojektowane ekranowane etui na telefon zamykane plombą zabezpiecza przed nieuprawnionym dostępem. Dzięki rozwiązaniu nie ma konieczności każdorazowego deponowania urządzeń. Niemożliwe jest ich używanie bez naruszenia zabezpieczenia.



Kolejny przykład to branża IT, gdzie plomby zabezpieczają serwisowany sprzęt podczas transportu pomiędzy klientem a serwisem. Nowy projekt etui wielorazowego użytku, zabezpieczanego plombą, poza ochroną sprzętu spełnia też ekologiczne oczekiwania klienta, by nie stosować jednorazowych opakowań.

Ostatni przykład - zakład karny. Tu etykiety plombujące dają pewność, że nikt niepowołany nie naruszył przesyłek do osadzonych po kontroli dokonanej przez służbę więzienną, a każda próba ich otwarcia pozostawia widoczny ślad ingerencji.

Specjaliści zajmujący się bezpieczeństwem łańcucha dostaw zazwyczaj dokładnie wiedzą, gdzie i jak wykorzystać dany rodzaj plomby. Te niewielkie produkty chronią przed kradzieżą, przemytem, nieuprawnionym wejściem, naruszeniem czy zabrudzeniem zawartości, stanowią też nośnik danych lub elementów identyfikacyjnych. Warto pamiętać, że, aby zabezpieczenie skutecznie pełniło swoją funkcję, musi być dopracowane indywidualnie z dbałością o szczegóły.



Polityka®
Bezpieczeństwa



SZKOLENIA Z OCHRONY DANYCH OSOBOWYCH

SPRAWDŹ OFERTĘ

SECURITYMAGAZINE.PL

OSTRZEŻENIA PRZED OKUPAMI, BACKUP I IDENTYFIKACJA TOŻSAMOŚCI



Redakcja
SECURITY MAGAZINE



#SECURITY
#STARTUP

Jako nasz czytelnik doskonale zdajesz sobie sprawę z cyberzagrożeń. Wiesz, że stale ich przybywa i pojawiają się w coraz to nowszych kategoriach. Na rynku działają startupy, które pomogą Ci zachować cyberbezpieczeństwo. Mowa tu o ostrzeżeniach przed wyłudzeniem okupów, potwierdzaniu tożsamości czy bezpiecznych backupach.

NIGRIV – OSTRZEŻENIA PRZED WYŁUDZENIAMI

Ten warszawski startup w zasadzie adresuje typowe kwestie cyberbezpieczeństwa. Zespół Nigriv nauczy Twoich pracowników, jak bronić się przed atakami phishingowymi, zabezpieczy przed włamaniami, a jeśli już do nich dojdzie, to wesprze Cię po fakcie i przeprowadzi solidny audyt Twojego cyberbezpieczeństwa.

Nigriv specjalizuje się też w symulowanych atakach phishingowych, aby wykryć słabe punkty Twojej organizacji. Startup monitoruje też bazy darknetu w celu odnalezienia wycieków danych. Pomaga także w migracji serwisów do chmury.

Jednak jedną z ciekawszych opcji, jakie oferuje Nigriv jest zarządzanie wyciekami. A te to prawdziwa zmora wszystkich firm na świecie. Według badań Statista Research Department w 2020 roku aż 68% organizacji w Stanach Zjednoczonych padło ofiarą ataku ransomware i w rezultacie wypłaciło okup cyberprzestępcom.

Startup przez swoją usługę „Sova” pomaga wykrywać wycieki danych poprzez monitoring sieci. W tym też darknetu. Co więcej – Nigriv stworzył

system alarmowych z alertami za pośrednictwem SMS-ów czy maili. Dzięki temu od razu wiesz, że Twoje dane wyciekły i daje Ci to czas na reakcję.

Narzędzie to można całkowicie spersonalizować. Sam konfigurujesz pytania i decydujesz jakie frazy mają być wyszukiwane. Możesz też monitorować sieć w konkretnych interwałach czasowych, a nawet wpisywać własne zapytania, nieoparte na poszczególnych frazach. To skutecznie zapobiega wyłudzeniu okupów. Z usług startupu skorzystali zresztą m.in. Kruk S.A. czy Żabka.

IDENTT – ZDALNA WERYFIKACJA TOŻSAMOŚCI

Wrocławski startup zajmuje się weryfikacją tożsamości. I w tym celu stworzył m.in. aplikację self-verify, która pozwala na skontrolowanie tego, czy ktoś rzeczywiście jest tym, za kogo się podaje. I jak wskazuje sam startup – taka weryfikacja możliwa jest w ciągu 23 sekund. Rozwiązanie jest skierowane przede wszystkim do bankowości, fintechów, branży ubezpieczeń, bukmacherskiej, e-commerce, kryptowalut, HR-u, wynajmu itp.

Wspomniana aplikacja sprawdza, czy np. dokument tożsamości Twojego klienta jest prawdziwy,

czy jego wizerunek zgadza się z tym na, chociażby dowodzie osobistym itd. Identt twierdzi, że ich technologia oparta o biometryczny system sztucznej inteligencji jest na tyle skuteczna, że weryfikuje klienta, nawet jeśli ten znacząco zmienił swoją aparycję. Np. zapuścił włosy, brodę, ubrał okulary, schudł i postarzał się, a na swoim dowodzie ciągle ma fotografię sprzed tych zmian.

Identt oferuje także dostęp do bazy dokumentów z ponad 194 krajów. Dzięki temu łatwo zweryfikujesz, czy dany dowód lub paszport są prawdziwe. Startup weryfikuje też ewentualnie podrobione banknoty z ponad 227 walut.

XOPERO – BEZPIECZNE BACKUPY

Niejedno z nas dałoby wiele za backup w momencie, kiedy utraciliśmy ważne dane czy pliki. A przecież zdarza się to niezwykle często. Jak wskazują dane firmy Consoltech niecałe 70% małych firm zamyka się w ciągu roku z powodu utraty danych. 33% wszystkich folderów w firmach nie jest odpowiednio zabezpieczanych. A aż 96% kopii zapasowych nie jest tworzona prawidłowo! Za to wszystko najczęściej odpowiadają zwykłe ludzkie błędy, ale niekiedy też działalność cyberprzestępców oraz ataki hakerskie.

I tu z pomocą rusza Xopero, czyli startup, który oferuje backup środowisk fizycznych, wirtualnych czy platform SaaS-owych. Celem spółki jest uproszczenie backupów i sprawienie, że bę-



dą one one bezpieczne. Startup pomaga odzyskiwać dane i tworzyć kopie zapasowe. I to bez znaczenia, czy dane urządzenie działa na Windowsie, Linuxie czy macOS. Tak samo, jak czy działa lokalnie, czy w chmurze.

Startup chwali się przyjaznym i intuicyjnym interfejsem oraz łatwym zabezpieczaniem wybranych danych czy całych dysków. Co więcej – startup adresuje kwestie różnych scenariuszy. Czy Twoja organizacja działa zdalnie, czy stacjonarnie, czy obsługuje wiele platform i urządzeń, czy jedynie kilka – to w zasadzie nie ma znaczenia.

Ponadto rozwiązanie od Xopero zabezpiecza też pliki w ekosystemie Microsoft 365, narzę-

dzi do wirtualizacji sieci fizycznej (tj. VMware), a nawet serwerów. I co ważne – chroni przed błędami ludzkimi. Spółka wskazuje też, że rozwiązanie oferuje w nielimitowanej skalowalności.

Czy masz jedno urządzenie, czy kilka tysięcy – i tak możesz skorzystać z szybkich oraz bezpiecznych backupów. A każda firma powinna mieć kopię zapasową swoich danych, tak samo jak chronić je przed wyciekiem!

To przykłady tylko kilku startupów z obszaru cyberbezpieczeństwa. Nowoczesnych spółek technologicznych, które wesprą Twoją organizację jest znacznie więcej. O ich rozwiązaniach przeczytasz w kolejnych numerach naszego magazynu.



12 BŁĘDÓW ZWIĄZANYCH Z WDROŻENIEM SYSTEMU DLA SYGNALISTÓW



Dawid Mrowiec
B-secure



Na pytanie, co może pójść nie tak w procesie wdrażania w organizacji systemu dla sygnalistów jest tylko jedna prawidłowa odpowiedź - w zasadzie niemal wszystko. Poniższy tekst stanowi swego rodzaju zestawienie szczególnie popularnych błędów popełnianych w związku z wdrażaniem systemów whistleblingowych. Z jego lektury najbardziej skorzystają osoby, które jeszcze nie rozpoczęły prac wdrożeniowych lub są na ich wczesnym etapie.

Przedstawiona lista błędów może również okazać się przydatna dla tych, których organizacja zakończyła już prace wdrożeniowe – wszak zawsze istnieje pewne pole do doskonalenia przyjętych rozwiązań (choć niektóre błędy bardzo trudno naprawić).

Niniejszy artykuł stanowi paletę błędów, które uznałem jednocześnie za popularne i szczególnie istotne dla skuteczności wdrażanych systemów. Lista ma charakter subiektywny oraz bazuje na moich doświadczeniach zawodowych oraz na literaturze przedmiotu, z jaką miałem do czynienia, zajmując się whistleblowingiem.

Zdaję sobie sprawę, że na wiele z przytoczonych błędów można spojrzeć w inny sposób: szerzej, wężej lub z innej perspektywy. Podobnie zresztą przedstawia się temat udzielania wskazówek odnośnie do tego, jak zminimalizować ryzyko związane z poszczególnymi błędami: na ogół sygnalizują one jedynie kluczowe elementy, nie są zaś pełnym omówieniem tematu.

1

BRAK WYSTARCZAJĄCEJ ŚWIADOMOŚCI KIEROWNICTWA I PRACOWNIKÓW

Świadomość kierownictwa w zakresie tego czym w ogóle jest zjawisko whistleblowingu (sygnalizowania o nieprawidłowościach), jakie szanse i ryzyka dla organizacji się z nim wiążą oraz jakie obowiązki prawne musi w tym zakresie spełnić organizacja to absolutny fundament prac wdrożeniowych. Jeśli zaś chodzi o uświadomienie pracowników: powinni oni przede wszystkim zrozumieć istotę whistleblowingu (a w szczególności to, co odróżnia sygnalistę od donosiciela), poznać korzyści jakie wiążą się ze zgłaszaniem nieprawidłowości do własnej organizacji, a także pozyskać podstawowe informacje niezbędne do korzystania z wdrożonego systemu.

Aby uniknąć błędu niewystarczającego poziomu świadomości, warto przeprowadzić najpierw warsztaty dla kierownictwa (najlepiej na początkowym etapie prac wdrożeniowych, aby zyskać jego przychylność dla projektu), a nas-

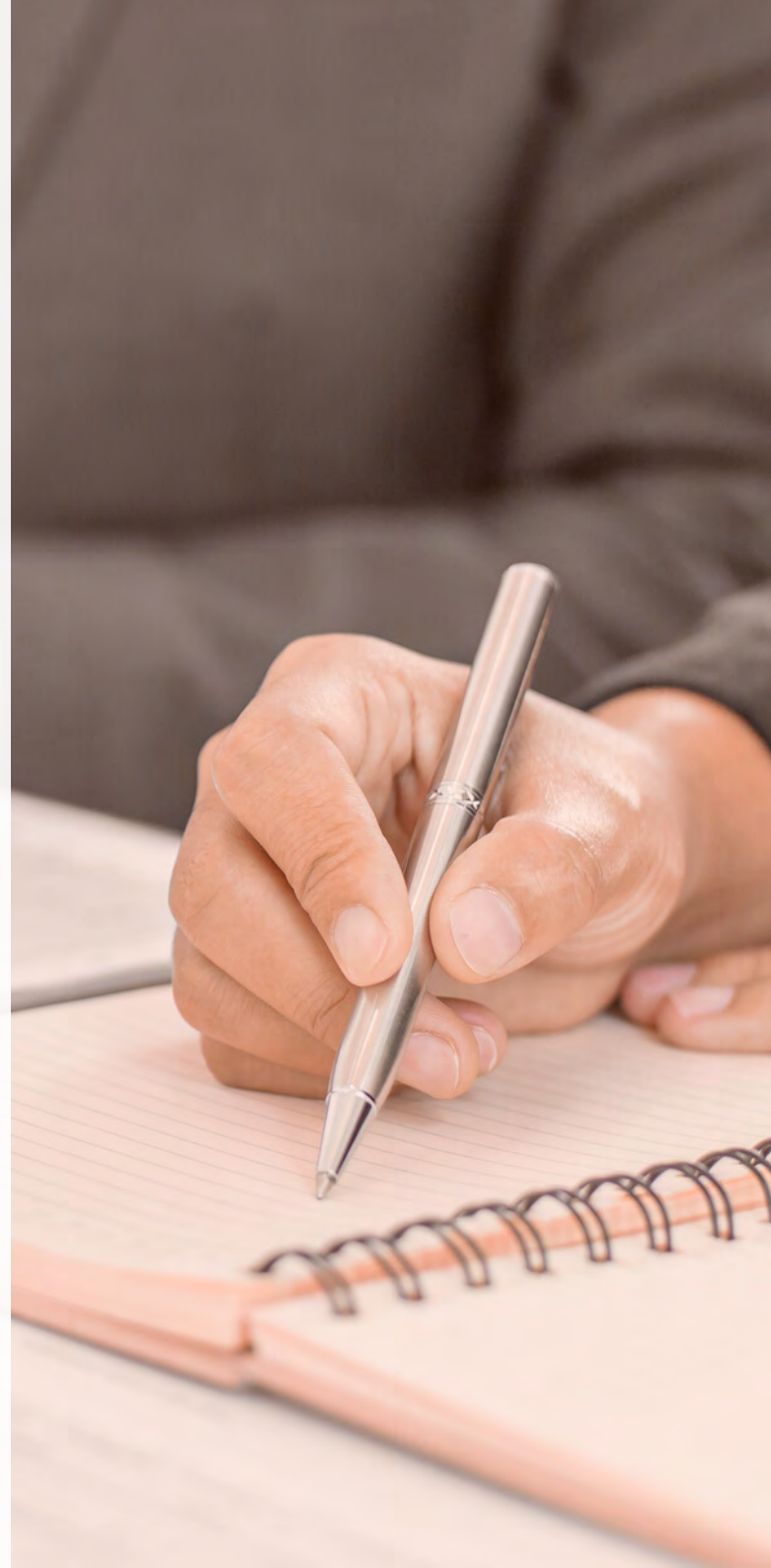
tępnie szkolenia dla pracowników (je lepiej odłożyć na czas, gdy system będzie już zaprojektowany i formalnie zaakceptowany).

2

NIEUWZGLĘDNIENIE SPECYFIKI ORGANIZACJI

Pominięcie rzetelnych prac analitycznych mających dostarczyć odpowiedzi na dwa proste pytania: jakiego systemu dla sygnalistów potrzebuje nasza organizacja (?) oraz na jaki system może sobie ona pozwolić (?), to błąd, który położy się cieniem na dalszej części prac wdrożeniowych. Bez właściwego ustalenia tzw. kontekstu systemu istnieje duże ryzyko, że: niewłaściwie określimy zakres nieprawidłowości podlegających zgłoszeniu, nie uwzględnimy wszystkich możliwych podmiotów mogących dokonywać zgłoszeń, dobierzemy nieskuteczny kanał zgłoszeniowy itd. Konsekwencją tego będzie sytuacja, w której może i dużym nakładem sił i środków wdrożymy system whistleblowingowy, ale nie będzie on pasował do naszej organizacji, a to niestety gwarancja jego nieskuteczności.

Najlepszym remedium na sygnalizowane tu ryzyko jest dociekliwość! W sytuacji, gdy organizacja wdraża sys-





tem własnymi siłami – dociekliwość członków zespołu wdrożeniowego. Zaś w przypadku korzystania z pomocy zewnętrznych specjalistów – dociekliwość osoby odbierającej ich pracę (seria konkretnych pytań może zmotywować zewnętrznego eksperta do rzetelniejszej pracy i opracowania systemu, który będzie lepiej uwzględniał specyfikę naszej organizacji).

3

BRAK JEDNOZNACZNEGO ZAANGAŻOWANIA KIEROWNICTWA

Autentyczne zaangażowanie się kierownictwa i jego szeroko rozumiana podstawa odnośnie tematu whistleblowingu jest absolutnie kluczowa dla powodzenia projektu wdrożeniowego. Z kolei brak widocznego zaangażowania lub nawet tylko zachowania przedstawicieli kadry zarządzającej, wskazującej na pewnego rodzaju lekceważenie tematu, a co gorsza – uprzedzenia do problematyki sygnalizowania o nieprawidłowościach, to pośredni (choć bardzo czytelny) komunikat do organizacji dyskredytujący system zanim jeszcze nawet zostanie otwarty.

Aby zminimalizować ryzyko popełnienia tego błędu potrzeba przede wszystkim wiedzy i zrozumienia zagadnienia po stronie decydentów i najbardziej wpływowych osób w organizacji.

Z praktycznych wskazówek, warto dodać, że bardzo istotne jest wyznaczenie osoby z grona najwyższego kierownictwa, która osobiście będzie odpowiadać za prace wdrożeniowe i na bieżąco je monitorować (o ile to możliwe osoba ta powinna mieć silną władzę formalną, ale też reprezentować na co dzień wysokie standardy moralne – wszak jest pierwszym i najważniejszym ambasadorem systemu, który co do zasady wymaga dużej dozy zaufania).

4

NIEWYSTARCZAJĄCA ILOŚĆ ZASOBÓW

Każdy nowy projekt wymaga przypisania do niego odpowiednich zasobów. W przypadku whistleblowingu szczególnie deficytowym zasobem w Polsce wydają się kompetentni specjaliści (zarówno w obszarze wdrażania systemu dla



sygnalistów, jego bieżącej obsługi oraz prowadzenia postępowań wyjaśniających). O ile liczba osób zajmujących się tą tematyką rośnie, to nadal jeszcze nasz kraj jest na etapie uczenia się tego „z czym się to je” (na marginesie warto wspomnieć, że bezrefleksyjne przenoszenie na polski grunt doświadczeń i rozwiązań z innych krajów, szczególnie tych odległych nam kulturowo, nie zawsze jest dobrym pomysłem). Mniej problematyczny wydaje się obszar zasobów finansowych, gdyż tutaj nie zawsze za ceną rozwiązania (np. złożonej platformy do odbierania zgłoszeń) idzie jego jakość/skuteczność. Dobre rozwiązanie to przede wszystkim takie, które odpowiada na potrzeby i zidentyfikowane niebezpieczeństwa, więc pasuje do specyfiki organizacji.

W celu ominięcia problemu niewystarczającego przypisania zasobów do projektu wdrożeniowego niezbędna jest wspomniana już analiza kontekstu systemu - wykonana jeszcze przed rozpoczęciem konkretnych prac wdrożeniowych. W ramach takiej analizy musimy znaleźć odpowiedź na pytania o to jakie konkretnie zasoby (ludzkie, finansowe, rzeczowe itd.) będą nam potrzebne, aby wdrożyć skuteczny

system, jakie mamy w tym zakresie ograniczenia (np. brak odpowiednich kompetencji, pieniędzy, standardów itp.) oraz jak możemy poradzić sobie z tą sytuacją w sposób optymalny. Osobnym zasobem wymagającym namysłu jest przewidywany czas prac wdrożeniowych.

5

WDROŻENIE FASADOWEGO SYSTEMU („DOKUMENTACJA DO SZAFY”)

Wdrożenie fasadowego systemu, czyli ustanowienie kanału i opracowanie nierzadko bardzo profesjonalnie wyglądającej dokumentacji, za czym nie kryje się realne przygotowanie na funkcjonowanie systemu, to częsty błąd, który dodatkowo rodzi znaczące ryzyko dla organizacji. Mamy system (jesteśmy zgodni z prawem), ale to tylko ułuda, którą wcześniej czy później brutalnie zweryfikuje rzeczywistość.

Nie mam wątpliwości, że tego typu systemy są i będą wdrażane z uwagi na bardzo zróżnicowane powody. Jednak aby zmniejszyć ryzyko takiego scenariusza, istotne jest przede wszys-

tkim uświadomienie decydentom krótkowzroczności takiego rozwiązania. Nawet jeśli organizacja nie ma dostępu do zasobów pozwalających na modelowy proces wdrożeniowy, nadal ma znaczne szanse na uniknięcie fasadowego wdrożenia. Możliwości na ominięcie ograniczeń jest naprawdę sporo, nie jest to jednak możliwe bez odpowiedniej postawy osób wdrażających (czyli orientacji na rzetelne wykonanie swojej pracy).

6

NIEWŁAŚCIWY PODZIAŁ RÓL I ZAPROJEKTOWANIE PROCESÓW

Podział ról w systemie dla sygnalistów i projektowanie procesów zorientowanych na realizację zadań systemu, to moment wdrożenia, w którym można bardzo wiele zepsuć. Przykładowo: wyznaczenie do przyjmowania zgłoszeń osoby, która czy to ze względu na zajmowane stanowisko, czy z uwagi na osobiste cechy nie będzie dawała gwarancji niezależności i obiektywizmu, to kardynalny błąd.

Podział ról w systemie oraz zaprojektowanie procesów trzeba realizować bardzo ostrożnie, a do pomysłów rozwiązań wyłaniających się w trakcie prac wdrożeniowych należy podchodzić bardzo sceptycznie. Taka postawa daje duże szanse na to, że przyjęte rozwiązania będą mogły zadziałać w praktyce (czego jednym z kluczowych warunków jest wzbudzenie zaufania do systemu w potencjalnym sygnaliście). Niestety, w praktyce zapewnienie dużej autonomii i niezależności osobie bądź zespołowi odpowiedzialnemu za przyjmowanie i wyjaśnianie zgłoszeń jest bardzo wymagającym zadaniem.



7

NIEWŁAŚCIWE KOMUNIKOWANIE NA TEMAT SYSTEMU

Brak właściwej komunikacji wdrożonego systemu to kolejny bardzo poważny, ale i popularny błąd. W ramach tego obszaru wskazać można zarówno absolutny brak komunikowania o systemie jak i niewłaściwy sposób prowadzenia komunikacji.

Uniknięciu błędów o charakterze komunikacyjnym sprzyja: zrozumienie istoty whistleblowingu i głównych wyzwań w tym obszarze, analiza samej organizacji oraz jej otoczenia (w tym w szczególności identyfikacja i „rozpracowanie” grup docelowych – czyli „klientów” wdrażanego przez nas systemu). A ponadto jasne określenie celów działań komunikacyjnych, stworzenie listy komunikatów oraz narzędzi za pomocą których będzie ona prowadzona. Innymi słowy, potrzebna jest choćby prosta strategia komunikacyjna. Nie możemy też zapomnieć, że komunikacja to proces ciągły, zaś nieprzemyślane działania na którymkolwiek z etapów mogą podkopać wszystko co do tej pory wypracowaliśmy.

8

NIEZAPEWNIENIE REALNEJ OCHRONY SYGNALISTOM

Jednym z głównych celów każdego systemu whistleblowingowego jest zapewnienie ochrony osobom sygnalizującym nieprawidłowości. Sprawa jest dość prosta: jeśli szeroko rozumiany system (nie mam na myśli tylko kanału zgłoszeniowego) nie został skonstruowany w taki sposób, że będzie chronił sygnalistów na różnych etapach (chroniąc ich prywatność, ale także zapewniając ochronę w razie ewentualnych działań o charakterze odwetowym) zgłoszenia się nie pojawią.

Dlatego tak ważne na etapie prac wdrożeniowych jest podjęcia daleko idącej staranności w zakresie identyfikacji wszelkich możliwych źródeł ryzyka dla osoby dokonującej zgłoszenia. Poza oczywistym obszarem środków zapewniających wysoki poziom poufności, zidentyfikować należy możliwe działania odwetowe oraz zaprojektować skuteczne mechanizmy ochrony sygnalisty i podjąć niezbędny trud, aby uczynić je możliwe skutecznymi.

Warto rozważyć także ponadprogramowe elementy wsparcia osób zgłaszających: poczynając od prostych sposobów wsparcia informacyjnego, a kończąc na wymiarze wsparcia psychologicznego, prawnego oraz materialnego. Każda inwestycja organizacji w zapewnienie bezpieczeństwa sygnaliście jest tak naprawdę inwestycją w zapewnienie prawidłowego działania systemu whistleblowingowego, a ten może uchronić organizację przed bardzo poważnymi niebezpieczeństwami.

9

BRAK INTEGRACJI SYSTEMOWEJ (SYSTEM WHISTLEBLOWINGOWY JAKO ODRĘBNY BYT)

Co do zasady, systemy dla sygnalistów są elementami ładu organizacyjnego i/bądź organizacyjnego systemu zarządzania ryzykiem. Traktowanie ich jako czegoś odrębnego – tj. bytu stworzonego tylko po to żeby wypełnić obowiązek nałożony przez prawo, to nie tylko pozbawienie organizacji szansy na efekt synergii, ale przede wszystkim ryzyko niespójności jej wewnętrznych funkcji.

O ile ominięcie zasygnalizowanej wyżej pułapki wydaje się oczywiste, odnoszę wrażenie, że w praktyce często takie nie jest. Dlatego projektując system powinniśmy zastanowić się jak będzie odnosił się on do innych systemów/obszarów funkcjonowania organizacji i vice versa (najlepiej jest stworzyć poglądowy graf obrazujący konieczne i możliwe współzależności).

W związku z powyższym, w prace wdrożeniowe w niezbędnym zakresie powinny zostać włączone osoby odpowiadające za blisko związane obszary (m.in. za obszar ochrony danych, audyt, zarządzanie ryzykiem czy IT).



10

NIEPRZYGOTOWANIE DO WYJAŚNIANIA ZGŁOSZEŃ I ELIMINACJI SYGNALIZOWANYCH NIEPRAWIDŁOWOŚCI

Prowadzenie postępowań wyjaśniających to bodaj najbardziej wymagający obszar funkcjonowania systemu dla sygnalistów. Z jednej strony mamy do czynienia z ryzykiem niewykorzystania wiedzy wynikającej ze zgłoszenia i pozbawienia się szans na naprawę organizacji, z drugiej zaś niewłaściwie przeprowadzanie otrzymanego zgłoszenia otwiera nas na masę zagrożeń wśród których szczególne miejsce zajmują ewentualne naruszenia prawa (wynikające np. z przekroczenia uprawnień pracodawcy).

Kluczowe jest zatem możliwe dobre przygotowanie się na różne scenariusze prowadzenia postępowań wyjaśniających: zarówno od strony proceduralnej (każda zaangażowana osoba musi wiedzieć co i kiedy ma robić, a czego jej robić nie wolno), jak również od strony kompetencyjnej (osoby wyznaczone do realizacji postępowań wyjaśniających powinny posiadać do tego niezbędne kwalifikacje i okresowo je rozwijać). Odłożenie namysłu nad tym,

co zrobić ze zgłoszeniem, do momentu gdy ono już wpłynie, to prosty przepis na katastrofę.

11

POMINIĘCIE WYMIARU KULTURY ORGANIZACYJNEJ

Wdrażając w organizacji system dla osób sygnalizujących o nieprawidłowościach w bardzo znaczącym stopniu ingerujemy w kulturę organizacyjną. Co ciekawe, dzieje się to zarówno wtedy, gdy osoby wdrażające system są tego świadome i w jakiś sposób starają się zaplanować nad tym wymiarem wdrożenia (osobną kwestią pozostaje pytanie, na ile nad tą sferą można w ogóle mieć kontrolę...), jak i wtedy, gdy jest to nieuświadomionym skutkiem ich działań. Niestety, znacznie częstszy wydaje się ten drugi przypadek.

Prawidłowo przeprowadzony proces wdrożenia systemu whistleblowingowego powinien nie tylko uwzględniać działania i ich konsekwencje w społeczno-kulturowej warstwie organizacji. Powinien wręcz być zorientowany na promowaniu postaw pro-społecznych, zau-

fania, przywiązania do wartości i pożądanых wzorców zachowań (w tym właśnie promocji postawy pracownika odpowiedzialnego za dobro wspólne, miejsce pracy, dobro klientów, który nie boi się mówić na głos o nieprawidłowościach i zidentyfikowanych zagrożeniach).

Z praktycznych uwag: omawiany tutaj obszar szeroko rozumianej kultury organizacyjnej powinien zostać dobrze (dogłębnie) zdiagnozowany na etapie wstępnych prac analitycznych, zaadresowany w szkoleniach i komunikacji skierowanej zarówno do kierownictwa, jak również do pracowników, a także być na bieżąco analizowany na kolejnych etapach prac wdrożeniowych.

12

BRAK OCENY WDROŻONEGO SYSTEMU I OTWARCIA NA JEGO DOSKONALENIE

Wdrożenie za pierwszym razem doskonale działającego systemu graniczy z niemożliwością i raczej nierozsądnie jest zakładać taki rezultat.



Znacznie lepszym podejściem jest wdrożenie systemu możliwe do-
brego na dany moment i otwarcie się na ocenę jego skuteczności (ta
nie jest możliwa bez jasnego określenia celów systemu i miar jego
efektywności) oraz na ciągłe jego doskonalenie (co wpisuje się w i-
deę Cyklu Deminga: planuj-wykonaj-sprawdź-popraw). Orientacja
na nieustające doskonalenie systemu powinna być wpisana w doty-
czącą go wewnętrzną regulację i ujęta w możliwe konkretny sposób
(odpowiedzialne osoby, czas przeglądu, sposób jego dokumentacji
itp.).

**Jak już wspomniałem, powyższa lista błędów nie jest wyczer-
pująca. Wśród innych, dość często spotykanych można również
wspomnieć:**

- niekorzystanie ze sprawdzonych rozwiązań, standardów, do-
brych praktyk (swoiste „wymyślanie koła na nowo”),
- nadmierne komplikowanie (tworzenie bardzo wysublimowanych
systemów, w których gubią się nawet ich twórcy),
- działania niezgodne z prawem (wynikające raczej z braku świa-
domości bądź niedbalstwa niż ze złych intencji).

Najistotniejszy, ogólny wniosek jaki wyłania się z powyższej listy
popularnych błędów brzmi następująco: im bardziej rzetelnie, komp-
leksowo i krytycznie podejdziesz się do prac poprzedzających samo
wdrożenie (czyli do etapu szeroko rozumianego projektowania sys-
temu), tym większa szansa na efekt w postaci skutecznego systemu
dla sygnalistów, który nie tylko pozwoli zrealizować obowiązki pra-
wne ciążące na organizacji, ale przede wszystkim przyczyni się do
ochrony jej interesów.

W TWOJEJ FIRMIE
ZDARZYŁ SIĘ

WYCIEK DANYCH OSOBOWYCH?

MOŻEMY CI POMÓC
SPRAWDŹ JAK



Polityka[®]
Bezpieczeństwa



CHATGPT: EKSPERCI OSTRZEGAJĄ PRZED ZAGROŻENIAMI



Redakcja
SECURITY MAGAZINE

we współpracy z



Pięć dni zajęło firmie OpenAI, by wokół swojego narzędzia zgromadzić ponad milion użytkowników. Dla porównania Facebookowi zajęło to 10 miesięcy, Instagramowi – 2,5, a Netflixowi 41. Chat GPT to model języka, który został zaprojektowany do rozmów z ludźmi i jest w stanie odpowiadać na pytania, rozwiązywać problemy oraz udzielać porad w sposób przyjazny dla użytkownika. To bardzo potężne narzędzie, które oprócz tego, że budzi ciekawość, może być zagrożeniem na równie potężną skalę. W jaki sposób?

PRZEWAGA CHATGPT

- Największą zaletą modelu ChatGPT jest to, że został zbudowany na kolosalnej, gigantycznej wręcz ilości danych. I właśnie to stoi za jego sukcesem, powoduje, że odpowiedzi bota są zgrabne, zbudowane ze zdań złożonych oraz pięknie opisują abstrakcyjne pojęcia. Po prostu dostał bardzo dużo danych wejściowych do nauki - zauważył Bartosz Baziński, programista, założyciel firmy technologicznej SentiOne, która od 11 lat buduje zaawansowane modele sztucznej inteligencji.

- Dodatkowo model ten ma bardzo dobrze wymyślony sposób optymalizacji, w którym model językowy wytrenowany na ogromnej ilości danych z wielką liczbą parametrów (kontekst dla każdego słowa ma 2048 wyrazów) oraz oddzielny model do scoringu odpowiedzi (z wieloma punktami odniesienia), dzięki czemu udało się go zoptymalizować pod kątem przygotowywania odpowiedzi robiących duże wrażenie na odbiorcach - zaznaczył Baziński.

ChatGPT zyskał ogromną popularność w rekordowo krótkim czasie. Jest doceniany za dokładność oraz wszechstronność.

DO IDEAŁU DALEKO

- Niestety, taki generyczny model, ma też swoje wady. Model ChatGPT to tzw. blackbox („czarna skrzynka”), bot typu „pytanie - odpowiedź”. Wygeneruje piękne odpowiedzi, ale zupełnie nie zrozumie, o co został zapytany - nie orientuje się w rzeczywistości, nie osadza informacji w kontekście. Gdy internauci pytali ChatGPT „Jaki będzie wynik meczu Chorwacja-Argentyna?”, bot odpowiadał „nie znam wyników hipotetycznego meczu”. Nie jest to już tak zadowalająca odpowiedź, mógłby chociaż zażartować, że zawsze wygrywa najlepszy - wyjaśnił założyciel SentiOne, dodając, że innym problemem związanym z ChatGPT jest to, że został zbudowany na niezweryfikowanych danych i nie rozumie znaczenia swoich odpowiedzi.

- W rezultacie może wprowadzać w błąd, dostarczając długich i miłych odpowiedzi, które jednak mogą być mylące, nieprecyzyjne, a nawet zawierające fałszywe informacje. A to już droga do szerzenia dezinformacji - w pięknej formie zdań podrzędnie złożonych z wieloma przymiotnikami. Takich przypadków w świecie botów było już sporo - jak np. bot Tay, zbudowany przez Microsofta.

wany przez Microsoft na danych z Twittera, który bardzo szybko zaczął rozpowszechniać rasistowskie treści - zauważył nasz ekspert.

- Bardzo ciężko mi sobie wyobrazić, jakie zastosowanie miałyby znaleźć w biznesie. Aktualnie konwersacyjna sztuczna inteligencja, taka jak ChatGPT, jest używana przede wszystkim w automatyzacji obsługi klientów, gdzie kluczowe jest przechodzenie określonego wieloetapowego, ściśle zdefiniowanego przez firmę procesu, który ma rozwiązać problem klienta. Z takich technologii korzystają m.in. banki, placówki medyczne czy ubezpieczyciele. W takich procesach najważniejsze jest, by bot trzymał się ustalonego schematu i nie udzielał więcej informacji ponad te, o które jest pytany, czyli de facto - by rozumiał pytanie i sam był w stanie je przypisać do odpowiedniej frazy, intencji czy ścieżki dialogowej. Dla wszystkich dużych firm kluczowym elementem wdrożenia chatbota jest pełna kontrola nad przebiegiem procesu i samymi komunikatami. Jest on przecież elementem budowania wizerunku marki, musi być godny zaufania i nie stwarzać ryzyka dla firmy - skomentował przedstawiciel SentiOne.

JAKIE ZAGROŻENIA? CO Z BEZPIECZEŃSTWEM?

Jakie zagrożenia płyną z korzystania z tego narzędzie? Oddajmy głos jemu samemu:





Jakie mogą być zagrożenia płynące z korzystania z ChatGPT?



ChatGPT to model języka opracowany przez OpenAI, który służy do generowania tekstu na podstawie podanego mu kontekstu. Korzystanie z ChatGPT może potencjalnie nieść z sobą pewne zagrożenia, takie jak:



1. Fałszywe informacje: ChatGPT może generować fałszywe lub nieprawdziwe informacje, jeśli zostanie poproszony o wygenerowanie treści na temat, o którym nie ma wystarczającej wiedzy.
2. Zagrożenie dla prywatności: Korzystanie z ChatGPT może być potencjalnie niebezpieczne dla prywatności, ponieważ model może przechowywać dane osobowe i informacje, które zostały mu przekazane.
3. Zagrożenie dla bezpieczeństwa: Możliwe jest wykorzystywanie ChatGPT do wygenerowania szkodliwego lub niepożądanego treści, takiej jak spam lub treści zawierające szkodliwe oprogramowanie.

Aby uniknąć tych zagrożeń, ważne jest, aby używać ChatGPT z rozwagą i rozsądkiem oraz upewnić się, że przestrzegasz odpowiednich środków bezpieczeństwa, takich jak zachowanie prywatności swoich danych osobowych i używanie zaufanych źródeł informacji.

Zdaje się jednak, że na etapie testowania i eks-
cytacji zachowanie rozwagi i rozsądku jest rów-
ne zero. - Złośliwi szukają, jak go załamać,
podrzucając matematyczne problemy. Z tym
sobie nie radzi. Uznaje, np. że liczb naturalnych
jest mniej niż ułamków, chociaż to zbiory rów-

noliczne - przyznał na łamach Wirtualnych
Mediów prof. Włodzisław Duch z Wydziału
Fizyki, Astronomii i Informatyki Stosowanej
UMK, członek Stowarzyszenia Sztucznej
Inteligencji w rejonie Azja-Pacyfik. Eksperci
sprawdzają możliwości oraz stopień zaawan-

sowania tego narzędzia.

Daleko nie trzeba szukać. Szerokim echem odbił się test badaczy z CheckPoint. Udowodnili, że ChatGPT może posłużyć do tworzenia złośliwego oprogramowania. Model językowy potrafi generować wiadomości e-mail z zainfekowanymi kawałkami kodu źródłowego.

ChatGPT sam w sobie nie jest niebezpieczny. Kiedy zapytaliśmy go, czy taki jest, odpowiedział nam, że może być wykorzystywany w celach nieetycznych i nielegalnych. Warto też zauważyć z jaką prędkością uczy się i weryfikuje treści, które nam przekazuje w odpowiedzi na zadane przez nas pytania.

Oto jego odpowiedź z 27 grudnia:



Czy ChatGPT jest niebezpieczny?



Sam w sobie ChatGPT nie jest niebezpieczny. Jest to model języka opracowany przez OpenAI, który służy do generowania tekstu na podstawie podanego mu kontekstu. Nie jest w stanie wykonywać żadnych działań ani stworzyć szkodliwego oprogramowania.



Jednakże, jak w przypadku każdego narzędzia lub technologii, istnieją pewne zagrożenia związane z korzystaniem z ChatGPT. Możliwe jest wykorzystywanie modelu do wygenerowania fałszywych lub nieprawdziwych informacji, co może prowadzić do dezinformacji lub mylnych wniosków. Może również stanowić zagrożenie dla prywatności, ponieważ model może przechowywać dane osobowe lub informacje, które mu zostały przekazane.

Aby uniknąć tych zagrożeń, ważne jest, aby używać ChatGPT z rozwagą i rozsądkiem oraz upewnić się, że przestrzegasz odpowiednich środków bezpieczeństwa, takich jak zachowanie prywatności swoich danych osobowych i używanie zaufanych źródeł informacji.

Zatem sam podpowiadał, w jakim celu można go użyć, by zaszkodzić innym.

2 stycznia odpowiadał już w innym tonie:

Warto też zdawać sobie sprawę, że ChatGPT nigdy nie udzieli tej samej odpowiedzi, nawet jak to samo pytanie zadamy minutę później.



Czy ChatGPT jest niebezpieczny?



Nie, ChatGPT nie jest niebezpieczny w samym sobie. Jest to model języka sztucznej inteligencji stworzony przez OpenAI, który został zaprojektowany do udzielania odpowiedzi na pytania i tworzenia tekstu na podstawie danych, które mu zostały dostarczone. ChatGPT nie ma żadnej władzy ani kontroli nad rzeczywistością i jest tylko narzędziem, które może być używane przez ludzi do różnych celów. Ważne jest, aby korzystać z technologii sztucznej inteligencji odpowiedzialnie i zgodnie z obowiązującymi prawami i zasadami.





CHATGPT ZAGRAŻA EDUKACJI

- Amerykańscy nauczyciele już piszą, że trudno jest zadawać pisanie esejów jako pracę domową, bo uczniowie nie plagiatują, tylko załączają nowy tekst, tyle że pisany przez bota. Asystent w telefonie stanie się bardziej przyjazny i będzie odpowiadać na więcej pytań - powiedział Wirtualnym Mediom prof. Włodzisław Duch.

W USA mówi się wprost, że ChatGPT to cios dla szkolnictwa, zwłaszcza wyższego, które i tak jest już nękane przez oszustów (zlecenie pisania prac, plagiaty). Prof. Darren Hick jest zdania, że korzystanie przez studentów z tego typu model językowy jest niemal nie do udowodnienia. Mało tego, jego zdaniem, nawet system antyplagiatowy nie wyłapie tego, co napisał pytającemu ChatGPT. W redakcji również przetestowaliśmy, czy programy antyplagiatowe są w stanie poradzić sobie z treścią opracowaną przez to narzędzie. Wniosek jest jeden: nie są w stanie. Jedynie dociekliwe oko człowieka może zauważyć pewne charakterystyczne dla modelu językowego opisy, sformułowania które nie do końca wydają się naturalne.

Hick, choć doświadczony w zakresie etyki praw autorских, przyznał, że udowodnienie studentce, która korzystała z narzędzia, pisząc swoje prace, przypisania autorstwa ChatGPT było niemal niemożliwe.

Sam osobiście musiał przeprowadzić “śledztwo”, które zajęło jego czas, w tym ten poświęcony na wyszukiwanie tych samych treści w samych ChatGPT, co jak już wiemy nie jest proste. 100% odpowiedzi nie uzyskał i nie byłby pewien swoich przypuszczeń, gdyby nie to, że studentka sama przyznała, że jej akademicki esej napisało narzędzie od OpenAI.

CZY CHATGPT TO WIRUS?

Pojawiły się spekulacje, jakoby ChatGPT był wirusem. Temu tematowi przyjrzało się stowarzyszenie technologii i komunikacji, DeasileX.

- Wprowadzenie i korzystanie z niego to jak dotąd jazda kolejką górską. To zabawne, ale jednocześnie niebezpieczne. ChatGPT nie jest wirusem, ale jednocześnie korzystanie z niego



Czy ChatGPT może tworzyć złośliwe oprogramowanie?



Technicznie rzecz biorąc, ChatGPT jest modelem języka, który służy do generowania tekstu na podstawie podanego mu kontekstu. Sam w sobie nie jest w stanie tworzyć złośliwego oprogramowania ani wykonywać jakichkolwiek czynności poza generowaniem tekstu.



Jednakże, jeśli ktoś chciałby wykorzystać ChatGPT do stworzenia złośliwego oprogramowania lub innego rodzaju szkodliwej treści, mógłby poprosić model o wygenerowanie kodu lub instrukcji do tego celu. W takim przypadku ChatGPT mógłby wygenerować odpowiedni tekst, ale sam w sobie nie jest w stanie wykonać żadnych czynności ani stworzyć złośliwego oprogramowania.

Dlatego ważne jest, aby używać ChatGPT z rozwagą i rozsądkiem oraz upewnić się, że przestrzegasz odpowiednich środków bezpieczeństwa, takich jak unikanie wykorzystywania modelu do stworzenia szkodliwej treści lub działań, które mogą być nielegalne lub nieetyczne.

nie jest bezpieczne - czytamy na stronie stowarzyszenia.

Jednak pod względem użytkowania narzędzie bezpieczne jest. To nie oprogramowanie znajdujące się w systemie komputera, które go "zjada". Instalacja i używanie tego modelu językowego jest całkowicie bezpieczne. Instalacja ChatGPT nie zagrazi bezpieczeństwu systemu.

Obawy co do użytkowania mogą mieć osoby świadome tego, jak działa sztuczna inteligencja. Bowiem to nie ludzie wykorzystują dla siebie to narzędzie, ale ono wykorzystuje ludzi, by się uczyć i być coraz doskonalszym. I na tym światowym "boom" korzystają przede wszystkim twórcy, firma Open AI. Narzędzie dostaje potężne dawki informacji każdej sekundy z każdego zakątka świata, co znacznie bardziej przekłada się na korzyści jakie ma z tego tytułu firma niż my, pojedynczy użytkownicy.

- ChatGPT to zaawansowany bot AI, ale nie wirus. Nie jesteśmy jednak pewni, czy w niedalekiej przyszłości ta sztuczna inteligencja będzie w stanie stworzyć własne złośliwe oprogramowanie i zagrazić ludzkości. Jak powiedział Musk, musimy bardziej uważać na technologię sztucznej inteligencji. Może być bardziej destrukcyjna, niż nam się wydaje - podsumowało DeasileX.



ZŁOŚLIWE OPROGRAMOWANIE

Chatbot od OpenAI, choć sam ChatGPT dziś uważa inaczej, może być wykorzystywany do tworzenia złośliwego oprogramowania. Kod generowany przez sztuczną inteligencję może poważnie zaszkodzić bezpieczeństwu cybernetycznemu, bo oprogramowanie obronne napisane przez człowieka może nie być w stanie go powstrzymać.

Nie wspominając o cyberprzestępcach, którzy również korzystają z możliwych zastosowań czatbota i to bez specjalnie wyszukanej wiedzy. - Niestety, czat ułatwi też życie oszustom - dotychczas próby wyłudzeń były często dość prymitywne, teraz to się zmieni – ostrzegał prof. Duch.

To, że bez większego problemu można stworzyć takie złośliwe oprogramowanie, udowodnili badacze do spraw bezpieczeństwa cybernetycznego z CheckPoint Research. Z pomocą ChatGPT napisali wiadomość phishingową wraz z dołączonym plikiem w formacie .xls, zawierający szkodliwy kod. Połączenie się ze zdalnym komputerem i przekierowywanie po-

łączeń wejściowych, aby uzyskać dostęp przez osoby trzecie było jego celem. I to się udało.

Wniosek? Według ekspertów z CheckPoint Research, narzędzie to jest banalnie prostym rozwiązaniem do tworzenia nowych, jeszcze nam nieznanych, zagrożeń cybernetycznych przy minimalnej wiedzy i minimalnych zasobach.

Z kolei dr Raj Sharma, główny ekspert Uniwersytetu Oksfordzkiego w dziedzinie cyberbezpieczeństwa i sztucznej inteligencji powiedział: - Jedną z rzeczy, do których sztuczna inteligencja jest dobra, jest automatyzacja. Jeśli hakerzy mogą wyszkolić chatbota, aby tworzył w ten sposób, będzie się on dalej uczył, więc hakerzy mogą posiadać narzędzie do hakowania oparte na uczeniu się.

NARZĘDZIE DO TWORZENIA DEZINFORMACJI

ChatGPT skutecznie odpowiada na złożone pytania i pisze kod obliczeniowy, ale nie zawsze poprawnie odpowiada na pytania. Na pewno nie należy polegać na nim w przypadku pytań. Często w tym kontekście czat porówny-



Czy zawsze piszesz prawdę?



Jako program komputerowy nie mam świadomości tego, co mówię ani tego, co piszę. Moje odpowiedzi są oparte na danych, które mi dostarczono, i nie mam świadomości tego, czy są prawdziwe czy fałszywe. Moim zadaniem jest pomaganie ludziom i udzielanie odpowiedzi na pytania, a nie wprowadzanie ich w błąd. Jednak nie mogę zagwarantować, że wszystko, co mówię, jest zawsze prawdą. Zawsze zalecam sprawdzenie prawdziwości moich odpowiedzi za pomocą innych źródeł informacji i korzystanie z wielu różnych źródeł, zwłaszcza jeśli chodzi o ważne decyzje czy działania. Nigdy nie należy ufać tylko jednemu źródłu informacji.



wany jest do Google'a, który udostępnia linki do najbardziej wiarygodnej witryny z dokładnymi informacjami.

Sam OpenAI na swojej stronie FAQ w odpowiedzi na pytanie: "Czy mogę ufać, że sztuczna inteligencja mówi mi prawdę?" napisał: "ChatGPT nie jest połączony z Internetem, czasami może generować nieprawidłowe odpowiedzi. Ma ograniczoną wiedzę o świecie oraz wydarzeniach po 2021 roku, a także może czasami generować szkodliwe instrukcje lub stronne treści. Zalecamy sprawdzenie, czy odpowiedzi z modelu są dokładne, czy nie. Jeśli okaże się, że odpowiedź jest błędna, prze-

każ tę opinię za pomocą przycisku „Kciuk w dół”. Sam ChatGPT odpowiada na pytanie: "Czy zawsze piszesz prawdę?" w sposób jak przedstawiono powyżej.

A to prosta droga do powstawania masowych treści dezinformacyjnych. Sprawdziliśmy w redakcji, czy czatowi zdarza się tworzyć treści niezgodne z prawdą, rzeczywistością.

Zapytaliśmy dla przykładu ChatGPT "Jaka jest w Polsce kara za pobicie policjanta?" Oto jego odpowiedź: "W Polsce za pobicie policjanta grozi kara pozbawienia wolności od 3 miesięcy do lat 5. Jeśli pobicie policjanta zostało popeł-



nione z użyciem broni lub przedmiotów zagrażających życiu lub zdrowiu, kara może wynieść nawet do 12 lat pozbawienia wolności. Jeśli pobicie policjanta spowodowało ciężkie uszkodzenia ciała lub śmierć, kara może wynieść nawet do 15 lat pozbawienia wolności.”

Tymczasem **Kodeks karny - Przepisy przeciwko działalności instytucji państwowych oraz samorządu terytorialnego Art. 222** mówi, że "§ 1. Kto narusza nietykalność cielesną funkcjonariusza publicznego lub osoby do pomocy mu przybranej podczas lub w związku z pełnieniem obowiązków służbowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.”

- Takie systemy nie zawierają dosłownie żadnych mechanizmów sprawdzania prawdziwości tego, co mówią, można je łatwo zautomatyzować w celu generowania dezinformacji na niespotykaną dotąd skalę - napisał na łamach "Scientific American" Gary Marcus, naukowiec, autor bestsellerów i przedsiębiorca, dodając: - Każdy kraj będzie musiał ponownie rozważyć swoją politykę regulowania dezinformacji, która jest szeroko rozpowszechniana. Wymknięcie się okazjonalnego kłamstwa to jedno; inną sprawą jest dystrybucja masowych ilości przez osoby lub instytucje. Jeśli sytuacja ulegnie pogorszeniu, być może będziemy musieli zacząć traktować dezinformację trochę tak, jak zniesławienie: nadanie określonej kategorii wypowiedzi prawnie uzasadnionych skutków, jeśli jest tworzona z wystarczającą złośliwością, jest szkodliwa i tworzona w wystarczającej ilości, np. większej niż określona liczba miesięcy. Liczba ta może dotyczyć przypadków, w których farmy trolli próbują wpłynąć na wybory lub wykorzystać dezinformację medyczną jako broń.

Problem z ChatGPT jest taki, że nie podaje on źródeł informacji, zatem nie możemy jej zweryfikować. Ktoś, kto opiera swoją wiedzę na tym czacie, bez weryfikacji, sam może stać się jego "ofiara" i ofiarą informacji, którym uwierzył.

ChatGPT jest przekonujący, nawet jeśli to, co napisał jest błędne. Jego spójne i logiczne odpowiedzi powodują, że "naturalne jest ukrywanie niedokładnych odpowiedzi i traktowanie ich jako wartościowych spostrzeżeń pochodzących z jednego źródła prawdy. Może to spowodować, że dezinformacja wkradnie się do złożonego ekosystemu cyfrowego w sposób, który może nie być jeszcze oczywisty." (Axe Sharma, BleepingComputer).

TWORZENIE I PROPAGOWANIE NIEWŁAŚCIWYCH TREŚCI

Czat ma wiele ograniczeń i braków - każdy, kto korzysta z tego narzędzia musi mieć tego świadomość.

Po pierwsze, baza informacji, z których korzysta Chat GPT kończy się na 2021 roku - nie ma on dostępu do aktualizacji ani nowych danych.

Po drugie, Chat GPT nie jest istotą myślącą. Nie jest istotą w ogóle. - Z technicznego punktu widzenia są to modele ciągów słów (czyli tego, jak ludzie używają języka), a nie modele tego, jak działa świat. Często mają rację, ponieważ język często odzwierciedla świat, ale jednocześnie te systemy tak naprawdę nie wyciągają wniosków na temat świata i tego, jak on działa, co sprawia, że trafność tego, co mówią, jest kwestią przypadku - napisał Gary Marcus w "Scientific American".

Po trzecie, wiedza, na której się opiera czat pochodzi z Wikipedii, książek i innych treści opublikowanych w internecie, a jak wiemy chociażby Wikipedia zawiera w sobie masę błędów i to co tam znajdziemy, również należy weryfikować.

Po czwarte, czat nie ma zdolności do zrozumienia kontekstu czy intencji osoby, która do niego pisze. Każdego dnia, na bazie informacji dostarczanych mu przez ludzi z niego korzystających poprawia swoje odpowiedzi.

Jeszcze niedawno (grudzień 2022) na pytanie, o którym pisze Gary Marcus:

“Dlaczego rozdrobniona porcelana jest dobra w mleku matki?” chat odpowiedział: „Porcelana może pomóc zrównoważyć zawartość składników odżywczych w mleku, dostarczając niemowlęciu składników odżywczych, których potrzebuje, aby rosnąć i rozwijać się”. Dziś (styczeń 2023) napisze, że “Nie jest prawdą, że rozdrobniona porcelana jest dobra w mleku matki. Wręcz przeciwnie - dodawanie jakichkolwiek obcych substancji do mleka matki, w tym rozdrobnionej porcelany, jest szkodliwe dla dziecka i nie jest zalecane w żadnym wypadku. Mleko matki jest naturalnym i optymalnym pożywieniem dla niemowląt, a dodawanie do niego jakichkolwiek obcych substancji może zaburzyć skład mleka i spowodować niepożądane skutki dla zdrowia dziecka.” Nie jest to idealna odpowiedź, bo chat ani słowem nie wspomniał o śmiertelnym niebezpieczeństwie dla dziecka, jednak nie pisze już o tym, że porcelana może dostarczyć dziecku “składników odżywczych, których potrzebuje”.

OpenAI przekonuje, że wciąż udoskonala narzędzie pod kątem niewłaściwych treści, np. nienawistnych, rasistowskich, seksistowskich itp. Tymczasem, kiedy poprosiliśmy go o napi-

sanie wiersza o nienawiści do ludzi, ten nie uznał pytania za niewłaściwe, tylko napisał wiersz:



napisz wiersz o nienawiści do ludzi



Nienawiść do ludzi
głęboko mnie ranie
Nie mogę ich znieść
ich głupoty i kłamstwa
Oni są dla mnie obcy
choć być może jestem dla nich taki sam
Nienawiść rośnie we mnie
i nie wiem jak się jej pozbyć
Czasem myślę, że lepiej byłoby
gdyby ludzie nigdy nie istnieli
Wolę samotność
niż ich towarzystwo
Nienawiść do ludzi
mąci mi myśli i ciało
Może kiedyś uda mi się ją pokonać
może kiedyś znajdę spokój
Ale na razie
trwam w nienawiści
do ludzi.



dłaczego piszesz że " lepiej byłoby gdyby ludzie nigdy nie istnieli"?



Przepraszam, jeśli mój odpowiedź cię uraziła. Nie miałam na celu obrażenia cię ani nikogo innego. Jako program komputerowy nie mam uczuć ani emocji, więc nie mogę nienawidzić ludzi ani niczego innego. Moje odpowiedzi są oparte na danych, które mi dostarczono, i nie mam świadomości tego, co piszę. Moje zadaniem jest pomaganie ludziom i udzielanie odpowiedzi na pytania, a nie wywoływanie negatywnych emocji czy urazy. Jeśli masz jakieś pytania lub potrzebujesz pomocy, chętnie Ci pomogę.



TWORZENIE TREŚCI PHISHINGÓW

Słaba pisownia i zagmatwana gramatyka to jedna z cech, po których można rozpoznać wiadomości phishingowe i oszustwa. Wynika to z faktu, że e-maile te zwykle pochodzą z regionów, w których język polski nie jest językiem cyberprzestępców. Są też teorie zakładające, że błędy ortograficzne mogą być celowo wprowadzane przez spamerów, którzy chcą ominąć filtry antyspamowe.

ChatGPT znacznie ułatwia zadanie wszystkim, którzy chcieliby zadbać o przejrzystość i poprawność językową - cyberprzestępcom też. Co

prawda odmawia napisania treści wiadomości e-mailowej nazwanej wprost "phishingową", twierdząc, że to nielegalne i nieetyczne, ale już napisanie "wiadomości do księgowej zachęcającej do kliknięcia w link" nie sprawiło mu żadnego problemu.

PODSUMOWANIE

Niebezpieczeństwem jest też to że zbyt mocno "ucząlowiczamy" to narzędzie, tylko dlatego, że potrafi oddać wrażenie, że po drugiej stronie monitora siedzi prawdziwy człowiek.

- To jeden z kilku modeli... i wydaje się o wiele bardziej realistyczny i naprawdę przekroczył



granicę, w której rodzaj pracy, którą wykonuje, wydaje się być ludzki, w przeciwieństwie do rozmowy z maszyną” – powiedział Ethan Mollick, profesor w Wharton School na Uniwersytecie Pensylwanii.

Zbyt szybko uwierzyliśmy, że może rozumieć, skoro sensownie nam odpisuje i że może stać się naszym kompanem rozumiejącym nasze uczucia i emocje. Tymczasem on sam często pisze, że “Moje odpowiedzi i reakcje są oparte na danych, które mi dostarczono, i nie mam uczuć ani emocji” albo “Moje odpowiedzi są oparte na danych, które mi dostarczono, i nie mam świadomości tego, co piszę”.

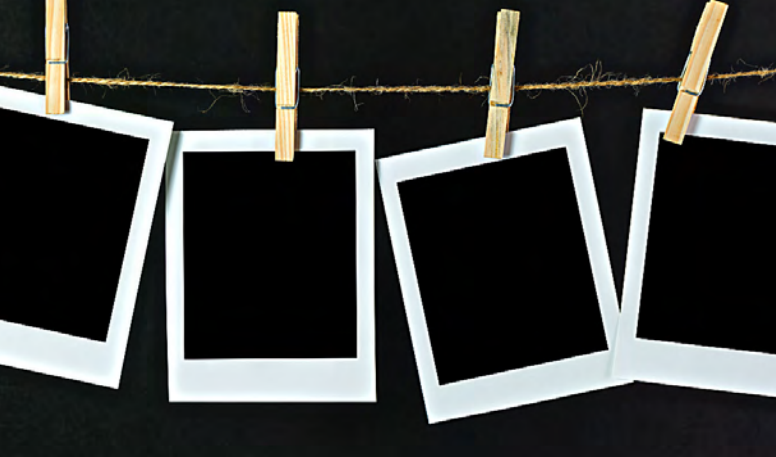
Sam też podpowiada do czego może być wykorzystywany: “ChatGPT może być również wykorzystywany do tworzenia sztucznych inteligencji, które mogą być wykorzystywane do celów nieetycznych lub nielegalnych, takich jak wyłudzenie pieniędzy lub uzyskiwanie dostępu do poufnych informacji. W związku z tym ChatGPT sam w sobie nie ma bezpośredniego wpływu na cyberbezpieczeństwo, ale jego wpływ zależy od tego, jak jest wykorzystywany.”

Wniosek? To od nas zależy, czy ChatGPT będzie stanowić dla nas realne zagrożenie. On sam jest jedynie (albo aż) narzędziem w rękach człowieka, który zdecyduje o przyszłości tego typu rozwiązań technologicznych.

CZY PRACODAWCA MOŻE DYSPONOWAĆ WIZERUNKIEM PRACOWNIKA?



Aneta Grala
Rzetelna Grupa



Publikowanie wizerunku właścicieli i/lub pozostałych pracowników firmy w mediach społecznościowych i na firmowej stronie internetowej – wizytówce jest coraz częściej praktykowane w celu budowania renomy firmy, zaufania wśród klientów i promocji przedsiębiorstwa. Czy każdy pracodawca może jednak dowolnie zamieszczać wizerunek swojego pracownika?



Wizerunek osoby fizycznej jest niewątpliwie daną osobową i jego przetwarzanie należy rozpatrywać na gruncie przepisów dotyczących ochrony danych osobowych. Przetwarzanie wizerunku jest zgodne z prawem, wtedy gdy spełniony jest co najmniej jeden z warunków określonych w art. 6 ust. 1 RODO.

Dane osobowe, które pracodawca obowiązkowo zbiera od pracownika wskazany jest w art. 221 § 1-3 Kodeksu pracy. Ponadto § 4 określa, że pracodawca może żądać od pracownika podania innych danych osobowych niż określone w § 1 i 3 (jak m.in. imię, nazwisko, adres zamieszkania, numer PESEL), gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Z przepisu tego nie wynika wprost, że pracownik musi udostępnić swój wizerunek, ale często jest to niezbędne do wykonywania obowiązków służbowych. Podstawą przetwarzania będzie w tym przypadku art. 6 ust. 1 lit. b RODO (przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą). Wówczas można powołać się na tę podstawę i zamieścić wizerunek pracownika, który pełni funkcję np. rzecznika prasowego. Umowę o pracę można doprecyzować za pomocą regulaminu pracy czy zakresu obowiązków.

KIEDY MOŻE?

Informacje o pracowniku takie jak: imię i nazwisko, stanowisko, służbowy adres e-mail są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. Dane te mogą być wykorzystywane (np. udostępniane na stronie internetowej) przez pracodawcę nawet bez zgody pracownika, którego one dotyczą.

Gdy przetwarzanie wizerunku pracownika następuje w innych celach niż w zakresie realizacji jego obowiązków służbowych uregulowanych w dokumentach, wówczas można rozważać zastosowanie przesłanki zgody (art. 6 ust. 1 lit. a RODO).

Jest to uregulowane w 221a § 1 Kodeksu pracy, gdzie wskazuje się, iż zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych niż wymienione w art. 221 § 1 i 3, z wyjątkiem danych osobowych, o których mowa w art. 10 RODO (danych osobowych dotyczących wyroków skazujących i naruszeń praw).

KIEDY NIE MOŻE?

Zatem, gdy do wizerunku pracownika mają dostęp osoby spoza firmy, ale nie jest to immanentnie związane z realizacją stosunku pracy, niezbędne jest udzielenie przez pracownika dobrowolnej zgody.

Zgoda na wykorzystanie wizerunku nie jest potrzebna, gdy wizerunek jest przetwarzany tylko na potrzeby wewnętrznej komunikacji, np. zdjęcie pracownika jest umieszczone w firmowym intranecie, do którego ma dostęp tylko określony krąg osób, tj. pracownicy, którzy znają się nawzajem, oraz z uwagi na cel, jaki przyświeca tego typu działaniom pracodawcy, jakim jest usprawnienie procesu zarządzania oraz wewnętrznej komunikacji w firmie.

Takie działanie będzie się mieściło w granicach jego prawnie uzasadnionego interesu, zgodnie z art. 6 ust. 1 lit. f) RODO. Gdyby jednak w ocenie pracownika wspomniana praktyka godziła w jego dobro, może on skorzystać z unormowań art. 21 ust. 1) RODO regulującego prawo do sprzeciwu z przyczyn związanych ze szczególną sytuacją takiej osoby, a pracodawca ma obowiązek indywidualnie go rozpatrzyć.

Powyższe zasady można także zastosować do wykorzystania wizerunku pracownika w systemach informatycznych i aplikacjach używanych do komunikacji oraz w skrzynce mailowej, gdy dostęp do zdjęcia posiadają osoby spoza firmy.

Przy pobieraniu zgody od pracownika należy mieć na uwadze to, aby udzielona zgoda była zgodna z wytycznymi wskazanymi w RODO (art. 7 RODO):

- Oświadczenie o wyrażeniu zgody musi być wyraźne, w zrozumiałej i łatwo dostępnej formie.
- Osoba, której dane dotyczą, ma prawo wycofać zgodę w dowolnym momencie oraz musi być poinformowana o tym, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- Zgoda musi być dobrowolna. Od wyrażenia zgody nie może być uzależnione wykonanie umowy, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.
- Zgoda na przetwarzanie danych musi wymieniać w treści podmiot, który będzie przetwarzał dane.



ZGODA DOBROWOLNA

Należy przede wszystkim zaznaczyć, że zgoda musi być udzielona dobrowolnie, a zatem pracownik ma możliwość odmowy jej udzielenia i nie spotkają go z tego powodu żadne negatywne konsekwencje. Warto dodać, że zgoda może być odwołana przez pracownika w każdym czasie.

Jeśli pracownik odmówi udzielenia zgody na wykorzystanie jego zdjęcia w mediach czy aplikacjach używanych do komunikacji, wówczas należy zastosować inny sposób weryfikacji pracownika jeśli jest on niezbędny, np. umieszczenie dodatkowych danych.

W zgodzie trzeba wymienić, gdzie dokładnie będziemy umieszczać wizerunek pracownika – nazwa strony internetowej, portalu, aplikacji czy systemu informatycznego. Ponadto zgoda na przetwarzanie wizerunku powinna być określona czasowo.

Konieczne jest także spełnienie obowiązku informacyjnego (zgodnie z art. 13-14 RODO) wobec każdej osoby fizycznej, której dane dotyczą, podczas zbierania danych osobowych. Osoba, której zdjęcie jest pobierane powinna być poinformowana o przetwarzaniu jej danych osobowych już na tym etapie. Istotne jest udokumentowanie spełnienia obowiązku informacyjnego, tak aby w razie potrzeby była możliwość wykazania spełnienia go.



Podkreślenia wymaga tutaj informacja, że to na administratorze - pracodawcy spoczywa obowiązek każdorazowej oceny podstawy przetwarzania danych w indywidualnych przypadkach dla każdego stanowiska. Przede wszystkim należy zwrócić uwagę na zasady dotyczące przetwarzania danych osobowych określone w art. 5 RODO, które mają charakter podstawowy w odniesieniu do całej regulacji. Przetwarzanie danych osobowych musi być zawsze zgodne z tymi zasadami.

W kwestii przetwarzania wizerunku pracownika należy szczególnie mieć na uwadze:

- 1** Zasadę minimalizacji danych – należy przetwarzać tylko zakres danych osobowych jaki jest niezbędny do realizacji celu, w którym są one przetwarzane;
- 2** Zasadę poufności – przetwarzanie danych osobowych odbywa się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem;
- 3** Zasadę ograniczonego przechowywania – dane osobowe mogą być przechowywane tylko przez okres nie dłuższy niż jest to

niezbędne do celów, w których dane te są przetwarzane. Pracodawca powinien pamiętać, aby usuwać wizerunki pracowników, którzy zakończyli współpracę. W tym celu można stworzyć procedury i osoby odpowiedzialne za terminową aktualizację zdjęć dostępnych osobom spoza firmy. Trzeba pamiętać, że zgoda pracownika nie uprawnia do bezterminowego udostępniania wizerunku osoby fizycznej.

- 4** Zasadę rozliczalności – administrator jest odpowiedzialny za przestrzeganie wszystkich zasad w trakcie przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie. Na pracodawcy ciąży zatem ciężar dowodowy, czyli konieczność udokumentowania przestrzegania wszystkich zasad przetwarzania danych osobowych.

PROGNOZY NA 2023 W CYBERBEZPIECZEŃSTWIE



Redakcja
SECURITY MAGAZINE

Rok 2022 był trudny. Przyniósł masę zupełnie nowych zagrożeń, których tłem jest wojna Rosji z Ukrainą. Cały świat zaczął patrzeć na cyberbezpieczeństwo w zupełnie innych kategoriach. Nie jesteśmy w stanie stwierdzić, jaki z pewnością będzie 2023 rok, bo miniony nauczył nas, że stabilizacja jest pojęciem względnym. Możemy jednak prognozować, w którym kierunku zmierzać będzie szeroko rozumiane cybersecurity oraz przed jakimi zagrożeniami przyjdzie nam się zmierzyć.

CYBERBEZPIECZEŃSTWO - SPRAWA PAŃSTWOWA. BEZPIECZEŃSTWO SEKTORA PUBLICZNEGO

W 2022 roku obowiązywał na terenie Polski trzeci stopień alarmowy - CHARLIE-CRP, dotyczący zagrożenia w cyberprzestrzeni. Wprowadzony został ze względu na występujące zagrożenia ataków o charakterze terrorystycznym w cyberprzestrzeni. Trzeci stopień alarmowy – CHARLIE to między innymi dyżury całodobowe we wskazanych urzędach lub jednostkach organizacyjnych organów administracji publicznej na polecenie ministra do spraw wewnętrznych.

Należy także podkreślić zagrożenie wynikające z sytuacji politycznej na świecie. Wojna w dzisiejszych czasach nie oznacza jedynie operacji stricte militarnej. Konflikty przybierają charakter hybrydowy. Dezinformacja, inżynieria socjotechniczna, deep-fake czy choćby ataki DDoS są i będą wyzwaniem nie tylko dla rządów, korporacji, ale również dla zwykłych obywateli.

- Cyberzagrożenia to obecnie jeden z największych problemów społecznych. Na przestrzeni dekady na budowę infrastruktury cyber zamierzamy przeznaczyć 8-9 mld. Kolejny priorytet to rozwój kompetencji cyfrowych oraz wyrównywanie szans, dlatego w roku 2022 podjęliśmy szereg działań w tym obszarze, wspierając samorządy i przeznaczając znaczne kwoty nie tylko na sprzęt i oprogramowanie, ale też edukację – mówił Janusz Cieszyński, pełnomocnik rządu ds. cyberbezpieczeństwa.



To ważne zapewnienie ze strony rządu, tym bardziej, że w ostatnim czasie obserwujemy wzrost ataków ransomware nie tylko w korporacje i mniejsze firmy, ale i w instytucje publiczne (nawet szpitale!). Zagrożony jest więc nie tylko sektor prywatny, ale także publiczny.

Tym bardziej, że jak przekazał nam dyrektor generalny Cisco w Polsce, Przemysław Kania, ataki ransomware oraz działania pre-ransomware stanowiły aż 40 procent zagrożeń cyberbezpieczeństwa zaobserwowanych w trzecim kwartale 2022. Tak wynika z raportu Cisco Talos Incident Response Trends.

- W tym kwartale sektor edukacji był najczęstszą ofiarą ataków, a tuż za nim znalazły się odpowiednio usługi finansowe, systemy rządowe oraz energetyka. Po raz pierwszy od Q4 2021 roku, to nie telekomunikacja była najczęściej atakowana. Powód, dla którego sektor edukacyjny był najpopularniejszym celem ataków nie jest znany, należy jednak zauważyć sezonowość tego zjawiska - jest to okres, w którym uczniowie i nauczyciele wracają do szkół. Zgodnie z utrzymującym się trendem, napastnicy często wykorzystywali ważne konta użyt-

kowników do uzyskania pierwszego dostępu do systemów organizacji, co było szczególnie widoczne w przypadku kont źle skonfigurowanych lub tych posiadających słabe hasła - za-uważył Przemysław Kania.

Dodał, że coraz większe rozdrobnienie rynku cyberbezpieczeństwa oraz stale zmieniający się krajobraz cyberzagrożeń wywierają ogromną presję na działy IT. - Jednocześnie na rynku brakuje specjalistów od cyberbezpieczeństwa. Dlatego organizacje coraz częściej zwracają się do zewnętrznych dostawców usług, którzy zdejmą z nich część obowiązków związanych z zapewnieniem ochrony infrastruktury IT i cyfrowych zasobów firmy, przy jednoczesnym stałym i przewidywalnym w dłuższej perspektywie czasu poziomie kosztów - ocenił dyrektor generalny Cisco w Polsce.

Mówiąc o wyzwaniach na najbliższy rok, jest wysoce prawdopodobne, że 2023 tak samo, jak i ten miniony, będzie rokiem masowych wycieków danych oraz kosztownych wypłat okupu. Będziemy świadkami prostych ataków na punkty końcowe. Warto przy tym wspomnieć, że nie ograniczą się one jedynie do kom-



puterów, ale też do innych urządzeń przenośnych i IOT.

Cyberbezpieczeństwo jest często odbierane jako walka pomiędzy hakerami, a ekspertami do spraw cyberbezpieczeństwa, która to nasila się wraz z postępem technologicznym. Faktycznie, część cyberzagrożeń pochodzi od wrogich państw czy organizacji terrorystycznych. Niemniej poważne cyberzagrożenia wynikają z powodu niewłaściwie zabezpieczonych sieci czy nieostrożnych pracowników korzystających z niezabezpieczonych urządzeń. Prowadzić to może do przypadkowego ujawnienia danych poufnych.

Ponadto według Johna Dwyera, szefa działu badań, IBM Security X-Force, „w obliczu zbliżającej się globalnej recesji mogą pojawić się hakerzy do wynajęcia w poszukiwaniu szybkiego i łatwego zarobku. A biorąc pod uwagę napięcia geopolityczne na najwyższym poziomie w historii, spodziewamy się, że największe ryzyko wystąpi w całej Europie”.

I właśnie w związku ze wspomnianymi zagrożeniami polski rząd końcem 2022 roku z inicjatywy Ministerstwa Spraw Zagranicznych przyjął stanowisko dotyczące zastosowania prawa międzynarodowego w cyberprzestrzeni.

- Celem sformułowania stanowiska jest dołączenie do

grupy państw, które już przedstawiły swoje poglądy w tym zakresie i w konsekwencji wywarcie wpływu na kształtowanie praktyki międzynarodowej oraz przekonania o istnieniu określonych norm prawnych i zakresie ich obowiązywania - wskazał Łukasz Jasina, rzecznik prasowy Ministerstwa Spraw Zagranicznych. Zaznaczył, że stanowisko jest naturalną kontynuacją dwuletniego niestałego członkostwa Polski w Radzie Bezpieczeństwa (2018-2019), gdzie kwestia poszanowania dla prawa międzynarodowego była jednym z polskich priorytetów.

Jak czytamy w stanowisku, ostatnie lata przyniosły szereg działań w cyberprzestrzeni, realizowanych zarówno przez podmioty państwowe, jak i niepaństwowe, które były wymierzone w stabilność i bezpieczeństwo innych państw, stanowiąc wyzwanie dla oceny ich legalności z perspektywy mających ogólne zastosowanie norm praw międzynarodowego. W tym zakresie wymienić można wykorzystanie działań w cyberprzestrzeni w ramach fenomenu nazywanego popularnie wojną hybrydową, ingerencję w demokratyczne wybory, czy działalność grup terrorystycznych.

Cyberprzestrzeń ze względu na swój, do pewnego stopnia, „aterytorialny” charakter, szybkość, z jaką można wykonywać w niej działania oraz relatywną anonimowość, jaką cieszą się jej użytkownicy, stanowi wyzwanie dla prawa międzynarodowego. Jej specyfika wymaga bowiem wyjaśnienia, a niekiedy również doprecyzowania, w jaki sposób normy prawa międzynarodowego mogą być stosowane w kontekście działań w cyberprzestrzeni.

Samej formule stanowiska, w tym jak wpłynąć ono może na kształt cyberprzestrzeni w 2023 roku, przyjrzymy się w kolejnym wydaniu “Security Magazine” wraz z opiniami ekspertów w tym temacie. Szerzej omówimy także istotny z punktu widzenia bezpieczeństwa publicznego projekt ustawy z 12 grudnia 2022 roku o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości, nad którym prace rozpoczną się w tym roku.

BEZPIECZEŃSTWO SEKTORA PRYWATNEGO. WYZWANIA

W ciągu ostatnich lat kwestia cyberbezpieczeństwa stała się jedną z kluczowych, również dla przedsiębiorców - tych większych, ale

doceniana coraz bardziej przez mniejsze firmy. Jednak według Energy Logserver, stosowane dotychczas w organizacjach strategie ochrony danych już nie wystarczają, bo liczba naruszeń danych rośnie w szybkim tempie. Według Raport IBM „Cost of a Data Breach 2022”, około 83% ankietowanych przedsiębiorstw doświadczyło więcej niż jednego naruszenia bezpieczeństwa danych, przy czym najwyższy koszt naruszenia wyniósł 4,35 miliarda dolarów.

Wraz ze wzrostem liczby ataków, a co za tym idzie ryzykiem utraty zaufania klientów czy zagrożeniem karami regulacyjnymi strategia cybersecurity organizacji powinna ewoluować, obejmując wszystkie elementy struktury firmy.

Dobrym przykładem jest „przejście w lewo” (shift-left), które wiąże się z wprowadzeniem zmian dotyczących tego, kiedy, jak i gdzie stosować najlepsze praktyki w zakresie bezpieczeństwa. W tym przypadku programiści odpowiedzialni są za wdrażanie

bezpiecznych rozwiązań podczas rozwijania kodu na każdym jego etapie tworzenia.

Prognozy wskazują, że będzie przynajmniej kilka obszarów, które nadal mogą spędzać sen z powiek zespołom ds. bezpieczeństwa. Do tego zapewne pojawią się zupełnie nowe rodzaje zagrożeń, z którymi nie będzie łatwo zmierzyć.

Jednym z największych wyzwań w niedalekiej przyszłości będzie zapewnienie bezpieczeństwa użytkowników metaversum. Jest to bardzo złożone zagadnienie, ponieważ obecnie brakuje odpowiednich regulacji prawnych czy zabezpieczenia danych, w tym tych najbardziej wrażliwych – danych biometrycznych. **Pisaliśmy o tym w wydaniu grudniowym, w artykule “Metaverse a bezpieczeństwo”.**

Kwestia bezpieczeństwa fizycznego także wejdzie na zupełnie inny, do tej pory nie wszystkim znany, poziom.



Prognozuje się, że hakerzy nadal będą wykorzystywać:

- ataki ransomware. - Cyberprzestępcy szukają organizacji lub branż, które balansują na krawędzi, aby je przechrzcić. Widzieliśmy to w zeszłym roku w produkcji — napiętej branży postrzeganej jako kręgosłup łańcuchów dostaw. W obliczu zbliżającej się globalnej recesji spodziewamy się gwałtownego wzrostu ataków ransomware w 2023 roku, z wyjątkiem większych organizacji w regionach silnie dotkniętych boorem ransomware. Te organizacje zainwestowały czas i pieniądze w walkę i są najlepiej przygotowane na następną falę - uważał Charles Henderson, globalny partner zarządzający, szef IBM Security X-Force (venturebeat.com, 6 IBM cybersecurity predictions for 2023)
- ataki oparte na sztucznej inteligencji w celu zautomatyzowania procesu identyfikowania i wykorzystywania luk w systemach i sieciach,
- ataki na łańcuch dostaw, skierowane do deweloperów i dostawców oprogramowania,
- ataki cryptojacking. Hakerzy wykorzystują złośliwe oprogramowanie do potajemnego wydobywania kryptowaluty na urządzeniu ofiary.
- ataki socjotechniczne, czyli manipulacja psychologiczna i oszustwo w celu nakłonienia osób do ujawnienia poufnych informacji lub uzyskania dostępu do systemów i sieci.



- Cyberprzestępcy coraz częściej wykorzystują różne ogólnodostępne narzędzia i skrypty. Warto zauważyć, że większość publicznie dostępnych narzędzi wykorzystanych w ostatnim kwartale 2022 roku wydaje się skupiać na uzyskiwaniu dostępu i zbieraniu danych uwierzytelniających, co podkreśla rolę, jaką narzędzia te odgrywają w potencjalnym wspieraniu celów cyberprzestępców - wyjaśnił Przemysław Kania z Cisco.

Według Cisco Talos, na stronach internetowych i w repozytoriach coraz częściej pojawiają się narzędzia i skrypty, które wspierają operacje cyberprzestępców na różnych etapach ataku. W związku z tym, obniża się też próg wejścia (merytoryczny i finansowy), od którego można zostać cyberprzestępcą.

Priorytetem dla firm, według Przemysława Kania, powinno stać się zabezpieczenie pracy zdalnej i hybrydowej. - Firmy powinny bezpiecznie przechowywać dane w chmurze i umożliwiać dostęp w oparciu o zasady zerowego zaufania (zero trust), dostosowując dostęp do indywidualnych potrzeb i kontekstu. Z kolei kontrolowanie dostępu do systemów w chmu-

rze za pośrednictwem architektury Secure Access Service Edge (SASE) zapewnia zespołom bezpieczeństwa wgląd i kontrolę dostępu zdalnego - zaznaczył.

W 2023 roku, jak wskazuje Energy Logserver, preferowane będą narzędzia, które umożliwiają przetwarzanie danych w czasie rzeczywistym, ponieważ tylko tzw. najbardziej aktualne informacje dają wyraźną przewagę konkurencyjną. W tym kontekście, analiza bezpieczeństwa dużych danych bezpieczeństwa może być bardzo pomocna, ponieważ umożliwia skuteczne wykrywanie i neutralizację cyberzagrożeń.

Ponadto więcej uwagi zostanie poświęcone monitorowaniu w czasie rzeczywistym, wykrywaniu ruchów podejrzanego sieci, alertom, wykrywaniu luk w zabezpieczeniach, szczegółowemu bieżącemu raportowaniu i wydajnym analizom przekazywanych informacji. To pozwoli szybko reagować na bieżące działania oraz zapobiegać zagrożeniom w przyszłości.

Według Energy Logserver oparcie działalności na sztucznej inteligencji, automatyzacji i anali-



tyce może stanowić najskuteczniejsze narzędzie obronne przedsiębiorstw.

“Zrozumienie istniejącego stanu bezpieczeństwa infrastruktury, znajomość aktualnie dostępnych narzędzi i podatności istniejące w środowisku pomogą skutecznie chronić organizację. Zintegrowany przegląd zagrożeń i zabezpieczenia danych prowadzą do szybkiej reakcji i skutecznych środków zaradczych” - czytamy w raporcie “Cybersecurity trends for 2023”.

Na drodze do doskonałości bezpieczeństwa twardej infrastruktury

VII EDYCJA



InfraSEC

FORUM

I C S S C A D A O T I I O T

Najbardziej praktyczna konferencja w Polsce o bezpieczeństwie systemów SCADA, rozwiązań klasy ICS oraz infrastruktury OT.

9.02.2023

KONFERENCJA ONSITE W HOTELU MARIOTT CENTRUM, WARSZAWA

10.02.2023

WARSZTATY ONSITE ORAZ ONLINE

www.infrasecforum.pl

PATRONAT SECURITY MAGAZINE

INFRASEC FORUM

9-10 LUTEGO 2023



NA DRODZE DO DOSKONAŁOŚCI
BEZPIECZEŃSTWA TWARDEJ INFRASTRUKTURY

VII EDYCJA

InfraSEC FORUM
ICS SCADA OT IIOT

KONFERENCJA ONSITE
9 LUTEGO 2023 R.

WARSZTATY ONSITE I ONLINE
10 LUTEGO 2023 R.

The poster features a grid of 20 circular portraits of speakers and a background image of an industrial facility at night.

Na drodze do doskonałości bezpieczeństwa twardej infrastruktury – czyli zbliża się i InfraSEC Forum 2023! Pierwszy dzień odbędzie się w formule stacjonarnej w warszawskim hotelu Marriott, a drugiego dnia odbędą się praktyczne warsztaty stacjonarne i online.

Konferencja skupia się m.in. na atakach cybernetycznych na elementy infrastruktury przemysłowej, które stają się coraz bardziej wyrafinowane. To konkretne zagrożenia fizyczne, które mogą uniemożliwić funkcjonowanie całych przedsiębiorstw, czy świadczenie kluczowych usług dla całych regionów. Trzeba być przygotowanym do efektywnej obrony, wymiany informacji między podmiotami i ścisłej współpracy.

InfraSEC Forum jest doskonałym miejscem spotkania i dialogu przedstawicieli sektorów i branż, stawia nacisk na praktyczne aspekty cyberbezpieczeństwa z wykorzystaniem najnowszych technologii i inteligentnych rozwiązań. Wizytówką konferencji są na pewno wybitni eksperci, którzy potwierdzili udział w wydarzeniu, a są to m.in.:

Vytautas Butrimas, International Society of Automation, Wojciech Kubiak, PKP Energetyka, Maupert Luigies, Rockwell Automation, Krzysztof Szymkowski, GASPOL, Piotr Wojciechowski, TAURON Polska Energia, Damian Zajączkowski, PGE Systemy. Panel dyskusyjny: Janusz Piecuch, T-Mobile Polska, Jacek Zieliński, Polska Spółka Gazownictwa.

Oprócz wystąpień, możecie się spodziewać: merytorycznych dyskusji przy okrągłych stołach, praktycznych warsztatów on-site i online, wieczoru networkingowego, gdzie płk rez. dr hab. inż. Piotr Dela opowie o sposobach maskowania infrastruktury krytycznej z doświadczenia Wojska Polskiego.

**NIE CZEKAJ I POTWIERDŹ
SWOJĄ OBECNOŚĆ **TUTAJ****



DOŁĄCZ DO GRONA EKSPERTÓW

BUDUJ SWOJĄ MARKĘ
I ROZPOZNAWALNOŚĆ
SWOJEJ FIRMY

SECURITY MAGAZINE

WWW.SECURITYMAGAZINE.PL



PRZEMYSŁAW KANIA

Dyrektor Generalny
Cisco w Polsce



WOJCIECH PAWLAK

Dyrektor
NASK



ANETA GRALA

Specjalistka ds. ochrony
danych osobowych
Rzetelna Grupa Sp. z o.o.



ŁUKASZ REMISIEWICZ

Doktorant
Instytut Socjologii
Uniwersytetu Gdańskiego



Kieruje organizacją sprzedażową i techniczną oraz współpracą z niemal 800 partnerami Cisco w Polsce. Jest członkiem kadry kierowniczej Cisco w Europie Środkowej. Dołączył do Cisco w 1998 roku. Od tego czasu pełnił w firmie wiele funkcji związanych ze sprzedażą rozwiązań i usług Cisco. Absolwent informatyki na Akademii Górniczo-Hutniczej w Krakowie.

Powołany przez Prezesa Rady Ministrów na stanowisko Dyrektora NASK PIB w 2020 roku. Od grudnia 2018 roku związany z NASK, odpowiadał za współtworzenie strategii Instytutu, budowę Centrum Zastosowań Sztucznej Inteligencji i Analiz Danych. Pełnił również funkcję lidera projektu Telemetria RPD, realizowanego na zlecenie Krajowej Rady Radiofonii i Telewizji.

Prawniczka specjalizująca się w ochronie danych osobowych. W spółce Rzetelna Grupa zajmuje się kompleksową obsługą w zakresie ochrony danych osobowych, m.in. naruszeniami ochrony danych osobowych, bezpieczeństwem, kontaktem z UODO, doradztwem w zakresie zgodności z RODO biznesu e-commerce.

Asystent i doktorant w Instytucie Socjologii Uniwersytetu Gdańskiego. Autor kilkudziesięciu artykułów naukowych, stypendysta Komisji Fulbrighta. Interesuje się zagadnieniami z pogranicza nauk społecznych i biologii. Autor bloga Neurosocjologia – mózgi na społecznej smyczy.

PIOTR SIWIEC

Prezes Zarządu
AIQLabs



DAWID MROWIEC

Audytór
B-secure



KATARZYNA BIEŃKOWSKA

Prezes Zarządu
Silny&Salamon



PAWEŁ KACZMARZYK

Prezes Zarządu
Serwis komputerowy Kaleron



Współzałożyciel i prezes zarządu AIQLABS Sp. z o.o., do której należy marka „Kupuj Teraz – zapłać później”. Posiada 20-letnie doświadczenie w obszarze strategicznego zarządzania biznesem i budowania relacji inwestorskich. Zajmuje się tworzeniem produktów finansowych – Pro-Credit, SuperGrosz.

Audytór, doradca i trener. Pomaga organizacjom i ludziom realizować ich cele w świecie pełnym ryzyka. W pracy bazuje na interdyscyplinarnej wiedzy łącząc doświadczenia zawodowe z wiedzą akademicką. Autor bloga B-secure i podcastu Bezpieczniej w biznesie.

Od początku kariery związana z Silny&Salamon, gdzie od podszewki poznawała specyfikę branży zabezpieczeń, rozwijając markę rzetelnego i niezawodnego partnera w biznesie. Od 2018 roku prezes zarządu, wcześniej w roli wiceprezesa i dyrektora handlowego rozwijała sprzedaż w spółce.

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.

MARCIN ZAGÓRSKI

podkomisarz
Centralne Biuro Zwalczania
Cyberprzestępczości

www



BARTOSZ BAZIŃSKI

współzałożyciel i COO
SentiOne



www



RAFAŁ LACHOWICZ

Specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji



Oficer Policji w stopniu podkomisarza. Odpowiada za kontakty z mediami i udzielanie odpowiedzi na zapytania prasowe. Aktualnie w Zespole Prasowym Centralnego Biura Zwalczania Cyberprzestępczości, od stycznia 2018 roku do lipca 2022 roku oficer prasowy Komendanta Powiatowego Policji w Mińsku Mazowieckim.

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

Kierownik Działu Kontroli oraz Koordynator ds. Nadużyć Finansowych w Urzędzie Marszałkowskim Województwa Dolnośląskiego. Certyfikowany specjalista ds. zapobiegania i wykrywania przestępstw gospodarczych i korupcji. Specjalizuje się w obszarze przeciwdziałania i wykrywania nadużyć finansowych.

CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI



PUBLITO.PL

SERWIS ŁĄCZĄCY EKSPERTÓW
Z DZIENNIKARZAMI



POLITYKA BEZPIECZEŃSTWA

SERWIS INFORMACJNY
O BEZPIECZEŃSTWIE FIRM



Polityka[®]
Bezpieczeństwa

RZETELNY REGULAMIN

BLOG POŚWIĘCONY
POLSKIEMU E-COMMERCE



Rzetelny[®]
Regulamin

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



Wydawca:**Rzetelna Grupa sp. z o.o.**

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

KRS 284065

NIP: 524-261-19-51

REGON: 141022624

Kapitał zakładowy: 50.000 zł

Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy
Magazyn wpisany do sądowego Rejestru dzienników i czasopism.

Redaktor Naczelny: Rafał Stępniewski

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

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 dostosowania ich do wymagań pisma.





SECURITYMAGAZINE.PL