10(19)/2023

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

# SECURITY MAGAZINE

Bezpieczeństwo | Technologia | Wiedza | Najlepsze standardy

## Atak phishingowy z perspektywy ofiary

## Przepis na atak phishingowy Krok po kroku

## Jak oszuści wykorzystują LinkedIn do cyberataków?

## Ransomware i MŚP. Skuteczne strategie obronne przed cyberporwaniami

## W służbie bezpieczeństwu Październik miesiącem cyberświadomości

# SPIS TREŚCI



# SZANOWNI PAŃSTWO,

**dzięki inicjatywie ENISA, cała Europa przez cały październik skupia się na promowaniu bezpieczeństwa w sieci, a my, z dumą, stajemy na czele tej misji w Polsce.**

**Współpracując z Państwowym Instytutem Badawczym NASK, dążymy do tego, by każdy użytkownik internetu miał dostęp do najnowszej wiedzy i najlepszych praktyk w zakresie cyberbezpieczeństwa.**

**W tym roku postanowiliśmy pójść krok dalej. Nie tylko przygotowaliśmy dla Was wydanie pełne merytorycznych artykułów, ale również zaprosiliśmy do współpracy firmy, które są Wam dobrze znane. Ich wkład w to wydanie jest nieoceniony, a efekty tej synergii zobaczyć możesz zarówno na łamach naszego magazynu, jak i w mediach społecznościowych.**

**Chcielibyśmy podziękować wszystkim, którzy przyczynili się do powstania tego wydania, w szczególności NASK, który objął nad nim patronat honorowy. Podziękowania składamy też dla Centralnego Biura Zwalczania Cyberprzestępczości za wsparcie i zaufanie.**

**Wspólnie tworzymy coś wyjątkowego, co ma realny wpływ na bezpieczeństwo w sieci.**

**Zapraszam do lektury i życzę inspirujących treści. Niech ten październik będzie dla Was miesiącem pełnym nowej wiedzy i świadomości w zakresie cyberbezpieczeństwa.**

**Dobrej lektury!**

Rafał Stępniewski



**SZCZEGÓŁY STR. 115**

## DOŁĄCZ DO CBZC

Masz pasję do technologii i chcesz pomagać w zapewnianiu bezpieczeństwa w cyberprzestrzeni? Służba w CBZC może być dla Ciebie idealnym wyborem.

Centralne Biuro Zwalczania Cyberprzestępczości to jednostka organizacyjna Policji, która posiada komórki w każdym mieście wojewódzkim w kraju, skupiająca się na zapobieganiu, ściganiu i zwalczaniu przestępczości w cyberprzestrzeni. Służba w CBZC to nie tylko praca przed komputerem. To też udział w wielu operacjach, szkoleniach krajowych i międzynarodowych. Najnowsze rozwiązania z zakresu informatyki śledczej, czynności operacyjne i procesowe. Praca w takim środowisku jest niezwykle ekscytująca i daje możliwość rozwoju zawodowego w różnych aspektach.

**Co daje służba w CBZC?**

1. Gwarancję stałego rozwoju i poszerzania swoich umiejętności.
2. Perspektywę rozwiązywania skomplikowanych problemów, analizowania dowodów cyfrowych i pracę z wykwalifikowanymi specjalistami na szczeblu krajowym i międzynarodowym.
3. Stabilność zawodową. Na stanowisku związanym z bezpośrednim zwalczaniem cyberprzestępczości oprócz policyjnego wynagrodzenia przysługuje specjalne świadczenie, które wynosi pomiędzy ok. 5100 zł - 9500 zł brutto.

Jesteś zainteresowany walką z cyberprzestępczością? Służba w CBZC może być dla Ciebie pasjonującym wyzwaniem. Da Ci możliwość realnej poprawy bezpieczeństwa innych w sieci oraz rozwijania swoich umiejętności.

Dołącz do walki z cyberprzestępczością i pomóż w tworzeniu bezpiecznej przyszłości w wirtualnym świecie! Wstąp do CBZC! #stanpodobrejstronie


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

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

*Redakcja "Security Magazine"*

## JAK CHRONIĆ BIZNES PRZED ZAGROŻENIAMI?

Zaniedbania w dziedzinie bezpieczeństwa informatycznego to zaproszenie cyberprzestępców do zarabiania naszym kosztem. Zobacz, co możesz zrobić, żeby zabezpieczyć swoją firmę przed phishingiem, malware oraz innymi popularnymi atakami. **Przeczytaj przewodnik Grandmetric o cyberbezpieczeństwie w biznesie**, zabezpiecz się, by nie musieć uczyć się na błędach! Materiał pomoże Ci zabezpieczyć Twoją organizację i rozpocząć świadome zarządzanie cyberbezpieczeństwem.

## WSPÓŁPRACA MIĘDZY NASK A CBZC

Państwowy Instytut Badawczy NASK i Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) podpisały specjalne porozumienie, formalizując swoją dotychczasową współpracę w zakresie cyberbezpieczeństwa. Porozumienie, podpisane 29 września 2023 r., stanowi ważny krok w umacnianiu działań obu instytucji przeciwko cyberprzestępczości. Dyrektor NASK, Wojciech Pawlak, podkreślił znaczenie tej współpracy, dziękując pracownikom CBZC za ich wkład. Nadinspektor Adam Cieślak z CBZC wyraził nadzieję na dalsze umocnienie partnerstwa. Współpraca będzie obejmować wymianę informacji, technologii oraz realizację wspólnych projektów edukacyjnych i prewencyjnych.

W praktyce współpraca między działającym w strukturach NASK zespołem CSIRT NASK a CBZC realizowana była regularnie już przed podpisaniem porozumienia. Pracownicy CBZC byli także współautorami wielu publikacji realizowanych przez NASK, współprowadzili webinary, przekazywali dane statystyczne i angażowali się w wiele przedsięwzięć o charakterze edukacyjnym.


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

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

*Redakcja "Security Magazine"*

## JAK PRZYGOTOWAĆ FIRMĘ DO DORA I NIS 2?

Secfense, firma działająca w obszarze cyberbezpieczeństwa, przygotowała praktyczny poradnik dla przedsiębiorców „Analiza regulacji DORA i NIS2 w kontekście cyberbezpieczeństwa przedsiębiorstw w UE" wyjaśniający, kogo dotyczą regulacje DORA i NIS 2 oraz jakich konkretnych działań wymagają od organizacji. Powstał we współpracy z ekspertami Fundacji Law4Tech. Celem nowych regulacji jest ochrona instytucji państwowych i przedsiębiorstw działających w obszarach kluczowych przed cyberzagrożeniami. Budzą jednak dużo wątpliwości.

Jak przygotować organizację do ich wprowadzenia? Kogo w szczególności obowiązują i zastosowania jakich rozwiązań chroniących przed cyberprzestępcami wymagają? - *W rozporządzeniu i dyrektywie trudno jest znaleźć konkretne zalecenia dotyczące technologii, które należy wdrożyć. To dlatego poprosiliśmy prawników z Fundacji Law4Tech o przygotowanie specjalistycznej analizy DORA i NIS 2 pod kątem wymagań stawianych firmom, odpowiedzialności za wprowadzenie nowych przepisów oraz konkretnych technologii, które UE zaleca wdrożyć. Szczególną uwagę poświęciliśmy w tej analizie mechanizmom silnego uwierzytelniania, które są dziś podstawowym zabezpieczeniem wszechstronnie chroniącym przed nieuprawnionym dostępem do kluczowych zasobów informacyjnych* – mówi **Tomasz Kowalski, współzałożyciel i CEO Secfense.**

Na podstawie raportu powstał e-book, zawierający najważniejsze informacje o nowych aktach prawnych, opis obowiązków, jakie z nich wynikają, dane na temat osób odpowiedzialnych za wdrożenie oraz kar, które grożą organizacjom za niedostosowanie się do nowych wymagań. Duża część poradnika poświęcona jest rozwiązaniom MFA. E-book można pobrać bezpłatnie ze strony Secfense.


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

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

*Redakcja "Security Magazine"*


Polityka ®
Bezpieczeństwa
EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA
BEZPIECZEŃSTWO
W ZASIĘGU TWOJEJ
RĘKI!
CAŁY PAŹDZIERNIK Z WIEDZĄ O CYBERBEZPIECZEŃSTWIE
NA POLITYKABEZPIECZENSTWA.PL
KLIKNIJ I CZYTAJ ZA DARMO

# W SŁUŻBIE BEZPIECZEŃSTWU. PAŹDZIERNIK MIESIĄCEM CYBERŚWIADOMOŚCI

Rafał Stępniewski
Security Magazine

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

**W październiku, pod egidą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, cała Europa skupia się na promowaniu bezpieczeństwa w sieci. Polska, z inicjatywą prowadzoną przez Państwowy Instytut Badawczy NASK, nie pozostaje w tyle. W tym wydaniu przybliżamy czytelnikom temat inżynierii społecznej, jednego z najbardziej zdradliwych zagrożeń w cyberprzestrzeni. Współpracując z ekspertami i instytucjami, chcemy zwiększyć świadomość i przygotować Czytelników do stawienia czoła cyberzagrożeniom.**

## PO RAZ KOLEJNY...

Każdego roku każdy październik, dzięki inicjatywie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ENISA, staje się miesiącem promującym bezpieczeństwo w sieci. Celem jest popularyzacja wiedzy o cyberbezpieczeństwie, zwiększenie świadomości i wymiana dobrych praktyk wśród użytkowników internetu. Polską edycję kampanii ECSM od początku koordynuje Państwowy Instytut Badawczy NASK.

W ubiegłym roku włączyliśmy się do inicjatywy, zgłaszając wydanie październikowe jako nasz wkład w popularyzację wiedzy. W tym roku zaprosiliśmy do współpracy firmy, które naszym Czytelnikom są już znane, z którymi realizowaliśmy już wiele projektów.

I w trakcie przygotowań do Europejskiego Miesiąca Cyberbezpieczeństwa, choć czasu nie było wiele, nasi partnerzy stanęli na wysokości zadania. Dla Czytelników przygotowali zarówno inspirujące, wypełnione po brzegi cenną wiedzą artykuły dotyczące cyberbezpieczeństwa. A dla internautów - grafiki, infografiki, filmiki z poradami i historiami z życia wziętymi.

Artykuły z niezwykle cennymi wskazówkami, poradami znajdziesz właśnie w tym wydaniu. Multimedia - w mediach społecznościowych naszych, naszych partnerów i patronów. Przez cały miesiąc będziemy razem prezentować na naszych kanałach grafiki i filmiki związane z poradami i ciekawostkami dotyczącymi socjotechnik: jak je w ogóle rozpoznać? Jak je odróżnić od innych cyberoszustw? Jakie są ich rodzaje? Jak się im nie dać? Co zrobić, kiedy już wpadło się w sidła cyberprzestępcy?

## OTO NASI PARTNERZY...

Na naszą propozycję wspólnego projektu odpowiedziały firmy: **Grandmetric, Perceptus, Marken Systemy Antywirusowe - Bitdefender Polska, Adrian Sroka, Sygnisoft SA, Barracuda, Secfense, Concept Data i Nomios Group.**

**Grandmetric** od 2015 r. skupia się na rozwiązywaniu problemów z wydajnością sieci oraz bezpieczeństwem cyfrowym firm. Prowadzi audyty, doradza przy projektach transformacyjnych i dostarcza sprawdzony sprzęt IT. Lubi dzielić się wiedzą, a ich materiały czyta 32 tys. inżynierów miesięcznie.

**Perceptus** od 2008 roku specjalizuje się w dziedzinie cyberbezpieczeństwa, zajmując się między innymi szyfrowaniem danych, ich backupem i archiwizacją. Jednocześnie Perceptus realizuje projekty własne, wdrażając rozwiązania w obszarze wysokich technologii. Świadczy też usługę Security Operations Center.

**Marken Systemy Antywirusowe** na rynku od 1999 r. Oficjalny dystrybutor w Polsce **Bitdefender** - Globalnego Lidera Cyberbezpieczeństwa. W 2022 r. Bitdefender uznany za silnego wykonawcę w raporcie The Forrester Wave™ dla EDR, wyróżniony w Gartner Hyper Cycle dla Endpoint Security: XDR, EDR i EPP.

**Adrian Sroka.** Kluczowe aspekty: pragmatyczne bezpieczeństwo w tworzeniu oprogramowania, metodologia shift left, budowa społeczności Security Champions. Największy sukces to opracowanie i wdrożenie autorskiego programu dbania o bezpieczeństwo aplikacji i zbliżenie do siebie działów dewelopementu oraz bezpieczeństwa.

**Sygnisoft SA,** na rynku od 2006 r., początkowo jako e-Business Solutions. Twórca systemów, aplikacji internetowych i mobilnych. Realizuje projekty dla lokalnych przedsiębiorstw i międzynarodowych korporacji. Wdraża platformę iGamingową dla jednej ze spółek Skarbu Państwa, która zastąpi amerykańskie rozwiązanie, a będą z niej korzystać miliony Polaków.

**Secfense,** z siedzibą w Krakowie, powstał w 2018 r. Stworzył User Access Security Broker, narzędzie pozwalające na komple-

ksowe i szybkie wdrożenie technologii MFA w każdej firmie. W 2023 r. został wybrany do programu Google for Startups Growth Academy: Cybersecurity. Jest członkiem FIDO Alliance.

**Barracuda Networks** powstała w 2003 r. w Stanach Zjednoczonych. Jest producentem rozwiązań z obszaru bezpieczeństwa IT do ochrony poczty e-mail, aplikacji webowych, sieci, danych i infrastruktury IT. W 2023 r. wprowadziła na rynek platformę SASE (Secure Access Service Edge) dla firm i dostawców MSP.

**Concept Data**, z siedzibą w Warszawie, jest na rynku od 2016 r. Wdraża rozwiązania IT wspierające biznes m.in. w sektorze bankowym i telekomunikacyjnym. Jest partnerem największych globalnych producentów. Specjalizuje się głównie w obszarach cyberbezpieczeństwa, tożsamości cyfrowej i Service Desk.

**Nomios Poland** z siedzibą w Warszawie, od 11 lat na rynku jako niezależny dostawca nowoczesnych systemów cyberbezpieczeństwa, sieci krytycznych dla biznesu, rozwiązań chmurowych i usług zarządzanych. Największy sukces: realizacja projektu NASK dla OSE jako dostawa systemu stanowiącego infrastrukturę bezpieczeństwa.

Chcę też zaznaczyć, że ta fantastyczna współpraca nie miałaby szansy na realizację gdyby nie kilka osób, które odpowiadały za niezwykle sprawną i owocną komunikację między naszą redakcją a autorami eksperckich treści i grafik. Za to gorące podziękowania.

## PATRONI SĄ NASZYM WSPARCIEM I MOTYWACJĄ...

Patronat nad naszą wspólną inicjatywą objął NASK. Oprócz tego, że nasz wspólny projekt został oficjalnie zakwalifikowany do inicjatyw Europejskiego Miesiąca Cyber-

bezpieczeństwa, koordynowanego w Polsce przez NASK, to przeszliśmy pozytywną weryfikację NASK w ramach patronatu honorowego. To dało nam i naszym partnerom możliwość posługiwania się informacją o przyznaniu honorowego patronatu NASK-PIB oraz umieszczania logotypu NASK-PIB w materiałach informacyjno-promocyjnych, związanych z wydarzeniem. Taka forma wsparcia jest dla nas niezwykle cenna i stanowi potwierdzenie wysokiej jakości oraz znaczenia naszej inicjatywy w obszarze cyberbezpieczeństwa. Patronat honorowy NASK-PIB podnosi prestiż naszego projektu, co przekłada się na większe zaufanie wśród partnerów i czytelników oraz wzbogaca merytoryczną stronę naszego przedsięwzięcia.

Nasz projekt został dostrzeżony i doceniony przez NASK, co motywuje nas do dalszej pracy i realizacji naszego motto: "w służbie bezpieczeństwu".

A skoro o służbie mowa, zaznaczę, że patronem projektu, który zorganizowaliśmy z myślą o ECSM 2023, jest również Centralne Biuro Zwalczania Cyberprzestępczości. Tu kieruję podziękowania do Pana Komendanta za zaufanie i gotowość do współpracy. Podziękowania kieruję również do Zespołu Prasowego CBZC.

To dla nas duże wyróżnienie, że możemy współpracować z tak prestiżową i profesjonalną jednostką, jaką jest Centralne Biuro Zwalczania Cyberprzestępczości. Jego doświadczenie, wiedza i zaangażowanie w działania na rzecz bezpieczeństwa w cyberprzestrzeni są dla nas nieocenione. Dzięki temu patronatowi nasza inicjatywa stanie się jeszcze bardziej skuteczna i dotrze do jeszcze szerszego grona odbiorców.

Współpraca ta przyniesie wymierne korzyści dla obu stron, a przede wszystkim dla społeczności internetowej, która dzięki temu może stać się lepiej przygotowaną do stawienia czoła cyberzagrożeniom.

## CZY UDA SIĘ PRZEŁAMAĆ STEREOTYPY?

Wydanie, które masz przed oczami, jest przepełnione merytoryką, z masą precyzyjnie przygotowanych treści dotyczących w głównej mierze inżynierii społecznej. To jedno z tych wydań, któremu poświęciliśmy mnóstwo czasu i energii. To też jedno z tych wydań, które po raz kolejny obala mit, że branża cybersecurity jest hermetyczna, nie lubiąca dzielić się wiedzą, zbyt techniczna, czy nawet pozbawiona ludzkiego wymiaru.

Inżynieria społeczna, będąca głównym tematem tego wydania, bo jest to również temat tegorocznego ECSM, pokazuje, jak ważny jest czynnik ludzki w świecie cyberbezpieczeństwa.

To właśnie ludzie, ich emocje, nawyki i zachowania są celem dla przestępców, którzy wykorzystują różne techniki manipulacji, aby osiągnąć swoje cele. W tym wydaniu postawiliśmy na głębokie zrozumienie mechanizmów działania inżynierii społecznej, analizując różne przypadki i metody. Nasi eksperci pokazali m.in., jak socjotechnika wygląda zarówno z perspektywy cyberprzestępcy, jak i ofiary.

Branża cybersecurity to przecież nie tylko o kody, technologie i złożone systemy. To przede wszystkim ludzie – jak się komunikują, jakie podejmują decyzje i jakie są ich słabości.

**Mam więc nadzieję, że to wydanie dostarczy Ci nie tylko cennej wiedzy, ale także zainspiruje do refleksji nad własnymi nawykami i zachowaniami w sieci.**

Polityka® Bezpieczeństwa

# ANALIZA FORMALNA WYCIEKU DANYCH

MASZ 72 GODZINY NA POWIADOMIENIE UODO O INCYDENCIE

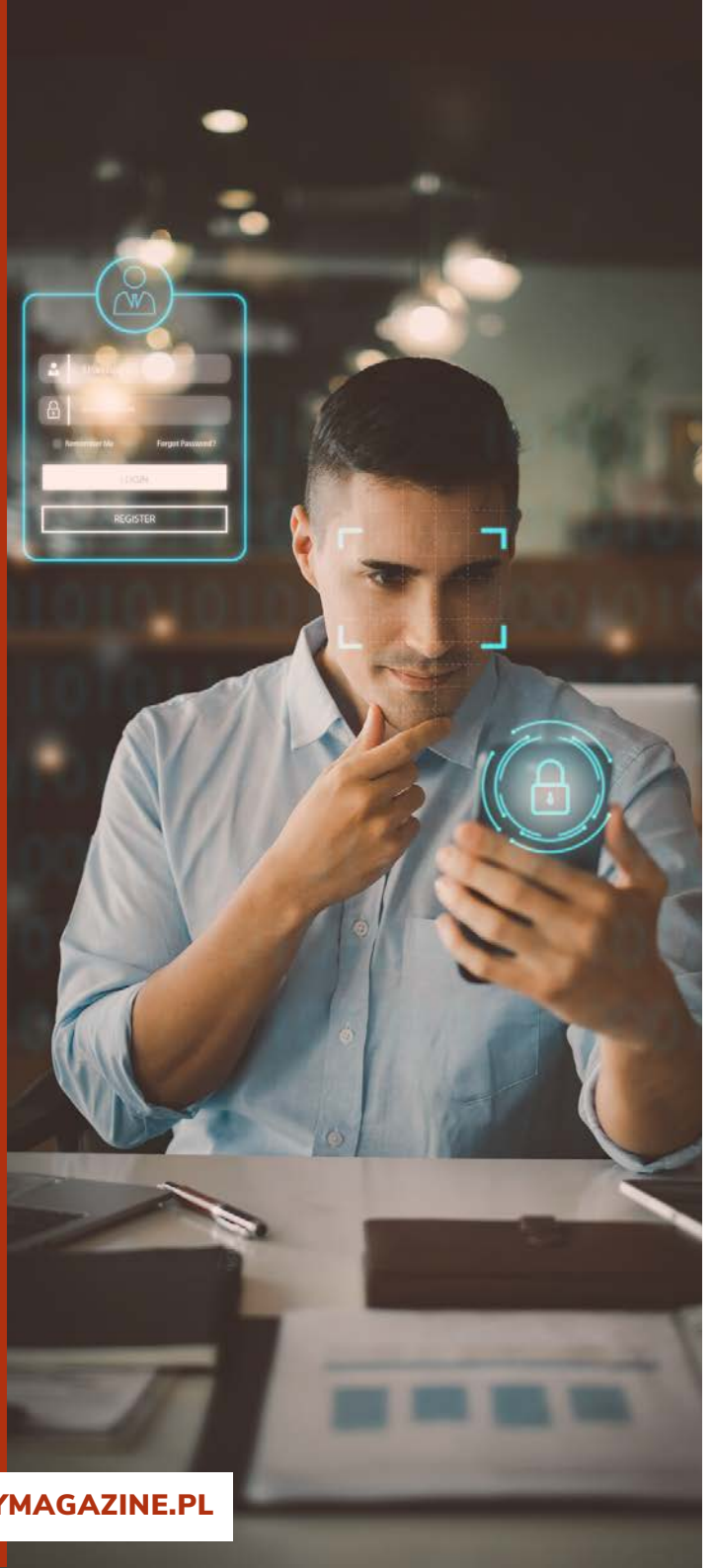
**SPRAWDŹ OFERTĘ**

# JAK MINIMALIZOWAĆ RYZYKO WŁAMAŃ POPRZEZ SILNE HASŁA ORAZ ZARZĄDZANIE NIMI?

**Klaudia Jędrzejczak-Krasieńko**
Sygnisoft SA


**Jedną ze strategicznych kwestii w zarządzaniu polityka bezpieczeństwa, są zasady związane z wykorzystaniem haseł dostępowych do różnych serwisów. Dane te są pierwszą linią obrony przed atakami cybernetycznymi, dlatego ich jakość ma kluczowe znaczenie. Słabe hasła są łatwe do złamania, co czyni je celem dla hakerów. Często ludzie wybierają proste hasła, łatwe do zapamiętania i używają ich wielokrotnie, otwierając tym samym drzwi cyberprzestępcom.**

# Jak minimalizować ryzyko włamań poprzez silne hasła i zarządzanie nimi?




Różnorodność ataków cybernetycznych dotyczących haseł jest ogromna. Od brutalnych prób odgadnięcia hasła (brute force), ataki słownikowe, po ataki typu keylogger, czy te wykorzystujące phishing. Słabe hasła stwarzają zagrożenia dla danych i reputacji firmy. Jeśli cyberprzestępcy uzyskają nieuprawniony dostęp do systemów, mogą zaszkodzić poufności, integralności oraz dostępności danych biznesowych i osobistych.

Zawsze, nawet przy najwyższej klasy zabezpieczeniach, warto zdawać sobie sprawę z czynnika ludzkiego. Często pracownicy używają słabych haseł dla wygody, dodatkowo zapamiętują je w swoich przeglądarkach i nigdy ich nie zmieniają, chyba że, system to wymusi. Edukacja pracowników i zwiększanie świadomości w zakresie bezpiecznego zarządzania hasłami jest nieoceniona.

Wprowadzanie skutecznych strategii zarządzania hasłami to inwestycja w cyberbezpieczeństwo firmy. Wdrażając świadome praktyki i wykorzystując narzędzia do zarządzania hasłami, zminimalizujemy ryzyko ataków, zapewniając bezpieczeństwo i stabilność naszego biznesu. Ochrona danych i reputacji przedsiębiorstwa jest w naszych rękach.

## CZYM SĄ SILNE HASŁA?

Jednym z fundamentalnych aspektów ochrony są silne hasła. W dzisiejszym świecie, gdzie technologia odgrywa kluczową rolę, zabezpieczenie swoich danych staje się priorytetem.

Silne hasła to sekwencje znaków, które są trudne do odgadnięcia lub złamania. Są to kombinacje liter, cyfr i znaków specjalnych, które zabezpieczają dostęp do kont, systemów czy danych.

Istota silnych haseł leży w ich złożoności i trudności odgadnięcia, co sprawia, że są skuteczną barierą dla potencjalnych atakujących.

**Cechy silnych haseł:**

- **Długość** - im dłuższe hasło, tym trudniejsze do złamania. Rekomendowane długości to co najmniej 12 znaków.
- **Różnorodność** - hasła powinny zawierać różnorodne rodzaje znaków, takie jak duże czy małe litery, cyfry oraz znaki specjalne. Ta różnorodność czyni je bardziej złożonymi, trudniejszymi do odgadnięcia.
- **Brak przewidywalności** - ważne jest, aby hasła były nieprzewidywalne i nie oparte na łatwo dostępnych informacjach, takich jak imiona czy daty urodzenia. Należy unikać oczywistych sekwencji lub słów, które można znaleźć w słowniku.
- **Unikalność** - każde hasło powinno być unikalne dla danego konta czy systemu. Unikając wielokrotnego wykorzystywania tego samego hasła, minimalizujemy ryzyko, że jego złamanie wpłynie na inne konta.
- **Brak logicznych zależności** - silne hasła nie powinny opierać się na logicznych zależnościach, takich jak kolejność klawiszy na klawiaturze czy proste wzory. Wprowadzenie chaosu w układ znaków sprawia, że stają się one bardziej nieprzewidywalne.

Odpowiednio zabezpieczone hasło znacząco utrudni hakerom zadanie, a nawet może skutecznie ich odstraszyć. Wprowadzając silne hasła, stawiamy solidne fundamenty pod bezpieczeństwo naszych danych. Jest to pierwszy, podstawowy krok, który każdy z nas może podjąć, aby zwiększyć swoją cyberodporność. To nie tylko kwestia technologii, ale także świadomości i odpowiedzialności. Trudne do odgadnięcia hasła to inwestycja w nasze bezpieczeństwo online.

## MENEDŻERY HASEŁ JAKO SKUTECZNE NARZĘDZIA DO ZARZĄDZANIA HASŁAMI

Już wiemy, jak powinny być zbudowane hasła oraz czego należy unikać, ale jak to wszystko

zapamiętać? Nasza pamięć niestety bywa zawodna, a notowanie haseł w poczciwym notatniku, schowanym na dnie szuflady w naszym biurku też nie jest zbyt bezpieczne i odchodzi do lamusa. Zarządzanie wieloma silnymi hasłami może okazać się niemałym wyzwaniem. Na szczęście istnieją narzędzia, które pomagają w tym zadaniu, zapewniając wygodę i bezpieczeństwo. Przyjrzyjmy się, dlaczego menedżer haseł to skuteczne narzędzie i dokonajmy przeglądu kilku popularnych aplikacji stworzonych do tych celów.

**Menedżer haseł jako skuteczne narzędzie do zarządzania hasłami:**

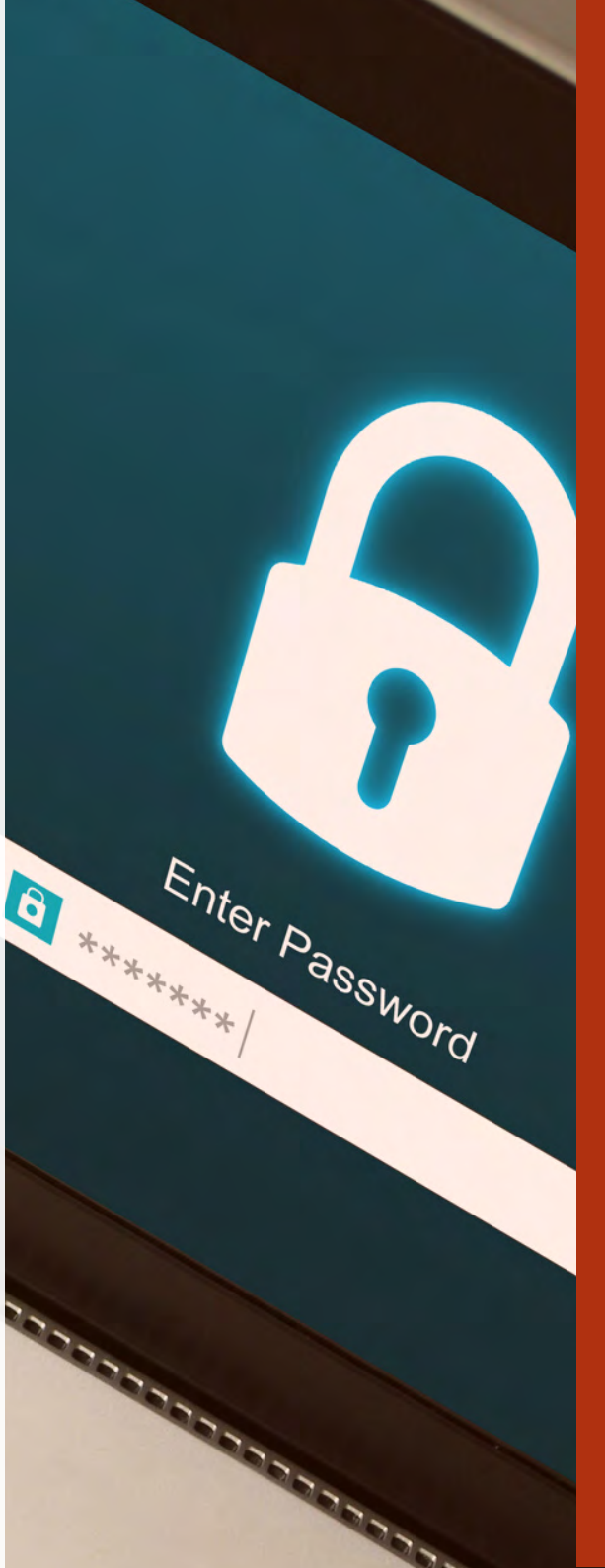
a) **Zarządzanie i przechowywanie haseł** - menedżer haseł pozwala na przechowywanie wszystkich haseł i loginów w jednym bezpiecznym miejscu. Użytkownik może zabezpieczyć taką aplikację jednym silnym hasłem głównym.

b) **Generowanie silnych haseł** - menedżery oferują funkcję automatycznego generowania skomplikowanych, długich haseł, które są trudne do odgadnięcia. To eliminuje potrzebę zapamiętywania skomplikowanych sekwencji znaków.

c) **Synchronizacja na różnych urządzeniach** - dzięki temu, że hasła są przechowywane w chmurze, można mieć do nich dostęp z różnych urządzeń, co znacznie ułatwia korzystanie z kont i aplikacji na co dzień.

**Przegląd popularnych narzędzi:**

**LastPass** to popularny menedżer haseł, idealny dla użytkowników prywatnych, jak i biznesowych. Dbając o bezpieczeństwo, wykorzystuje silne 256-bitowe szyfrowanie AES, chroniąc dane przed hakerami. Powiadamia też o słabych czy powtarzających się hasłach i monitoruje Dark Web w poszukiwaniu wycieków danych. Jest kompatybilny z wieloma popularnymi przeglądarkami oraz systemami operacyjnymi.

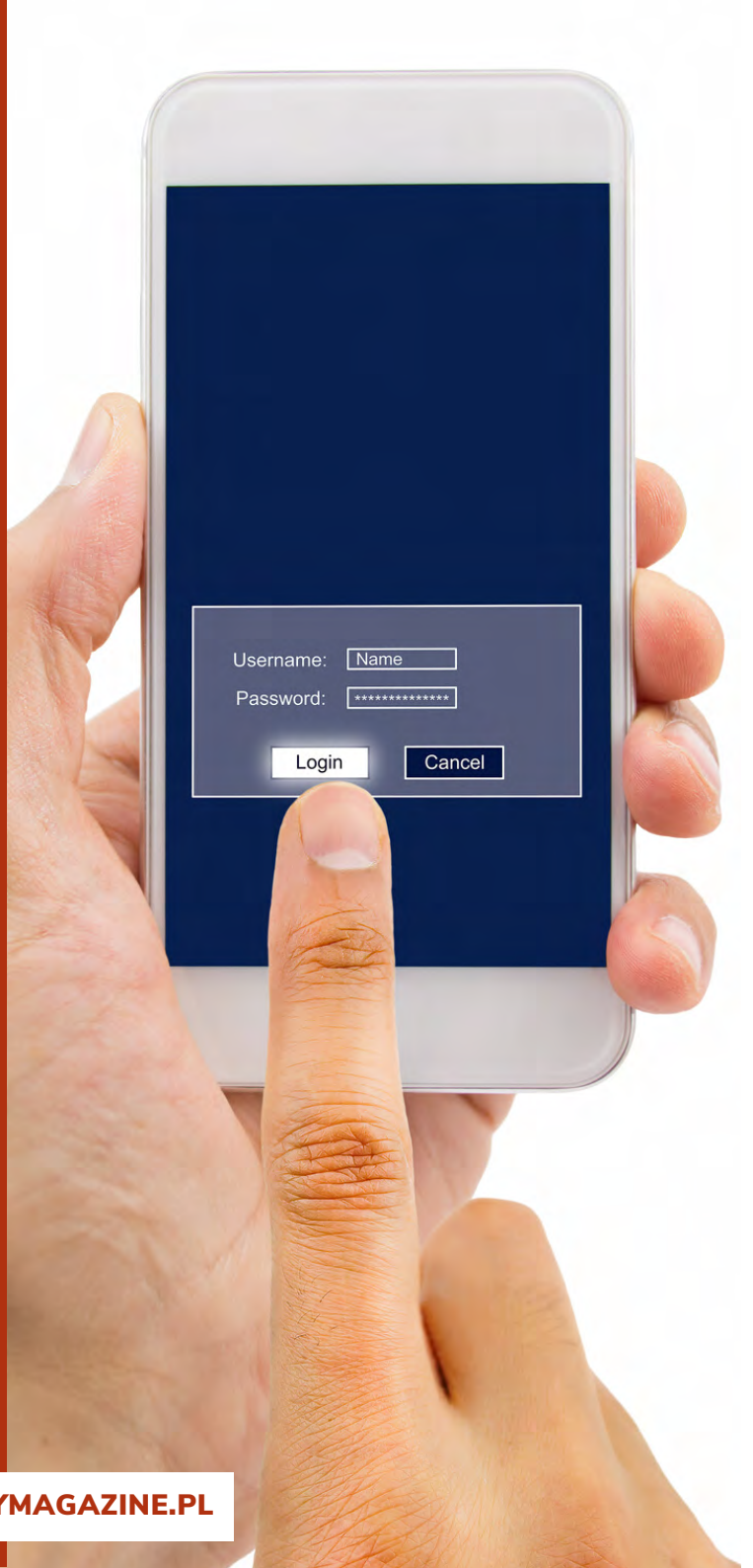


LastPass dodaje warstwę ochrony poprzez funkcję PBKDF2-SHA256, której działanie sprawia, że atak brute force na główne hasło jest niemożliwy. Dla dodatkowego zabezpieczenia oferuje uwierzytelnianie wieloskładnikowe, w tym 2FA, SMS-y, klucze sprzętowe i logowanie biometryczne. Istotne jest, że LastPass działa w oparciu o model "zero-knowledge", co oznacza, że dane i główne hasło są absolutnie poufne nawet dla pracowników LastPass. Dodatkowo, LastPass spełnia surowe regulacje dotyczące ochrony danych, takie jak GDPR (RODO), zapewniając tym samym pełną ochronę informacji.

**Dashlane** to doskonały menedżer haseł, który gwarantuje maksymalne bezpieczeństwo. Korzysta z zaawansowanej technologii szyfrowania, aby chronić hasła i dane. Tworzona przez niego architektura bezpieczeństwa opiera się na opatentowanych rozwiązaniach, uniemożliwiając dostęp do informacji osobom postronnym, w tym pracownikom Dashlane. Dashlane oferuje różnorodne poziomy szyfrowania, takie jak AES 256-bit, PBKDF2 i zabezpieczenia SSL/TLS, zapewniając bezpieczną komunikację. Dodatkowo, obsługuje uwierzytelnianie 2FA i umożliwia logowanie biometryczne przy użyciu Face ID i odcisku palca.

Jest zgodny z regulacjami GDPR (RODO). W zestawie z Dashlane znajduje się usługa VPN. Aplikacja działa na urządzeniach mobilnych oraz w popularnych przeglądarkach. Niestety, nie ma aplikacji na komputery dla systemów Windows, Mac, Linux, dostępne są aplikacje na Android i iOS.

**1Password** jak dwa poprzednie, wykorzystuje potężne 256-bitowe szyfrowanie AES, które jest powszechnie używane przez banki i instytucje wojskowe. Wszystkie informacje przechowywane w skrytkach 1Password są zabezpieczone szyfrowaniem end-to-end. Podczas przesyłania hasła na serwery 1Password, korzystamy z protokołów TLS/SRP w celu dodatkowego zabezpieczenia. Aplikacja gwarantuje, że podczas rejestracji generowany jest unikatowy Secret Key, który wraz z hasłem głównym służy do szyfrowania i odszyfrowywania danych. Dla wzmocnienia bezpieczeństwa kluczy używa technologii PBKDF2, co zapewnia odporność na ataki słownikowe. Aplikacja jest również kompatybilna z uwierzytelnianiem 2FA. Aplikacja działa na urządzeniach z systemami Android i Windows, macOS, ChromeOS, Linux. Posiada rozszerzenia na wszystkie popularne przeglądarki.




Na rynku istnieje wiele menedżerów haseł, więc z pewnością każdy znajdzie coś dla siebie. Oprócz tych wymienionych oraz opisanych powyżej, warto zwrócić uwagę na: NordPass, RoboForm, Keeper, Sticky Password. Tego typu menedżery są niezwykle pomocne, umożliwiają przechowywanie silnych haseł w bezpieczny sposób oraz ułatwiają korzystanie z wielu kont online. Każde z wymienionych narzędzi ma swoje mocne strony, dlatego zawsze warto porównać kilka rozwiązań.

## TECHNOLOGIE WSPOMAGAJĄCE - MFA, 2FA I BIOMETRIA

Zapewnienie odpowiedniego poziomu bezpieczeństwa w sieci jest dziś priorytetem. Silne hasła są ważnym elementem, ale wspomaganie ich dodatkowymi technologiami to kluczowy krok w zabezpieczaniu kont. Dwuetapowe uwierzytelnianie (2FA) oraz wieloskładnikowe uwierzytelnianie (MFA) to dwie znaczące metody w tym kontekście. Współcześnie istnieje szereg metod uwierzytelniania MFA, które pozwalają użytkownikom zweryfikować swoją tożsamość.

**Oto najpopularniejsze technologie stosowane w ramach uwierzytelniania MFA:**

- uwierzytelnianie za pomocą SMS,
- powiadomienia Push,
- uwierzytelnianie hasłem poprzez e-mail,
- uwierzytelnianie przez telefon,
- uwierzytelnianie tokenem sprzętowym - wykorzystywany jest specjalny token sprzętowy, niewielkie urządzenie służą-

ce do autoryzacji. Token generuje losowe hasło, które użytkownik wprowadza podczas logowania. Jest powszechnie stosowany w sektorach bankowych, ubezpieczeniowych i inwestycyjnych;

- soft token, czyli token aplikacyjny - coraz popularniejsze staje się uwierzytelnianie oparte na aplikacjach, takich jak np. Google Authenticator, które generują kody jednorazowe na smartfonie użytkownika;
- uwierzytelnianie biometryczne - stanowi najbardziej zaawansowaną metodę weryfikacji. Wykorzystuje indywidualne cechy fizyczne użytkownika, takie jak odcisk palca, kształt twarzy, tęczówka oka, a nawet charakterystyczne zachowania, np. gesty.

Dzięki różnorodności tych technologii użytkownicy mogą wybrać sposób uwierzytelnienia, który najlepiej spełnia ich potrzeby i zapewnia wysoki poziom bezpieczeństwa.

## DLACZEGO WARTO WDROŻYĆ POLITYKĘ HASEŁ W FIRMIE?

Wdrożenie polityki haseł w firmie jest niezwykle istotne z perspektywy zapewnienia bezpieczeństwa danych i systemów informatycznych. Oto kilka kluczowych powodów, dlaczego warto to zrobić:

- **Ochrona przed nieautoryzowanym dostępem.** Polityka haseł pozwala na kontrolę dostępu do systemów, aplikacji i danych. Silne hasła stanowią pierwszą linię obrony przed potencjalnymi cyberatakami, uniemożliwiając nieuprawnionym osobom uzyskanie dostępu do wrażliwych informacji.
- **Zminimalizowanie ryzyka naruszeń bezpieczeństwa.** Ustalanie zasad dotyczących długości, złożoności i okresu ważności haseł pozwala zminimalizować ryzyko naruszeń bezpieczeństwa. Przemyślana polityka haseł sprawia, że atakującym jest znacznie trudniej odgadnąć lub złamać hasła.

- **Zabezpieczenie danych klientów i pracowników.** Wiele firm przechowuje wrażliwe dane swoich klientów i pracowników. Przemyślana polityka haseł pozwala zabezpieczyć te informacje przed niepożądanym wykorzystaniem, kradzieżą tożsamości czy innymi cyberzagrożeniami.
- **Zgodność z regulacjami prawno-organizacyjnymi.** Wiele regulacji (np. RODO) nakłada obowiązek stosowania silnych haseł. Wdrożenie odpowiedniej polityki haseł jest nie tylko kwestią bezpieczeństwa, ale również zgodności z obowiązującymi przepisami prawa.
- **Uniknięcie utraty reputacji.** Incydenty związane z naruszeniami bezpieczeństwa, wyciekami danych czy włamaniami do systemów mogą znacznie zaszkodzić reputacji firmy. Działając zgodnie z dobrze opracowaną polityką haseł, firma minimalizuje ryzyko takich incydentów oraz utraty zaufania klientów.

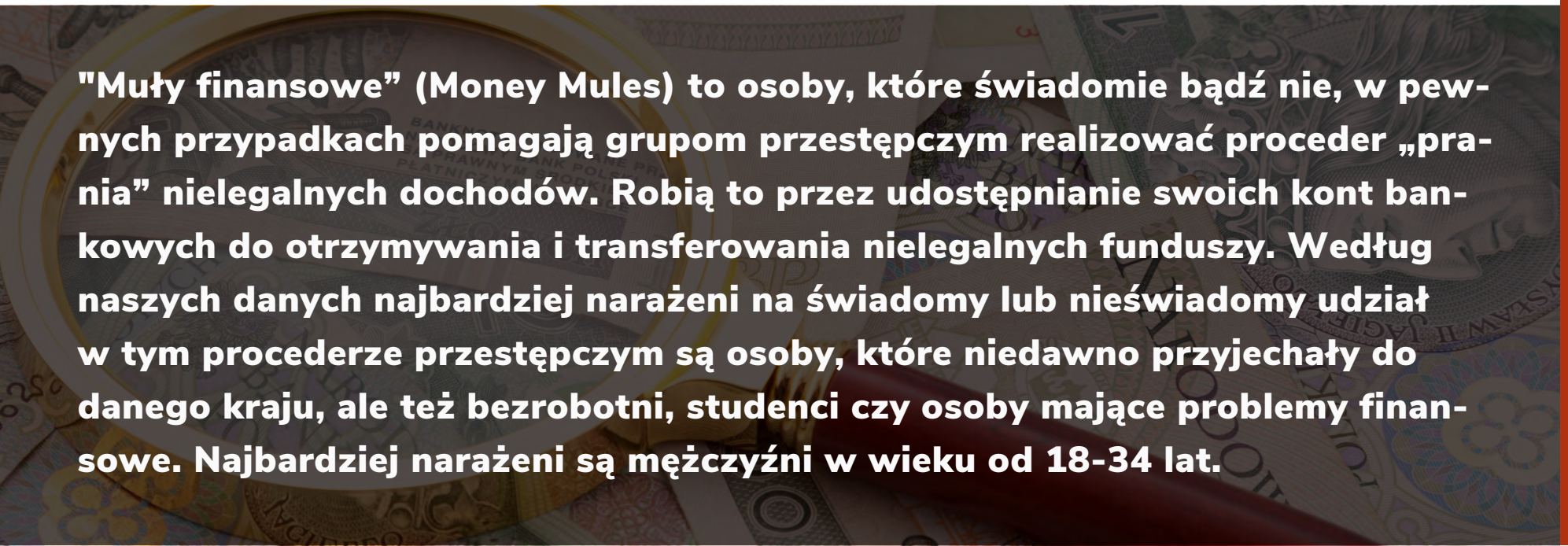
Wprowadzenie i egzekwowanie spójnych, odpowiednio zdefiniowanych zasad dotyczących haseł przyczynia się do zwiększenia poziomu ochrony przed zagrożeniami związanymi z cyberbezpieczeństwem.

Współczesne środowisko biznesowe, splatające się z cyfrowym światem, zobowiązuje przedsiębiorstwa do zabezpieczania swoich aktywów i danych w sposób skuteczny. Inwestycja w świadomość pracowników, szkolenia dotyczące bezpieczeństwa oraz narzędzia wspierające są wręcz obowiązkiem każdej odpowiedzialnej firmy.


Rzetelny Regulamin®
Kompleksowa obsługa prawna Twojego e-commerce

# MUŁY FINANSOWE – SPOSÓB NA „PRANIE PIENIĘDZY”

podkom. Marcin Zagórski
Centralne Biuro Zwalczania Cyberprzestępczości



**"Muły finansowe” (Money Mules) to osoby, które świadomie bądź nie, w pewnych przypadkach pomagają grupom przestępczym realizować proceder „prania” nielegalnych dochodów. Robią to przez udostępnianie swoich kont bankowych do otrzymywania i transferowania nielegalnych funduszy. Według naszych danych najbardziej narażeni na świadomy lub nieświadomy udział w tym procederze przestępczym są osoby, które niedawno przyjechały do danego kraju, ale też bezrobotni, studenci czy osoby mające problemy finansowe. Najbardziej narażeni są mężczyźni w wieku od 18-34 lat.**

## KTO MOŻE ZOSTAĆ MUŁEM FINANSOWYM?

Często są to osoby, które niedawno przybyły do danego kraju. Mają trudności finansowe, pozostają bezrobotne. Odnotowuje się także wzrost liczby przypadków, w których w nielegalnym obrocie pieniędzmi udział biorą młodzi ludzie. Przestępcze oferty kierowane są do studentów znajdujących się w trudnej sytuacji finansowej.

Jednym ze sposobów rekrutacji są ogłoszenia o ofercie pracy. Przestępcy udający przedsiębiorców oferują szybki zysk. Jedyne czego wymagają to przelew niewielkiej kwoty. Zwykle tłumaczą to koniecznością uzyskania potwierdzenia tożsamości. W ten sposób organizatorzy tego procederu uzyskują dostęp do konta osób. Często poza świadomością przez konta mułów finansowych przechodzą znaczne sumy pieniędzy.

Niestety, konsekwencje dla osób, które stały się mułami finansowymi mogą być bardzo bolesne. Więzienie, a w dalszej perspektywie tzw. przestępcza przeszłość, co może negatywnie wpłynąć na pracę. Może się zdarzyć, że takie osoby nie będą mogły założyć konta bakowego. Nie będą mogły uzyskać kredytu np. na zakup mieszkania.

## JAK WYGLĄDA REKRUTACJA NA TZW. MUŁA?

Grupy przestępcze wykorzystują do tego nowe technologie i trendy, organizując i opracowując nowe systemy pozyskiwania ludzi poprzez:

- pozornie legalne ogłoszenia o pracę („agenci finansowi"),
- fałszywe komentarze potwierdzające legalność firmy lub pracodawcy,
- bezpośredni kontakt za pośrednictwem poczty elektronicznej,
- portale społecznościowe (np.: posty na zamkniętych grupach),
- wiadomości wysyłane za pośrednictwem szyfrowanych komunikatorów.

## DLACZEGO LUDZIE POMAGAJĄ PRZESTĘPCOM PRAĆ PIENIĄDZE?

Przestępcom chodzi o ukrycie pochodzenia nielegalnie zdobytych pieniędzy. Osoby stające się mułami finansowymi kuszone są obietnicą łatwych pieniędzy. Mechanizm działania jest prosty: muły przesyłają skradzione pieniądze między kontami, często w różnych państwach, w imieniu innych osób i zwykle otrzymują część funduszy, które przechodzą przez ich własne konta. Nawet jeśli tzw. „muły” nie są osobami bezpośrednio zaanga-

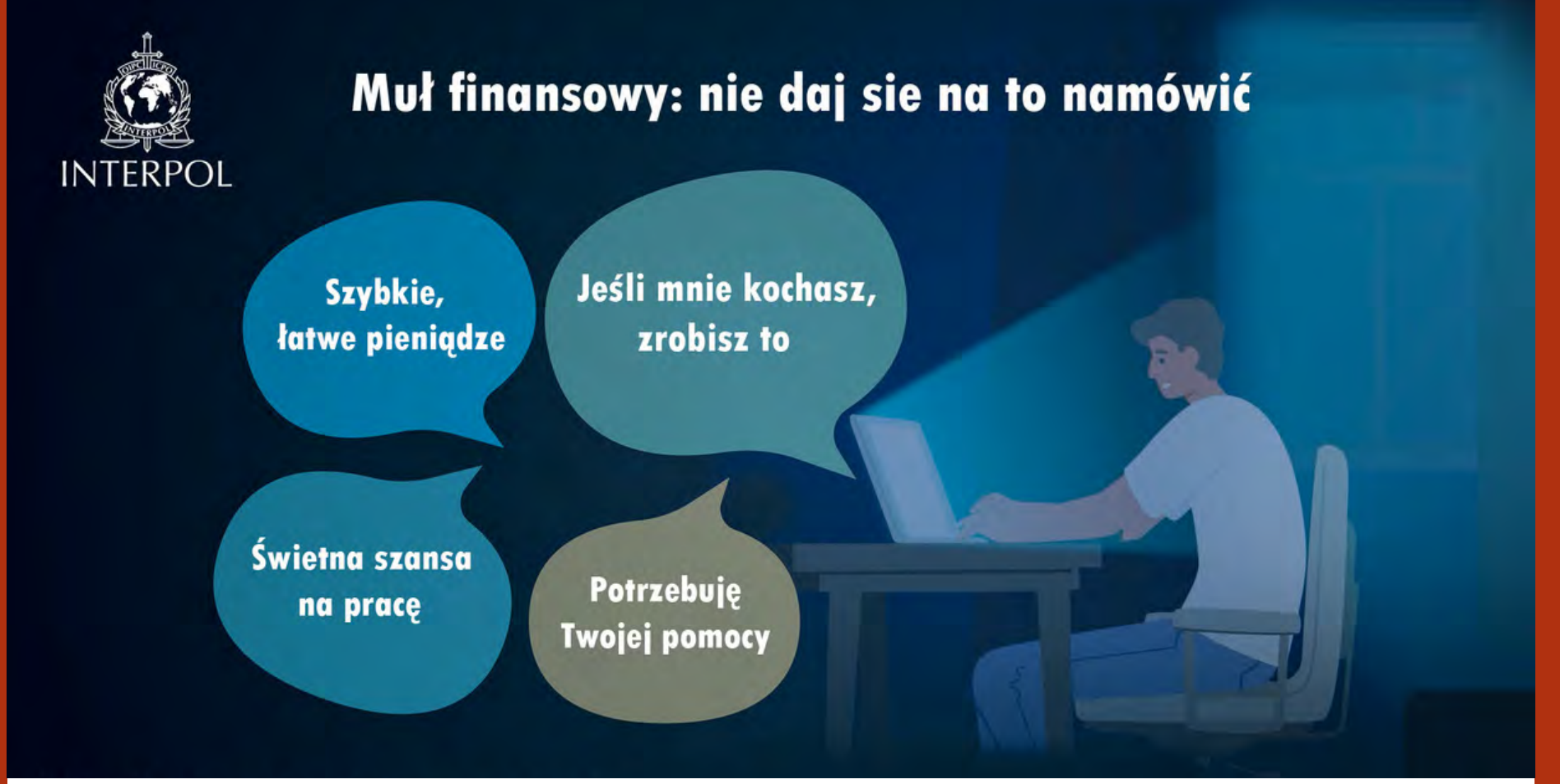

żowanymi w proceder generowania pieniędzy (cyberprzestępstwo, płatności i oszustwa on-line, narkotyki i handel ludźmi itd.), działają one nielegalnie uczestnicząc w procederze tzw. „prania pieniędzy” pochodzących z przestępstwa, pomagając w ten sposób grupom przestępczym łatwo rozprowadzać skradzione fundusze na całym świecie i pozostać anonimowymi.

Jeżeli taki „muł finansowy” zostanie złapany na wspomaganiu przestępczego procederu, nawet jeśli robi to nieświadomie, może ponieść odpowiedzialność karną, a także mieć poważne problemy w uzyskaniu kredytu hipotecznego czy chociażby otworzeniu konta bankowego. Ponad 90% transakcji pieniężnych przy użyciu tzw. „mułów finansowych jest związanych z cyberprzestępczością.


Nielegalnie pozyskiwane pieniądze często pochodzą z ataków typu "phishing”, złośliwego oprogramowania, oszustw związanych z zakupami on-line oraz dokonywanymi poprzez płatności z wykorzystaniem bezgotówkowych form tj. karty płatnicze.

**Co może wskazywać, że bierzemy udział w nielegalnym procederze prania pieniędzy?**

- nieznajoma osoba obiecuje łatwy zarobek,
- ogłoszenia o pracę firm zagranicznych poszukujących „lokalnych /krajowych agentów” do działania w ich imieniu,




- adres e-mail nadawcy został stworzony prawdopodobnie z wykorzystaniem bezpłatnej usługi internetowej, gdzie nazwa domeny i login nie pasują do nazwy firmy,
- przesyłane wiadomości zawierają złą pisownię oraz błędy ortograficzne,
- wszystkie interakcje oraz transakcje dotyczące pracy będą wykonywane on-line,
- specyfika pracy zakłada wykorzystywanie konta bankowego do transferu pieniędzy,
- w ofercie pracy brak jest wymienionych wymagań dotyczących wykształcenia lub doświadczenia zawodowego,

## JAK SIĘ PRZED TYM CHRONIĆ ?

- Jeśli okazja brzmi zbyt dobrze, prawdopodobniej tak nie jest.
- Ostrożnie sprawdzaj e-maile, otrzymane z nieznanych adresów, jak i rozważnie podchodź do wpisów na stronach internetowych me-


diów społecznościowych obiecujących możliwości zarabiania pieniędzy.

- Sprawdź dane kontaktowe firmy oferującej pracę (adres pocztowy, telefon stacjonarny, stronę internetową) czy są prawidłowe oraz czy firma jest zarejestrowana w Polsce.
- Bądź szczególnie ostrożny w przypadku ofert pracy od osób lub firm z zagranicy, gdyż trudniej będzie zweryfikować ich działalność, czy jest zgodna z prawem.
- Nigdy nie podawaj nikomu swojego konta bankowego, ani innych danych osobowych, chyba że znasz osobę i jej ufasz.

## CO ROBIĆ?

Jeśli po przeczytaniu powyższych informacji uwa-

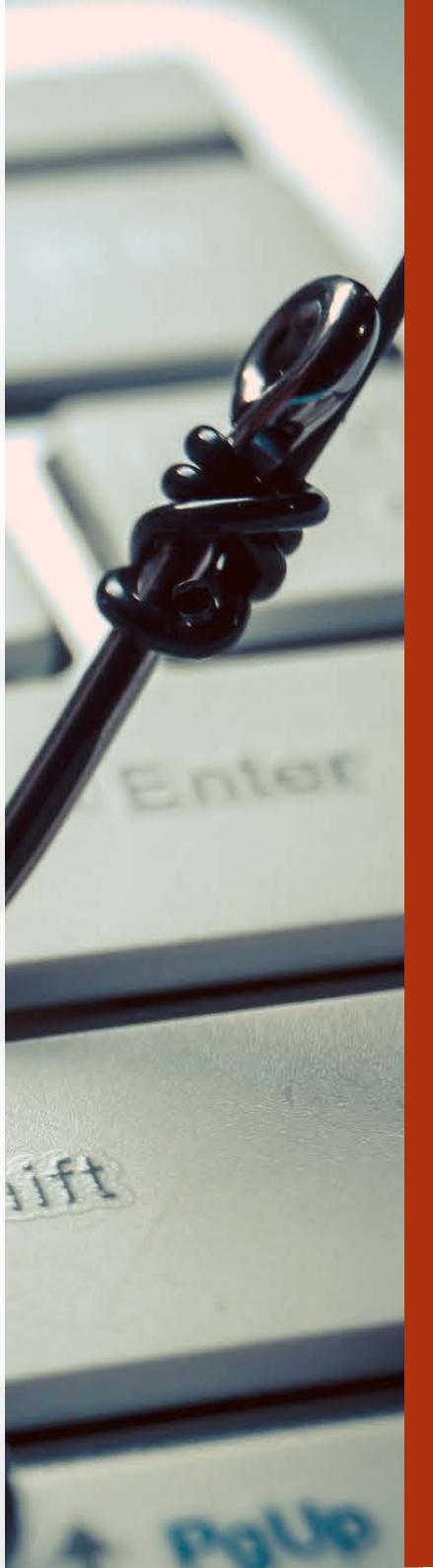
żasz, że uczestniczysz w przestępczym procederze, natychmiast przestań przekazywać pieniądze, powiadom swój bank o transakcji, jaką przeprowadziłeś oraz powiadom organy ścigania! Nie odpowiadaj na przesłane e-maile oraz nie klikaj na żaden z linków, które zawierają podejrzane treści!

## KAMPANIA PREWENCYJNA W MEDIACH

Centralne Biuro Zwalczania Cyberprzestępczości już po raz drugi aktywnie włączyło się w kampanię profilaktyczną opisującą skalę zjawiska oraz określającą odpowiedzialność, która grozi osobom podejmującym działania wyczerpujące znamiona „mułów finansowych” (money mules).

Działania będą miały na celu uświadomienie obywatelom powagi przedmiotowego przestępstwa, a w szczególności ostrzeżenie przed odpłatnym udostępnianiem własnych danych osobowych lub rachunków bankowych do różnego rodzaju pośrednictwa finansowego m.in. w Internecie. Działania CBZC podejmowane są pod auspicjami Europejskiego Centrum ds. Cyberprzestępczości (EC3) działającego przy Europolu (Europejskiego Urzędu Policji) oraz we współpracy z Bankowym Centrum Cyberbezpieczeństwa Związku Banków Polskich. Europol to Europejski Urząd Policji mieszczący się w Hadze (Królestwo Niderlandów), powstały w roku 1999 Zadaniami Europolu jest m.in. zwiększanie poziomu bezpieczeństwa w Europie poprzez zapewnianie pomocy organom ścigania w państwach członkowskich UE.

Z kolei EC3 (Europejskie Centrum ds. Cyberprzestępczości) powołane w 2013 roku ma na celu wzmocnienia działań związanych z egzekwowaniem prawa w sprawach dotyczących cyberprzestępczości w UE, a tym samym na rzecz ochrony europejskich obywateli, przedsiębiorstw i rządów przed przestępczością internetową.

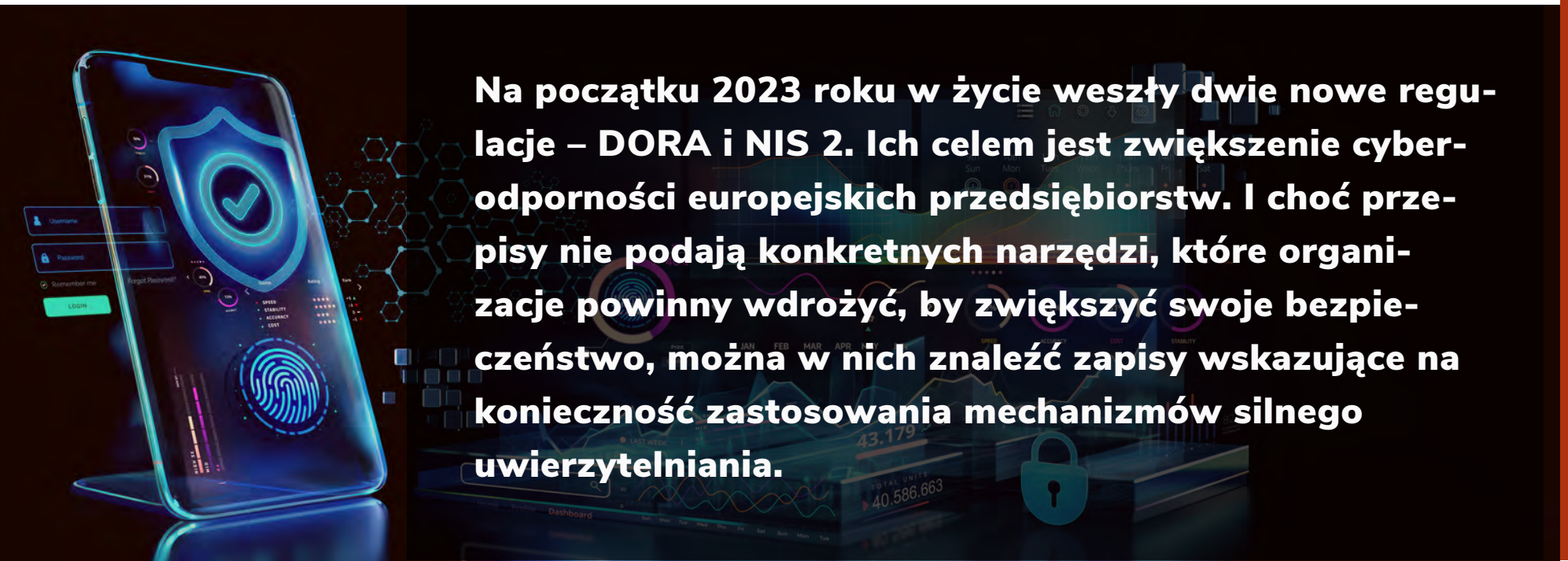



*Błędy się zdarzają. Jeśli podejrzewasz, że możesz być zaangażowany w proceder prania pieniędzy, natychmiast go zakończ.*


Polityka ®
Bezpieczeństwa
SZKOLENIA
Z OCHRONY DANYCH
OSOBOWYCH
SPRAWDŹ OFERTĘ

# WIELOSKŁADNIKOWE UWIERZYTELNIANIE W ŚWIETLE DORA I NIS 2

**Tomasz Kowalski**
Secfense



**Na początku 2023 roku w życie weszły dwie nowe regulacje – DORA i NIS 2. Ich celem jest zwiększenie cyberodporności europejskich przedsiębiorstw. I choć przepisy nie podają konkretnych narzędzi, które organizacje powinny wdrożyć, by zwiększyć swoje bezpieczeństwo, można w nich znaleźć zapisy wskazujące na konieczność zastosowania mechanizmów silnego uwierzytelniania.**

DORA (rozporządzenie dotyczące operacyjnej odporności cyfrowej sektora finansowego) i NIS 2 (dyrektywa dotycząca środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa) dość ogólnikowo mówią o tym, w jaki sposób zabezpieczać zasoby firmowe. Wymagają jednak zastosowania odpowiednich strategii, polityk, procedur, protokołów i narzędzi ICT, które pozwolą zabezpieczyć systemy, aplikacje i bazy danych, w szczególności zaś uniemożliwią dostęp do nich niepowołanym osobom.

Jakich narzędzi zabezpieczających użyć? Z ekspertami Fundacji Law4Tech przeanalizowaliśmy teksty obu dokumentów. Okazuje się, że tak DORA, jak i NIS 2 wskazują mechanizmy wieloskładnikowego uwierzytelniania jako podstawowe narzędzia zabezpieczające w organizacjach.

## DORA: „PODMIOTY FINANSOWE WDRAŻAJĄ MECHANIZMY SILNEGO UWIERZYTELNIANIA”

Przekaz rozporządzenia DORA jest jasny. Pada w nim jednoznaczne sformułowanie: podmioty finansowe wdrażają silne mechanizmy uwierzytelniania.

Organizacje nie powinny mieć żadnych wątpliwości dotyczących interpretacji tego zapisu – regulacja ta w sposób bezpośredni nakłada na podmioty finansowe obowiązek wdrożenia silnych mechanizmów uwierzytelniania, nie pozostawiając im pola do własnego uznania.

Dodajmy do tego jeszcze kilka słów wyjaśniania. DORA, a dokładniej art.4, przewiduje możliwość zróżnicowania ochrony ICT zgodnie z zasadą proporcjonalności. Innymi słowy, podmioty finansowe powinny dostosować ochronę swoich zasobów do swojej wielkości, ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności realizowanych usług. Większe podmioty, działające na większą skalę, powinny mieć zabezpieczenia na wyższym poziomie niż organizacje mniejsze.

Jak jednak rozróżnić te organizacje, które uznać za mniejsze, a które za większe? DORA nie daje jednoznacznych odpowiedzi. Każde przedsiębiorstwo musi samodzielnie oszacować swoją wielkość oraz skalę działania, po czym wdrożyć odpowiednie środki ochrony. Czy uczyni to poprawnie?
O tym będzie decydować Komisja Nadzoru Finansowego (KNF) przy okazji przeprowadzania kontroli.

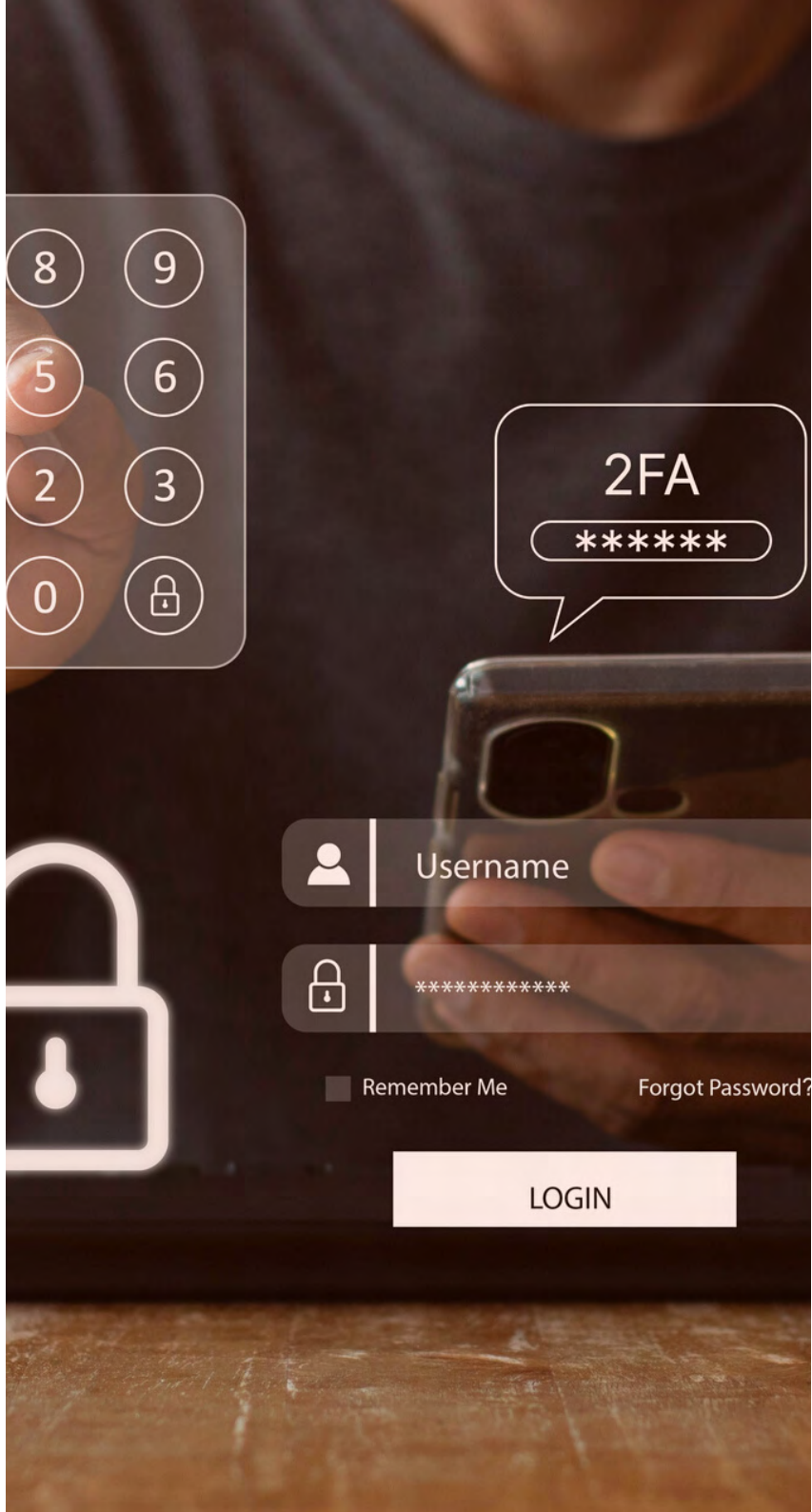
Można zatem przypuszczać, że w miarę stosowania przepisów DORA będą się pojawiały kolejne interpretacje przepisów wydawane przez KNF. Nie należy się jednak spodziewać rezygnacji z wymogu stosowania mechanizmów silnego uwierzytelniania. Wpisuje się on bowiem w aktualne rekomendacje krajowych instytucji nadzorczych.

Już w październiku 2022 r. Komisja Nadzoru Finansowego podkreśliła w jednym ze swoich pism, że *"brak stosowania silnego, wieloskładnikowego uwierzytelnienia klientów jest nieakceptowalnym ryzykiem"*. W opinii prawników, z którymi się konsultowaliśmy, nie należy więc mieć wątpliwości co do stanowiska krajowego organu nadzorczego w tej sprawie.

## NIS 2: PODSTAWĄ JEST WDROŻENIE ODPOWIEDNICH ŚRODKÓW BEZPIECZEŃSTWA

Dyrektywa NIS 2 nakłada na podmioty kluczowe i ważne obowiązek wprowadzenia podstawowych praktyk cyberhigieny. Należą do nich między innymi zasada zerowego zaufania, regularna aktualizacja oprogramowania, odpowiednia konfiguracja urządzeń, segmentacja sieci, zarządzanie tożsamością i dostępem lub świadomość użytkowników, organizacja szkolenia dla pracowników oraz szerzenie wiedzy na temat cyberzagrożeń, phishingu i technik inżynierii społecznej.

Według NIS 2 organizacje samodzielnie powinny ocenić własne zdolności w zakresie cyberbezpieczeństwa i w stosownych przypadkach wdrożyć odpowiednie technologie zabezpieczające, takie jak systemy oparte na sztucznej inteligencji (AI) lub uczeniu maszynowym (ML), aby poprawić swoje zdolności do ochrony przed cyberprzestępcami.




Co tu ukrywać – to daleko idące wymagania i rekomendacje. Jeśli zatem rozwiązania oparte na AI czy ML mają stać się standardem w przedsiębiorstwach, tym bardziej mechanizmy silnego uwierzytelniania powinny zostać uznane za podstawowy mechanizm ochronny i stanowić fundament ekosystemu cyberbezpieczeństwa w organizacji.

Tym bardziej, że technologia ta jest rekomendowana coraz częściej przez administrację publiczną i organy nadzoru różnych sektorów, w tym Urząd Ochrony Danych Osobowych. UODO podniósł ten temat m.in. przy sprawie Morele.

W swojej decyzji z 10 września 2019 roku podkreślał: *„kontrola dostępu i uwierzytelnianie to podstawowe środki bezpieczeństwa mające na celu ochronę przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Zapewnienie dostępu uprawnionym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów i usług to jeden z wzorcowych elementów bezpieczeństwa”*.

## CZYM JEST SILNE UWIERZYTELNIANIE I JAK JE SZYBKO WDROŻYĆ?

Przepisy nie pozostawiają zatem wątpliwości – firmy z sektora finansowego i organizacje działające w obszarach uznanych za kluczowe i ważne dla gospodarki i społeczności będą musiały zastosować mechanizmy silnego uwierzytelniania.

Silnego, czyli wymagającego co najmniej dwóch elementów potwierdzających tożsamość użytkownika. Dlaczego to takie ważne?

Uwierzytelnianie wieloskładnikowe (MFA, multi-factor authentication) jest jednym z najlepszych sposobów zabezpieczenia się przed phishingiem, socjotechniką i kradzieżą uwierzytelnień. Zwiększa bezpieczeństwo procesu logowania, wymagając użycia co najmniej dwóch niezależnych składników uwierzytelniania. To może być coś, co dana osoba wie (składnik wiedzy), coś, co dana osoba ma (składnik posiadania), lub to, kim dana osoba jest (składnik cechy).

- **Składniki wiedzy** to między innymi wzory blokady, hasła, kody PIN i osobiste pytania, na przykład pytanie o nazwisko panieńskie matki.
- **Składniki posiadania** to obiekty fizyczne w tym klucze kryptograficzne lub lokalne uwierzytelniacze (na przykład smartfony).
- **Składniki cech** opierają się na danych biometrycznych i obejmują rozpoznawanie twarzy, linii papilarnych czy głosu.

Jeśli organizacji zależy na poprawie bezpieczeństwa aplikacji, może dodać więcej składników lub użyć bardziej zaawansowanych metod uwierzytelniania.

Na rynku jest wiele rozwiązań z obszaru MFA, firmy mają więc w czym wybierać. Jedną z możliwości jest wybór rozwiązania User Access Security Broker, które umożliwia wdrożenie MFA na dowolnej aplikacji w 5 minut oraz wprowadzenie MFA w całej organizacji w 7 do 14 dni. Technologia umożliwia implementację dowolnego MFA, w tym także najskuteczniejszego dziś FIDO2, na każdej aplikacji bez ingerencji w jej kod.

DORA zaczyna obowiązywać 17 stycznia 2025 roku. Termin wdrożenia NIS 2 mija 17 października 2024 roku. Czasu na dostosowanie się do nowych przepisów jest coraz mniej. Firmy, które już teraz przeanalizują swoją sytuację, systemy zabezpieczeń, procedury i strategie i wprowadzą wymagane technologie oraz polityki, będą mogły nie tylko ze spokojem patrzeć w przyszłość, ale też skutecznie walczyć z nasilającymi się atakami cyberprzestępców.

Więcej informacji na temat obowiązków, jakie nakładają na firmy nowe regulacje, można znaleźć w bezpłatnym e-booku **“Analiza regulacji DORA i NIS2 w kontekście cyberbezpieczeństwa przedsiębiorstw w UE”** przygotowanym na podstawie niezależnego raportu Fundacji Law4Tech.

ZAMÓW

# AUDYT BEZPIECZEŃSTWA

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

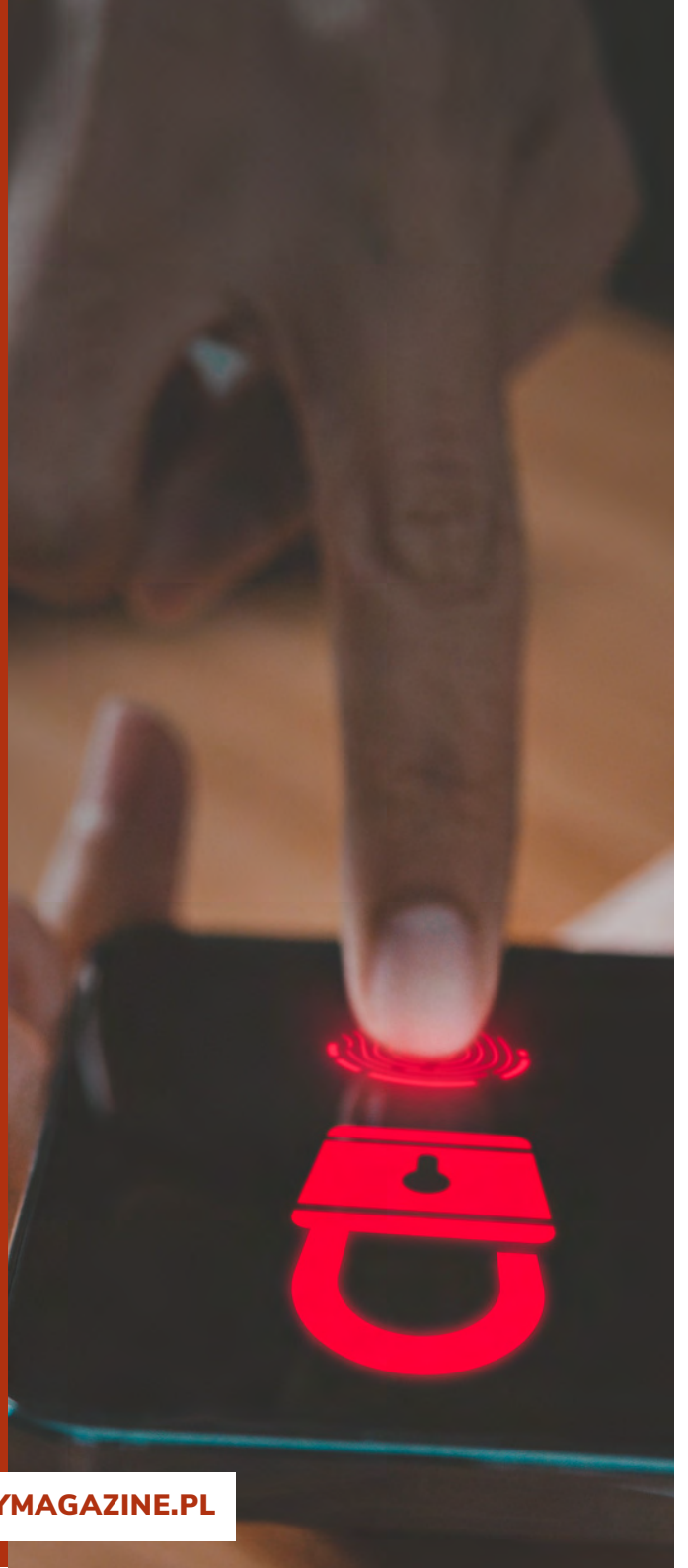
## DOWIEDZ SIĘ WIĘCEJ!

Polityka® Bezpieczeństwa

# KAROL GOLISZEWSKI: SZYFROWANIE - CYBEROCHRONA CZY CYBER-ZAGROŻENIE?

**Karol Goliszewski**
Grandmetric

**W wywiadzie z Karolem Goliszewskim z Grandmetric, zagłębiamy się w temat szyfrowanej transmisji danych, poznając jej zalety, zagrożenia oraz nowoczesne technologie stosowane do wykrywania potencjalnych zagrożeń. Jakie są najnowsze trendy w dziedzinie szyfrowania, jakie wyzwania niesie ze sobą zarządzanie własnym urządzeniem certyfikacji i jakie kroki organizacje powinny podjąć, by chronić swoje dane?**



**Jakie są główne zagrożenia związane z szyfrowaną transmisją danych i jakie technologie są obecnie stosowane do ich wykrywania?**

**Karol Goliszewski:** Paradoksem procesu szyfrowania danych jest to, że jest to proces służący zabezpieczaniu – i w tym miejscu musimy postawić kropkę. Choć brzmi to jak zjawisko pozytywne, pożądane, oczywiście nie zawsze tak jest, ponieważ szyfrowanie przeprowadzane jest w celu ochrony danych i tożsamości... no właśnie, zarówno osoby uczciwej, jak i przestępców. Jest to broń obosieczna, ponieważ zapewnia spokojny sen ludzi prawych, dbających o swoje interesy, jak i tych, którym zależy na skutecznym ukrywaniu się przed organami ścigania.

W odniesieniu do gruntu MŚP, szyfrowanie pozwala na zachowanie poufności treści biznesowych – e-maili, plików, operacji bazodanowych, komunikacji audio i wideo, etc. Jednak dokładnie taką samą technikę wykorzystują oszuści, chcący zagrozić naszym interesom, ukrywając w szyfrowanej transmisji zagrożenia dla naszego biznesu: złośliwe załączniki w poczcie, malware czy tunele, którymi stopniowo penetrują nasze zasoby w celu zdobycia bezcennych informacji i wykorzystania ich później w celach zarobkowych – nieważne, czy to przez handel na czarnym rynku, czy przez szantażowane.

Nie możemy stuprocentowo uchronić się przed tym zjawiskiem, bo producenci zabezpieczeń, są o krok za przestępcami – a nie odwrotnie. Nie zmienia to faktu, że współczesne mechanizmy wykry-

wania zagrożeń w komunikacji szyfrowanej są niezwykle skuteczne. Warto więc się nad nimi pochylić i wdrożyć je w swojej organizacji.

Czołowi producenci urządzeń i systemów security w swoich produktach, jak firewalle klasy Next-Generation, czy systemy XDR, oferują złożone mechanizmy pozwalające na rozszyfrowanie transmisji, skanowanie jej (np. pod kątem wzorców ataków hackerskich, złośliwego oprogramowania czy treści phishingowych) i ponowne zaszyfrowanie – a to wszystko w czasie rzeczywistym. W czasach, gdy lekko szacując 90% komunikacji odbywa się przy pomocy protokołów szyfrowanych, możliwość inspekcji takiego ruchu jest nie opcjonalna, ale wprost konieczna.

**Firewalle Next-Generation – jakie są ich możliwości w zakresie ochrony ruchu szyfrowanego?**

**K.G.:** Firewall klasy Next-Generation, w odróżnieniu od swoich tradycyjnych odpowiedników, oferuje wielowarstwową ochronę transmisji, także szyfrowanej. Jego zdolność do odczytywania komunikacji zaszyfrowanej jest kluczowa, aby móc w ogóle zajrzeć w jej treść i gruntownie ją zbadać nim podejmie się decyzję o tym, czy może ona trafić do odbiorcy, czy też powinna być z jakiegoś względu zablokowana.

Jak to wygląda „od kuchni”? Firewall, stojąc na styku sieci lokalnej z Internetem, jest pośrednikiem między serwerem zdalnym a klientem w sieci lokalnej. Odpowiada za jednoczesne zestawienie dwóch sesji: między sobą a klientem oraz między sobą a serwerem. Takie umiejscowienie daje mu pełną transparentność komunikacji w obu kierunkach, ponieważ szyfrowanie odbywa się nie w relacji klient-serwer, a klient-firewall oraz firewall-serwer, co skutkuje tym, że negocjacja połączenia szyfrowanego zachodzi de facto między firewallem a klientem oraz firewallem i serwerem.

Bezpośrednio na firewallu transmisja jest odszyfrowana, w związku z czym ruch można poddać dokładnej analizie przy udziale szeregu mechanizmów bezpieczeństwa, takich jak:

- **IPS (Intrusion Prevention System)**, wykrywającym wzorce ataków hackerskich na podstawie znanych sygnatur ataków. Jeżeli jakiś hacker próbował się ukryć pod płaszczykiem szyfrowania, to ten mechanizm z pewnością go zdemaskuje i udaremni jego próby kompromitacji sieci,
- **antimalware,** sprawdzających transmisję na okoliczność występowania w niej złośliwego kodu, którego wzorce firewall zna i systematycznie aktualizuje,
- **analiza treści,** niedopuszczająca na przykład do uruchomienia stron internetowych zawierających określony kontekst, odebrania maili zawierającego konkretne słowa kluczowe czy linki, itp.,
- **ochrona przed sabotażem** poprzez rozpoznawanie kontekstu aplikacji i ich blokowanie, co jest na przykład przydatne w sytuacjach, gdy użytkownik lub hacker próbuje ominąć zabezpieczenia sieci przedsiębiorstwa, wykorzystując do tego oprogramowanie VPN lub proxy firm trzecich.

**Jakie są potencjalne wady i ryzyka związane ze skanowaniem transmisji szyfrowanej? Czy istnieją sytuacje, w których skanowanie może prowadzić do naruszenia prywatności lub bezpieczeństwa danych?**

**K.G.:** Zalety z wykorzystywania możliwości skanowania transmisji szyfrowanej są niezaprzeczalne, także dalece przewyższają korzyściami potencjalne ryzyko, które, choć niewielkie, istnieje, i którego należy być świadomym. Jakiekolwiek mechanizmy pośredniczące w transmisji między klientem a serwerem, niezależnie od tego, czy jest to firewall klasy Next-Generation, czy zdolne do analizy ruchu szyfrowanego programy XDR lub podobne, mają dostęp do odszyfrowanej, a zatem w pełni czytelnej, porcji danych.

Jeżeli wskutek błędu producenta takiego rozwiązania dojdzie do wycieku przesyłanych, odszyfrowanych danych, lub będzie można w jakikolwiek sposób uzyskać do nich wgląd, będzie to stanowiło poważne zagrożenie dla bezpieczeństwa danych, ich poufności czy integralności. W takich przypadkach należy się obawiać ataków man-in-the-middle, których cechą charakterystyczną jest udział atakującego w procesie transmisji danych.

Dodatkowo należy mieć świadomość, że producen-


tom rozwiązań security powierzamy pieczę nad danymi na tę krótką chwilę, podczas której np. firewall Next-Generation dokonuje inspekcji ruchu odszyfrowanego. Jeżeli boimy się sabotażu ze strony samego producenta, w myśl którego mógłby on wykorzystać bez naszej wiedzy odczytane przez swoje produkty dane, zawierające poufne dane firmy, przesyłane loginy i hasła, etc., to, technicznie rzecz biorąc, są one uzasadnione, ale patrząc na całokształt tego procesu – pozbawione są sensu.

Producenci tych rozwiązań zarabiają na ochronie danych, w dodatku silnie strzegą swojej reputacji. Jeżeli w ich szeregach nie ma naprawdę zmotywowanych i wyspecjalizowanych sabotażystów w zespołach programistycznych, tego typu teorie możemy pozostawić jedynie w sferze czystej abstrakcji.

**Dlaczego, oprócz certyfikatów wystawianych przez zewnętrzne urzędy CA, warto mieć także własną, lokalną jednostkę tego typu?**

**K.G.:** Lokalny urząd certyfikacji pozwala na udoskonalenie logowania, uzyskiwanie chronionego dostępu do poszczególnych elementów infrastruktury przedsiębiorstwa oraz weryfikowania tożsamości.

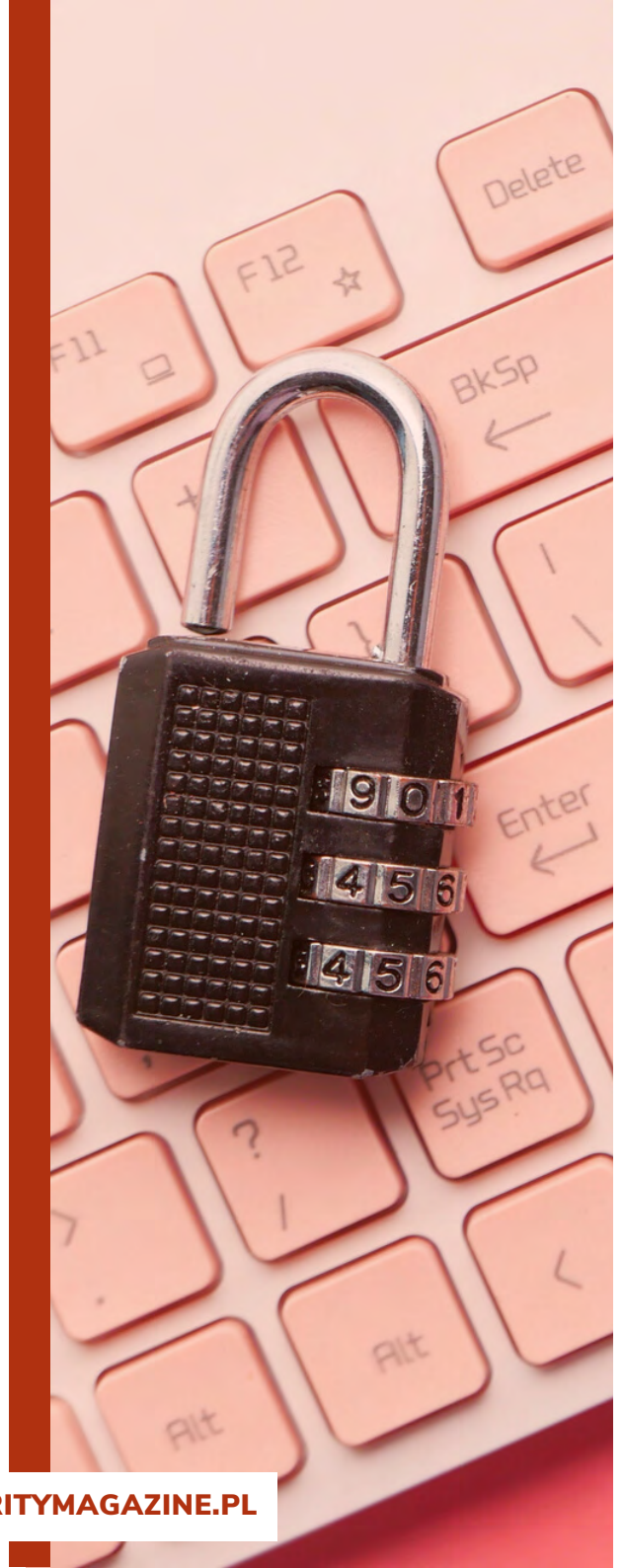
Infrastruktura klucza publicznego (PKI) sprawdza się doskonale w Internecie, np. do potwierdzenia autentyczności usługi serwerów bankowych, serwisów transakcyjnych. Dlaczego

jednak warto zainwestować w instalację i utrzymanie własnego rozwiązania typu PKI? Odpowiedź nie jest trudna: by wyprzeć ze środowiska infrastruktury lokalnej kłopotliwe hasła, których kradzież (np. wskutek phishingu) to najprostsza droga do wycieku i/lub utraty danych przedsiębiorstwa.

Posiadając własne CA (Certification Authority) możemy sprawić, by nasi pracownicy logowali się do komputerów nie hasłem, a kartą inteligentną. Tą samą kartą zresztą możemy (posiadając system budynkowej kontroli dostępu) dać im możliwość dojścia do określonych pomieszczeń w budynku firmy.

Certyfikaty wygenerowane przez lokalne CA pomogą nam zabezpieczyć dostęp do sieci, ponieważ w oparciu o nie możemy ustawić uwierzytelnianie oraz autoryzację w systemach klasy NAC (Network Access Control). Zarządzanie certyfikatami i powiązanymi z nimi uprawnieniami w środowisku z własnym CA to trywialna sprawa. Jednym kliknięciem możemy uprawnienia dla użytkownika rozszerzać, ograniczać lub całkowicie zablokować.

A co z ochroną infrastruktury krytycznej? Działy IT szczególnie docenią fakt, że certyfikaty wygenerowane we własnym CA i zaimportowane do interfejsów managementowych urządzeń i systemów IT pozwolą na zabezpieczenie połączenia administracyjnego. Nie dopuszczą też do ataku man-in-the-middle, ponieważ każda próba podmiany połączenia przez hakera wygeneruje ostrzeżenie. W jego wyniku połączenie powinno zostać natychmiast rozłączone, a sieć uznana za skompromitowaną, co powinno uruchomić natychmiastowe czynniki zaradcze w postaci poszukiwania i wyeliminowania intruza i luki, którą się do nas dostał.




**Jakie są wyzwania związane z zarządzaniem własnym urządzeniem certyfikacji (CA) i jakie praktyki najlepsze pomagają w ich przezwyciężeniu?**

**K.G.:** Własny urząd certyfikacji jest stosunkowo bezproblemowy we wdrożeniu i utrzymaniu, ale przy założeniu, że administrator bardzo konsekwentnie będzie się trzymał kilku krytycznie istotnych reguł:

- będzie ściśle chronił klucz prywatny urzędu, ponieważ jego wyciek oznacza nieodwracalną kompromitację struktury całego PKI,
- nie dopuści do obsługi CA przez osoby do tego celu niepowołane (w myśl zasady: „nie powierzę nikomu niezaufanemu uniwersalnego klucza do wszystkich zamków”),
- będzie dbał o ciągłość aktualności certyfikatów generowanych dla poszczególnych podmiotów,
- skonstruuje redundantne środowisko usługi CA oraz zabezpieczy je najlepszą dostępną formą kopii zapasowej, jako usługę o najwyższym statusie krytyczności.

Wśród best practices dla CA znajdziemy także zapis o tym, by jedna z instancji (główna – root) miała postać maszyny fizycznej, w dodatku wyłączonej praktycznie na stałe – włączanej tylko w celu odnowienia certyfikatów dla podmiotów SubCA.

**W jaki sposób certyfikaty cyfrowe wydawane przez CA pomagają w potwierdzaniu tożsamości stron podczas szyfrowanej komunikacji?**

**K.G.**: Chcąc poświadczyć swoją tożsamość np. w banku czy podczas kontroli policyjnej, okazujemy na żądanie dokument tożsamości, np. dowód osobisty.

Stanowi on dowód na to, że jesteśmy tym, za kogo się podajemy. Pracownik banku lub policjant po jego obejrzeniu są przekonani, że rozmawiają z osobą upoważnioną do zawarcia umowy kredytowej lub z właścicielem pojazdu.

Niezbędną do wykonania dalszych czynności pewność uzyskują dlatego, że ufają urzędowi, który wystawił dla nas dowód osobisty – np. urzędowi miasta, która jako instytucja zaufania publicznego ma uprawnienia do wydawania tego typu dokumentów, których podstaw do podważania autentyczności (teoretycznie) nie ma.

Identycznie jest z CA (Certification Authority), który pełni rolę takiego urzędu. Jeżeli zatem np. firma posiadająca sklep internetowy sprzedający rowery chce, by był on w Internecie widoczny dla wszystkich jako sklep faktycznie należący do przedsiębiorstwa produkującego rowery, zwraca się ona do wybranego CA (jak do urzędu) o wystawienie certyfikatu (jak dowodu osobistego) potwierdzającego, że witryna sklep-rowerowy.com.pl należy do firmy „Rowery sp. z o.o.".

Wówczas firma ta musi przejść szereg procesów weryfikujących. Jeżeli weryfikacja przebiegnie pomyślnie, urząd CA wydaje certyfikat (dowód osobisty) dla strony sklep-rowerowy.com.pl poświadczający, że jest to faktycznie witryna należąca do firmy „Rowery sp. z o.o." i że transakcje dokonywane za pośrednictwem tego sklepu są bezpieczne dla kupującego, bo realizowane z prawdziwym, a nie podstawionym, kontrahentem.

Jeżeli użytkownik korzystający z witryny sklep-rowerowy.com.pl nadal ma wątpliwości, czy warto zostawić w tym sklepie internetowym jakieś pieniądze, może sprawdzić, czy CA, który wystawił certyfikat dla tego sklepu, jest zaufanym podmiotem w Internecie (czyli, jak w przypadku urzędu miasta, czy jest instytucją zaufania publicznego). Interpretację tego faktu najczęściej ułatwiają nam przeglądarki internetowe, które dokonując weryfikacji ważności certyfikatu dla strony, jego atrybutów oraz CA, który go wystawił, wyświetlają nam tzw. „zieloną kłódkę" przy połączeniach uważanych za w pełni bezpieczne i zaufane, oraz „czerwoną kłódkę" wraz z ostrzeżeniem, gdy okazuje się, że coś się nie zgadza, zatem może dojść do niebezpieczeństwa kradzieży naszych danych, tożsamości, haseł czy pieniędzy.

Czy takiemu mechanizmowi można ufać bezwzglę-

dnie? Nie zawsze, bo tego typu certyfikat wystawiony przez zaufanego w Internecie CA kosztuje niejednokrotnie grosze (nawet kilkadziesiąt złotych), więc w teorii można za kilkadziesiąt złotych podszyć się pod np. stronę bankową i wymuszać tym samym dane logowania do systemów bankowych od nieprzeczuwających zagrożenia użytkowników.

Ale to tak jak w życiu: dowód osobisty można przecież podrobić. W praktyce jednak nie jest to takie proste, bowiem oprócz CA sprawdzana jest (jak wspomniałem wcześniej) długa lista innych atrybutów, takich jak np. nazwa strony internetowej, która bardzo skutecznie udaremnia tego typu próby ataków phishingowych.

Konkluzja jest taka, że zwyczaje, instytucje i hierarchie znane nam z życia codziennego w tym przypadku zostały w sposób doskonały przeniesione do płaszczyzny Internetu i innych usług sieciowych, od wielu lat doskonale sprawdzając się w roli strażnika naszych danych i interesów w cyfrowej rzeczywistości.

**Jakie są najnowsze trendy i innowacje w dziedzinie szyfrowania transmisji danych? Czy istnieją nowe technologie lub metody, które mogą zastąpić obecne praktyki?**

**K.G.:** Szyfrowanie samo w sobie jest trendem, które w IT było obecne od zawsze, jednak na upowszechnienie się szyfrowania transmisji i danych w użytku komercyjnym, trzeba było czekać długo. Tak było choćby z przejściem z komunikacji przy użyciu protokołu HTTP na HTTPS. Dość powiedzieć, że dopiero w 2016 (!) roku przeglądarki zaczęły wyraźnie ostrzegać użytkowników o fakcie połączenia z serwerem WWW z wykorzystaniem nieszyfrowanego protokołu HTTP! Dopiero wówczas producent przeglądarki Chrome, firma Google, wprowadziła wyraźne i uciążliwe dla użytkownika ostrzeżenia, że przebywa na stronie internetowej, z serwerem której komunikacja jest nieszyfrowana.

Prawdopodobnie ten mały-wielki krok wykonany przez Google (i kontynuowany słusznym trendem przez pozostałych producentów przeglądarek internetowych) sprawił, że obecnie niemal nie sposób jest spotkać stronę w Internecie nie wykorzystującą szyfrowanego połączenia.

Niewiele, bo raptem kilka lat wcześniej, wprowadzono szyfrowanie danych w telefonach komórkowych oraz komputerowych systemach operacyjnych. Nie zawsze jednak była to opcja domyślna bądź nie zawsze sprzęt pozwalał na uruchomienie takiego szyfrowania.

Dopiero od kilku lat możemy mówić o tym, że szyfrowanie w urządzeniach konsumenckich – domowych, biurowych, itp. upowszechniło się na dobre. Producenci komputerów i telefonów komórkowych domyślnie szyfrują zawartość pamięci i tylko w nielicznych przypadkach, intencjonalnie da się ją wyłączyć.

Przeglądanie Internetu poprzez HTTPS, komunikacja z systemami poczty elektronicznej poprzez szyfrowane protokoły pocztowe, szyfrowanie transmisji głosu i wideo podczas wideokonferencji – to wszystko to trendy oczywiste dzisiaj, ale praktycznie niestosowane (choć techniczne możliwości w zasadzie były!) jeszcze dekadę temu.

Odpowiadając na pytanie: najnowszym trendem w dziedzinie szyfrowania transmisji danych oraz danych samych w sobie jest... po prostu stosowanie szyfrowania. Współcześnie niemal każdy protokół komunikacji musi być w standardzie szyfrowany. Starsze protokoły komunikacji posiadają już swoje szyfrowane odpowiedniki. Należy więc zacząć od własnego środowiska i odpowiedzieć sobie na pytanie: czy na pewno stosuję szyfrowanie tam, gdzie się da? Jeśli tak, to czy algorytmy szyfrujące, które stosuję, nie posiadają podatności? Jeśli nie, to z czego to wynika? Z nieprzystosowanego sprzętu? Z przestarzałego systemu?

Dążmy do tego, by te niebezpieczne cechy wyeliminować raz na zawsze. Z jakich nośników korzystać do przenoszenia i przechowywania danych? Warto stosować takie, które szyfrują zawartość. To tak powszechne rozwiązania, że powinny być jedynym słusznym standardem. Obecne praktyki w zakresie szyfrowania, transmisji czy przechowywania danych, są słuszne i – dopiero teraz to można powiedzieć – nareszcie dojrzały. Trzeba je tylko konsekwentnie stosować lub stosować w ogóle.

**Jakie są najważniejsze kroki, które organizacje powinny podjąć, aby zapewnić skuteczną ochronę danych i szyfrowanie w obliczu rosnących cyberzagrożeń?**

**K.G.**: Przede wszystkim zacząć szyfrować dane i transmisję, jeśli wciąż tego nie robią.

Po drugie: tam, gdzie się da, przejść na logowanie z użyciem certyfikatów.

Po trzecie: zacząć powszechnie stosować mechanizmy uwierzytelniania wieloskładnikowego (MFA) lub przynajmniej dwuskładnikowego (2FA). Czynnik ludzki bywa zawodny, czasami zdarza się nam wpaść w sidła phishingu, czasami padniemy ofiarą ataku socjotechnicznego. W każdym z przypadków osoba nieupoważniona wchodzi w posiadanie naszego loginu i hasła, osiągając swój cel. Dodatkowy czynnik logowania pozwoli nam uchronić się przed phishingiem, nie dopuści do uskutecznienia próby logowania w przypadku wycieku hasła i dzięki temu pozwoli nam spać spokojniej.

Po czwarte: zadbać o bezpieczeństwo pracy zdalnej. Sprzęt pracowników, niezależnie od miejsca, w którym aktualnie pracują, powinien być chroniony przez firmowego firewalla poprzez zawijanie całego ruchu sieciowego właśnie przez niego, przy użyciu szyfrowanego VPN-a. Wówczas mamy pewność, że nawet po podłączeniu do publicznej sieci Wi-Fi w jakimś podejrzanym zakątku świata, nikt nie będzie w stanie podsłuchać naszej transmisji.

**Dziękuję za inspirującą rozmowę.**

SECURITYMAGAZINE.PL

# PRZEPIS NA ATAK PHISHINGOWY - KROK PO KROKU

Adrian Sroka


**Ataki phishingowe z każdym rokiem stają się popularniejsze i niestety ich skuteczność też wzrasta. Efektywna obrona przed nimi nie polega jedynie na przestrzeganiu wyuczonych zasad. Ciągła edukacja pracowników i zaznajamianie ich z regułami takimi jak: nie klikajmy w linki, sprawdzajmy, kto jest prawdziwym nadawcą, bądźmy uważni na treść wiadomości, jest istotna. Jednak nie wystarczy, żeby całkowicie zniwelować ryzyko związane z tym zagrożeniem.**

W związku z powyższym warto poznać tego typu ataki od strony atakującego oraz zobaczyć, jak na poziomie firmy możemy pokrzyżować mu plany.

## CELE ATAKÓW PHISHINGOWYCH

Na samym początku jednak zastanówmy się nad tym, jak zazwyczaj wygląda atak phishingowy. Na potrzeby tej analizy wyróżniamy dwa rodzaje tego ataku. Atak ogólny, skierowany zazwyczaj do dużej liczby osób. Tu przykładem jest dobrze znany już atak „na Nigeryjskiego księcia", który liczy na skuteczność wynikającą z efektu skali — może ktoś spośród wielu adresatów otworzy wiadomość. Kolejny rodzaj to atak nakierowany. W tym przypadku atakujący wysyła złośliwą wiadomość konkretnej osobie, używając różnych informacji na jej temat, aby się uwiarygodnić.

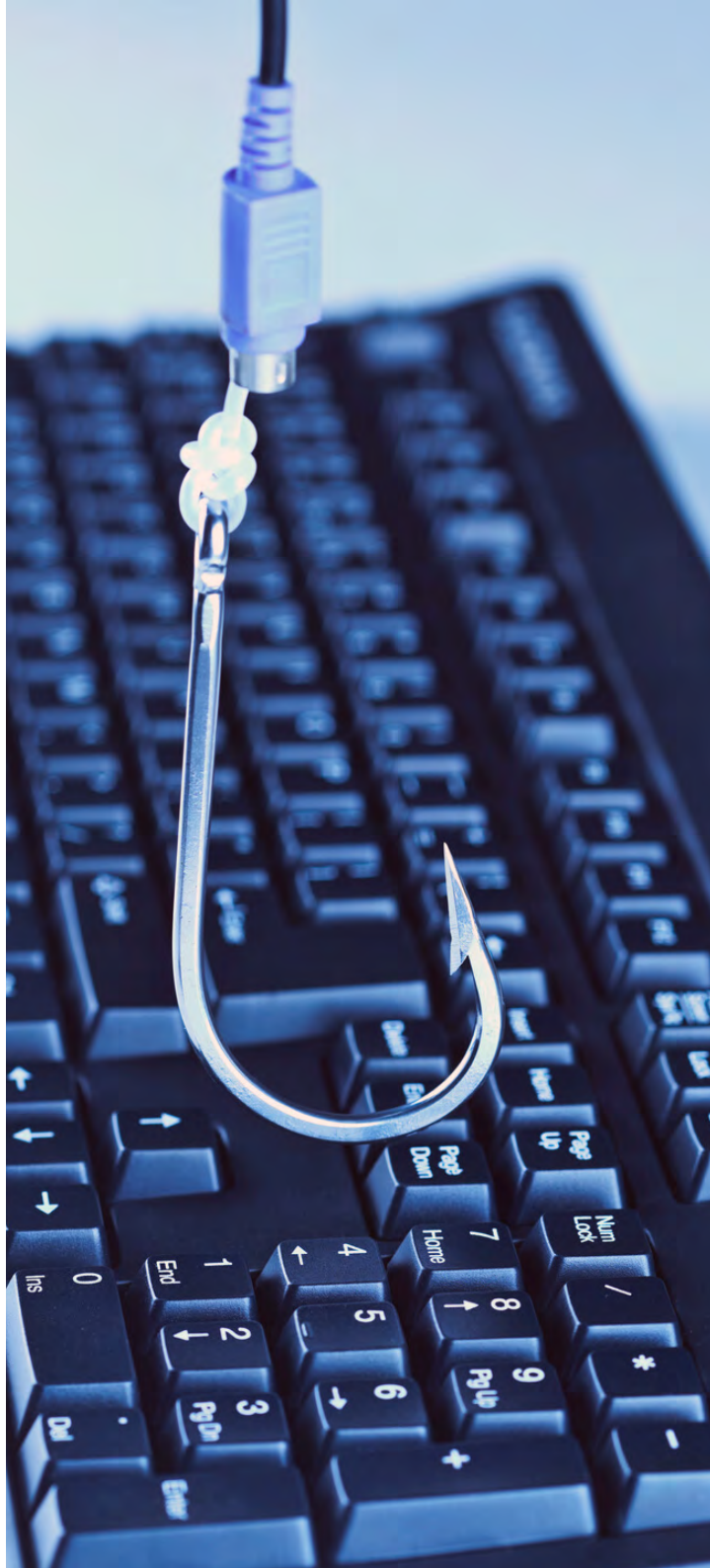
**Co może być celem takich ataków? W większości przypadków podstawowym celem jest zaszkodzenie atakowanej osobie poprzez np.:**

- kradzież danych lub pieniędzy,
- kradzież haseł,
- zainfekowanie wirusem,
- wykorzystanie podatności zero day do zainfekowania systemu.

Dodatkowo w niektórych bardziej zaawansowanych kampaniach phishingowych jeden atak może być tylko metodą na poznanie szczegółów na temat głównego celu ataku np. prezesa firmy i pomóc w kolejnych atakach.

## ANALIZA PRZEPROWADZANIA ATAKÓW PHISHINGOWYCH

Znając więc cel, dla którego atakujący dokonują ataków phishingowych, możemy spojrzeć na to, w jaki sposób przygotowują się i przeprowadzają tego typu działania.



**Rozpoznanie i plan**

Pierwszym krokiem do przeprowadzenia ataku phishingowego, jest zaprojektowanie tego, co ma być jego wynikiem oraz zbadanie celu ataku.

W przypadku ataków ogólnych trzeba zaplanować złośliwą akcję i jej trigger (wyzwalacz). Mówiąc konkretniej, atakujący zaczyna od określenia oczekiwanego efektu (np. kradzież danych osobowych) oraz rozważa, jak zachęcić odbiorcę do wykonania złośliwej akcji (np. wejścia w dyskusję i wysłania danych).

W przypadku ataków nakierowanych (np. na konkretną firmę) pierwszy krok przygotowań to analiza danej organizacji. Np. na LinkedIn (czy w innych mediach społecznościowych) można zidentyfikować osoby, na które warto się powołać w podrobionym mailu (np. administratora, który każe zmienić hasło).

Dla przykładu: gdy celem ataku jest kradzież haseł, można przygotować kampanię, która kilku pracownikom firmy wyśle mail z informacją o konieczności zmiany hasła.

Zadbajmy zatem, żeby nasi pracownicy nie publikowali w innych sieciach społecznościowych żadnych wewnętrznych informacji, takich jak nazwy systemów, szczegółów technicznych lub dokładnych relacji pomiędzy osobami w biurze.

**Zdobycie listy odbiorców**

W przypadku ataku ogólnego, atakującym zależy głównie na dużej skali. Chcą więc zdobyć jak największą bazę maili w miarę pasujących do scenariusza. Najlepszym miejscem do znalezienia takiej bazy jest kupno takiej listy z DarkWebu. Już za około 100$ można łatwo zdobyć miliony adresów. Jednak tak pozyskana lista jest zwykle bardzo słabej jakości.

Lepszym źródłem działających adresów email są strony lub aplikacje różnych firm. Źle zaprojektowane systemy mogą pozwolić na pobranie listy wszystkich zarejestrowanych adresów email. Da to atakującemu darmowe źródło całkiem wartościowych (gdyż niedawno działały i nie są zbiorem przypadkowym) adresów.

**Do ataku nakierowanego znów źródłem wiedzy mogą być media społecznościowe, jeżeli atak dotyczy konkretnej firmy. Wystarczy wykonać trzy kroki:**

1. odkryć schemat tworzenia adresu (np. imię.nazwisko@firma.pl) np. na stronie firmy lub testując przy pomocy narzędzia (patrz 3.),
2. znaleźć listę pracowników danej firmy (źródłem może być LinkedIn),
3. z użyciem narzędzi do weryfikacji adresów e-mail (np. https://tools.emailhippo.com/) sprawdzić hipotezy i zweryfikować, czy dany adres email działa czy nie.

Jak widać, zdobycie adresów email naszych pracowników nie jest trudne. To, co możemy, a nawet powinniśmy zrobić, to zabezpieczenie adresów e-mail naszych klientów, które są przechowywane w naszych systemach IT i tutaj właśnie istnieje ryzyko wycieku.

Zadbajmy o to, by pobranie listy adresów email nie było możliwe w żadnej formie.

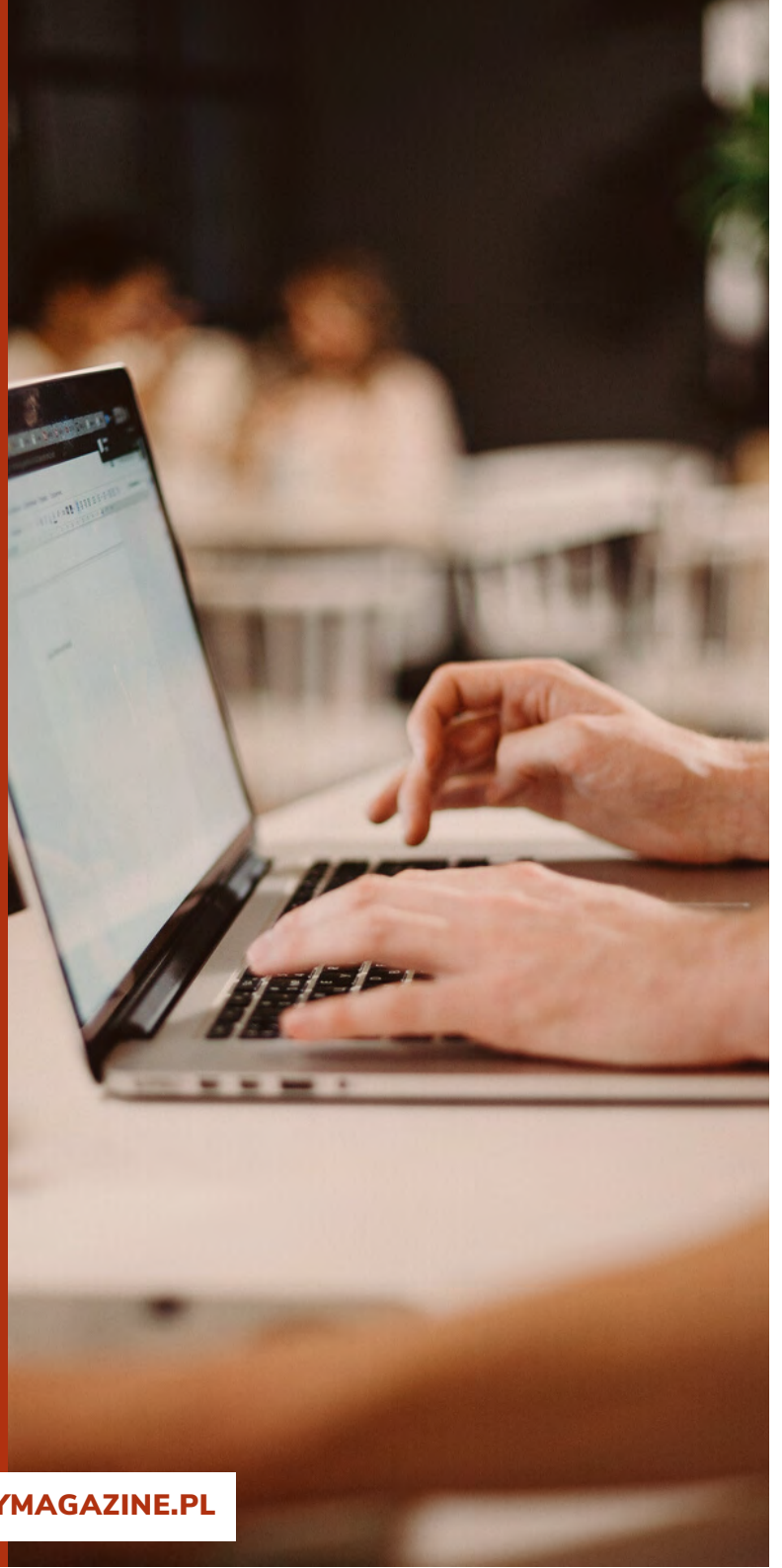
## PRZYGOTOWANIE SFAŁSZOWANEJ WIADOMOŚCI

Czas na spreparowanie faktycznej wiadomości. Aby atak się powiódł, wiadomość musi być wiarygodna. Zatem istotne jest odpowiednie słownictwo oraz wygląd maila.

Jeżeli atakujący podszywa się pod istniejący mail z systemu (np. zmianę hasła), najprościej jest otrzymać tego typu mail i użyć dokładnie tego samego szablonu. W innym przypadku warto zdobyć wzór stopki i wyglądu maila.

Niezależnie jednak od wizualnego aspektu złośliwej wiadomości, kluczowe jest zaprojektowanie treści. Ważne jest, żeby treść maila działała odpowiednio pod względem psychologicznym (np. zmuszając do szybkiej akcji bez zastanowienia). Często tego typu wiadomości zawierają różne elementy perswazji w postaci:

- ponaglenia (sprawa jest pilna i wymaga podjęcia natychmiastowych działań),
- podkreślenia istotności danej akcji (dane muszą zostać przekazane do regulatora),
- powołania się na kogoś innego w firmie.



**Jak tu utrudnić pracę atakującemu?**

- Uwrażliwiajmy pracowników na dokładnie te aspekty psychologiczne, które początkowo budują zaniepokojenie, ale często są też idealnym papierkiem lakmusowym złośliwych wiadomości.
- Niektóre systemy pozwalają na zweryfikowanie prawdziwości wiadomości (np. po zalogowaniu na swoje konto można przejrzeć historię komunikacji). Dodając tego typu funkcjonalność do naszych systemów, możemy ochronić naszych klientów.

## TESTOWANIE DOSTARCZALNOŚCI

To już ostatni etap ataku. Złośliwa wiadomość musi zostać dostarczona do skrzynki odbiorczej potencjalnej ofiary. Jest to łatwiejsze, gdy adres email nadawcy będzie podszywał się pod kogoś z zaufanej domeny.
Niestety tego typu podszywanie się pod inną osobę jest możliwe, gdy firma dla swojej domeny nie ma zaimplementowanych odpowiednich zabezpieczeń na poziomie rejestrów (takich jak DKIM, DMARC, SPF). Na szczęście są to standardowe mechanizmy i dość łatwo jest je skonfigurować dla wszystkich swoich domen. Nawet dla tych, z których firma nie wysyła maili. Warto o tym pamiętać, żeby nikt nie podszył się pod nasze adresy email, czym mógłby negatywnie wpłynąć na naszą reputację.

Oczywiście, ktoś może podszyć się pod adres z innej, znanej domeny (np. microsoft.com). Jeżeli więc ta domena nie byłaby zabezpieczona, potrzebne nam są filtry antyspamowe na poziomie

silnika poczty. O ile sam filtr działa w miarę skutecznie, to warto zachęcać pracowników do zgłaszania podejrzanych wiadomości. Gdy 50 osób w firmie dostanie tę wiadomość, zgłoszenie jej jako SPAM przez jedną spowoduje, że pozostałe jej już nie zobaczą.

## ATAK FAKTYCZNY

Na wypadek gdyby wszystkie podjęte przez nas działania okazały się niewystarczające, warto zadbać jeszcze tylko o jedno - odpowiednią ochronę przed skutkami ataku phishingowego, czyli:

- wdrożenie uwierzytelniania wieloskładnikowego (MFA) w aplikacjach używanych przez pracowników;
- stosowanie oprogramowania antywirusowego;
- regularne aktualizacje sprzętu i oprogramowania.

## PODSUMOWANIE

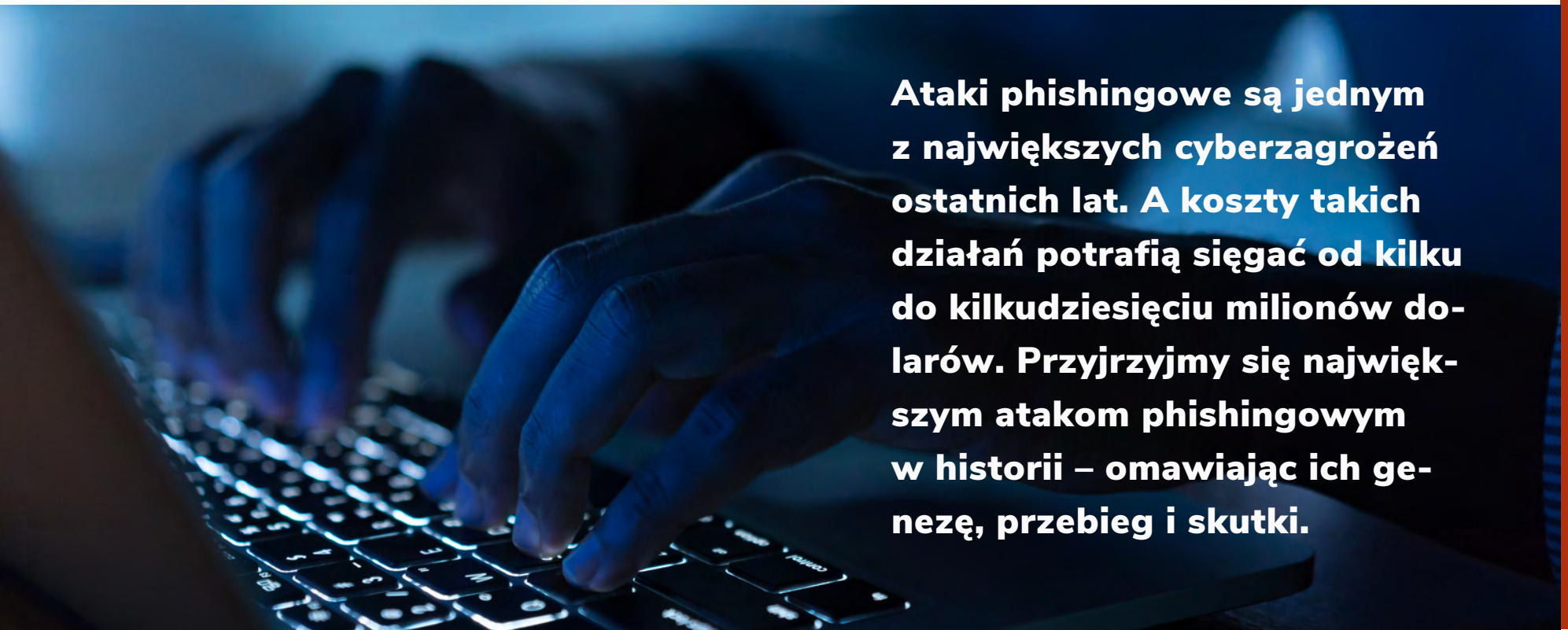
Widzimy, że ataki phishingowe są skuteczne i niezwykle proste do przeprowadzenia, stąd wynika ich niesłabnąca popularność. Co zatem zrobić, by móc spać spokojnie?
Sprawdźmy, czy wszystkie opisane tutaj zabezpieczenia są wdrożone w naszej firmie. Przede wszystkim dbajmy o wiedzę pracowników w tym zakresie, bo to oni są punktem ataku wycelowanego w naszą firmę i to ich czujność jest tutaj kluczowa.
Bądźmy gotowi na najgorsze. Pamiętajmy o zabezpieczeniach nie tylko “przed” atakiem, ale także “po” nim. Będą one swego rodzaju drugą linią obrony, która pozwoli wyeliminować lub ograniczyć ewentualne skutki ataku.

Na koniec pamiętajmy o komunikacji. Jak poradziliśmy sobie po ataku, też może o naszej firmie dobrze świadczyć. Obecnie wiele firm pada ofiarą ataków, ale nie wszystkie mogą powiedzieć, że dzięki wdrożonym zabezpieczeniom zminimalizowały ich skutki.

SECURITYMAGAZINE.PL

# NAJWIĘKSZE ATAKI PHISHINGOWE W HISTORII

Redakcja
SECURITY MAGAZINE



**Ataki phishingowe są jednym z największych cyberzagrożeń ostatnich lat. A koszty takich działań potrafią sięgać od kilku do kilkudziesięciu milionów dolarów. Przyjrzyjmy się największym atakom phishingowym w historii – omawiając ich genezę, przebieg i skutki.**

## ATAKI PHISHINGOWE – NAJPOPULARNIEJSZE ZAGROŻENIE W SIECI

Jeśli chodzi o działalność cyberprzestępczą, to nie ma popularniejszej formy niż ataki phishingowe. Szacuje się, że każdego dnia wysyłanych jest ok. 3,4 mld wiadomości typu spam. Sam Google blokuje codziennie około 100 mln maili phishingowych. A według danych atlasVPN w I kwartale 2022 r. Linkedln był marką, pod którą cyberprzestępcy najczęściej się podszywali. Na drugim miejscu znalazło się DHL – 14%.

Co więcej – zgodnie z informacjami podanymi przez SpamLaws.com aż 45% wszystkich maili, które otrzymaliśmy w 2021 r. były spamem – nierzadko powiązanym z atakami phishingowymi. Dodatkowo, według Statisa.com prawie 30% tego typu wiadomości pochodziło z Rosji, 14% z Chin, 10,7% z USA, 5,2% z Niemiec, a 3,7% z Niderlandów (Holandii).

A co gorsza – najczęściej ofiarami ataków phishingowych są... młodzi ludzie, bo z pokolenia Z oraz Y (milenialsi). W przypadku amerykańskich zetek to te zgodnie z badaniami Deloitte padają trzykrotnie częściej ofiarą phishingu niż boomerzy. Choć zdawałoby się, że to młodsze generacje są lepiej przystosowane do poruszania się w internecie i powinny mieć swoisty radar, wykrywający cyberzagrożenia.

Ponadto według Digital Guardian report 90% naruszeń cyberbezpieczeństwa korporacyjnego wynika z phishingu. To nie koniec złych wiadomości. Z badań Cyphere dowiadujemy się, że 90% ataków phishingowych realizowanych za pośrednictwem komunikatorów miało miejsce przy użyciu

WhatsAppa. Na drugim miejscu znalazł się Telegram – 5%.

Ataki phishingowe stały się na tyle poważne, że według brytyjskiego rządu stanowią najbardziej destrukcyjną formę cyberprzestępczości dotykające tamtejsze przedsiębiorstwa w 2022 r. Dość powiedzieć, że według raportów IBM w 2022 r. średni koszt wycieku danych po ataku phishingowym wynosił 4,35 milionów dolarów.

Przejdźmy jednak do firm, które wyjątkowo mocno ucierpiały z powodu phishingu.

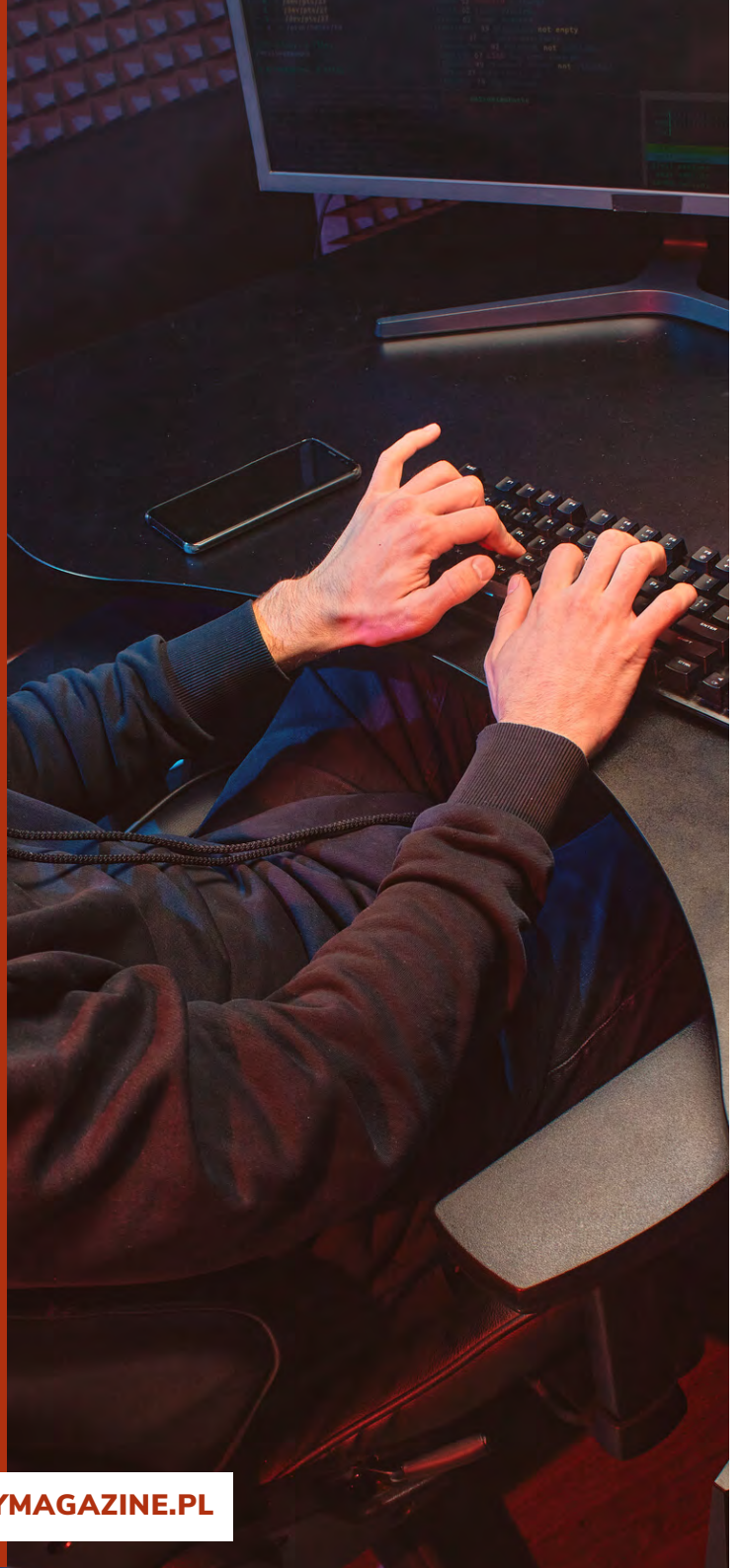
## ATAK PHISHINGOWY NA FACEBOOKA I GOOGLE

W latach 2013–2015 Litwin Evaldas Rimasauskas dokonał udanego ataku phishingowego na Facebooka i Google, pozbawiając tym samym firmy dużo ponad 100 milionów dolarów. Litewski cyberprzestępca wraz ze swoimi współpracownikami stworzyli przekonujące fałszywe maile, które wyglądały, jakby były wysłane przez pracowników tajwańskiej firmy Quanta. Przedsiębiorstwa, z którym Google i Facebook wielokrotnie współpracowali i dokonywali wielomilionowych transakcji.

Rimasauskas wymierzył swój atak w działy księgowości gigantów technologicznych. Co ciekawe – cyberatak był na tyle wyrafinowany, że Evaldas założył firmę o bliźniaczej nazwie, co jej tajwański odpowiednik. Stworzył wówczas fałszywe pieczątki przedsiębiorstwa, adresy e-mail i faktury. Wszystko wyglądało jakby było wystawione przez tajwańską spółkę. Do księgowych Google'a i Facebooka trafiły sfałszowane umowy i faktury za sprzęt. Następnie Rimasauskas poprosił ich o uregulowanie płatności na konta bankowe, które założył na Cyprze i Łotwie.

Cyberoszustwo okazało się na tyle skuteczne, że Google zapłaciło domniemanej Quancie 23 miliony dolarów, a Facebook 98 milionów.

Ostatecznie w 2017 r. Evaldas został ujęty przez litewski rząd i dokonano jego ekstradycji do Stanów Zjednoczonych. Litwin zgodził się oddać 50 milionów dolarów. Obecnie został skazany na 30 lat pozbawienia wolności. Ponadto cały czas utrzymywał, że był słupem i kazano mu utworzyć cały proceder, a on sam miał w ogóle nie ruszać pieniędzy wyłudzonych od gigantów technologicznych. Może być w tym ziarnko prawdy, bo na razie jego współpracowników – nie ujęto.



## COLONIAL PIPELINE – RANSOMWARE WYSYŁANY PRZEZ MAILE

Colonial Pipeline, czyli sieć rurociągów ciągnąca się od Zatoki Meksykańskiej do Nowego Jorku o długości prawie 9 tys. kilometrów to jedna z najważniejszych firm operacyjnych, które dostarczają nawet 45% paliw z rafinerii. Nic zatem dziwnego, że organizacja stała się celem cyberataku. W maju 2021 r. miliony Amerykanów dotknęło wstrzymanie działalności po tym, jak doszło do naruszenia cyberbezpieczeństwa sieci biznesowej oraz systemu rozliczeniowego Colonial Pipeline.

Najmocniej doświadczyli tego konsumenci i linie lotnicze (m.in. American Airlines, które nie otrzymało paliwa do silników odrzutowych) na wschodnim wybrzeżu Stanów Zjednoczonych. Cyberatak zaczął się od uzyskania dostępu do sieci spółki przez cyberprzestępczą grupę znaną jako DarkSide. Włamania dokonali za pomocą rozsyłania ransomware – najprawdopodobniej właśnie dzięki atakom phishingowym, pozyskując hasło do konta VPN. Cyberprzestępcom udało się wykraść 100 GB danych w ciągu zaledwie dwóch godzin!

Aby zapobiec rozprzestrzenianiu się wirusa ransomware Colonial Pipeline zamknęło rurociąg. Następnie sprawę zaczęła badać firma Mandiant. O cyberataku powiadomiono również FBI, Agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury, Departament Energii Stanów Zjednoczonych i Departament Bezpieczeństwa Wewnętrznego.

Co najgorsze – sprawa zakończyła się... zapłaceniem okupu DarkSide za uzyskanie klucza deszyfrującego. Ten umożliwił personelowi IT firmy odzyskanie kontroli nad systemami.

CEO Joseph Blount zgodził się zapłacić cyberprzestępcom 75 bitcoinów, które wówczas miały wartość ok. 4,4 miliona dolarów. Później zresztą stanął z tego powodu przed amerykańskim kongresem, gdzie był przesłuchiwany, dlaczego zgodził się na zapłacenie okupu. Ostatecznie agentom FBI udało się odzyskać 64 z 75 bitcoinów z haraczu. Jednak w momencie ich przejęcia były one warte już ok. 2,4 miliona dolarów.

## CRELAN BANK STRACIŁ 70 MILIONÓW EURO

Ofiarą udanego ataku phishingowego w 2016 r. padł też belgijski Crelan Bank. Cyberprzestępca (lub cała ich grupa – sprawców do dziś nie ujęto) spoza Belgii podszył się pod CEO – Luca Verselego – rzeczonego banku i wyłudził tym samym 70 milionów euro. Zastosowano tutaj tzw. BEC – Business E-mail Compromise, czyli atak phishingowy, w którym sprawca podszywa się pod osobę z wysokiego stanowiska w danej organizacji lub zewnętrznego klienta czy dostawcę.

Atak phishingowy został wykryty dopiero podczas wewnętrznego audytu. Bank od razu powiadomił władze Belgii, a także Komitet ds. Ryzyka i Audytu Banku. Jednak jak wskazał sam CEO – organizacja posiadała rezerwy, dzięki czemu mogli ponieść taką stratę bez konsekwencji dla klientów i partnerów firmy. Mimo to był to jeden z największych i najdroższych ataków phishingowych w historii.

## ATAK PHISHINGOWY NA FACC

FACC (Fischer Advanced Composite Components AG) to austriacka firma aeronautyczna, która również doświadczyła poważnego ataku phishingowego i podobnie jak w poprzednim przypadku – za sprawą BEC.

Do cyberataku doszło w styczniu 2015 r., kiedy do jednego z pracowników działu finansowego trafił mail od rzekomego CEO FACC – Waltera Stephana. Oczywiście, tak naprawdę był to mail wysłany przez cyberoszusta, który przejął skrzynkę mailową Stephana.

W treści wiadomości „Walter Stephan” prosił swojego pracownika o przelew 50 milionów euro na rzekomy rozwój jednego z projektów fir-

my. FACC szybko odkryło atak phishingowy, ale zdołało zatrzymać przelew jedynie na 10,9 miliona euro. Reszta pieniędzy trafiła na konta w Słowacji oraz Azji.

Cyberatak ujawniono rok później, a rada nadzorcza spółki podjęła decyzję o zwolnieniu Waltera Stephana z funkcji CEO ze względu na rażące naruszenie swoich obowiązków. Zwolniona została także Minfen Gu – CFO przedsiębiorstwa. Co więcej – w 2018 r. Gu i Stephan zostali pozwani przez FACC na 10 milionów dolarów.
W pozwie zarzucano im, że nie zrobili wystarczająco dużo, by chronić przedsiębiorstwo przed cyberoszustami. Jednak w 2019 r. austriackie sądy oddaliły oba pozwy. Sprawców dotychczas nie ujęto.

## ATAK NA UPSHER-SMITH LABORATORIES

Z kolei w 2014 r. doszło do jednego z największych ataków phishingowych na firmę farmaceutyczną w historii. Mowa tutaj o Upsher-Smith Laboratories. Cyberprzestępcy wysłali maila do koordynatora ds. zobowiązań w Upsher-Smith Laboratories, ponownie podając się za CEO przedsiębiorstwa. Cyberoszuści przekonali pracownika firmy do dokonania dziewięciu przelewów z banku firmy – Fifth Third Bank na łączną kwotę ponad 50 milionów dolarów.

Choć przedsiębiorstwu w końcu udało się wykryć cyberatak, to zablokowali jedynie jeden przelew. Organizacja straciła łącznie ok. 39 milionów dolarów wraz z odsetkami. Ostatecznie Upsher-Smith Laboratories zdecydowało się na pozwanie banku Fifth Third Bank za jej zdaniem – niedopilnowanie sprawy. W pozwie organizacja wskazywała, że bank przeoczył wiele sygnałów ostrzegawczych takich jak pospieszny charakter żądań, naleganie na zachowanie poufności, odejście od rutynowych procedur, podejrzanych beneficjentów przelewów itd.

Przelanych pieniędzy na razie nie udało się odzyskać ani ująć sprawców. Sprawa sądowa nadal się toczy, a obie organizacje nie udzielają w tej sprawie komentarzy.

## ATAK PHISHINGOWY, KTÓRY WYKRYŁO FBI

W 2015 r. firma Ubiquiti Networks zajmująca się sieciami komputerowymi również doświadczyła cyberataku z wykorzystaniem phishingu. I ponownie – podszyto się tutaj pod CEO organizacji. W tym przypadku nie znamy jednak wszystkich szczegółów sprawy, bo właściciel firmy – Robert Pera – nie ujawniał za wiele informacji. Mimo to wiemy, że przedsiębiorstwo oszukano na prawie 47 milionów dolarów, a o cyberataku dowiedziało się... dzięki FBI.

Amerykańskie Federalne Biuro Śledcze po monitorowaniu rachunku bankowego spółki zależnej Ubiquiti Networsk w Hongkongu, wykryło podejrzane przelewy i powiadomiło organizację. Dopiero wówczas przedsiębiorstwo wszczęło śledztwo i zablokowało dalsze przelewy. Straty wyceniono na 10% wartości firmy. Ubiquiti Networks wszczęło postępowanie sądowe i dzięki temu udało się odzyskać 14,9 miliona dolarów.

Organizacja starała się także odzyskać pozostałe 31,8 miliona. Amerykańskie or-gany ścigania ciągle pracują nad wykryciem spraw-ców cyberataku.

Jak widać – cyberataki z wykorzystaniem metod phishingowych są poważnym zagrożeniem dla przedsiębiorstw. A niejednokrotnie straty mogą sięgać kilkudziesięciu milionów dolarów czy euro. Co ważne – bardzo często w przypadku przedsiębiorstw cyberprzestępcy starają się podszywać pod wysoko postawione osoby w firmach, klientów czy dostawców zewnętrznych i w ten sposób wyłudzają pieniądze.

Nie zawsze udaje się wykryć sprawców i odpowiednio ich ukarać, jak było to w przypadku Evaldasa Rimasauskasa. Sprawy takie mogą ciągnąć się latami i niekoniecznie skończyć sukcesem. Dlatego tak ważne jest dbanie o bezpieczeństwo w swojej organizacji.

SECURITYMAGAZINE.PL

# ATAK PHISHINGOWY Z PERSPEKTYWY OFIARY. JAK DZIAŁAJĄ FIRMY? TO ZALEŻY...

**Karol Wodzicki**
Concept Data

**Michał Kudela**
Concept Data


**Z raportu CERT Polska wynika, że phishing stanowił aż 64 proc. wszystkich incydentów bezpieczeństwa obsłużonych w 2022 r. Ta liczba nie zaskakuje. Cyberprzestępcy wspierani przez sztuczną inteligencję wysyłają wiadomości phishingowe na szeroką skalę. Nie każda firma potrafi się przed nimi ochronić. Co dzieje się w przedsiębiorstwie atakowanym za pomocą phishingu?**

Cyberprzestępcy korzystają z różnych rodzajów phishingu, natomiast najczęściej decydują się na masowe wysyłki sfabrykowanych e-maili lub na ataki ukierunkowane.

W pierwszym przypadku za cel obierają dużą grupę pracowników, do których kierują wiadomości zawierające złośliwe załączniki lub linki do spreparowanych stron. W drugim przypadku koncentrują swoje wysiłki na konkretnej osobie – np. prezesie czy dyrektorze finansowym. Podszywają się pod współpracownika lub znaną organizację i w ich imieniu piszą e-mail z prośbą o weryfikację danych czy wykonanie jakiejś akcji.

Oba sposoby przynoszą atakującym bardzo dobre rezultaty. Dobrze przygotowany e-mail lub bardzo szeroko rozesłana wiadomość kończy się tym, czego oczekują przestępcy – kliknięciem w link, zainstalowaniem złośliwego oprogramowania lub przekazaniem ważnych danych.

Jak radzą sobie w takich sytuacjach zaatakowane firmy? Na kilka sposobów. Wszystko zależy od ich wielkości, branży, w jakiej działają, technologii, jakimi dysponują, i świadomości pracowników.

## SCENARIUSZ 1. REAKCJA ZAUTOMATYZOWANA

W najlepszej sytuacji są firmy, które funkcjonują w regulowanych branżach, np. finansowej. Przepisy, którym podlegają, wymuszają zadbanie o bezpieczeństwo danych, zatem organizacje te dysponują odpowiednimi technologiami pozwalającymi na szybką i skuteczną reakcję na cyberatak. Podobnie działają duże przedsiębiorstwa, które również inwestują w systemy bezpieczeństwa. W przypadku ataku phishingowego wiele dzieje się w tych organizacjach automatycznie.

Automatycznie, czyli jak? Zacznijmy od poczty elektronicznej. Wdrożone systemy filtrują e-maile w oparciu o różne algorytmy oraz informacje, którymi wymieniają się na bieżąco między sobą (np. informują się o tym, że wiadomość z jakiegoś adresu lub z konkretnym załącznikiem jest złośliwa). Używają aktualizowanych cały czas sygnatur i już na poziomie sieciowym wykrywają szkodliwe e-maile, blokują je i nie dopuszczają do rozesłania wiadomości phishingowych do pracowników.

Oczywiście, może się zdarzyć, że szkodliwy e-mail przedrze się przez takie zapory, trafi do adresata, który kliknie w link czy załącznik.

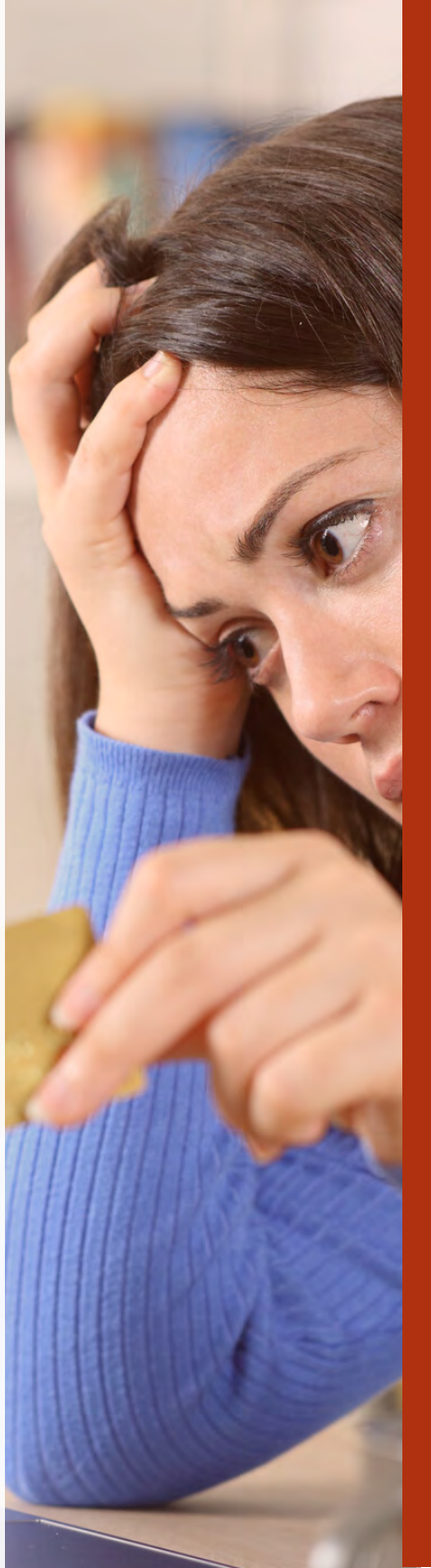
Wtedy włączają się systemy bezpieczeństwa zainstalowane na stacjach końcowych właśnie po to, by wyeliminować złośliwe oprogramowanie, wyizolować taką stację i nie dopuścić do rozprzestrzeniania się zagrożenia na inne komputery czy usługi. Jeśli atak obejmie kilka stacji roboczych, można również wyizolować część sieci, w której znajdują się zainfekowane urządzenia.

W takich przypadkach z pomocą przychodzą też systemy Identity Management, które pozwalają zablokować tożsamość zaatakowanej osoby. Mając nazwę użytkownika i hasło, cyberprzestępca może się bowiem dostać do wielu systemów w organizacji, nie tylko tych powiązanych ze stacją roboczą. Dlatego ważne jest nie tylko zabezpieczenie komputera, ale i wszystkich usług – właśnie za pomocą zablokowania tożsamości czy zmiany hasła. Dzięki technologiom można to zrobić automatycznie, jednym kliknięciem.

## SCENARIUSZ 2. A U MNIE COŚ NIE DZIAŁA...

Zupełnie inaczej wygląda sytuacja w mikro i małych firmach, zatrudniających klika, kilkadziesiąt osób i niedziałających w branżach, które wymagają zastosowania różnych systemów zabezpieczeń. W przypadku tych podmiotów świadomość zagrożeń jest zazwyczaj dość niska. Jeśli używają jakichś systemów, często są to kupione razem z komputerami programy antywirusowe.

Oczywiście, w ich przypadku prawdopodobieństwo zainfekowania stacji roboczej jest bardzo wysokie. Co więcej, pracownik, który klika w podejrzany link i podaje swoje dane lub pobiera złośliwy załącznik, często w ogóle nie ma świadomości, że zrobił coś, czego nie powinien zrobić. Orientuje się, że coś jest nie tak, dopiero wtedy, gdy zaczynają zgłaszać się do niego różne osoby z informacjami o tym, że wysyła dziwne wiadomości do swoich kontaktów. Lub – gdy komputer zaczyna bardzo głośno pracować, nagrzewa się i przestaje być wydajny (bo zainstalowane oprogramowanie nieustannie coś liczy i zużywa



CPU w 100%).

Co robi w tym momencie? Zwykle idzie do osoby odpowiadającej w firmie za komputery, w przypadku większych firm – do serwisu, który zabiera stację roboczą i przeinstalowuje cały system operacyjny. To zajmuje dużo czasu i działa na krótką metę – nigdy nie mamy gwarancji, że złośliwe oprogramowanie nie zainfekowało już innych urządzeń/systemów lub nasze poświadczenia nie są używane w innych systemach organizacji.

## SCENARIUSZ 3. CISZA PRZED BURZĄ

Cyberprzestępca może też dostać się do stacji roboczej należącej do firmy i... nie robić nic. A przynajmniej nie wykonywać akcji, które mogą być zauważone przez pracowników czy klientów. Bywa bowiem, że atakujący nie chce się ujawnić, ponieważ jego celem jest rekonesans, zbieranie informacji o firmie, jej strukturze, konkurencji, tajemnicy handlowej itd. W przeprowadzeniu tego typu ataków bardzo pomaga sztuczna inteligencja, która pozwala na tworzenie zautomatyzowanego i mądrego złośliwego oprogramowania, które tak długo pozostaje w sieci firmowej, aż zgromadzi istotne dla atakującego dane.

Jednym z celów atakującego, który dostał się do jakiejś stacji roboczej, może też być zdobycie danych uwierzytelniających i zalogowanie się do urządzenia, które nie jest monitorowane. To częsty scenariusz w przypadku słabo chronionych urządzeń IoT. Cyberprzestępcy wykorzystują zdobyte dane do przejęcia dostępu do np. kamery, która nie jest chroniona, nie ma antywirusa. Jest więc bezpiecznym miejscem, z którego można wykonywać kolejne ataki na zasoby IT organizacji.

## JAK CHRONIĆ SIĘ SKUTECZNIEJ?

Każda firma – niezależnie od swoich budżetów czy wielkości – może podjąć dodatkowe działania, które pozwolą jej skuteczniej walczyć z atakami phishingowymi.

**Podnoszenie świadomości pracowników**

Podstawą całego systemu zabezpieczeń muszą być szkolenia pracowników. To przecież ludzie odbierają e-maile phishingowe i od ich zdolności odróżnienia złośliwej wiadomości od bezpiecznej niejednokrotnie zależy to, czy atak się powiedzie. Na rynku dużo jest dziś platform szkoleniowych, z których warto korzystać regularnie, by być na bieżąco z najnowszymi technikami stosowanymi przez przestępców.


**Korzystanie z usług dostawców dbających o bezpieczeństwo**

Mniejsze firmy, które nie mają dużych budżetów na zaawansowane technologie, mogą używać usług chmurowych od znanych, zaufanych dostawców, którzy dbają o bezpieczeństwo udostępnianych narzędzi. Mowa przede wszystkim o poczcie elektronicznej dostępnej w modelu SaaS (Software as a Service), która ma wbudowane mechanizmy filtrujące przychodzące wiadomości. Podobnie działają także duzi operatorzy telekomunikacyjni, którzy np. analizują SMS-y i blokują te, które zawierają złośliwe linki.

**Ograniczanie dostępu do zasobów**

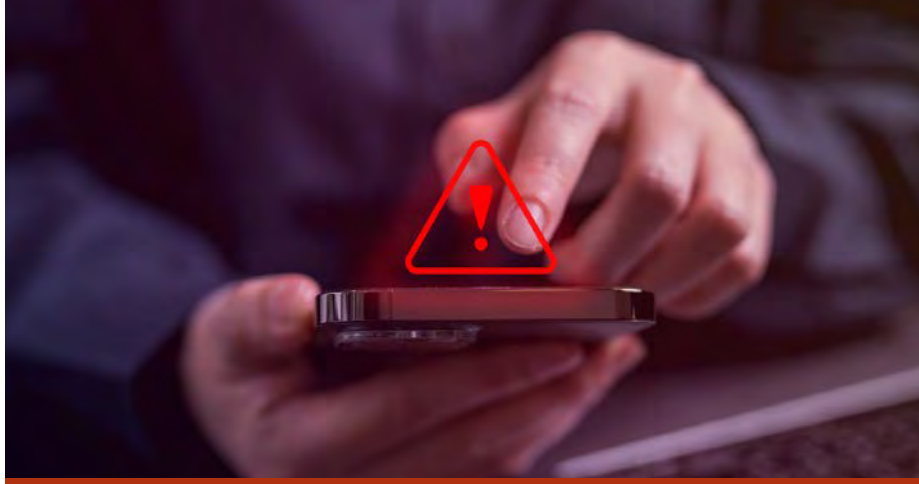
W każdym przedsiębiorstwie warto też wprowadzić zasadę najmniejszego dostępu polegającą na przyznawaniu pracownikom dostępów tylko i wyłącznie do tych zasobów, które są im aktualnie potrzebne do pracy. Im mniejsze uprawnienia ma pracownik, tym mniejsze szkody wyrządzi firmie cyberprzestępca, które przejmie dane uwierzytelniające takiej osoby.

Firmy różnie reagują na ataki phishingowe. Najważniejsze jest jednak to, że każde przedsiębiorstwo może wciąż rozszerzać wiedzę pracowników oraz stosować różnorodne rozwiązania, zwiększając tym samym poziom swojej cyberodporności. Warto to robić, bo cyberprzestępcy są kreatywni i na pewno nie zrezygnują ze tak skutecznej metody działania, jaką jest phishing.

SECURITYMAGAZINE.PL

# RANSOMWARE I MŚP. SKUTECZNE STRATEGIE OBRONNE PRZED CYBER-PORWANIAMI

**Michał Zalewski**
Barracuda Networks



**W 2022 roku 73% organizacji doświadczyło skutecznego ataku ransomware, a 38% zostało zaatakowanych więcej niż jeden raz, wynika z raportu Barracuda Networks. Aż 42% ofiar trzech lub więcej ataków ransomware zapłaciło okup, aby przywrócić zaszyfrowane dane. 69% incydentów ransomware zaczęło się od phishingowej wiadomości e-mail. Jak widać, ransomware jest realnym zagrożeniem dla firm.**

Na początku chciałbym podkreślić jedną rzecz – jest bardzo duża szansa na to, że cyberprzestępcy zaatakują także Twoją firmę. Są oni bowiem naprawdę bardzo twórczy, bez problemu znajdą nowy sposób na przedarcie się przez nawet najlepszą ochronę. I będą go wykorzystywać aż do momentu, w którym eksperci ds. cyberbezpieczeństwa przygotują przedsiębiorstwa i ich systemy na tego typu schemat działania.

Pytanie nie brzmi więc ‘czy’, a ‘kiedy’ Twoja firma będzie musiała zmierzyć się ze skutkami ataku ransomware. Dobra wiadomość jest taka, że nawet na taką sytuację można się przygotować.

## CO WARTO WIEDZIEĆ O RANSOMWARE?

Ransomware, czyli złośliwe oprogramowanie, które szyfruje dane na urządzeniach i żąda okupu, ma już ponad 30 lat. Jego tradycyjna wersja jest wykorzystywana przez przestępców do infiltracji sieci docelowych i wyszukiwania cennych lub krytycznych danych biznesowych. Następnie umożliwia oszustom zaszyfrowanie danych i przesyła żądanie okupu. W zamian za zapłacenie go przestępcy obiecują dostarczyć klucz deszyfrujący, który pozwala odzyskać stracone informacje. Często obietnica ta nie jest spełniana.

Przejęcie kontroli nad danymi atakowanej firmy i odcięcie jej wszelkich możliwości dostępu do tych danych staje się jednak dziś zbyt skomplikowane. To dlatego przestępcy coraz chętniej odchodzą od tradycyjnych technik szyfrowania kluczowych zasobów informacyjnych atakowanego. Znacznie łatwiej jest im po prostu skopiować i ukraść dane, następnie zażądać zapłaty za ich nieupublicznianie lub zaoferować je na sprzedaż w Darknecie, czyli ukrytej, niewidocznej dla standardowych przeglądarek sieci, w której między innymi kwitnie handel nielegalnymi towarami.

Niezależnie od tego, który wariant wybiorą cyberprzestępcy, firmy muszą spodziewać się

poważnych konsekwencji. Pojedynczy udany atak ransomware może sparaliżować codzienne operacje biznesowe i łańcuchy dostaw klientów, powodując chaos i straty finansowe, a wyciek danych jest w stanie zniszczyć reputację przedsiębiorstwa i jego relacje z klientami.

## PRZEZORNY ZAWSZE ZABEZPIECZONY

Skoro konsekwencje ataków ransomware są tak poważne, dlaczego tak niewiele firm sektora MŚP jest przygotowanych na walkę z tym zagrożeniem? W moim odczuciu powodem jest przede wszystkim to, że małe i średnie przedsiębiorstwa nie podlegają wielu regulacjom, do których muszą się stosować firmy duże. Bardzo często wdrażają jedynie procedury wymagane przez RODO.

A tak naprawdę to od procedur trzeba zacząć, choć są one dla MŚP często bardzo dużym wyzwaniem. Jednak zupełnie nie chodzi o to, by wszyscy przedsiębiorcy zabrali się za lekturę grubych książek o ISO 27001 czy certyfikowali się w zakresach planów BCM. Chodzi o przygotowanie prostego, jednostronicowego planu działania na wypadek sytuacji kryzysowej.

**Ten plan powinien odpowiadać na kilka pytań:**

- Które zasoby są najbardziej krytyczne dla firmy?
- Jak określić powagę sytuacji, w jakiej znalazła się firma? (Jedna z możliwości: w skali o 1 do 10, gdzie 1 oznacza, że wszystko działa i dopiero widać, że coś złego/podejrzanego miało miejsce, 5 – część ważnych systemów nie działa do końca poprawnie, 10 – główne i krytyczne systemy przestały funkcjonować).
- Jakie zasoby ma firma? Odpowiedź na to pytanie najlepiej przygotować w formie prostej tabelki, w której spiszemy systemy od tych najistotniejszych (serwery systemów sprzedażowych, CRM, środowisko ERP, systemy monito-

rowania, cyfrowa centralka VoIP itd.) do tych mniej ważnych (np. systemy do wysyłania newsletterów).

- Kto ma dostęp do tych zasobów? Kto ma dostęp zdalny, do czego?
- Jak długo firma może operować bez działania poszczególnych systemów (czyli od którego momentu od zatrzymania systemu firma zaczyna ponosić straty finansowe)?
- Jak zorganizować komunikację z pracownikami/współpracownikami w sytuacji problematycznej? W takim momencie jesteśmy pod ogromną presją i nie chcemy tracić czasu na odpowiadanie na nieustające pytania. Rozwiązaniem może więc być oddelegowanie jednego z pracowników do odbierania telefonów/e-maili, tablica informacyjna, przekierowanie całego ruchu do sekretariatu itd.
- Kogo powiadomić o sytuacji? (To może być np. operator Internetu, Policja, zarząd, firmy, z którymi współpracujemy i od których kupujemy usługi).
- Gdzie zgłosić incydent? (Zawsze warto zgłosić incydent do CERT Polska, bo eksperci tam pracujący często są w stanie coś podpowiedzieć oraz pomóc w rozwiązaniu trudnej sytuacji).

Mając taki dokument, firma będzie w stanie zdecydowanie szybciej zadziałać w przypadku każdego cyberataku. A szybkość reakcji jest w takich przypadkach kluczowa.

## UWAGA – ATAK RANSOMWARE! JAK DZIAŁAĆ?

No właśnie, teoria teorią, ale jak działać w sytuacji, w której dochodzi do zaszyfrowania danych na skutek ataku ransomware?

**Najważniejsze są następujące kroki:**

**Krok 1.** Iść zrobić sobie kawę.

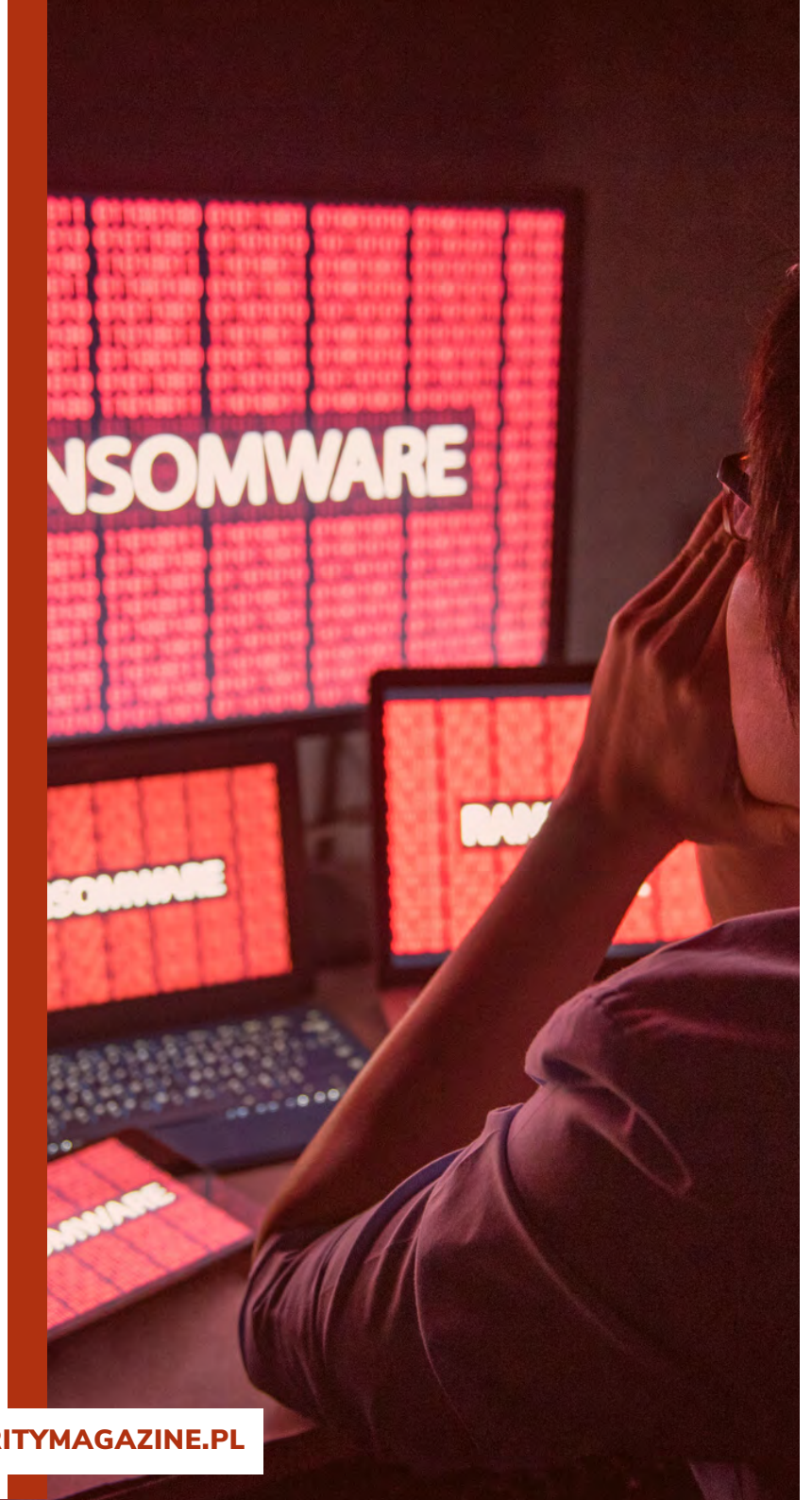
**Krok 2.** Złapać parę oddechów.

**Krok 3.** Spokojnie przejść przez przygotowaną wcześniej listę zawierającą prostą procedurę oraz schemat wyjaśniający, co należy zrobić w pierwszej kolejności.

**Krok 4**. Systematyczne wprowadzać działania naprawcze.

Chaos jest naszym wrogiem w tego typu sytuacjach. To dlatego tak ważne jest uspokojenie się, wyciszenie myśli i dopiero wtedy – przystąpienie do działania. Według planu.

By zminimalizować skutki cyberataku, musimy przede wszystkim zadbać o dane – jak najszybciej




je odzyskać i przywrócić sprawność biznesową firmy.

W takich przypadkach korzystamy z systemów backupu, które nie tylko pozwalają przywrócić wszystkie dane, ale też mogą wesprzeć nas w jak najszybszym powrocie do wykonywania służbowych czynności. Np. funkcja LiveBoot/CloudLiveBoot dostępna w naszym rozwiązaniu do backupu Barracuda Backup umożliwia szybki (nawet tymczasowy) dostęp do najbardziej krytycznych danych, zanim cała procedura odzyskiwania danych zostanie zakończona, a nawet zanim jeszcze się rozpocznie. Natychmiastowy eksport danych czy e-maili pozwala kontynuować pracę i współpracę z klientami.

Najistotniejsze w przypadku cyberataku jest jednak ustalenie, jak do niego doszło. Zbadanie, którędy cyberprzestępca przeniknął do naszej sieci. Pomogą w tym systemy zbierania logów, takie jak Firewall Insights, dzięki któremu można prześledzić całą historię zdarzeń w obrębie ruchu sieciowego, czy systemy klasy XDR (extended detection and response) lub SIEM/SOAR, które nie tylko chronią i odpierają atak, ale także widzą, co się dzieje i dzięki korelacjom pozwalają retrospektywnie zbadać, co się wydarzyło.

## POMOCNA DŁOŃ TECHNOLOGII

No dobrze, ale czy to oznacza, że jesteśmy bezbronni i mamy po prostu siedzieć i czekać na cyberataki? Oczywiście nie. Jest cały szereg rozwiązań, które pomogą firmom wal-

czyć z atakami ransomware. Ransomware może infiltrować sieć przy użyciu wielu różnych wektorów, a nawet ich kombinacji. Oznacza to, że aby zapobiec przedostawaniu się oprogramowania ransomware do systemów, należy zastosować kompleksowy, zintegrowany zestaw rozwiązań oraz platform do ochrony poczty e-mail, aplikacji, ruchu sieciowego, interakcji internetowych i danych, niezależnie od tego, gdzie się znajdują.

Kluczowe są rozwiązania chroniące pocztę elektroniczną – w końcu większość incydentów ransomware rozpoczyna się od wiadomości e-mail. Systemy backupu – aby móc odzyskać dane w razie ataku, wielowarstwowa ochrona sieci i VPN-y.

Firmy powinny też stosować dostęp do danych, aplikacji i systemów w modelu Zero Trust (Cloud-Gen Access), czyli zakładać, że każda osoba znajdująca się w ich sieci może być intruzem, zgodnie z doktryną „always assume breach" – „zakładaj odgórnie, że w każdej chwili możesz być w trakcie jakiegoś ataku czy włamania".

Technologie to jedno. Żadna firma nie będzie jednak bezpieczna, jeśli jej pracownicy nie będą świadomi zagrożeń.

To przecież oni otwierają e-maile phishingowe i klikają w podejrzane linki. Dlatego tak ważne są szkolenia pracowników i ciągłe podnoszenie ich świadomości. Tłumaczenie, w jaki sposób działają cyberprzestępcy, czym jest socjotechnika, na co zwracać uwagę w sieci. Im lepiej wyedukowane zespoły, tym lepiej zabezpieczona firma i jej zasoby.

Nie unikniemy cyberataków. Możemy jednak tak przygotować się do działania, by w przypadku ich wystąpienia spokojnie zareagować, jak najsprawniej odzyskać dane i kontynuować pracę, a także dowiedzieć się, w jaki sposób cyberprzestępca dostał się do naszej sieci.

Z taką wiedzą będziemy mogli jeszcze lepiej zabezpieczyć się przed kolejnymi atakami, a tym samym – zadbać o stabilność firmy w starciu z cyberprzestępcami.

SECURITYMAGAZINE.PL

# TE STARTUPY POMOGĄ CI W PRZYPADKU ATAKÓW PHISHINGOWYCH

Redakcja
SECURITY MAGAZINE


**Ataki phishingowe są jednymi z najczęstszych cyberzagrożeń na świecie. A na domiar złego rozwój sztucznej inteligencji będzie tylko rozwijać tę niechlubną gałąź. Na szczęście na rynku pojawia się coraz więcej rozwiązań dostarczanych przez startupy, które pozwalają przeciwdziałać phishingowi.**

## JERICHO SECURITY – AI W WALCE Z PHISHINGIEM

Nowojorski startup Jericho Security ma na celu zwalczanie coraz bardziej wyrafinowanych ataków phishingowych, które wykorzystują postęp w technologii generatywnej sztucznej inteligencji. Ostatnie lata przyniosły wzrost liczby cyberataków, omijających tradycyjne metody obrony. Organizacja postanawia zwalczać ogień ogniem, zaprzęgając sztuczną inteligencję do przeciwdziałania cyberatakom.

To ważne o tyle, że tradycyjne formy ataków phishingowych będą już praktycznie nieużywane. O wiele szybciej i nierzadko efektywniej jest tworzyć spersonalizowane wiadomości za pomocą AI. Sztuczna inteligencja może bardzo wyraźnie naśladować styl pisania poszczególnych osób w organizacjach.

Startup korzysta z przetwarzania języka naturalnego i niestandardowych modeli do tworzenia symulacji realistycznych i ewoluujących zagrożeń phishingowych. Dzięki temu Jericho Security oferuje proaktywne szkolenia pracowników, dostosowane do każdego użytkownika. To zupełnie inne podejście niż konwencjonalne narzędzia antyphishingowe, które opierają się na sztywnych heurystykach i nierzadko przestarzałych przykładach.

Organizacja oferuje swoje usługi za około 3 dolary miesięcznie na pracownika. Co za tym idzie – oferta jest dostępna dla praktycznie każdego przedsiębiorstwa, które musi stale rozwijać się w zakresie cyberbezpieczeństwa.

Startup niedawno zakończył też rundę finansowania, gdzie pozyskał 3 mln dolarów na rozwój. W spółkę zainwestował m.in. fundusz venture capital – Era.

## PERCEPTION POINT – ZWALCZANIE PHISHINGU

Podobny charakter działania ma także izraelski startup Perception Point z siedzibą w Tel Awiwie. Organizacja ta specjalizuje się w walce z coraz bardziej niebezpiecznymi atakami typu Business Email Compromise (BEC), które stanowią nowe zagrożenie phishingowe dotyczące przedsiębiorstw.

Ataki BEC odwzorowują korespondencję biznesową. Ich celem jest nakłonienie odbiorców do ujawnienia poufnych informacji finansowych. Raport roczny Perception Point za 2023 r. podkreśla, że

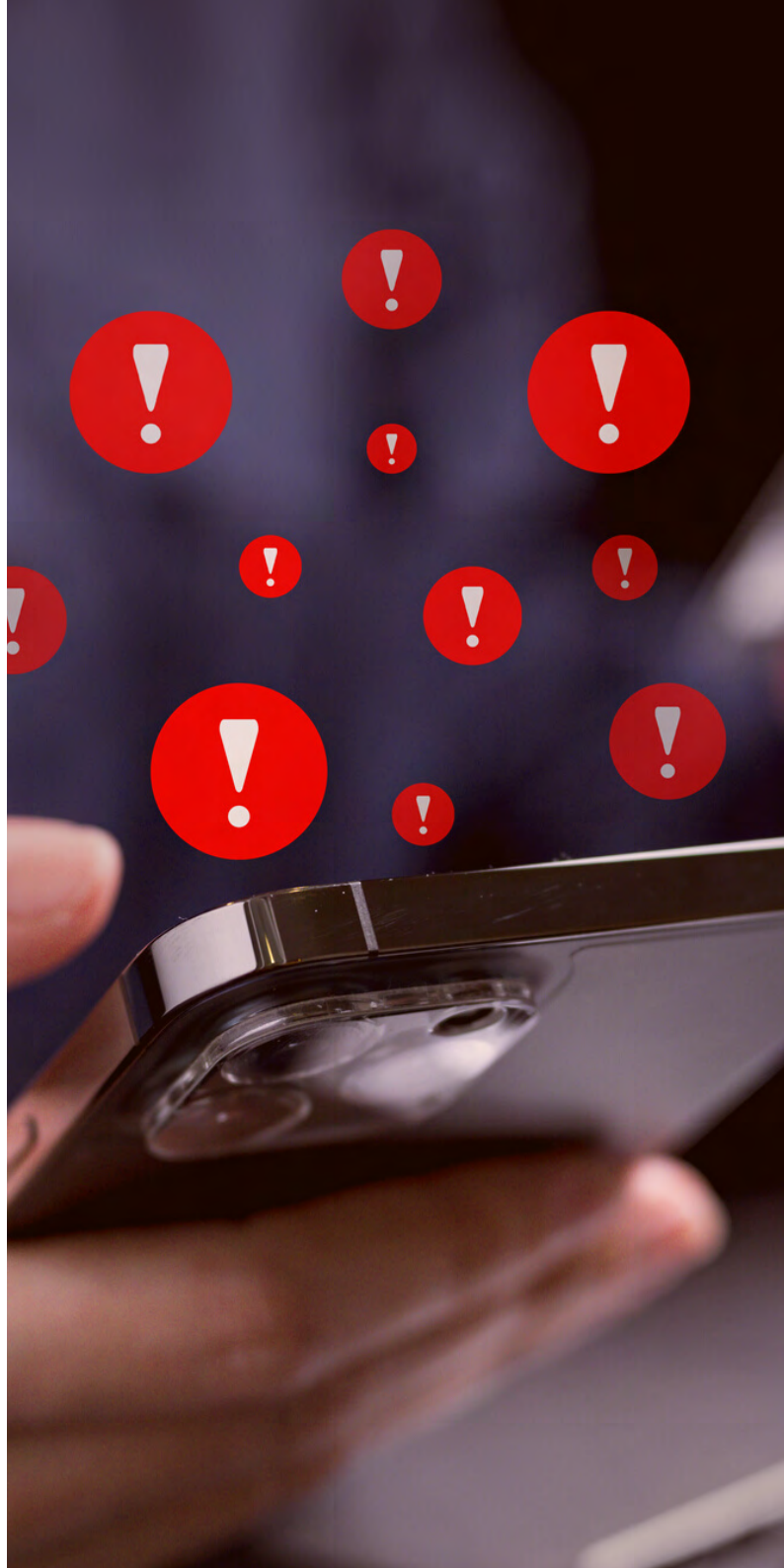
liczba ataków BEC wzrosła aż o 83% w porównaniu z ubiegłym rokiem. To dowód, jak poważnym wyzwaniem stają się te ataki, szczególnie że nie zawierają one złośliwych załączników, które mogłyby być tradycyjnie zidentyfikowane jako niebezpieczne. Co więcej – tu również pojawia się wątek generatywnej sztucznej inteligencji, która wykorzystywana jest do tworzenia tego typu wiadomości.

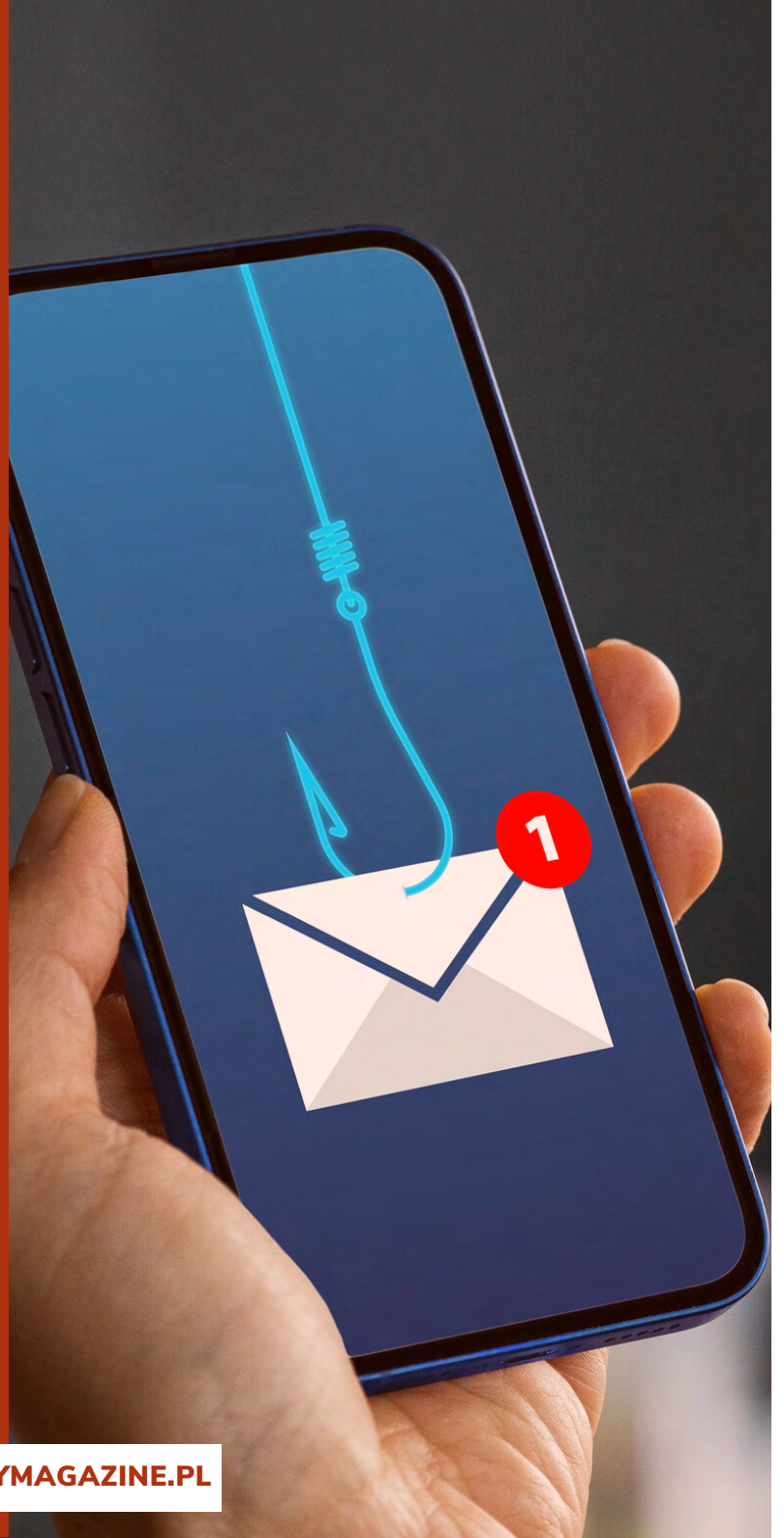
I podobnie jak w poprzednim przypadku Perception Point wykorzystuje sztuczną inteligencję do zwalczania tego typu cyberataków. Startup za pomocą wielowarstwowego generatywnego modelu sztucznej inteligencji jest w stanie wykrywać złośliwe maile i natychmiast usuwać je ze skrzynek odbiorczych. W celu identyfikacji cyberprzestępczych treści organizacja wykorzystuje duży model językowy – i to ponownie przykład zwalczania ognia ogniem, gdyż sami oszuści również używają podobnych oprogramowań.

Ponadto Perception Point korzysta ze sztucznej inteligencji umiejącej analizować kontekst sytuacyjny i behawioralny maili. Dzięki temu możliwe jest skuteczne rozpoznawanie niestandardowych zachowań, które mogą sugerować próby cyberoszustwa.

## TESSIAN – BEZPIECZEŃSTWO MAILI

Brytyjski startup Tessian, także specjalizujące się w bezpieczeństwie poczty e-mail i zwalcza zaawansowane cyberataki phishingowe. Dzięki wykorzystaniu uczenia maszynowego organizacja tworzy indywidualne modele zachowań użytkowników poczty e-mail, co pozwala na identyfi-





kację problematycznych wzorców i zapobieganie ryzykownym zdarzeniom, takim jak phishing czy wyciek danych.

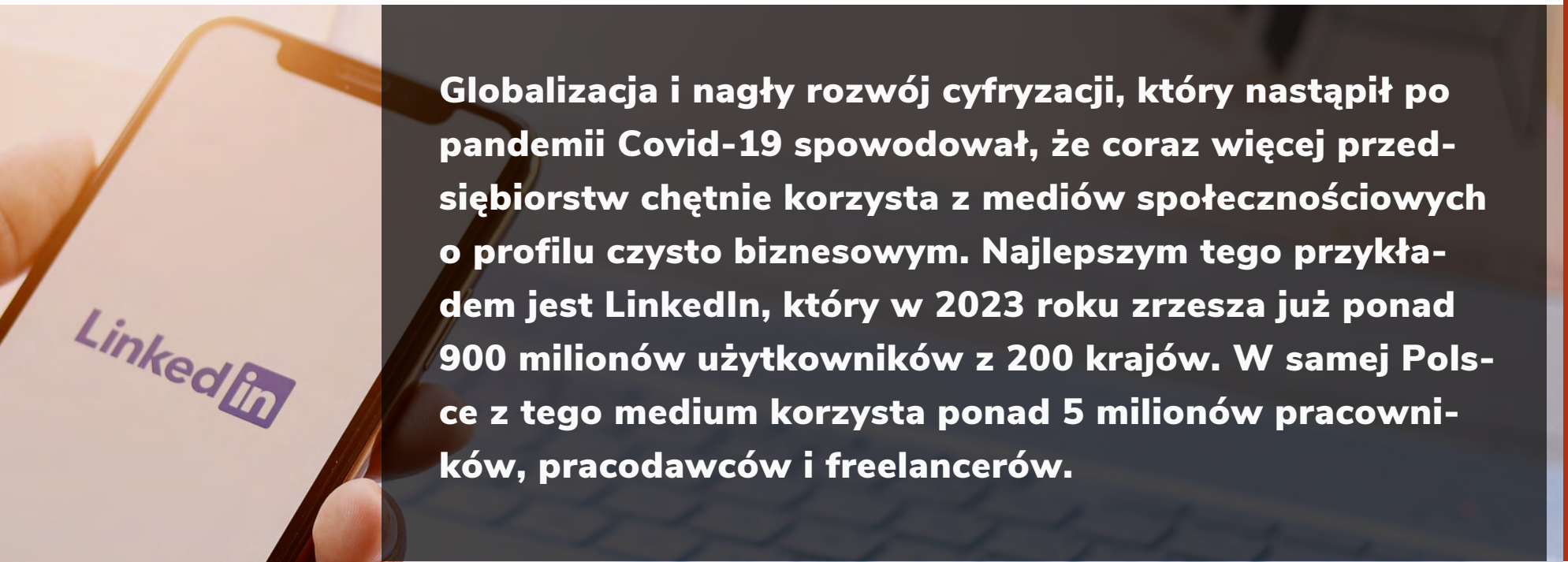
Co ważne – podobnie jak jej poprzednik – firma specjalizuje się w atakach typu BEC. Tessian, założony w 2013 roku, od momentu swojego powstania zdobywa uznanie klien-tów na całym świecie, w tym w sektorach prawnym, finansowym, opieki zdrowotnej i technologicznym. Wśród klientów znaleźli się giganci tacy jak Affirm, Arm, Investec oraz RealPage.

Szczególny wzrost startup odnotował w trakcie pandemii COVID-19, która wpłynęła na zmiany w sposobie pracy, co stworzyło nowe wyzwania związane z bezpieczeństwem. Wielu pracowników rozpoczęło pracę zdalną, co zwiększyło obszar potencjalnych cyberataków. Tessian wykorzystało to jako okazję do rozwoju i potroiło swoją bazę klientów z listy Fortune 500, oferując rozwiązania, które chronią przed zagrożeniami związanymi z ludzkim błędem.

Obecnie Tessian za pomocą modeli sztucznej inteligencji pomaga w przeciwdziałaniu przejmowania kont pracowników, usuwaniu niebezpiecznych maili, filtrowaniu oprogramowania typu ransomware, zapobieganiu wysyłania maili z wrażliwymi informacjami do niewłaściwych osób, powstrzymywaniem wycieków danych w wiadomościach czy wyłudzaniu informacji itd. itp.

# JAK OSZUŚCI WYKORZYSTUJĄ LINKEDIN DO CYBERATAKÓW?

**Piotr Rozmiarek**
Marken Systemy Antywirusowe - Bitdefender Polska




**Globalizacja i nagły rozwój cyfryzacji, który nastąpił po pandemii Covid-19 spowodował, że coraz więcej przedsiębiorstw chętnie korzysta z mediów społecznościowych o profilu czysto biznesowym. Najlepszym tego przykładem jest LinkedIn, który w 2023 roku zrzesza już ponad 900 milionów użytkowników z 200 krajów. W samej Polsce z tego medium korzysta ponad 5 milionów pracowników, pracodawców i freelancerów.**

Linkedin to niezbędne narzędzie służące do prowadzenia nowoczesnego biznesu, dzięki niemu można nawiązywać relacje biznesowe, poszukiwać pracowników i obserwować aktualne trendy w branży, w której działa nasza firma. To także miejsce, w którym zamieszczamy masę informacji o sobie, lub o naszym przedsiębiorstwie, co powoduje, że często możemy być na celowniku oszustów i nieuczciwej konkurencji.

## SCAM NA LINKEDIN – DLACZEGO JEST TAK POPULARNY?

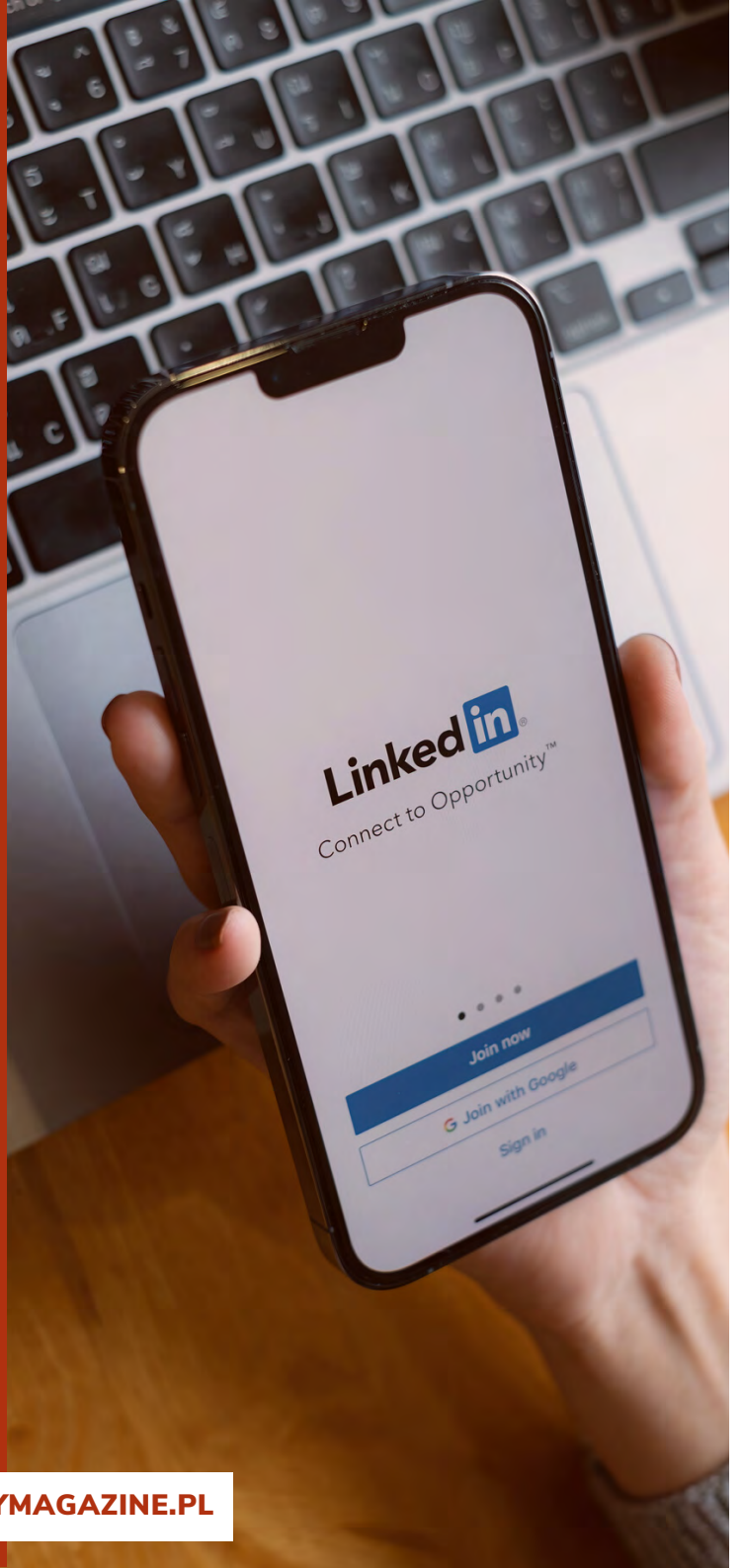
LinkedIn cieszy się wielką popularnością wśród scamerów z kilku powodów. Platforma ta zrzesza setki milionów użytkowników otwartych na zawieranie nowych relacji biznesowych. Pracownicy i pracodawcy korzystający z LinkedIn z reguły w przeciwieństwie do użytkowników innych mediów społecznościowych, takich jak X, Facebook i Instagram, nie ignorują zaproszeń od nieznajomych oraz wiadomości, które zawierają oferty biznesowe. Ten trend jest bardzo często wykorzystywany przez wszelkiego rodzaju cyberprzestępców, którzy podszywają się pod pracodawców i klientów, lub wykorzystują boty do zbierania danych.

Kolejnym powodem popularności LinkedIn wśród oszustów jest to, że użytkownicy i firmy, które mają profil na tym portalu, zamieszczają wiele cennych informacji o sobie i profilu swoich działalności. Wprawny oszust może wykorzystać te dane do tego, aby przeprowadzić skuteczny atak phishingowy skierowany przeciwko konkretnym pracownikom danej firmy.

Wiedząc już, skąd taka popularności platformy LinkedIn wśród oszustów, przeanalizujmy najpopularniejsze metody scamerów, którzy z niej korzystają.

## NAJPOPULARNIEJSZE METODY NA WYKORZYSTYWANIE LINKEDIN DO OSZUSTW

Numerem jeden wśród metod oszustwa na LinkedIn są kampanie phishingowe. Musimy jednak pamiętać o tym, że phishing na LinkedIn z reguły nie jest tak prymitywny, jak w przypadku innych mediów społecznościowych. Oszuści bardzo często doskonale znają metody z inżynierii społecznej i skutecznie manipulują swoimi rozmówcami. Scamerzy potrafią wykorzystać mechanizmy psychologiczne i cechy charakteru, zarówno te negatywne, jak chciwość i nadmierna




skłonność do ryzyka, jak i te pozytywne, np. altruizm i ambicję swoich ofiar do osiągnięcia swojego celu. Co więcej, informacje, które jako firma lub pracownik zamieszczamy na swoich profilach, mogą pomóc oszustowi w tym, aby przygotować spersonifikowaną i unikalną taktykę przeciwko nam.

Jednak, w jaki sposób może wyglądać takie oszustwo z perspektywy pracodawcy? Jeżeli prowadzisz firmę, działającą w branży IT, możesz otrzymać wiadomość od rzekomego pracownika np. Microsoftu lub Google z atrakcyjną ofertą na zakup ich produktów lub lukratywną ofertę współpracy. Następnie otrzymujemy link do formularza, w którym mamy pozostawić swoje dane, lub dokonać wpłaty online. Niestety, jeśli natrafiliśmy na oszusta, to strona z formularzem została najprawdopodobniej sfałszowana, a my podaliśmy hakerowi nasze cenne dane, które może sprzedać lub wykorzystać do innych oszustw. Jakich?

Niektórzy oszuści mogą posunąć się nawet do tego, że zarejestrują firmę o bliźniaczych danych do naszej, a następnie będą ją wykorzystywali do oszukiwania naszych klientów, których znajdą w liście obserwujących naszej firmy na LinkedIn. Oprócz tego mogą także stworzyć profile, które podszywają się pod pracowników naszej firmy i zamieszczać oferty pracy. Podczas „rekrutacji", oszust będzie proponował potencjalnym pracownikom uiszczanie opłat rekrutacyjnych lub oferty fałszywych, rzekomo bardzo atrakcyjnych inwestycji. Natomiast

jeśli wpisaliśmy dane związane z naszą bankowością, to istnieje ryzyko, że oszust wykorzysta je do włamania się na nasze konto bankowe.

Inne ryzyko wiąże się z zamieszczaniem przez pracowników firmy w swoich profilach danych, takich jak adresy e-mail. Dla przykładu - product manager umieszcza firmowy adres e-mail na swoim koncie: jan.iksiński@polit.com. Doświadczony oszust domyśli się, że w Twojej firmie adresy e-mail tworzone są zgodnie ze wzorem imię.nazwisko@domena.

Sprytny oszust może poszukać na LinkedIn księgowej, która pracuje w Twojej firmie. Gdy już pozna jej personalia i będzie wiedział, jaki jest jej adres e-mail, to będzie mógł zastawić na nią pułapkę. Może np. wykupić domenę bardzo podobną do naszego kontrahenta (dane kontrahenta może również znaleźć na jego profilu LinkedIn) i wysłać z niej wiadomość, w której zamieszcza zaległą fakturę, albo wysyła prośbę o korektę ostatniej faktury. Nasza księgowa, pomimo tego, że nie czekała na żadne dokumenty, to najprawdopodobniej pobierze załącznik i sprawdzi, o jaką fakturę chodzi. Ponieważ często korespondowała z tym kontrahentem i zna go, to nie będzie sprawdzała tego, że jedna litera domeny się nie zgadza. Pobrany plik może zawierać między innymi oprogramowanie szpiegowskie, dzięki któremu oszust z czasem pozna wszystkie dane do najważniejszych kont związanych z naszą firmą. Plik może okazać się także złośliwym oprogramowaniem typu ransomware, które zaszyfruje kluczowe zasoby naszej firmy i aby je odzyskać, będziemy musieli zapłacić okup.

Warto mieć na uwadze także to, iż oszustwa na LinkedIn mogą działać łańcuchowo. Wyobraź sobie, że jesteś freelancerem i tworzysz np. strony internetowe. Któregoś dnia otrzymujesz wiadomość na LinkedIn z prośbą o ofertę na specjalistyczną stronę internetową od pracownika firmy, w której pracuje kilkadziesiąt osób. Oferta zostaje zaakceptowana, a ty ustalasz telefonicznie szczegóły zlecenia. Po kilku tygodniach pracy kończysz projekt i wystawiasz fakturę za wykonaną pracę.

Niestety, firma nie ma zamiaru uregulować zaległej płatności. Gdy próbujesz skontaktować się z firmą, to rozmawiasz tylko z pracownikami biurowymi, którzy szczerze nie potrafią zrozumieć, dlaczego ich pracodawca nie opłacił faktury. Niestety, dzieje się tak, ponieważ oni także mogą być oszukiwani przez swojego pracodawcę i nie zdają sobie z tego sprawy. Istnieje pewne prawdopodobieństwo na to, że taka firma powstała tylko po to, aby być przykrywką dla oszusta, który nie ma zamiaru się wywiązać ze swoich zobowiązań wobec Ciebie, swoich pracowników oraz innych kontrahentów. Zamiast tego szybko zakończy działalność, nie ureguluje zapłaty za Twoją usługę, a stronę, którą stworzyłeś, sprzeda komuś innemu.

W czasie pandemii powstało wiele fałszywych firm, które opierały swoją „działalność" na pracy zdalnej i oferowały swoim pracownikom umowy prowizyjne. „Pracodawcy" podczas rekrutacji oraz szkolenia swoich pracowników korzystali z wielu technik manipulacyjnych znanych sekt oraz z firm działających w formacie MLM, przez co pracownicy pracowali przez wiele miesięcy bez jakiegokolwiek wynagrodzenia i nadal szczerze wierzyli w to, że ich pracodawca jest uczciwy.

Niestety, ich praca często polegała na oszukiwaniu kolejnych podmiotów i kontrahentów. Najgłośniejszym przykładem takiej firmy było brytyjskie przedsiębiorstwo Madbird, które działało w branży projektowej. Ali Ayad, czyli właściciel tej firmy spreparował swoje doświadczenie zawodowe. Ponadto oszukiwał swoich pracowników i klientów za pomocą historii o swoim rzekomym bogatym doświadczeniu zawodowym. Przez wiele miesięcy udawało mu się uniknąć zdemaskowania, ponieważ był bardzo charyzmatyczny, świetnie manipulował uczuciami swoich pracowników i korzystał ze skradzionych projektów, które rzekomo sam wykonał. Ostatecznie po nagonce medialnej po prostu zniknął z sieci. Pamiętajmy jednak, że tego typu „przedsiębiorstw" jest znacznie więcej,

także możemy się na nie natknąć.

## W JAKI SPOSÓB ZABEZPIECZYĆ FIRMĘ PRZED OSZUSTAMI NA LINKEDIN?

Najważniejszym elementem skutecznej ochrony przed oszustami na LinkedIn jest zabezpieczenie wszystkich urządzeń w naszej firmie za pomocą skutecznego systemu antywirusowego. Jeśli przetwarzamy lub gromadzimy dane krytyczne, to warto także rozważyć dodatkowe narzędzia wyposażone w technologię EDR i XDR. Dzięki nim będziemy mogli uchronić się przed niebezpieczeństwami związanymi ze złośliwym oprogramowaniem i sfałszowanymi stronami internetowymi, których jedynym celem jest kradzież naszych danych, takich jak: adres e-mail, hasła i dane bankowe.

Kolejnym istotnym etapem są regularne szkolenia swoich pracowników z zakresu podstawowych zasad cyberbezpieczeństwa. Wymagajmy od nich tego, aby korzystali z unikalnych, silnych haseł oraz, aby regularnie je zmieniali. Nauczmy ich także tego, aby nie pobierali podejrzanych plików i nie klikali w niebezpieczne, nieznane linki.

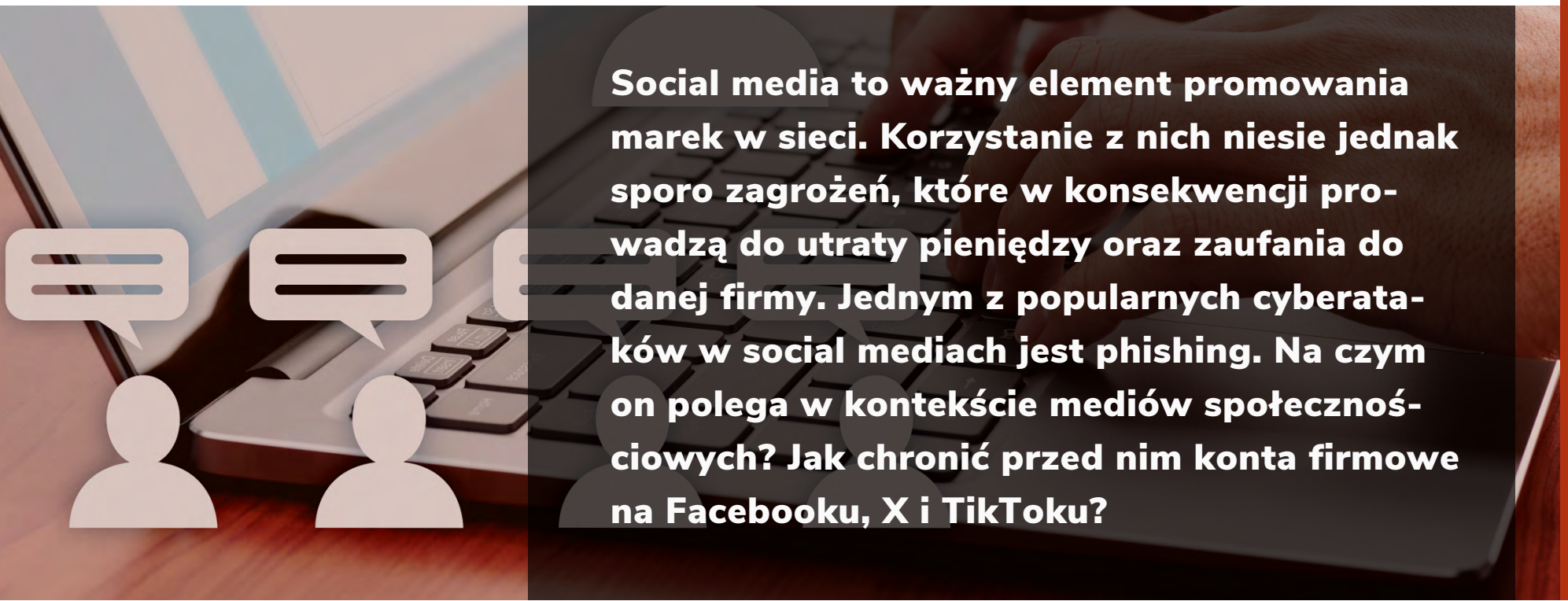
W przypadku otrzymania interesującej oferty na LinkedIn warto także wykonać telefon do centrali firmy, z którą rzekomo korespondujemy po to, by potwierdzić autentyczność pracownika. Zawsze dokładnie sprawdzajmy domeny adresów, z którymi korespondujemy, w tym także to, kiedy

zostały one zarejestrowane.

Jeśli już zdecydujemy się na wykonanie usługi z klientem, którego pozyskaliśmy na LinkedIn, to jeśli to możliwe, to sprawdźmy na naszych branżowych grupach, czy z ów „klientem” nikt wcześniej nie miał problemów. Dzięki zachowaniu czujności i wykonaniu kilku wyżej wymienionych kroków możemy znacząco zminimalizować ryzyko tego, że ktoś nas oszuka na LinkedIn.

# JAK CHRONIĆ KONTA FIRMOWE PRZED WYŁUDZENIAMI? FACEBOOK, X, TIK TOK

Redakcja
SECURITY MAGAZINE



**Social media to ważny element promowania marek w sieci. Korzystanie z nich niesie jednak sporo zagrożeń, które w konsekwencji prowadzą do utraty pieniędzy oraz zaufania do danej firmy. Jednym z popularnych cyberataków w social mediach jest phishing. Na czym on polega w kontekście mediów społecznościowych? Jak chronić przed nim konta firmowe na Facebooku, X i TikToku?**

## CO TO JEST PHISHING W SOCIAL MEDIACH?

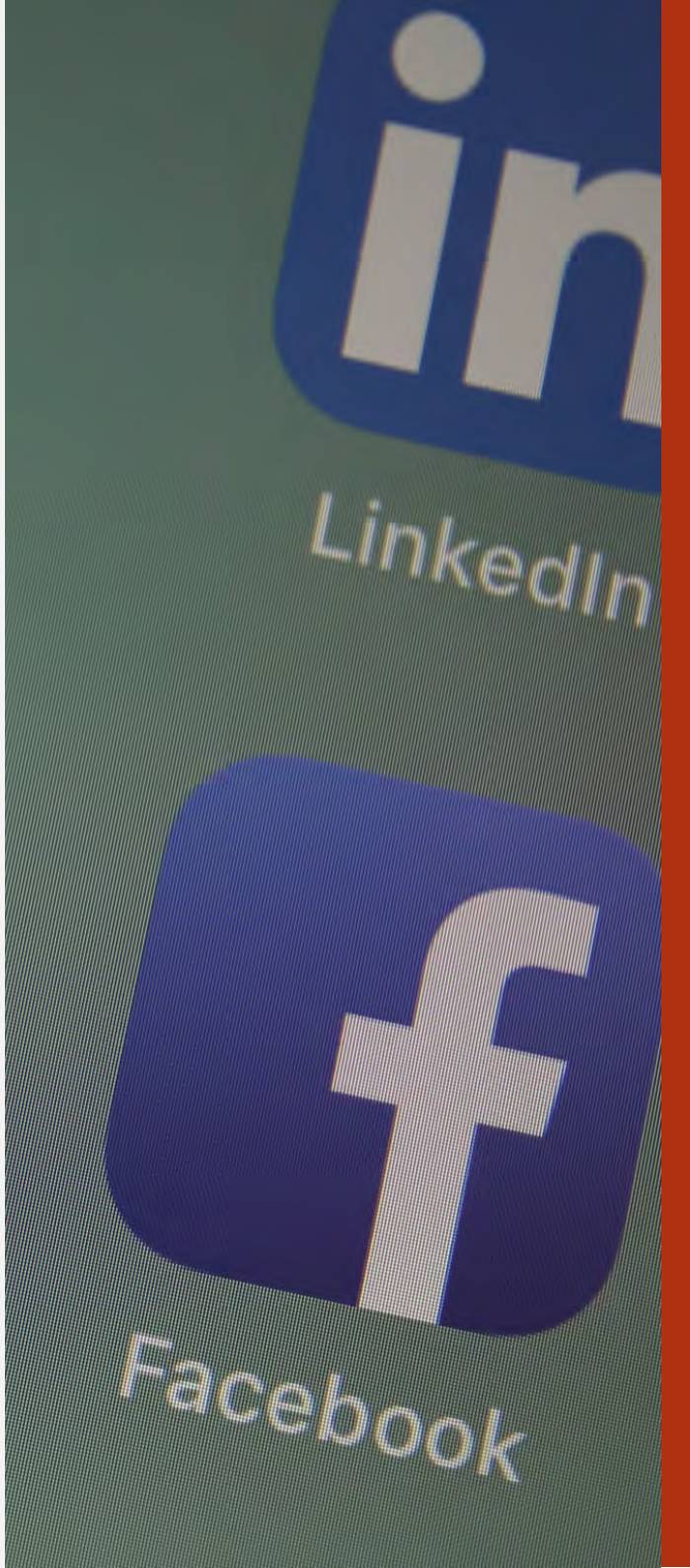
Taktyk phishingu jest wiele i mogą przybierać różne formy. Do tej najbardziej znanej należy tworzenie przez oszustów fałszywych stron imitujących marki, które cieszą się zaufaniem. Nieświadomi phishingu użytkownicy klikają linki i w ten sposób przekazują przestępcom swoje dane. Od ataków phishingowych nie są, oczywiście, wolne social media, o czym zapewne doskonale wiedzą osoby, które prowadzą profile firmowe na Facebooku, TikToku czy X (dawniej Twitter).

Firmy, które padły ofiarą cyberataków, tracą nie tylko pieniądze, ale przede wszystkim zaufanie, które żmudnie budowały. Dlaczego? Bo jeśli nieprawdziwy profil jest pierwszym kontaktem z „marką", istnieje duże prawdopodobieństwo, że potencjalny klient zostanie na zawsze utracony, jeśli będzie miał złe doświadczenia.

To samo dotyczy stałych klientów. Gdy z marką skojarzone zostanie negatywne doświadczenie, nawet jeśli był to efekt cyberataku, prawdopodobieństwo, że klient ponownie jej zaufa w przyszłości, będzie mniejsze. Co więcej, niezadowoleni użytkownicy mogą nawet rozpowszechniać negatywne recenzje na temat brandu za pośrednictwem mediów społecznościowych.

## TYPOWE TAKTYKI PHISHINGOWE W SOCIAL MEDIACH

Jedną z powszechnych taktyk phishingowych pojawiających się w mediach społecznościowych są oszustwa związane z podszywaniem się pod kierownictwo, znane również jako „oszustwo dyrektora generalnego". Taki cy-



cyberatak ma miejsce wtedy, gdy dyrektor generalny lub członek kadry kierowniczej zajmujący wysokie stanowiska w firmie, żąda informacji lub pilnego przelewu pieniężnego od pracownika zatrudnionego na niższym stanowisku.

Oszust wykorzystuje ludzką skłonność do bezkrytycznego wykonywania poleceń przełożonego. Ten rodzaj oszustw nasilił się podczas pandemii, kiedy praca zdalna stała się nową normą, a współpracownicy nie byli już fizycznie razem w biurze.

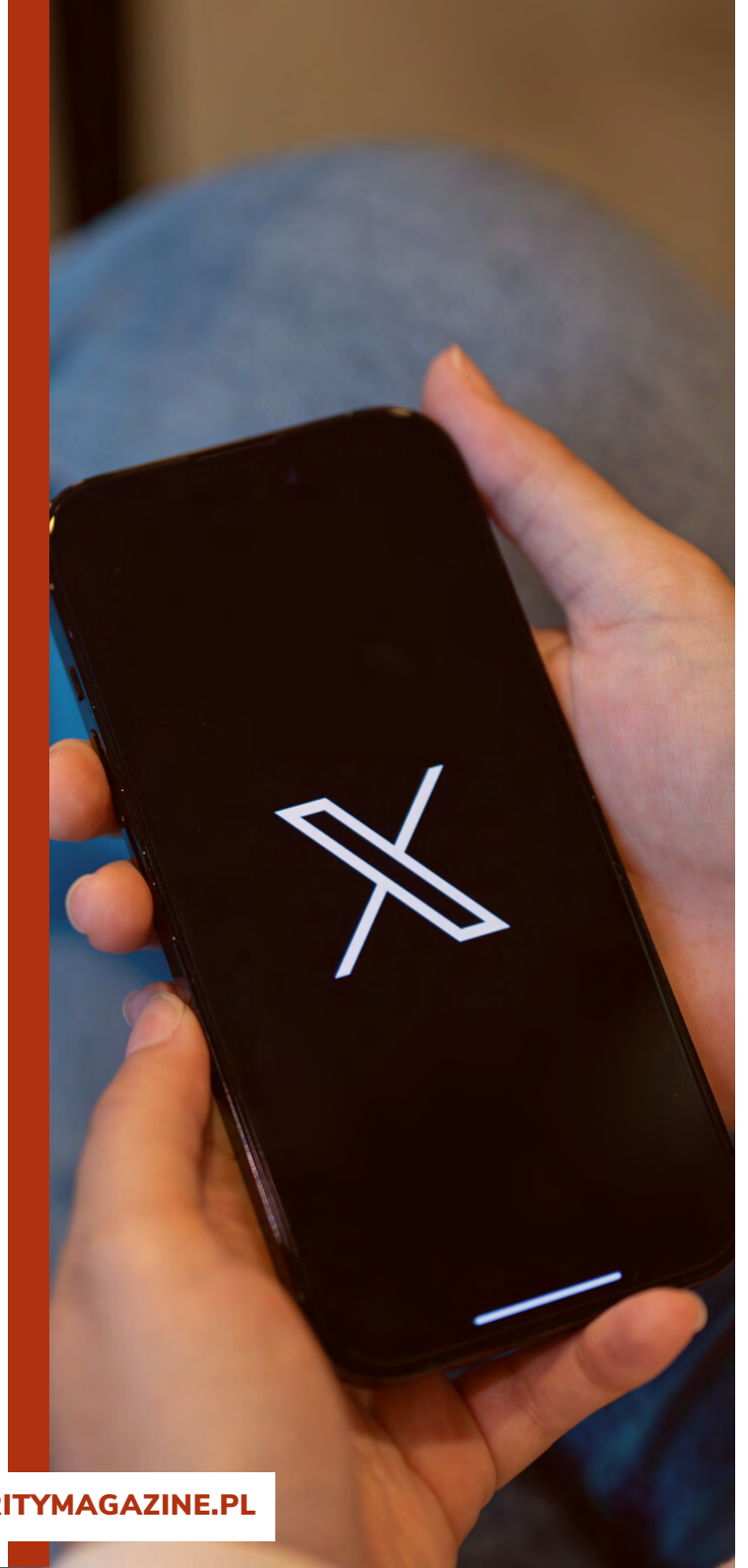
Kolejną metodą jest tworzenie fałszywych profili firmowych, które mogą podszywać się pod daną markę. Taki profil wówczas może tworzyć nieprawdziwe reklamy, prezentując produkty lub usługi skopiowane od legalnego sprzedawcy.

Cyberprzestępcy, aby wyłudzić dane, mogą również tworzyć fałszywe oferty pracy. Do tego typu oszustw najczęściej dochodzi na LinkedIn, czyli platformie stworzonej do szukania pracy. Media społecznościowe to także miejsce, gdzie wiele firm prowadzi również obsługę klienta. Oszuści, aby wprowadzić w błąd użytkowników danej platformy, kopiują elementy identyfikujące markę, a następnie deklarują chęć pomocy. Wówczas klient, wierząc, że jest w bezpiecznych rękach, udostępnia im np. swoje hasła.

## UDANY ATAK PHISHINGOWY W SOCIAL MEDIACH

Ataki phishingowe w mediach społecznościowych są stosunkowo powszechne, a ich skutki mogą być różnorodne. Dla przykładu, w sierpniu 2019 r. firma Fstoppers zgłosiła kampanię phishingową rozpoczętą na Instagramie, podczas której oszuści wysyłali prywatne wiadomości do użytkowników Instagrama, ostrzegając ich, że naruszyli prawa autorskie do zdjęć i żądając od nich wypełnienia formularza, aby uniknąć zawieszenia konta.

Jedna z ofiar otrzymała prywatną wiadomość z oficjalnego konta North Face, w której zarzucano jej naruszenie praw autorskich, i nakłoniono ją do skorzystania z łącza do „InstagramHelpNotice.com”, pozornie legalnej strony internetowej, na której użytkownicy proszeni są o podanie danych logowania. Ofiary, które wpadły w pułapkę, ostatecznie zapewniły hakerom dostęp do informacji o swoim koncie i innych danych osobowych powiązanych z kontem na Instagramie.



## NAJWIĘKSZE WŁAMANIE W HISTORII TWITTERA

Z kolei w lipcu 2020 roku na ówczesnym Twitterze, z kont znanych osobistości świata polityki, mediów i show biznesu wysłane zostały tweety zachęcające do wpłat na wskazany portfel bitcoinowy, aby otrzymać zwrot podwojonej kwoty. W ciągu półtorej godziny hakerzy zebrali kwotę bitcoinów odpowiadającą kwocie 118 tysięcy dolarów, czyli ok. 466 tysięcy złotych.

Wśród zhakowanych kont znalazły się te należące do m.in.: Apple, Ubera, Baracka Obamy, Joe Bidena, Billa Gatesa, Kanye Westa czy Kim Kardashian.

Czy to oznacza, że promowanie biznesu w social mediach się nie opłaca, bo jest zbyt niebezpiecznie? Oczywiście, że nie. Dlatego, zanim zostanie założone konto biznesowe na jakiejkolwiek platformie, warto najpierw dokładnie zapoznać się z jej specyfiką.

## FACEBOOK A PHISHING

Zacznijmy od Facebooka. Serwis ten uruchomiono na początku XXI wieku i stał się podstawową platformą łączącą ludzi, firmy, rodziny i klientów. Typowy atak phishingowy na tej platformie bazuje na wiadomości lub odnośniku z prośbą o podanie lub potwierdzenie danych osobowych. Niestety, gdy atak odbywa się w postaci wpisu na Facebooku lub wiadomości wysłanej przez Messenger, trudno jest go odróżnić od aktywności realnych osób lub marek.

Phishing na Facebooku służy cyberprzestępcom do zebrania danych, które umożliwiają hakerowi uzyskanie dostępu do kont użytkowników tego portalu. Po udanym ataku mogą pojawiać się wiadomości informujące o problemie z kontem na Facebooku oraz zawierające prośbę o zalogowanie się w celu rozwiązania problemu.

Takie wiadomości, oczywiście, bardzo często zawierają odnośnik, w który wystarczy kliknąć, aby znaleźć się na stronie do złudzenia przypominającej stronę Facebooka. Gdy użytkownik trafia na nią, pojawia się prośba o zalogowanie do konta. W ten sposób haker wykrada dane, dlatego zawsze przed zalogowaniem należy sprawdzać adres URL, aby mieć pewność, że przeniesienie nastąpi na stronę www.facebook.com. Wszystkie inne adresy prawdopodobnie są fałszywe.

## JAK ZABEZPIECZYĆ KONTO FIRMOWE NA FACEBOOKU?

Oto kilka wskazówek:

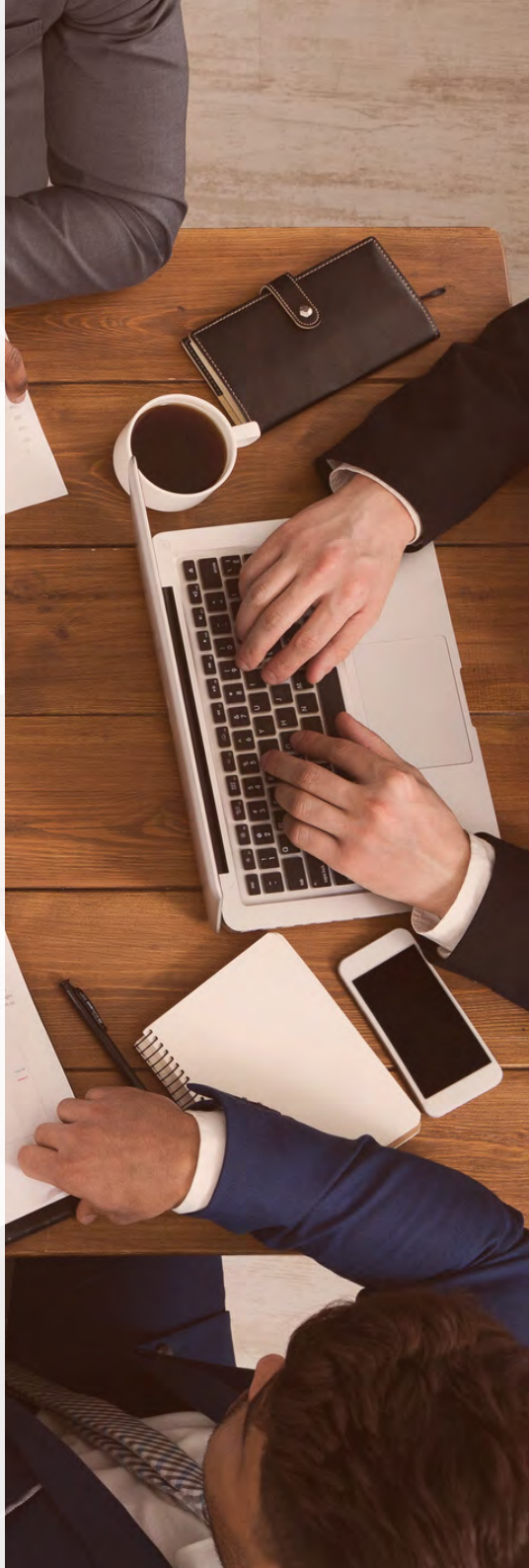
- Wyszukaj nazwę swojej marki lub produktu/usługi w wyszukiwarce Google (lub innych popularnych wyszukiwarkach) i sprawdź wyświetlane strony na Facebooku. Jeśli pojawią się strony, które nie należą do Ciebie, przejrzyj je.
- Przejdź bezpośrednio do Facebooka, a następnie użyj funkcji wyszukiwania, aby wyszukać nazwę swojej marki i produktu. Skorzystaj z funkcji filtra wyszukiwania, wybierz „Strony”, a następnie przejrzyj wyniki, aby sprawdzić, czy nie ma fałszywych stron.
- Możesz także użyć hashtagów (np., jeśli nazwa Twojej marki to „myrestaurant”, możesz spróbować wyszukać #myrestaurant. Spróbuj także wyszukać odmiany nazwy swojej marki, takie jak moja-restauracja, myrestaurantt itd. Niektórzy cyberprzestępcy mają tendencję do używania błędnej pisowni podczas tworzenia fałszywych stron na Facebooku, aby oszukać markę i potencjalnych gości.
- Możesz także skorzystać z wyszukiwarki Google i Grafiki Google, aby wyszukać swój produkt, a następnie ręcznie sprawdzić, gdzie na Facebooku wykorzystano zdjęcia Twojego produktu (w Grafice Google). Może to być świetny sposób na znalezienie ukrytych stron.

W kontekście zabezpieczenia konta firmowego w ten sposób, by cyberoszust nie wykorzystał prywatnego konta na Facebooku Twojego lub osoby z firmy do dostania się np. do menedżera reklam musisz pamiętać o kilku kluczowych sprawach:

# Jak chronić konta firmowe przed wyłudzeniami?

## Facebook, X, Tik Tok

- **Ustaw silne hasło.** Twoje hasło powinno być unikalne i skomplikowane, zawierające kombinację liter, cyfr i znaków specjalnych. Unikaj używania łatwych do odgadnięcia haseł, takich jak nazwy zwierząt, daty urodzenia czy nazwy firmy.
- **Włącz dwuetapowe uwierzytelnianie.** To dodatkowa warstwa zabezpieczeń, która wymaga podania kodu wysłanego na Twój telefon komórkowy lub adres e-mail podczas próby logowania z nieznajomego urządzenia. Zresztą, bez tego administrator i inne osoby przypisane do menedżera firmy mogą szybko stracić do niego dostęp. Facebook podał, że *"jeśli uwierzytelnianie dwuskładnikowe jest wymagane w przypadku Twojego Menedżera firmy, osoby korzystające z niego muszą je włączyć, aby uzyskać dostęp do Menedżera firmy. Osoby, które nie skonfigurowały uwierzytelniania dwuskładnikowego, nie będą mogły uzyskać dostępu do Twojego Menedżera firmy, dopóki nie włączą uwierzytelniania dwuskładnikowego* ***na swoim osobistym koncie na Facebooku.***"
- **Włącz Facebook Protect** - zaawansowany program zabezpieczeń, który pomaga chronić konto przed nieautoryzowanym dostępem.
- **Regularnie monitoruj aktywność na koncie.** Sprawdzaj regularnie dziennik aktywności na Facebooku ("Twoje informacje na Facebooku" - "Wyświetl aktywność swojego profilu i zarządzaj nim", zwłaszcza "Lokalizacja zalogowania"), aby upewnić się, że nie ma podejrzanych działań. Jeśli zauważysz coś niepokojącego, natychmiast zmień hasło.
- **Ogranicz dostęp do konta.** Upewnij się, że tylko zaufane osoby mają dostęp do Twojego konta firmowego. Regularnie przeglądaj listę osób, które mają uprawnienia do zarządzania Twoją stroną i usuwaj tych, którzy nie są już potrzebni.
- **Bądź ostrożny z wiadomościami i linkami.** Nie klikaj w podejrzane linki ani nie otwieraj podejrzanych wiadomości, nawet jeśli pochodzą od znajomych. Mogą to być próby phishingu.
- **Aktualizuj regularnie swoje oprogramowanie**. Upewnij się, że system operacyjny, przeglądarka i inne aplikacje są regularnie aktualizowane, aby chronić się przed znanymi lukami bezpieczeństwa.



## X A PHISHING

Facebook jest postrzegany jako platforma do utrzymywania kontaktu między znajomymi i rodziną, a X umożliwia interakcję z ludźmi z całego świata, których nigdy się nie spotkało w prawdziwym świecie. Ten poziom komfortu w kontaktach z obcymi ludźmi sprawił, że X stał się popularną platformą do przeprowadzania ataków phishingowych.

Hakerzy działający na X wykorzystują te same taktyki i techniki, co w innych mediach społecznościowych. Przestępca wysyła fałszywe wiadomości, które rzekomo pochodzą od X. Ich celem jest nakłonienie użytkownika do ujawnienia wrażliwych informacji, takich jak dane logowania, dane osobowe, a nawet dane karty kredytowej.

Po tego typu atakach phishingowych mogą następować kolejne, w tym atak „płać za obserwujących" (pay for followers). W tym przypadku haker wysyła ofierze wiadomość z propozycją załatwienia określonej liczby „obserwujących" za jedyne pięć dolarów. Ujawnienie danych osobowych oraz numeru karty kredytowej przez użytkownika otwiera mu furtkę do pobrania środków z jego konta i zalogowania się na jego koncie na X, aby kontynuować proceder wśród obserwujących ofiarę.

## JAK CHRONIĆ PROFIL FIRMOWY NA X PRZED CYBERATAKAMI?

Zabezpieczenie konta firmowego na X jest kluczowe dla ochrony danych firmy i reputacji. Jak to robić skutecznie? Na początek warto stworzyć silne hasło, które jest długie, złożone oraz zawiera wielkie i małe litery. Dobre zabezpieczenie konta nie powinno się składać z łatwo dostępnych informacji jak np. nazwa firmy, imię i nazwisko właściciela czy nazwy miejscowości, w której znajduje się firma. Aby utrudnić cyberprzestępcom włamanie się na konto, warto też regularnie zmieniać hasło oraz mieć włączone uwierzytelnienie dwuskładnikowe.

Aby chronić konto firmowe na X, warto ograniczyć liczbę osób, które mogą nim zarządzać. Najlepiej, aby tę możliwość miały tylko osoby, które są zaangażowane w działania marketingowe lub administracyjne. Pamiętaj także o regularnym przeglądaniu i aktualizacji listy osób mających dostęp do konta.

Ponadto warto zorganizować szkolenia dla pra-

cowników, aby ich uświadomić na temat zagrożeń związanych z bezpieczeństwem internetowym, phishingiem oraz regularnie robić kopie zapasowe ważnych danych i treści na swojej stronie X, aby zapewnić możliwość ich odtworzenia w przypadku utraty lub uszkodzenia. Należy również pamiętać, że zabezpieczanie konta firmowego na X to ciągły proces, który wymaga uwagi oraz świadomości ze strony właścicieli i administratorów konta.

## TIKTOK – DLACZEGO JEST NARAŻONY NA CYBERATAKI?

Kolejną platformą, na której coraz częściej pojawiają się konta firmowe, jest TikTok. Ma on ogromną bazę użytkowników, liczącą ponad 1 miliard osób, a treści hostowane na platformie gromadzą ponad miliard wyświetleń dziennie. Do tej pory konsumenci wydali na TikToku ponad 2,5 miliarda dolarów. Popularność tej platformy sprawiła, że stała się ona celem cyberataków.

Ze względu na specyfikę TikToka bardzo trudno odróżnić treści prawdziwe od tych, które produkują hakerzy. Jedną z najczęstszych prób oszustwa na tej platformie jest obietnica zwiększenia liczby polubień/obserwatorów/zasięgu. Oszuści często kontaktują się z ofiarami z propozycją zakupu polubień na TikToku, co zwiększy popularność i zasięg treści profilu. Jednak w wielu przypadkach oszuści przejmują pełną kontrolę nad kontem i blokują pierwotnemu użytkownikowi możliwość korzystania z niego.

Podobnie jak w przypadku serwisu X lub Facebook, oszuści nierzadko podszywają się pod inne marki lub osoby wpływowe. Dla profili firmowych jest to szczególne niebezpieczne w kontekście np. współpracy z influencerami.

Hakerzy, podszywając się pod znane, wpływowe osoby, zdobywają jak najwięcej niczego niepodejrzewających obserwujących, a następnie rozpowszechniają oszustwa związane np. z inwestycjami w kryptowaluty, publikują linki do złośliwego oprogramowania i dopuszczają się innych działań cyberprzestępczych. Dlatego przed rozpoczęciem współpracy bardzo dokładnie trzeba sprawdzić profil osoby, z którą chcemy współpracować.

Kradzież tożsamości marki na TikToku jest również niebezpieczna ze względu na phishing. Niestety cyberprzestępca podszywający się pod nasz brand może wysyłać wiadomości tekstowe, obiecując np. ogromny wzrost liczby obserwujących i polubień wraz z niebezpiecznym linkiem. Klikając link, użytkownik ryzykuje przekazanie hakerom danych konta i poufnych informacji lub ściągnięcie na swój sprzęt złośliwego oprogramowania.

## JAK CHRONIĆ KONTO FIRMOWE NA TIKTOKU?

Aby ochronić swoje konto na TikToku przed cyberatakami, staraj się nie pobierać bez weryfikacji aplikacji promowanych na TikToku. Zanim to zrobisz, przeprowadź rozeznanie i przeczytaj recenzje, aby mieć pewność, że dostajesz to, za co płacisz i że nie będziesz pobierać oprogramowania reklamowego ani złośliwego na swoje urządzenie. Warto też dokładnie sprawdzać autentyczność kont gwiazd. Najprostszym sposobem na znalezienie konta prawdziwej gwiazdy jest sprawdzenie zweryfikowanej odznaki. Każda legalna gwiazda będzie miała tę odznakę. Jednak nierzadko zdarza się, że oszuści wymyślają sposób na uzyskanie jej, dlatego np. w wyszukiwarce Google warto sprawdzić danego influencera wpisując jego nazwę oraz frazę „TikTok", aby znaleźć jej legalną nazwę.

Ponadto, jeśli jakieś konta promują szybkie sposoby na zdobycie polubień i obserwujących, to istnieje duże prawdopodobieństwo, że jest to oszustwo. Rozwój na TikToku zapewni Ci jedynie tworzenie wysokiej jakości treści.

## JAK UNIKNĄĆ PHISHINGU W MEDIACH SPOŁECZNOŚCIOWYCH?

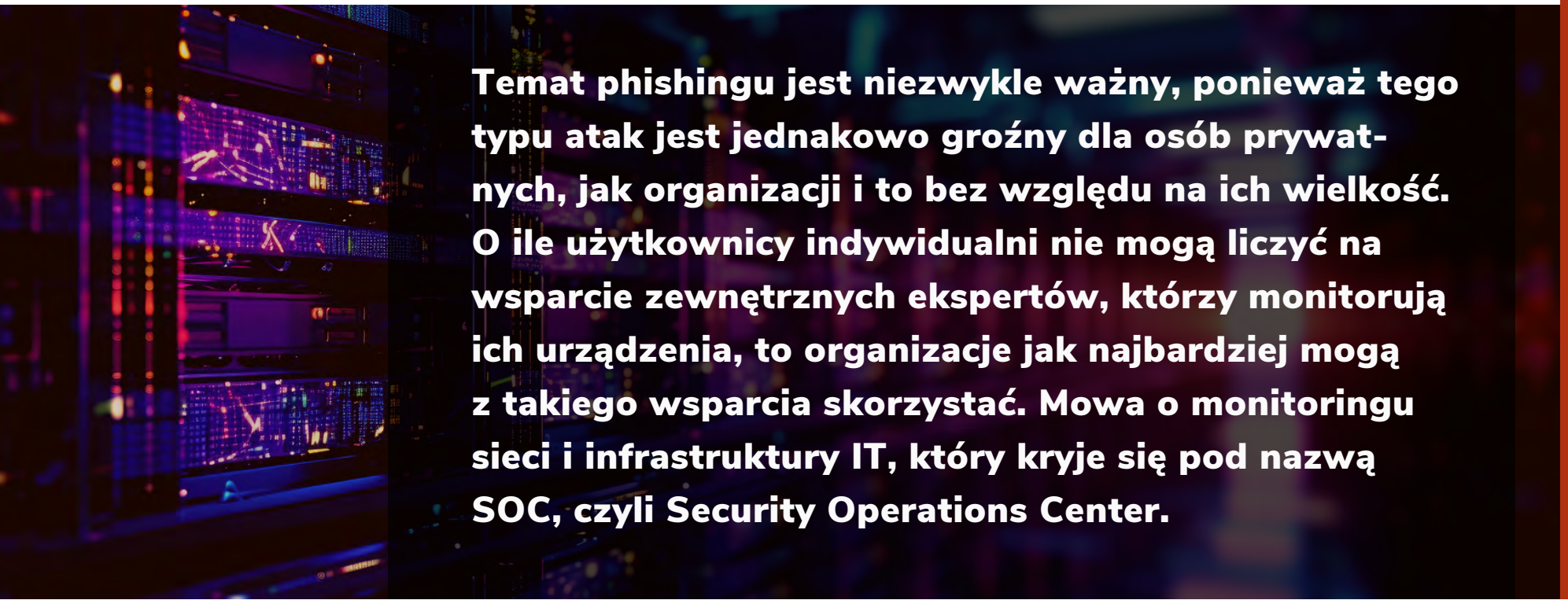
Najlepszym sposobem na uniknięcie uwikłania w oszustwo w mediach społecznościowych, niezależnie od tego, czy jesteś firmą, czy osobą fizyczną, jest połączenie edukacji i technologii. Do najbardziej skutecznych sposobów zapobiegania i unikania oszustw typu phishing w mediach społecznościowych należą takie zachowania jak:

# Jak chronić konta firmowe przed wyłudzeniami? Facebook, X, Tik Tok


- Nigdy nie akceptuj zaproszeń do grona znajomych od osób, których nie znasz.
- Nie używaj tego samego hasła i nazwy użytkownika do wszystkich swoich kont. Jeszcze lepiej jest aktualizować swoje dane co kilka miesięcy.
- Jeśli podejrzewasz witrynę internetową lub wiadomość e-mail, zawsze sprawdź adres URL lub adres e-mail pod kątem jakichkolwiek charakterystycznych oznak phishingu, takich jak literówki lub nieprofesjonalne adresy e-mail.
- Jeśli ktoś prosi o pieniądze, pamiętaj o potwierdzeniu jego tożsamości w trybie offline, podczas rozmowy telefonicznej.
- Nie bierz udziału w quizach z prośbą o podanie danych osobowych.
- Nie klikaj żadnych podejrzanych linków.
- Edukuj klientów i pracowników na temat kanałów komunikacji, których używasz do różnych celów.
- Wykrywaj fałszywe profile i podrabiane towary za pomocą zautomatyzowanego oprogramowania.

# MONITORING BEZPIECZEŃSTWA. WŁASNY ZESPÓŁ CZY OUTSOURCING?

**Łukasz Zajdel**
Perceptus Sp z o. o.



**Temat phishingu jest niezwykle ważny, ponieważ tego typu atak jest jednakowo groźny dla osób prywatnych, jak organizacji i to bez względu na ich wielkość. O ile użytkownicy indywidualni nie mogą liczyć na wsparcie zewnętrznych ekspertów, którzy monitorują ich urządzenia, to organizacje jak najbardziej mogą z takiego wsparcia skorzystać. Mowa o monitoringu sieci i infrastruktury IT, który kryje się pod nazwą SOC, czyli Security Operations Center.**

## JAK SOC IDENTYFIKUJE ATAK PHISHINGOWY W ORGANIZACJI?

Przeanalizujmy to na konkretnym przypadku.
W firmie, nazwijmy ją "ABC Sp z o. o. .", pracownicy otrzymują na swoje służbowe skrzynki e-mail podejrzane wiadomości, udające oficjalne komunikaty od firmy dostarczającej bardzo istotne dla ich pracy oprogramowanie. Wiadomość sugeruje konieczność natychmiastowej aktualizacji oprogramowania przy wykorzystaniu załączonego linka, by uniknąć utraty danych i uszkodzenia systemu. Zaniepokojeni pracownicy zgłosili tę sytuację do działu bezpieczeństwa IT, jednak ten już znał temat, ponieważ na urządzeniu UTM zabezpieczającym ruch sieciowy pojawił się alert, został przesłany do systemu SIEM i SOC obserwował już sytuację.

Uruchomiona została procedura identyfikacji ataku przy użyciu systemu SIEM, którego praca opiera się na analizie logów. System SIEM może być zintegrowany z innymi zabezpieczeniami, takimi jak systemy antywirusowe lub dedykowane systemy zapobiegające phishingowi. Te narzędzia dostarczają dodatkowych informacji lub ostrzeżeń na temat potencjalnych zagrożeń. W wyniku tych analiz, analitycy SOC mogą potwierdzić, czy doszło do próby ataku opartego na phishingu i podjąć odpowiednie kroki w celu ochrony firmy przed dalszymi zagrożeniami.

## JAK WYGLĄDAJĄ KOLEJNE ETAPY DZIAŁANIA?

**Krok 1: Weryfikacja logów z serwera e-mail**
Analitycy SOC sprawdzają logi z serwera e-mail, aby zobaczyć, które skrzynki odbiorców otrzymały podejrzaną wiadomość. Analiza tych logów pomahga zidentyfikować, którzy pracownicy byli potencjalnymi celami ataku.

**Krok 2: Analiza zawartości wiadomości**
Analitycy przeprowadzają analizę treści wiadomości phishingowej, obejmującą link do "aktualizacji oprogramowania". Skanują go w poszukiwaniu potencjalnych zagrożeń i domen, które mogą być związane z phishingiem.

**Krok 3: Analiza ruchu sieciowego**
Zauważają, że jeden z pracowników kliknął w link. Dział bezpieczeństwa analizuje ruch sieciowy generowany przez ten klik. To obejmuje identyfikację docelowej strony internetowej (sprawdzenie, czy była ona podejrzana) i ewentualne próby pobierania złośliwego oprogramowania.

**Krok 4: Analiza ruchu w sieciach wewnętrznych**
Analitycy sprawdzają logi sieciowe wewnętrzne, aby zobaczyć, czy jakiekolwiek urządzenia wewnętrzne próbowały się komunikować z podejrzaną stroną internetową lub inicjować jakiekolwiek nieznane połączenia.

Założeniem tego przykładu było posiadanie przez ABC Sp z o.o. własnego działu bezpieczeństwa IT. Możliwe są jednak również inne scenariusze - załóżmy, że SOC pracował jako zewnętrzny partner?

Wtedy pojawiają się kolejne kroki:
**Krok 5: Przekazanie informacji o potencjalnym ataku i zagrożeniu określonych obszarów infrastruktury,**
a następnie:
**Krok 6: Przekazanie rekomendacji nt. zalecanych możliwości przyszłego zabezpieczenia się przed atakiem.**

Często atak nie jest finalizowany od razu. Infekcja pozostaje w formie utajonej do momentu, kiedy kolejne urządzenia i systemy będą zainfekowane. Monitoring 24/7 pozwala uniknąć rozprzestrzeniania się zagrożenia i zabezpiecza infrastrukturę i sieć przed negatywnymi konsekwencjami, a firmę przed stratami.

## SOC W WEWNĘTRZNYCH STRUKTURACH FIRMY

Security Operations Center można budować w strukturach własnej firmy. Wymaga to wyodrębnienia tej komórki organizacyjnej i wyposażenia jej w odpowiednie systemy, które pozwalają na obserwację i analizę sytuacji oraz wykrywanie anomalii.

Plusem takiego rozwiązania jest pełna kontrola nad danymi i zachowanie pełnej tajemnicy funkcjonowania organizacji w jej wewnętrznych strukturach. Natomiast minusem są związane z tym wydatki.

Koszty budowy własnego SOC pojawiają się na kilku poziomach. Skuteczne zabezpieczenie sieci wymaga odpowiedniego oprogramowania, które zbiera informacje z urządzeń i sieci. Takie rozwiązania wymagają inwestycji, które TCO często generuje powtarzalne, bardzo istotne koszty.
Dodatkowo potrzebny jest zespół specjalistów, którzy właściwie odczytają i zinterpretują informacje dostarczane przez rozwiązania technologiczne.

Obecnie doświadczamy niedoboru specjalistów z obszaru cybersecurity na rynku, co bezpośrednio przekłada się na wysokość zarobków stanowiących minimalny akceptowalny próg dla osób, które posiadają odpowiednie kwalifikacje.

W związku z tym czynnik ludzki staje się deficytowym zasobem, o który zabiegają wszystkie organizacje zdecydowane na budowę własnego SOC, często bez względu na cenę, czyli poziom wynagrodzenia.

## OUTSOURCING USŁUG SOC

Możliwe jest również drugie rozwiązanie, które redukuje koszty związane z oprogramowaniem i budową własnego zespołu.

Jest to outsourcing usług związanych z monitoringiem sieci/systemów wewnętrznych w zewnętrznej firmie, specjalizującej się w obszarze cyberbezpieczeństwa.

Dzięki tej opcji organizacja korzysta z rozwiązań technologicznych i wyspecjalizowanej obsługi, nie ponosząc pełnych kosztów. Budowa działu SOC i wyposażenie go w odpowiednie narzędzia pozostaje po stronie usługodawcy, natomiast organizacja wybierająca tę formę obsługi czerpie korzyści wynikające z opieki specjalistów i gwarancji zabezpieczeń.

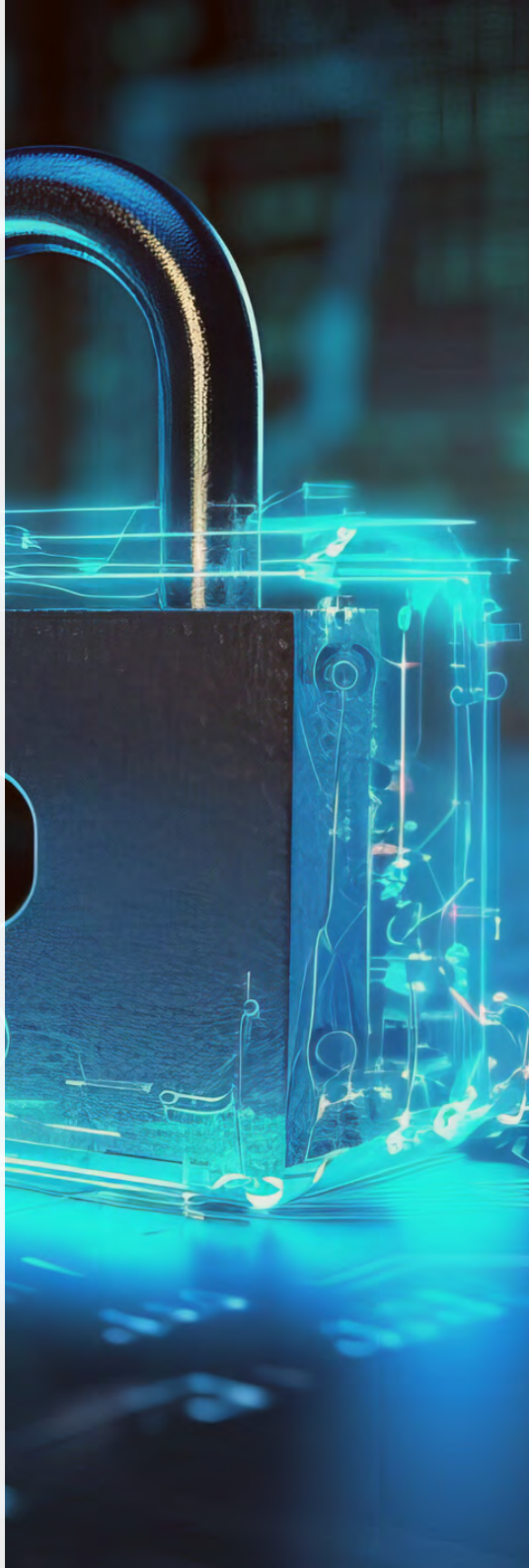
To rozwiązanie wymaga udostępnienia części wrażliwych informacji na temat infrastruktury organizacji zewnętrznej. Całość odbywa się oczywiście w oparciu o odpowiednie umowy i zastrzeżenia, niemniej są organizacje, które nie zaakceptują takiego rozwiązania.

## MODEL HYBRYDOWY

Trzecią drogą jest model hybrydowy – połączenie własnych kompetencji z zewnętrzną obsługą. Kiedy może być dobrym rozwiązaniem? Na przykład wtedy, gdy organizacja posiada wyspecjalizowany zespół, jednak nie jest on w stanie w pełni nadzorować bezpieczeństwa cyfrowego wszystkich jej zasobów.

Może to wynikać z tego, że organizacja skaluje swoją działalność, otwierając nowe biura czy filie, lub też zespół doświadczonych specjalistów nie jest skłonny do pracy w godzinach nocnych czy w weekendy. W takich sytuacjach może on stanowić CORE działania SOC, a zewnętrzny outsourcing staje się jego uzupełnieniem i tzw. trzecią zmianą, pracującą w godzinach niestandardowych.

Pozwala to zapewnić komfort pracy najbardziej doświadczonym jednostkom w SOC oraz budować stabilność zespołu nawet w czasach tak dużego zapotrzebowania na tę specjalizację. SOC Perceptus obsługuje klientów publicznych i prywatnych w obu opisanych wcześniej modelach. Działania naszego zespołu zapewniają opiekę nad siecią i infrastrukturą przez 24 h, 7 dni w tygodniu, 356 dni w roku.



# JAK ZEWNĘTRZNI SPECJALIŚCI MOGĄ POMÓC W ZABEZPIECZENIU TWOJEGO BIZNESU?

**Mirosław Szymczak**
Nomios Poland Sp. z o.o.

**Cyberzagrożenia są dziś codziennością. Nie wystarczy mieć tylko narzędzi do zabezpieczenia posiadanej infrastruktury. Kluczową rolę w tym wypadku odgrywają eksperci, którzy je obsługują. Wybór zewnętrznej firmy specjalizującej się w cyberbezpieczeństwie może pozytywnie wpłynąć na bezpieczeństwo, a także pozwoli zaoszczędzić środki na rozwój Twojej organizacji.**

Kluczem do zabezpieczenia Twojego biznesu jest nie tylko posiadanie odpowiednich narzędzi, ale przede wszystkim wykwalifikowanych specjalistów, którzy efektywnie z tych narzędzi korzystają. Inwestycja w zewnętrzną firmę pozwoli skupić się na Twojej głównej działalności, jednocześnie chroniąc Twoje cyfrowe aktywa.

## DLACZEGO FIRMY POWINNY ZDECYDOWAĆ SIĘ NA SKORZYSTANIE Z USŁUG "Z ZEWNĄTRZ"?

Kiedy mówimy o cyberbezpieczeństwie, wartość doświadczenia, specjalistycznej wiedzy oraz stałego dostępu do najnowszych informacji na temat zagrożeń jest nieoceniona. Wykorzystanie ekspertów z zewnątrz w dziedzinie cyberbezpieczeństwa oferuje wiele korzyści, które mogą znacząco wzmocnić zabezpieczenia każdej organizacji.

Poniżej, przygotowaliśmy listę korzyści, które naszym zdaniem związane są ze ścisłą współpracą oraz konsultacjami z ekspertami zewnętrznymi. Warto pamiętać, że każda firma lub organizacja mają inną specyfikę funkcjonowania i specjalizują się w innym sektorze, co przekłada się na rodzaje rozwiązań, jakie w ich przypadku sprawdzą się najlepiej.

**Głęboka specjalizacja** - eksperci z zewnątrz często specjalizują się w konkretnych obszarach cyberbezpieczeństwa, dzięki czemu mają unikalną wiedzę i doświadczenie, którym trudno jest dorównać wewnętrznym zespołom.

Zewnętrzne firmy specjalizujące się w obszarze cyberbezpieczeństwa **inwestują w najnowocześniejsze narzędzia i technologie**, które pomagają w wykrywaniu i reagowaniu na zagrożenia, dzięki czemu organizacje nie muszą inwestować w nie samodzielnie.

**Niższe koszty utrzymania** - utrzymanie wewnętrznego zespołu specjalistów od cyberbezpieczeństwa może być kosztowne, zwłaszcza jeśli weźmie się pod uwagę koszty rekrutacji, szkolenia i utrzymania takiego zespołu. Zatrudnienie ekspertów z zewnątrz pozwala na elastyczność kosztową, zachowanie ciągłości i dostosowanie zakresu usług do aktualnych potrzeb organizacji.

**Stałe szkolenia i aktualizacja wiedzy** - zewnętrzni specjaliści regularnie szkolą się i zdobywają nowe certyfikaty w dziedzinie cyberbezpieczeństwa, co pozwala im na bieżąco śledzić rozwijające się zagrożenia i odpowiednio na nie reagować.

**Obiektywność oceny stanu faktycznego i sytuacji** - eksperci oceniają systemy i praktyki organizacji z obiektywnego punktu widzenia, identyfikując potencjalne luki i słabości, które mogłyby zostać przeoczone przez wewnętrzny zespół.

W miarę wzrostu organizacji i jej potrzeb związanych z cyberbezpieczeństwem, zewnętrzni eksperci mogą dostosować swoje usługi, oferując dodatkowe wsparcie i zasoby, gdy są one potrzebne. **Ich elastyczność i skalowalność** to ogromna zaleta, tak by rozwiązania były aktualizowane i jednocześnie personalizowane do potrzeb i oczekiwań klientów w czasie rzeczywistym.

**Szybkie reagowanie i wysoka responsywność na incydenty** - dzięki stałemu monitorowaniu i specjalistycznemu doświadczeniu, zewnętrzni eksperci mogą szybko reagować na incydenty bezpieczeństwa, minimalizując potencjalne szkody dla organizacji.

Korzystanie z usług wyspecjalizowanych ekspertów z zewnątrz to inwestycja, która przynosi wiele korzyści. Nie tylko wzmacnia ona zabezpieczenia organizacji, ale także pozwala skoncentrować się na podstawowej działalności.

## CZYM JEST SOC?

Security Operations Center (SOC) to specjalistyczne centrum operacyjne poświęcone monitorowaniu, ocenie i reagowaniu na incydenty związane z bezpieczeństwem informatycznym. Celem SOC jest redukcja ryzyka powstania incydentu cybernetycznego oraz podnoszenie poziomu bezpieczeńs-


twa organizacji. W jego skład wchodzą wyspecjalizowani analitycy bezpieczeństwa i inżynierowie.

SOC w swojej strukturze działa w oparciu o trzy linie – L1, L2 oraz L3. Dzięki takiej organizacji dany alarm w infrastrukturze IT jest wstępnie analizowany oraz klasyfikowany przez analityków SOC (L1). Następnie, jeśli zachodzi konieczność alarm jest eskalowany w celu rozwiązania incydentu i stworzenia rekomendacji (L2). Finalnie, jeśli sytuacja tego wymaga wdrażana jest analiza wsteczna oraz analiza złośliwego oprogramowania (L3). W takim układzie każdy członek zespołu pełni określoną rolę w procesie wykrywania, analizy i reagowania na zagrożenia.

## NAJWAŻNIEJSZE FUNKCJE SOC

**Monitorowanie w czasie rzeczywistym** aktywności w sieci korporacyjnej, bazach danych oraz systemach i aplikacjach, aby na bieżąco wykrywać nieprawidłowości.

**Skuteczna analiza zagrożeń** - po wykryciu potencjalnego zagrożenia, zespół SOC dokładnie analizuje sytuację, a jeśli doszło do naruszenia bezpieczeństwa odpowiednio reaguje, aby zminimalizować szanse powtórnego incydentu.

**Reagowanie na incydenty** - w przypadku potwierdzenia naruszenia, SOC podejmuje działania mające na celu zahamowanie ataku i minimalizację szkód.

**Raportowanie i komunikacja** - SOC regularnie informuje zarząd firmy oraz odpowiednie zespoły IT o stanie bezpieczeństwa, potencjalnych za-

grożeniach oraz rekomendowanych działaniach.

**Udoskonalenie zabezpieczeń** - na podstawie zebranych danych i doświadczeń, SOC pomaga w ulepszaniu zabezpieczeń organizacji.

## JAKIE KORZYŚCI PRZYNOSI WDROŻENIE SOC?

Niezależnie od tego, czy firma zdecyduje się na własne SOC, czy też korzysta z usług zewnętrznego dostawcy, ważne jest, aby posiadała narzędzia i zasoby niezbędne do ochrony przed współczesnymi zagrożeniami.

**Ochrona 24/7**, ponieważ wiele cyberataków zachodzi poza standardowymi godzinami pracy. Dzięki SOC organizacje są chronione całą dobę.

Dodatkowo zespół SOC posiada **specjalistyczną wiedzę w zakresie najnowszych zagrożeń i technik obronnych.**

Dzięki skorzystaniu z zewnętrznego SOC organizacja może **skupić się na swojej podstawowej działalności** oraz relokować swój własny dział IT do innych zadań.

W przypadku incydentu, **natychmiastowa i skuteczna reakcja** jest kluczem do minimalizacji szkód. SOC zapewnia odpowiedź w czasie rzeczywistym.

## Z JAKICH ROZWIĄZAŃ Z ZAKRESU CYBERBEZPIECZEŃSTWA KORZYSTA SIĘ NAJCZĘŚCIEJ W RAMACH SOC?

**SIEM**

SIEM (Security Information and Event Management) to narzędzie, które zbiera, analizuje i interpretuje ogromne ilości danych z różnych źródeł w organizacji. Połączenie tego narzędzia z usługą SOC pozwala na głęboką analizę tych danych, umożliwiając szybkie wykrywanie i reagowanie na wszelkie zagrożenia cybernetyczne.

**EDR**

Endpoint Detection and Response (EDR) jest skoncentrowane na monitorowaniu i reagowaniu na zagrożenia dotyczące punktów końcowych, jak komputery czy serwery. EDR umożliwia analitykom SOC spojrzenie całościowo na infrastrukturę organizacji. Pozwala na lepsze wykrycie i zrozumienie wektorów ataków.

**SOAR**

Security Orchestration, Automation, and Response (SOAR) jest narzędziem pozwalającym zautoma-

tyzować część zadań w SOC. Umożliwia automatyczne reagowanie na różne typy zagrożeń, co znacząco przyspiesza czas reakcji i zmniejsza ryzyko błędów ludzkich.

## JAKIE KORZYŚCI NIESIE KORZYSTANIE Z ZEWNĘTRZNEGO SECURITY OPERATIONS CENTER?

**Zarządzanie usługami bezpieczeństwa**

Zewnętrzne SOC zapewnia pełne zarządzanie systemami bezpieczeństwa IT, co prowadzi do oszczędności kosztów związanych z budową i utrzymaniem własnej infrastruktury.

**Analiza incydentów**

Doświadczenie i wyspecjalizowane umiejętności zespołu SOC umożliwiają głęboką analizę wszelkich incydentów związanych z bezpieczeństwem. Nie można pozwolić sobie na wyłącznie powierzchowną analizę, która może okazać się niewystarczająca. Stąd niezwykle istotne, aby każde zdarzenie było sprawdzone i przeanalizowane z należytą starannością oraz dokładnością.

**Zmniejszenie kosztów utrzymania zespołu IT**

Outsourcing usług SOC pozwala na znaczące oszczędności w porównaniu z kosztami związanymi z budową i utrzymaniem własnego zespołu bezpieczeństwa dostoswanego do pracy ciągłej przez całą dobę i wszystkie dni w roku (24x7x365).

**Zmniejszenie liczby zadań własnego zespołu IT**

Korzystając z zewnętrznego SOC, wewnętrzny zespół IT może skupić się na innych priorytetowych zadaniach związanych bezpośrednio z prowadzonym rodzajem działalności.

**Podniesienie bezpieczeństwa danych i systemów**

Zewnętrzne SOC, działające w trybie ciągłym, zapewniają wysoki poziom monitorowania oraz reagowania na zagrożenia, co przekłada się na lepszą ochronę danych i systemów.

## NIE BĘDZIEMY PRZEKONYWAĆ, ŻE WARTO...

Inwestowanie w zewnętrznych ekspertów od cyberbezpieczeństwa to klucz do ochrony każ-

# Jak zewnętrzni specjaliści mogą pomóc w zabezpieczeniu Twojego biznesu?


dej organizacji w dzisiejszym świecie pełnym cyberzagrożeń.

Liczba zagrożeń stale rośnie i stają się one coraz groźniejsze dla ciągłości funkcjonowania podmiotów, a niektóre ze skutków cyberataków mogą być niemal nieodwracalne. Nomios, jako lider w rozwiązaniach cyberzabezpieczeń, dostarcza firmom nie tylko narzędzia, szereg usług szkoleniowych i wdrożeniowych ale także doświadczonych specjalistów gotowych pomóc w każdej sytuacji.

Czy taka inwestycja zwróci się w każdym przypadku? Najkrócej ujmując: tak. Dlaczego? Bo nawet rozmowa z ekspertem lub ekspertką w swojej dziedzinie, pozwala spojrzeć na cyberbezpieczeństwo z zupełnie innej perspektywy i dostarcza ogrom wartościowej wiedzy.

# PATRONAT
## SECURITY MAGAZINE

# DORA FORUM

## WDROŻENIE ROZPORZĄDZENIA DORA DLA PRAKTYKÓW!


**25-26 października w Warszawie odbędzie się DORA Forum – konferencja na temat rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego, czyli Digital Operational Resilience Act (DORA). Jeśli jesteś zainteresowany tematyką cyfrowej odporności operacyjnej, nie możesz przegapić tego wydarzenia!**

DORA Forum zapewni Ci wartościowe treści edukacyjne i stworzy przestrzeń, atmosferę sprzyjającą nawiązywaniu kontaktów biznesowych oraz wymianie poglądów z ekspertami, praktykami oraz przedstawicielami branż których dotyka regulacja. Będzie to idealna okazja do zdobycia praktycznej wiedzy, zdobycia cennych wskazówek o regulacji oraz do nawiązania nowych relacji w środowisku.

Celem DORA Forum jest nie tylko zapewnienie wartościowych treści edukacyjnych, ale w szczególności stworzenie platformy do wymiany doświadczeń, poglądów i ocen dotyczących regulacji oraz optymalnych strategii wdrożenia regulacji w organizacjach.
Agenda konferencji odzwierciedla 5 kluczowych filarów regulacji DORA. Podczas wystąpień, dyskusji na scenie, poświęconych takim tematom, jak zapewnienie cyberodporności organizacji, zarządzanie ryzykiem technologicznym, ryzyka łańcucha dostaw ICT, zarządzanie incydentami, współpraca i raportowanie oraz najważniejsze wyzwania spod znaku DORA, praktycy regulacji z sektora finansowego i ubezpieczeniowego podzielą się perspektywami, wyzwaniami i uwagami związanymi z wdrażaniem wymogów regulacji.
Będziemy mieli okazję gościć przedstawicieli Komisji Nadzoru Finansowego (KNF). To wyjątkowa możliwość zapoznania się z ich perspektywą i wymaganiami, wobec tego aktu w Polsce! Na scenie pojawią się również przedstawiciele rynku technologicznego, którzy zaprezentują innowacyjne rozwiązania oraz usługi wspierające spełnienie wymogów regulacji.

**Szczegółowe informacje oraz REJESTRACJA**

# PATRONI WYDANIA

NASK

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI
CBZC

**NASK** to Państwowy instytut Badawczy, którego misją jest poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności oraz bezpieczeństwa. Instytut prowadzi badania naukowe, prace rozwojowe, a także działalność operacyjną na rzecz bezpieczeństwa polskiej cywilnej cyberprzestrzeni. Ważnym elementem działalności NASK jest też edukacja użytkowników oraz promowanie koncepcji społeczeństwa informacyjnego, głównie w celu ochrony dzieci i młodzieży przed zagrożeniami, związanymi z użytkowaniem nowych technologii.

**Europejski Miesiąc Cyberbezpieczeństwa (ECSM)** to kampania organizowana przez agencję ENISA z inicjatywy Komisji Europejskiej. W tym roku skupia się na zagrożeniach, w których wykorzystywana jest socjotechnika. W Polsce koordynatorem kampanii jest NASK - PIB. Każda organizacja, która chce realizować misję ECSM może dołączyć do tej inicjatywy.

**Centralne Biuro Zwalczania Cyberprzestępczości** to jednostka Policji odpowiedzialna za rozpoznawanie, zapobieganie i zwalczanie cyberprzestępczości. Jednostką kierujr komendant Centralnego Biura Zwalczania Cyberprzestępczości, jako organ podległy komendantowi głównemu Policji. Funkcjonariuszom CBZC przysługuje w pełni możliwość prowadzenia działań operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz administracyjno-porządkowych, wynikających z ustawy o Policji.

# EKSPERCI WYDANIA

**KLAUDIA JĘDRZEJCZAK-KRASIEŃKO**
IT Project Manager
Sygnisoft SA

IT Project Manager w Sygnisoft SA, renomowanym dostawcy oprogramowania. Absolwentka Szkoły Głównej Handlowej, gdzie uzyskała tytuł magistra zarządzania. Prowadzi projekty informatyczne związane z branżą FMCG, turystyczną i eventową. Interesuje się marketingiem internetowym. Prywatnie pasjonatka turystyki górskiej i pieszych wędrówek

**KAROL GOLISZEWSKI**
Consulting Engineer
Grandmetric

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

**TOMASZ KOWALSKI**
CEO i współzałożyciel
Secfense

CEO i współzałożyciel firmy z branży cybersecurity Secfense. Posiada ponad 20-letnie doświadczenie w sprzedaży technologii IT, brał udział w setkach wdrożeń sprzętu i oprogramowania w dużych i średnich firmach z sektora finansowego, telekomunikacyjnego, przemysłowego i wojskowego.

**ADRIAN SROKA**
Security Architect

Architekt bezpieczeństwa i konsultant IT. Z pasją tworzy nowe rozwiązania oraz udoskonala istniejące, podnosząc jednocześnie ich techniczną, jak i funkcjonalną wartość. W pracy stosuje podejście oparte na współpracy i wiedzy. Zorientowany na zbliżanie do siebie bezpieczeństwa i dewelopmentu.

# EKSPERCI WYDANIA

**RAFAŁ STĘPNIEWSKI**
redaktor naczelny
**Security Magazine**

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

**MARCIN ZAGÓRSKI**
podkomisarz
Centralne Biuro Zwalczania Cyberprzestępczości

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.

**KAROL WODZICKI**
CISSP, Senior Security Architect
**Concept Data**

Architekt rozwiązań cyberbezpieczeństwa z ponad 20-letnim doświadczeniem. Jego celem jest szerzenie świadomości o zagrożeniach w cyfrowym świecie. Prywatnie „lata bokiem”, czyli driftuje.

**MICHAŁ KUDELA**
PAM Team Leader
**Concept Data**

Ma 8-letnie doświadczenie związane z systemami klasy IAM oraz PIM/PAM. W firmie kieruje zespołem zajmującym się wdrożeniami systemów klasy Identity Security. Odpowiada za realizacje projektów z zakresu zarządzania kontami i dostępem uprzywilejowanym oraz przeprowadzanie audytów identyfikacji oraz rekomendacji dotyczących ochrony przed kradzieżą tożsamości.

# EKSPERCI WYDANIA

**MICHAŁ ZALEWSKI**
inżynier
**Barracuda Networks**

Starszy inżynier bezpieczeństwa, trener techniczny zaawansowanych szkoleń z zakresu cyberbezpieczeństwa, tester penetracyjny ratujący klientów przed tragicznymi w skutkach lukami w firmowej infrastrukturze. Prelegent krajowych i zagranicznych konferencji branżowych. Wspiera klientów Europy Środkowo-Wschodniej w ich codziennej pracy z rozwiązaniami Barracuda Networks.

**PIOTR ROZMIAREK**
Account Manager
Marken Oficjalny dystrybutor
Bitdefender w Polsce

Magister filologii polskiej o specjalizacji nauczycielskiej oraz językoznawczo-redaktorskiej. Specjalista z zakresu cyberbezpieczeństwa, językoznawstwa, literaturoznawstwa oraz branży OZE. W wolnych chwilach sięga po książkę, gitarę lub teleskop.

**ŁUKASZ ZAJDEL**
Dyrektor Sprzedaży
**Perceptus Sp z o. o.**

Dyrektor Sprzedaży w Perceptus Sp z o. o. Od roku 2016 związany jest z branżą cybersecurity. Z sukcesem realizuje komplementarne projekty i wdrożenia rozwiązań związanych z bezpieczeństwem IT, zarówno dla klientów komercyjnych jak i publicznych.

**MIROSŁAW SZYMCZAK**
Sales Executive
**Nomios Poland Sp. z o.o.**

Ponad 20 lat doświadczenia w branży IT, między innymi w Cisco Systems, FireEye i Microsoft. W Nomios zajmuje stanowisko Sales Executive na rynkach europejskich, gdzie sprzedaż usług cybersecurity cieszy się dużym powodzeniem. Pasjonat chmury publicznej, w tym jej aspektami prawnymi.

# DOŁĄCZ DO GRONA EKSPERTÓW "SECURITY MAGAZINE"

# ZOBACZ WYDANIA

Wydanie 1/2022
POBIERZ


Wydanie 2/2022
POBIERZ


Wydanie 3/2022
POBIERZ


Wydanie 4/2022
POBIERZ


Wydanie 5/2022
POBIERZ


Wydanie 6/2022
POBIERZ


Wydanie 7/2022
POBIERZ


Wydanie 8/2022
POBIERZ


Wydanie 9/2022
POBIERZ


Wydanie 1(10)/2023
POBIERZ


Wydanie 2(11)/2023
POBIERZ


Wydanie 3(12)/2023
POBIERZ


Wydanie 4(13)/2023
POBIERZ


Wydanie 5(14)/2023
POBIERZ


Wydanie 6(15)/2023
POBIERZ


Wydanie 7(16)/2023
POBIERZ


Wydanie 8(17)/2023
POBIERZ


Wydanie 9(18)/2023
POBIERZ

# WYDAWCA

**Wydawca:**

**Rzetelna Grupa sp. z o.o.**

ul. Nowogrodzka 42 lok. 12
00-695 Warszawa

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

**Redaktor Naczelny: Rafał Stępniewski**

**Redaktor prowadząca: Monika Świetlińska**

Redakcja: Damian Jemioło, Joanna Gościńska, Katarzyna Leszczak

Projekt, skład i korekta: Monika Świetlińska



**Współpraca i kontakt: redakcja@securitymagazine.pl**


SECURITYMAGAZINE.PL