trzeci sektor
Nr 59–60 (3–4/2022) www.kwartalnik3sektor.pl

[ARTYKUŁ RECENZOWANY]

Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych

Phishing and related social engineering attacks as a threat to non-governmental organizations

DOI: 10.26368/17332265-59/60-3/4-2022-5

JULIA JANCELEWICZ
Santander Bank Polska
jjancelewicz@proton.me

SŁOWA KLUCZOWE
cyberbezpieczeństwo, phishing, socjotechnika, organizacje pozarządowe

KEYWORDS
cybersecurity, phishing, social engineering, non-governmental organizations

ABSTRAKT

W artykule opisano kluczowe zagadnienia dotyczące phishingu i pokrewnych ataków socjotechnicznych. Na podstawie teoretycznego wprowadzenia i praktycznych przykładów ze świata zestawiono najważniejsze informacje na temat tego zagrożenia cybernetycznego. Celem opracowania jest przedstawienie phishingu jako poważnego zagrożenia dla organizacji pozarządowych i zasugerowanie możliwych środków zapobiegawczych pozwalających uchronić się przed atakami. Zawarte w tekście informacje mają także ułatwić rozpoznawanie takich ataków na podstawie określonych charakterystyk. Ujęto również kluczowe elementy obrony przed tego typu atakami i dobre praktyki pomagające zwiększyć cyberbezpieczeństwo jednostki. Zaprezentowane modele uwzględniają rozwiązania zarówno organizacyjne, jak i systemowe, które mogą pozwolić na zatrzymanie ataku lub ograniczenie jego skutków.

ABSTRACT

The article describes the key issues regarding phishing and related social engineering attacks. Based on a theoretical introduction and practical examples from around the world, the most important information about this cyber threat is summarized. The aim of the study is to depict phishing as a serious threat to non-governmental organizations and to suggest possible preventive measures to protect against attacks. The information about specific characteristics of such attacks, presented in the text, may be helpful in identifying them. Apart from that, the key elements of defense against these types of attacks, as well as good practices that help to increase the cyber security of the individual are described. The presented models take into consideration both organizational and systemic solutions that can stop the attack or limit its effects.

Wraz z postępującą cyfryzacją tematyka cyberbezpieczeństwa staje się coraz ważniejsza. Powszechne wykorzystywanie technologii sprawia, że ataki cybernetyczne mogą dotknąć każdego. Chronienie danych, zarówno

własnych, jak i osób powiązanych z organizacją, jest konieczne, a zapewnianie bezpieczeństwa przetwarzanych informacji obejmuje obecnie także obszar cyfrowy. Szczególnie powszechnym i wartym poznania zagrożeniem jest phishing, który dla atakujących wiąże się z niskim kosztem i łatwością przeprowadzenia, a dla ofiar – z dużymi stratami. Motywy oszustów są zróżnicowane, obiektem zainteresowania może zaś być dowolny użytkownik. Organizacje pozarządowe są wyjątkowym celem ze względu na charakter działalności, której zakłócanie może być w interesie grup przestępczych lub nieprzychylnych rządów. Nie mamy tu do czynienia z jednostkowymi przykładami, lecz z powszechnym zagrożeniem, które choć nie zawsze wykryte i zidentyfikowane, dociera do wielu potencjalnych ofiar. W niniejszym artykule przybliżono tematykę socjotechnicznych ataków cyfrowych, przedstawiono również dobre praktyki i podstawy obrony przed tego typu atakami. Ze względu na rozległość zagadnienia tekst ma charakter wprowadzenia w problematykę ataków socjotechnicznych i zwrócenia uwagi na potrzebę podjęcia działań mających na celu zabezpieczenie organizacji przed zagrożeniami tego typu.

Czym jest phishing?

Phishing przez Komisję Nadzoru Finansowego jest definiowany jako metoda oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (na przykład danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań (Górnisiewicz i in. 2014). Można również określić je mianem ataków socjotechnicznych w cyberprzestrzeni. W tej samej publikacji Komisji Nadzoru Finansowego socjotechnika (także inżynieria społeczna) definiowana jest jako stosowanie różnorodnych środków psychologicznych i metod manipulacji w celu wyłudzenia od ofiary określonych informacji lub nakłonienia jej do realizacji określonych działań. „Phishing" jest jednak bardzo ogólnym pojęciem, które wymaga dalszej klasyfikacji, umożliwiającej precyzyjne opisanie przeprowadzanego ataku. Cechy, na podstawie których można dokonać podziału, to między innymi forma komunikacji z ofiarą, grupa docelowa ataku oraz typ złośliwej zawartości. Przykładowa klasyfikacja ze względu na wymienione czynniki:

- Forma komunikacji z ofiarą – oszuści wykorzystują wszelkie formy, platformy lub komunikatory, które umożliwiają kontakt z grupą docelową. Do najczęstszych kanałów dostarczenia phishingu należą komunikatory (WhatsApp, Messenger), platformy sprzedażowe (OLX, Allegro, Vinted), media społecznościowe (Facebook, LinkedIn) oraz wiadomości e-mail. Niektóre

ataki zostały nazwane odpowiednio ze względu na sposób dostarczenia oszustwa: „smishing" (oszustwa wysyłane za pośrednictwem wiadomości esemesowych) lub „vishing" (manipulacja za pośrednictwem telefonu).

- Grupa docelowa ataku – phishing może być kierowany zarówno do osób prywatnych, jak i do firm oraz organizacji. Niektóre ataki są dostarczane do szerokiego, dobranego losowo grona odbiorców, co sprawia, że nie są dostosowane do konkretnej ofiary. Ich przeciwieństwem jest „spear-phishing", który charakteryzuje precyzyjny wybór ofiary i przygotowanie ataku dopasowanego do odbiorcy. Jeszcze bardziej sprecyzowaną grupą docelową cechuje się „whaling", który tworzony jest z myślą o atakowaniu osób na wysokich stanowiskach, posiadających wpływy i podejmujących kluczowe decyzje.
- Złośliwa zawartość – ataki phishingowe można również podzielić na zawierające odnośnik do strony, ze szkodliwymi załącznikami oraz opierające się jedynie na manipulacji i wyłudzaniu informacji w bezpośredniej rozmowie lub za pośrednictwem wiadomości. Ataki mogą mieć na celu wyłudzenie danych płatniczych, osobowych lub do logowania (na przykład do bankowości elektronicznej), co najczęściej dzieje się w wypadku wiadomości zawierających odnośniki w treści wiadomości. Wiadomości zawierające pliki zwykle zachęcają do ich uruchomienia i wykonania kroków potrzebnych do instalacji programu, który docelowo może umożliwić atakującym dostęp do infrastruktury IT organizacji.

Mimo wskazanych różnic między atakami można wskazać łączące je najczęstsze charakterystyki. W badaniu realizowanym przez specjalistki z National Institute of Standards and Technology wyróżniono pięć podstawowych grup znaków szczególnych phishingu. Są to: błędy – w tym gramatyczne i literówki, elementy techniczne – odnośniki, pliki i właściwości wiadomości, wygląd wiadomości – na przykład jej układ czy zawarte logo, ikony, język i treść – między innymi presja czasu, ogólne sformułowania; powszechne taktyki – czyli znane scenariusze (Steves *et al.* 2019). Na podstawie obserwacji i własnych analiz postanowiono wyróżnić sześć szczególnie powszechnych charakterystyk, które są uniwersalne dla różnych sposobów komunikacji atakującego z ofiarą:

- Oddziaływanie na emocje – podstawą manipulacji jest wpływanie na ofiarę za pomocą wzbudzania wstydu lub strachu, ponieważ zastraszona osoba może obawiać się zwrócić po pomoc.
- Presja czasu – zachęcanie do nadzwyczajnego pośpiechu i budowanie scenariusza wymuszającego szybkie działanie to częsty zabieg w phishingu, który ma nakłonić ofiarę do podejmowania nieprzemyślanych decyzji. Ponadto uniemożliwia to skonsultowanie działań z zaufaną osobą.

- Atrakcyjne oferty („zbyt dobre, by były prawdziwe") – budowanie poczucia wyjątkowości w ofierze i informacje o niespotykanych nagrodach lub odziedziczonych fortunach to jedne z wielu scenariuszy, które mają uśpić czujność ofiary.
- Podszywanie się pod autorytet lub zaufaną jednostkę – ataki ze scenariuszami takimi jak oferta wysokiej wpłaty na rzecz fundacji lub informacja o podejrzanych działaniach na koncie ofiary, opierają się zwykle na wiarygodnym podszyciu się pod policję, bank lub przełożonego w organizacji.
- Niestandardowa lub niepokojąca treść – jeżeli forma lub treść komunikacji odbiega od normy, warto zweryfikować, czy na pewno wiadomość nie jest phishingiem. Wiadomości od najważniejszych instytucji i dużych firm nie powinny także zawierać błędów gramatycznych lub ortograficznych.
- Podejrzane załączniki bądź odnośniki – kluczowy element phishingu to szkodliwy odnośnik do strony internetowej lub plik. Jeżeli taka zawartość nie jest spodziewana, a w połączeniu z treścią wiadomości wygląda niepokojąco, należy traktować taką wiadomość z ostrożnością.

Poznanie rodzajów i charakterystyk ataków phishingowych jest pierwszym krokiem do skutecznej obrony przed tym zagrożeniem. Świadomość powszechności takich ataków powinna prowadzić do wniosku, że zagrożenie może dotknąć każdego i nie należy go lekceważyć.

Phishing w szerszej perspektywie

Phishing występuje zarówno jako pierwszy etap rozbudowanych ataków, jak i w elementarnych scenariuszach pozwalających atakującym błyskawicznie osiągnąć cele. Profil, metodyka i scenariusze ataków phishingowych zmieniają się wraz z okolicznościami i sytuacją na świecie. Na tematykę ataków może mieć wpływ sytuacja polityczna, ważne wydarzenia (na przykład sportowe) czy choćby pandemia. Zmiany scenariuszy mogą się wiązać również z porą roku i towarzyszącymi zdarzeniami. Przykładowo wzmożone zamówienia i zakupy realizowane przez Internet w okresie przedświątecznym sprzyjają tworzeniu ataków podszywających się pod firmy kurierskie, sklepy oraz portale ogłoszeniowe. Elastyczność formy, ciągły rozwój i możliwość szybkiej adaptacji do zmiennych warunków lub stosowanych zabezpieczeń to główne cechy wpływające na skuteczność phishingu.

Innymi cechami, które decydują o jego powszechności względem innych ataków, są łatwość stworzenia i przeprowadzenia oraz niski koszt. Oszuści działają często w zorganizowanych, wielopoziomowych grupach przestępczych, co pozwala dzielić zadania między członków i przeprowadzać działania na większą skalę (https://phishingtackle.com). Umożliwia to także przeprowadzanie innych działań i podejmowanie bardziej zaawansowanych

dalszych kroków po oszukaniu ofiary, zwiększających zyski z całego ataku. Z perspektywy organizacji pozarządowych istotna jest świadomość motywów atakujących. Główne cele atakujących to:

- zysk finansowy,
- kradzież danych lub tożsamości,
- działania będące elementem cyberwojny lub motywowane politycznie,
- możliwość dalszej propagacji złośliwego oprogramowania lub wyłudzenie kolejnych danych.

Atakujący mogą próbować utrudnić lub uniemożliwić działanie organizacji. Przykładem ataku, który jest jedynie inicjowany przez phishing, może być ransomware. Jest to złośliwe oprogramowanie, które blokuje użytkownikom dostęp do ich systemów lub plików osobistych (na przykład szyfrując je), a następnie żąda uiszczenia opłaty w zamian za jego przywrócenie (https://pl.malwarebytes.com). Jednym ze sposobów dostarczenia takiego oprogramowania do ofiary i przekonania jej do uruchomienia go jest właśnie mail phishingowy. Zaszyfrowanie danych lub nawet docelowo zupełne ich usunięcie, a także groźby upublicznienia uzyskanych w trakcie ataku informacji, to skuteczne sposoby na wstrzymanie działania organizacji oraz wyłudzenie pieniędzy (https://phishingtackle.com). Są to ataki przeprowadzane nie tylko w ramach spear phishingu, ale także masowo, bazując na uniwersalnych scenariuszach. Każdy może zostać celem ataku ransomware, a umiejętność rozpoznawania phishingu udaremnia plan atakujących na bardzo wczesnym etapie i jest wymieniana jako pierwszy sposób zapobiegania takim atakom na stronie Phishing Tackle.

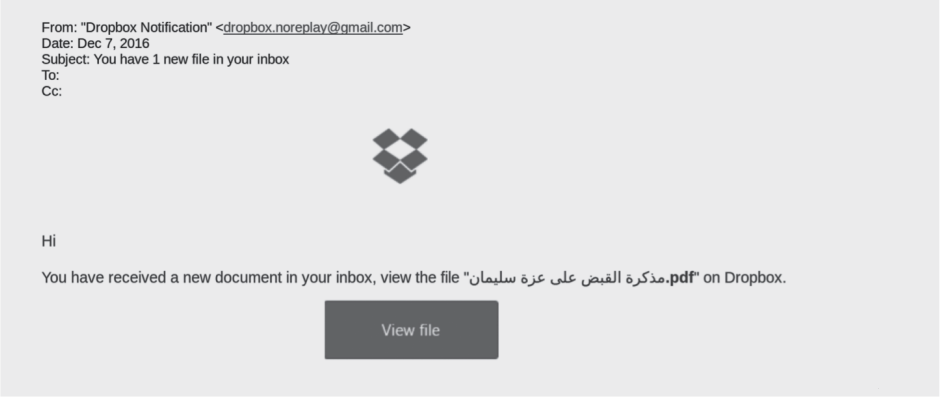
Przykładowe ataki

Ze względu na charakter działalności organizacjom pozarządowym grożą ataki motywowane politycznie – szczególnie w wypadku działalności humanitarnej i związanej z prawami człowieka oraz z praworządnością. Phishing może także okazać się niebezpiecznym narzędziem w rękach rządów, nie tylko powszechnie uważanych za niedemokratyczne, choćby w wypadku działań niezgodnych z interesami obecnej władzy. W ramach zobrazowania zagrożenia poniżej zostaną przedstawione przykładowe potwierdzone ataki, których konkretnym celem były organizacje pozarządowe.

Rzetelnie przeanalizowanym i udokumentowanym przykładem ataku uderzającego w organizacje pozarządowe jest kampania „Nile Phish". Został on przeprowadzony w Egipcie na przełomie 2016 i 2017 roku, a śledztwo w tej sprawie przeprowadziło Citizen Lab (https://citizenlab.ca). Doniesienia o tym, że źródło ataków to rząd Egiptu, wynikają z zaobserwowanej przez badaczy obszernej wiedzy atakującego na temat egipskich organizacji pozarządowych

oraz czasowej korelacji phishingu z działaniami rządu (między innymi aresztowaniami działaczy, którzy później byli wprost wymieniani w wiadomości phishingowych). Tłem wydarzeń było ograniczanie niesprzyjających rządowi prodemokratycznych działań organizacji pozarządowych, oficjalnie ze względu na podejrzenia o nielegalnej działalności i zagranicznym finansowaniu. Wiązało się to z aresztowaniami, zakazami podróży i innymi sankcjami prawnymi mającymi na celu utrudnienie lub uniemożliwienie im działania. Ponadto ustalono, że siedem organizacji pozarządowych w Egipcie, które zostały dotknięte wymienionymi sankcjami, było także celem ataków phishingowych. Scenariusz jednego z nich dotyczył aresztowania prawniczki i dyrektorki Centrum Wsparcia Prawnego dla kobiet Azzy Soliman. W wiadomości e-mail (ilustracja 1) znajdował się odnośnik do fałszywej strony usługi Dropbox, rzekomo zawierającej nakaz aresztowania działaczki. W rzeczywistości strona wyłudzała poświadczenia do konta w tej usłudze. Ataki były dokładnie zaprojektowane pod kątem dopasowania do adresatów, odpowiedniego czasu dostarczenia i działania na emocje aktywistów.

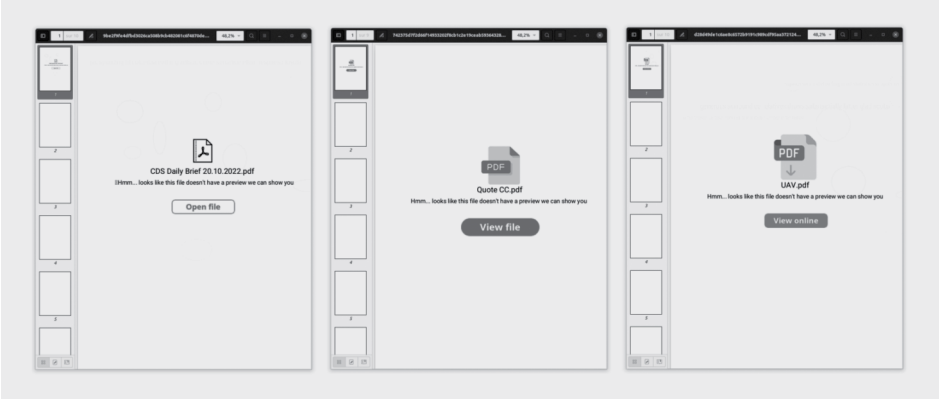
Ilustracja 1. Mail phishingowy z odnośnikiem rzekomo prowadzącym do pliku PDF zawierającego nakaz aresztowania Azzy Soliman. Źródło: https://citizenlab.ca.



Bliższym i bardziej aktualnym przykładem ataków, których celem są organizacje pozarządowe, jest działalność grup cyberprzestępczych powiązanych z Rosją lub wspierających jej działania. Według doniesień Threat Analysis Group, zespołu analizującego zagrożenia w firmie Google, rosyjska grupa Coldriver atakowała za pomocą phishingu między innymi organizacje pozarządowe związane z pomocą Ukrainie (https://blog.google). Dane z marca 2022 roku informują o próbach wyłudzenia poświadczeń między innymi do poczty elektronicznej oraz usług hostingu plików. Informacje

zebrane i opublikowane przez Sekoia.io w grudniu 2022 roku prezentują jednak dokładniejszy obraz działań tej grupy wraz z przykładowymi atakami i ich grupami docelowymi (https://blog.sekoia.io). Z dużą dozą pewności analitycy przypisują im ataki między innymi na polskiego dostawcę artykułów zbrojeniowych UMO oraz organizacje pozarządowe w Europie i Stanach Zjednoczonych. Ataki miały zapewne na celu utrudnienie pomocy humanitarnej oraz prawnej i naruszenie łańcucha dostaw wsparcia militarnego dla Ukrainy. Phishing był przeprowadzany przez pliki PDF dostarczone za pośrednictwem wiadomości e-mail, które zawierały w sobie odnośnik do strony wyłudzającej dane. Atakujący usiłował przekonać potencjalną ofiarę do przejścia na stronę za pomocą upozorowanego błędu w wyświetlaniu załącznika (ilustracja 2).

Ilustracja 2. Przykłady plików PDF wykorzystywanych w atakach przeprowadzanych przez grupę Coldriver. Źródło: https://blog.sekoia.io.



Przedstawione zostały jedynie pojedyncze przykłady przeprowadzanych ataków na organizacje pozarządowe, które nie prezentują wszystkich możliwych scenariuszy phishingu. Ponadto ataki socjotechniczne często nie są identyfikowane, zgłaszane lub analizowane przez specjalistów z zakresu cyberbezpieczeństwa, co skutkuje ograniczonym wyborem rzetelnie omówionych przykładów. Warto pamiętać, że ataki są skuteczne nie tylko ze względu na precyzyjne dopasowanie do odbiorcy. Nie należy lekceważyć zagrożenia, jakie niosą ze sobą także masowo rozsyłane kampanie.

Obrona przed phishingiem

Dynamiczny rozwój zagrożenia, jakim jest phishing, oraz jego powszechność sprawiają, że wdrożenie ochrony i działania prewencyjne są konieczne w każdej organizacji. Nie ma jednego prostego rozwiązania, które uchroni

przed tego typu atakami. Implementacja każdej zmiany związanej z zabezpieczeniami to działanie warte podjęcia.

Fiona Carroll, John Ayooluwa Adejobi i Reza Montasari (2022) w publikacji dotyczącej wykrywania phishingu oraz czynników wpływających na powodzenie ataków uznają efektywne działania szkoleniowe oraz rozwiązania prewencyjne dostarczane przez twórców systemów za kluczowe w obronie przed tego typu atakami. Uczestnicy przeprowadzanych przez nich badań również wskazywali potrzebę lepszej edukacji i szerzenia wiedzy na temat phishingu, a także skuteczniejszej detekcji szkodliwych treści przez platformy oferujące usługi poczty elektronicznej. W związku z tym uznaje się, że zwiększanie świadomości oraz szkolenie to podstawowy element obrony przed phishingiem i poprawy cyberbezpieczeństwa w organizacjach.

Poza wiedzą z zakresu bezpieczeństwa w sieci istotne jest także rozwijanie krytycznego myślenia oraz weryfikowanie informacji, z którymi ma się styczność. Samodzielne pozyskiwanie wiedzy z zaufanych źródeł należy do fundamentalnych umiejętności potrzebnych do skutecznej obrony przed phishingiem. Poza ogólnymi stronami informacyjnymi warto także obserwować portale publikujące aktualne wiadomości ze świata cyberbezpieczeństwa, takie jak Niebezpiecznik (niebezpiecznik.pl), Sekurak (sekurak.pl) i Zaufana Trzecia Strona (zaufanatrzeciastrona.pl).

Poza aktywnymi działaniami na rzecz edukowania pracowników oraz działaczy istotne jest także budowanie w organizacji zaufania i przejrzystości. Przestrzeń wolna od oceniania i piętnowania pozwala na swobodną komunikację czy konsultację z innymi. Zasięgnięcie opinii osoby bardziej doświadczonej w zakresie cyberbezpieczeństwa w wypadku wątpliwości dotyczących otrzymanej wiadomości może uchronić przed pochopną decyzją, która skutkowałaby powiedzeniem się ataku.

Nieodłącznym elementem obrony przed phishingiem są rozwiązania systemowe oraz dobre praktyki w zarządzaniu infrastrukturą teleinformatyczną w organizacji. Jak wskazują Yumi E. Suzuki i Sergio A. Salinas Monroy (2021) w publikacji dotyczącej prewencji ataków tego typu, tak zmienne zagrożenie wymaga holistycznej i wielowarstwowej obrony. Wymieniono pięć fundamentalnych etapów oraz ich części składowe, które mają na celu prewencję ataków oraz ograniczanie ich skutków. Są to w kolejności:

- zwiększenie koniecznego wkładu pracy atakującego w przygotowanie i przeprowadzenie ataku,
- podkreślenie odpowiedzialności użytkownika za podejmowane działania,
- zwiększenie prawdopodobieństwa wykrycia ataku,
- ograniczenie przestępcom możliwości dostępu do danych wrażliwych,
- próba uniknięcia takich ataków w przyszłości.

Dobre praktyki oraz rozwiązania pozwalające wykrywać i przerywać ataki phishingowe oraz zapobiegać im to między innymi korzystanie z systemu antywirusowego, rozwiązań poczty elektronicznej oferujących skuteczne filtry antyphishingowe oraz legalnego aktualnego oprogramowania od oficjalnych dostawców. Ponadto niezbędne może okazać się wdrożenie monitorowania cyberbezpieczeństwa w organizacji oraz stosownych procedur reagowania na incydenty bądź pojawiające się zagrożenia. Za jedne z najskuteczniejszych rozwiązań chroniących przed phishingiem uznawane jest wykorzystywanie bezpiecznej formy uwierzytelniania oraz autoryzacji, jaką daje dwuskładnikowe uwierzytelnianie 2FA (*2-factor authentication*). Może się ona odbywać za pomocą aplikacji generującej jednorazowe kody weryfikacyjne lub za pomocą kluczy fizycznych (na przykład marki Yubikey). Cybersecurity and Infromation Security Agency wymienia wdrożenie tego mechanizmu jako jeden z trzech najważniejszych działań, które należy podjąć najszybciej, tuż obok tworzenia kopii zapasowych danych i wdrożenia zarządzania aktualizacjami (https://www.cisa.gov).

Po zaimplementowaniu zabezpieczeń i przeprowadzeniu szkoleń warto weryfikować przygotowanie organizacji na atak. Audytowanie oraz testy phishingowe to integralna część zabezpieczania jednostki, która pozwala ocenić rezultaty wprowadzonych zmian i określić przestrzenie wymagające poprawy.

***

Phishing, cyfrowa odmiana socjotechniki, to nieustannie rozwijające się zagrożenie, które może dotknąć każdą firmę, organizację czy osobę prywatną. Jest to łatwy w stworzeniu, dostosowaniu i przeprowadzeniu atak, który zawdzięcza swoją skuteczność różnorodnym scenariuszom oraz oddziaływaniu na emocje potencjalnych ofiar. Jak pokazują przytoczone przykłady, organizacje pozarządowe są zagrożone phishingiem szczególnie wtedy, gdy realizują działania z zakresu aktywizmu politycznego, pomocy humanitarnej czy prawnej. Umiejętność rozpoznawania go na podstawie kluczowych charakterystyk oraz znajomość najnowszych ataków umożliwiają świadome podejmowanie decyzji w wypadku wątpliwości dotyczących bezpieczeństwa otrzymanej wiadomości. Warto podkreślić, że wdrożenie nawet minimalnych środków zabezpieczających organizację przed phishingiem może uchronić chociażby przed masowo rozsyłanymi wiadomościami, które są już znane i skutecznie wykrywane przez dostępne na rynku systemy antywirusowe. Implementacja rozwiązań zwiększających cyberbezpieczeństwo może opierać się nawet na darmowych rozwiązaniach niewymagających specjalistycznej wiedzy do ich stosowania. Najistotniejszym działaniem,

które, moim zdaniem, należy podjąć, jest efektywna edukacja użytkowników. Jeżeli wszystkie organizacyjne lub systemowe zabezpieczenia zawiodą, ostateczna ocena i decyzja należą do człowieka.

BIBLIOGRAFIA

Carroll, Fiona, Adejobi, John Ayooluwa. Montasari, Reza. 2022. How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society. *SN Computer Science*, 3, 170, https://doi.org/10.1007/s42979-022-01069-1 [dostęp: 20 grudnia 2022 roku].

Cyber Essentials, https://www.cisa.gov/cyber-essentials [dostęp: 20 grudnia 2022 roku].

Górnisiewicz, Mateusz, Obczyński, Radosław, Pstruś, Mariusz. 2014. *Bezpieczeństwo finansowe w bankowości elektronicznej - przestępstwa finansowe związane z bankowością elektroniczną*. Warszawa: Komisja Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp_finansowe_39005.pdf [dostęp: 20 grudnia 2022 roku].

Leonard, Billy. 2022. *Tracking cyber activity in Eastern Europe*, Threat Analysis Group, https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/ [dostęp: 20 grudnia 2022 roku].

Scott-Railton, John, Marczak, Bill, Raoof, Ramy, Maynier, Etienne. 2017. *Nile Phish; Large-Scale Phishing Campaign Targeting Egyptian Civil Society*, https://citizenlab.ca/2017/02/nilephish-report/ [dostęp: 20 grudnia 2022 roku].

Steves, Michelle P., Greene, Kristen K., Theofanos Mary F. 2019. *A phish scale: rating human phishing message detection difficulty*. Workshop on usable security (USEC).

Suzuki, Yumi E., Monroy, Sergio A. Salinas. 2022. Prevention and mitigation measures against phishing emails: a sequential schema model. *Security Journal*, 35, 1162-1182, https://doi.org/10.1057/s41284-021-00318-x [dostęp: 20 grudnia 2022 roku].

Threat & Detection Research Team. 2022. *Calisto show interests into entities involved in Ukraine war support*, https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/ [dostęp: 20 grudnia 2022 roku].

https://pl.malwarebytes.com/ransomware/ [dostęp: 20 grudnia 2022 roku].

https://niebezpiecznik.pl/ [dostęp: 20 grudnia 2022 roku].

https://phishingtackle.com/cyber-threat-actors/ [dostęp: 20 grudnia 2022 roku].

https://phishingtackle.com/ransomware/ [dostęp: 20 grudnia 2022 roku].

https://sekurak.pl/ [dostęp: 20 grudnia 2022 roku].

https://zaufanatrzeciastrona.pl/ [dostęp: 20 grudnia 2022 roku].