Rocznik Filozoficzny Ignatianum
The Ignatianum Philosophical Yearbook
Vol. 30, No. 3 (2024) s. 481–496
PL ISSN 2300–1402
DOI: 10.35765/rfi.2024.3003.25

Tomasz Śmigla
ORCID: 0009-0002-2005-333X
Uniwersytet Ignatianum w Krakowie

Kultura bezpieczeństwa w środowiskach firmowych w świetle nowoczesnych metod edukacji pracowniczej

Security culture in corporate environments in the context of modern employee education methods

Abstrakt

Nowoczesne przedsiębiorstwa są bytami w szczególny sposób narażonymi na cyberzagrożenia powiązane z *metodami* inżynierii społecznej, szeroko wykorzystywanymi przez cyberkryminalistów. Dziś środowiska firmowe muszą niemalże na co dzień mierzyć się z próbami kradzieży danych opartymi na wielu pochodnych współczesnych odmian phishingu, a jednym z głównych sposobów walki z tego rodzaju zagrożeniami pozostaje w dalszym ciągu edukacja pracownicza, która przyjmować może różne formy. Człowiek z reguły określany jest jako najsłabszy element „łańcucha bezpieczeństwa" danego poprawnie skonfigurowanego systemu informatycznego. Ten stan rzeczy biorą pod uwagę zarówno spółki samodzielnie przygotowujące programy edukacyjne i szkolenia dla swoich pracowników, jak i te, które przeprowadzanie tego rodzaju działań zlecają firmom zewnętrznym. Skuteczne kreowanie tzw. kultury bezpieczeństwa danej korporacji jest zadaniem niezwykle odpowiedzialnym, a przy tym wysoce nietrywialnym, a temat ten stosunkowo rzadko poruszany jest w literaturze

przedmiotu. Ciągła rewizja środków i metod prowadzenia programowych szkoleń i symulacji oraz zarządzanie działaniami przyczyniającymi się do współtworzenia zdrowego środowiska firmowego w zadowalającym stopniu odpornego na zagrożenia zewnętrzne powinny zatem stanowić jeden z głównych priorytetów jednostek administrujących lokalnymi instrumentami prewencji incydentów, które mają miejsce w danej spółce.

Słowa klucze: cyberbezpieczeństwo, bezpieczeństwo danych, kultura bezpieczeństwa, środowiska firmowe, edukacja pracownicza

Abstract

Modern enterprises are entities particularly vulnerable to cyber threats linked to social engineering methods widely used by cyber criminals. Today, corporate environments often have to face almost daily attempts at data theft based on many derivatives of modern varieties of phishing, and one of the main ways to combat such threats remains employee education, which can take various forms. A human being is generally identified as the weakest element in the "security chain" of a given correctly configured IT system. This state of affairs is taken into account both by companies preparing educational programs and training for their employees on their own, and those that outsource such activities to external companies. Effective creation of the so-called "security culture" within the scope of a given corporation is an extremely challenging and highly non-trivial task, and this topic is relatively rarely discussed in specialized literature. Continuous revision of the means and methods of conducting programmatic training and simulations, and management of activities contributing to the co-creation of a healthy corporate environment with a satisfactory degree of resistance to external threats, should therefore be one of the main priorities of the units administering local incident prevention instruments within the scope of a given company.

Keywords: cyber security, data security, security culture, corporate environments, employee education.

Wstęp

W świecie współczesnym, w dużej mierze definiowanym przez nowe technologie będące swoistym trzonem w zasadzie większości globalnych procesów komunikacyjnych, biznesowych, ekonomicznych i w znacznie szerszym znaczeniu kulturowych, nie trzeba daleko szukać przykładów, w których techniczny krajobraz utworzony po to, by usprawniać i optymalizować owe procesy, staje się polem działań cyberprzestępców

wykorzystujących nowoczesne środki techniczne w celu uzyskania jakiegoś rodzaju korzyści[1]. Wycieki danych pracowników firmy Uber 2022 i 2023 czy znacznie wcześniejszy wyciek danych setek milionów gości sieci hoteli Marriott wykryty w roku 2018 to tylko niektóre przykłady dziesiątek poważnych incydentów, które zostały wykryte i nagłośnione przez media w ostatnich latach[2]. Wiele tego rodzaju zdarzeń pozostaje niewykrytych, a z dużą dozą prawdopodobieństwa można także stwierdzić, iż spora część z nich zostaje zatajona przez wzgląd na chęć ochrony wizerunku dotkniętej nimi spółki. Słowem, bezpieczeństwo tak indywidualnego użytkownika sieci, jak i użytkownika będącego częścią wybranego kolektywu firmowego podejmującego dowolne w zasadzie działania biznesowe w cyberprzestrzeni ma kluczowe znaczenie dla ochrony tak dobrobytu osobistego pracowników, jak i dobrobytu korporacji, która użytkownika-pracownika zatrudnia oraz darzy go szczególnym rodzajem zaufania. W przeciwieństwie jednak do cyberataków mierzących bezpośrednio w indywidualnych użytkowników sieci, funkcjonujących w zakresie swojego własnego, prywatnego krajobrazu sieci i niepowiązanych bezpośrednio ze swoim środowiskiem pracy, cyberataki, których celem są środowiska firmowe, w wielu przypadkach potencjalnie narażają na straty finansowe oraz straty związane z utratą danych znacznie większą liczbę jednostek, a także często kładą na szali globalną reputację całych kolektywów firmowych[3]. Ostatecznie bardzo często to właśnie jednostka ludzka okazuje się tym elementem systemu, który zawodzi najczęściej, nie będąc w stanie poprawnie zidentyfikować zagrożenia i często nieświadomie podejmując działania na niekorzyść spółki[4].

1 Stefan Iovan, Alina-Anabela Iovan, „From cyber threats to cyber-crime", Journal of Information Systems & Operations Management 10/2 (2016): 425.\

2 Michael X. Heiligenstein, Uber Data Breaches: Full Timeline Through 2023, https://firewalltimes.com/uber-data-breach-timeline/ (dostęp: 01.07.2024); Josh Fruhlinger, Marriott data breach FAQ: How did it happen and what was the impact?, https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (dostęp: 01.07.2024).

3 Perera Srinath, Xiaohua Jin, Alana Maurushat, De-Graft Joe Opoku, „Factors affecting reputational damage to organisations due to cyberattacks", Informatics 9/28 (2022): 18–19; Iryna Leroy, „The relationship between cyber-attacks and dynamics of company stock: the role of reputation management", International Journal of Electronic Security and Digital Forensics 14/4 (2022): 313.

4 Stephen Lineberry, The human element: The weakest link in information security, https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html (dostęp: 01.06.2024).

Inżynieria społeczna i zagrożenia z nią powiązane

Do cyberataków najczęściej powodujących straty finansowe oraz wycieki danych, jednocześnie stosunkowo łatwych do przeprowadzenia, a co za tym idzie niezwykle popularnych w obecnych czasach, należy przede wszystkim *phishing* oraz wszystkie pochodne mu metody wyłudzania danych poprzez manipulację podpartą rozmaitymi technikami inżynierii społecznej, najczęściej na polu tradycyjnej komunikacji e-mailowej czy też social mediów i sprzężonych z nimi komunikatorów[5]. Według raportu opublikowanego w roku 2023 przez firmę Verizon *phishing* oraz pokrewny mu *pretexting* stanowią sumarycznie zasadniczą przyczynę 73% zgłaszanych wycieków danych[6]. W innym miejscu, w corocznym raporcie publikowanym przez firmę APWG na trzeci kwartał roku 2023, czytamy o rekordowej liczbie zarejestrowanych incydentów z tej kategorii w tym okresie[7]. W polskim raporcie CERT z roku 2022 możemy odnaleźć z kolei informację, że incydenty kategoryzowane jako *phishing*, a więc incydenty, w których wykorzystane były takie lub inne metody inżynierii społecznej, stanowiły w tymże roku 64% wszystkich zgłaszanych zdarzeń[8]. Jak widać, w szerokim krajobrazie cyberzagrożeń *phishing* jako szeroko pojęta kategoria ataków opartych na inżynierii społecznej i stosunkowo prostej manipulacji słownej pozostaje w zdecydowanej przewadze[9]. Istnieje także wiele przykładów działań takich jak bezpośrednie ataki z użyciem oprogramowania malware w formach, w których oprogramowanie takie wprowadzane jest do systemu docelowego z całkowitym pominięciem interakcji z użytkownikiem końcowym, ataki DDoS, czy ataki typu *man-in-the-middle* oraz wiele innych typów zdarzeń niepowiązanych bezpośrednio z aktami komunikacji sieciowej[10]. Zazwyczaj jednak obrona przed zagrożeniami tej kategorii może zostać w mniejszym lub większym stopniu zautomatyzowana przez kompetentnego administratora sieci firmowej,

5 Ahmed Aleroud, Lina Zhou, „Phishing environments, techniques, and countermeasures: A survey", Computers & Security 68 (2017): 162.

6 Verizon Data Breach Investigations Report 2023, https://www.verizon.com/business/resources/reports/dbir/ (dostęp: 05.05.2024).

7 APWG, Phishing Attack Trends Report – 3Q 2023, https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf (dostęp: 20.05.2024).

8 Raport Roczny z Działalności CERT Polska 2022, https://cert.pl/posts/2023/05/krajobraz-bezpieczenstwa polskiego-internetu-w-2022-roku/ (dostęp: 20.05.2024).

9 James Lance, Phishing Exposed (Burlington: Syngress Publishing, Inc., 2005).

10 Jibi Mariam Biju, Neethu Gopal, Anju J. Prakash, „Cyber attacks and its different types", International Research Journal of Engineering and Technology 6/3 (2019): 4849–4850.

a incydenty tego rodzaju nie tylko występują w większości przypadków znacznie rzadziej, ale także z uwagi na mniejszą popularność i stosunkowo łatwiejszą wykrywalność nie stanowią zazwyczaj istotnej części programów edukacji pracowniczej[11]. Twórcy tych programów skupiają uwagę najczęściej – jak się wydaje całkiem zasadnie – na uświadamianiu użytkowników końcowych o tych zagrożeniach, z którymi z dużą dozą prawdopodobieństwa spotkać się oni mogą w swoim środowisku pracy i którym, co znacznie ważniejsze, mogą oni bezpośrednio zapobiec, posiadając odpowiednią wiedzę i doświadczenie[12].

Człowiek-pracownik jako jednostka podatna na manipulację

Istnieje wiele sposobów zasadniczego podziału i kategoryzacji zagrożeń dotyczących środowisk korporacyjnych[13]. Do jednych z najbardziej podstawowych i zarazem najbardziej zasadnych należy podział na zagrożenia związany z trzema kategoriami osób mogących stać się swego rodzaju „punktami zapalnymi" strefy ryzyka w prawidłowo funkcjonującym przedsiębiorstwie. Odnosi się ona do pracowników działających na niekorzyść kolektywu celowo, podejmujących tego rodzaju działania poprzez zaniedbania wynikające z zawinionej niewiedzy oraz w wyniku podatności incydentalnej, a więc przez niewiedzę niezawinioną[14]. Pracownicy pierwszej kategorii spotykani są stosunkowo rzadko i działają najczęściej z pobudek finansowych, politycznych czy są kierowani innego rodzaju motywacjami prywatnymi[15]. Druga kategoria obejmuje jednostki niepodejmujące istotnych kroków, mających na celu podniesienie swoich kompetencji dotyczących bezpieczeństwa jako takiego poprzez

11 Quing Li, Gregory Clark, Security Intelligence: A Practitioner's Guide to Solving Enterprise Security Challenges (Hoboken: Wiley, 2015).

12 Markus Jakobsson, Steven Myers, Phishing and Countermeasures (Hoboken: Wiley-Interscience, 2006), 560–562.

13 M. Uma, Ganapathi Padmavathi, „A survey on various cyber attacks and their classification", International Journal of Network Security 15/5 (2013): 392; Andreea Bendovschi, „Cyber-attacks–trends, patterns and security countermeasures", Procedia Economics and Finance 28 (2015): 25; Biju, „Cyber attacks and its different types", 4849–4850.

14 Domenic Antonucci, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities (Hoboken: Wiley, 2017), 97–105.

15 Jeffrey Hunker, Christian W. Probst, „Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2 (2011): 6–7.

udział w proponowanych przez firmę szkoleniach, programach symulacji incydentów czy też programach edukacyjnych tworzonych z myślą o pracownikach – w efekcie w wielu przypadkach nie są w stanie albo poprawnie zidentyfikować zagrożenia, albo też bezpośrednio zapobiec danemu incydentowi w miarę ich personalnych możliwości[16]. Trzecią kategorię stanowią osoby, które siłą statystycznej pewności w wielu przypadkach stać się mogą prędzej czy później ofiarami dowolnego w zasadzie rodzaju ataku godzącego w dobrobyt kolektywu firmowego, którego są częścią. Można więc powiedzieć, że trzecia kategoria zawiera w sobie wszystkich bez wyjątku pracowników korporacji, pozostaje swego rodzaju niezmiennym, niemal zawsze obecnym „gwarantem niepewności". W dalszym ciągu bezpieczeństwo całego bytu firmowego figuratywnie leży w rękach pojedynczego pracownika, który w pewnym momencie może zostać postawiony przed decyzją mogącą z relatywną łatwością uchronić spółkę czy dany jej oddział przed wyciekiem danych i potencjalnie powiązanymi z nim stratami finansowymi bądź stać się przyczyną częściowego lub całościowego sukcesu cyberkryminalistów[17].

Istotnym aspektem dotyczącym sprawy bezpieczeństwa firmy w świetle działań podejmowanych przez jej pracowników w ramach wykonywania czynności związanych pośrednio bądź bezpośrednio ze środowiskiem pracy jest naturalna podatność ludzka na manipulację, którą w wielu przypadkach w stosunkowo prosty sposób wykorzystują cyberprzestępcy[18]. Jak już zostało wspomniane, zdecydowana większość cyberataków figurujących w corocznych bądź kwartalnych raportach firm monitorujących współczesny krajobraz cyberprzestępstw na szeroką skalę niemal zawsze odnosi się do przestępstw, u których podstaw leżą metody inżynierii społecznej, w wielu przypadkach w pewien sposób mocno upraszczane i sprowadzane kolektywnie do „phishingu"[19]. Wymyślne działania oparte na najnowszych, nieznanych jeszcze publicznie lukach

16 Ken H. Guo, Yufei Yuan, Norman P. Archer, Catherine E. Connelly, „Understanding nonmalicious security violations in the workplace: A composite behavior model", Journal of Management Information Systems 28/2 (2011): 222.

17 Li Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, Xiaohong Yuan, „Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", International Journal of Information Management 45 (2019): 21–22.

18 Christopher Hadnagy, Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails (Indianapolis: John Wiley & Sons, 2015), 61–67.

19 Phishing jako taki, wbrew pozorom, zawiera w sobie wiele różnych typów cyberataków opartych na manipulacji z wykorzystaniem metod inżynierii społecznej oraz w stosunkowo prosty sposób może wywołać eskalację działań i sprawić, że prosta kampania phishingowa przeobrazi się w cyberatak o naturze już czysto technicznej, prowadzący do całkowitej bądź częściowej kompromitacji systemu docelowego; Christopher

systemowych czy też incydenty pomijające całkowicie postać człowieka odgrywającego rolę pośrednika między atakującym a systemem docelowym nadal stanowią znacznie rzadszą kategorię zdarzeń, której przeciętny użytkownik systemu informatycznego często zwyczajnie nie jest w stanie zapobiec[20]. Inaczej sprawa ma się z zagrożeniami zawierającymi się w rozmaitych podkategoriach phishingu jako takiego[21]. Naturalna podatność człowieka na manipulację słowną czy też – korzystając ze znacznie szerszego i później wypracowanego terminu – inżynierię społeczną była już eksplorowana przez wielu uczonych, w tym Roberta Cialdiniego, czy Christophera Hadnagy'ego[22]. Jest ona nieodzowną częścią natury człowieka jako jednostki społecznej, przystosowanej do życia w grupach mających pierwotnie chronić go przed różnego rodzaju zagrożeniami oraz odgrywać rolę wsparcia w uwikłaniu w opozycję natura-kultura, gdzie kulturę rozumiemy jako wczesne krystalizujące się protoformy małych społeczności[23]. Zaufanie, jakim często wyjściowo darzymy ludzi, z którymi wchodzimy w rozmaite interakcje – a tych w ciągu dnia podejmujemy zazwyczaj stosunkowo wiele – w określonych sytuacjach stać się może słabością, która narazić może tak nas, naszych bliskich, jak i środowisko firmowe, w jakim funkcjonujemy, na poważne straty[24]. Skoro wiemy więc, że człowiek jest wyjściowo na manipulację w mniejszym lub większym stopniu podatny, a metody inżynierii społecznej są zazwyczaj tak łatwe do przyswojenia i zinternalizowania jak sięgnięcie po jedną z pozycji autorstwa wyżej wymienionych badaczy i uważne jej przestudiowanie tak przez przeciętnego obywatela, jak i przez cyberprzestępców, pojawia się pytanie: jak w poprawny sposób formalizować, standaryzować i na końcu wdrażać odpowiednie metody edukacyjne, mając na celu uzyskanie możliwości lepszego zapobiegania incydentom, które co roku dotykają setki środowisk firmowych na całym świecie, oraz jak uczynić ten konkretny rodzaj edukacji atrakcyjnym dla

Hadnagy, Unmasking the socialengineer: The human element of security (Hoboken: Wiley, 2014), 25–51.

20 Uma, Padmavathi, „A survey on various cyber attacks and their classification", 392.

21 Anze Mihelic, Igor Bernik, Matej Jevšček, Simon Vrhovec, „Testing the Human Backdoor: Organizational Response to a Phishing Campaign", Journal of Universal Computer Science 25/11 (2019): 1472.

22 Robert B. Cialdini, Influence: The Psychology of Persuasion (New York City: Harper Business, 2006); Christopher Hadnagy, Social Engineering: The Art of Human Hacking (Indianapolis: Wiley, 2015).

23 Adam B. Seligman, The Problem of Trust (Oxford: Princeton University Press, 2021), 31.

24 Kevin Mitnick, Art of Deception (Indianapolis: Wiley, 2002), 15–18.

jej podmiotów – pracowników korporacji? Odpowiedzią na to pytanie w mojej ocenie może być przywołany już tutaj byt teoretyczny, zamykający w sobie w zasadzie większość elementów poprawnie funkcjonującego bytu firmowego, czyli kultura bezpieczeństwa, i konieczność stałego jej tworzenia, formowania, pielęgnowania i rozwoju. Czym jest i jakie formy powinna przyjmować kultura bezpieczeństwa, będąca – jak się za moment okaże – nieodłącznym elementem każdego w zasadzie środowiska pracy, i jak w wydajny sposób ją budować? Istnieje wiele poprawnych odpowiedzi na to pytanie[25].

Kultura bezpieczeństwa

Czym więc jest kultura bezpieczeństwa? Wszakże środowiska korporacyjne, będące bytami funkcjonującymi w kontekstach własnej semiunikalnej przewodniej filozofii marki, szczególnego rodzaju filozofii kolektywu i jego wspólnego kierowanego rozwoju, a także idei wspólnoty opartej na szczególnym rodzaju wymiany symbolicznej między tworzącymi ją zrzeszonymi indywidualnościami, odznaczają się często ponadprzeciętną złożonością wewnętrzną, która często utrudnia wyszczególnienie i opis tak ogólnego – jak się z początku wydaje – elementu[26]. Pośród wielu cech i wyróżników tego, co określamy dzisiaj szerokim terminem „kultury korporacyjnej" oraz wielu jej typów, podtypów oraz związanych z nią bytów symbolicznych i archetypów, niezwykle istotną jej częścią jest jednak właśnie „kultura bezpieczeństwa"[27]. W tym terminie wyraża się holistyczne podejście do kształtowania i konstruowania podstawowych założeń filozofii bezpieczeństwa organizmu firmowego, przez który rozumiemy zbiorowość ludzką prowadzącą podczas wykonywania czynności zawodowych regularnie bądź semiregularnie istotne interakcje

25 Johan F. van Niekerk, Rossouw von Solms, „Information security culture: A management perspective", Computers & Security 29/4 (2010): 485–486; Edwin D. Frauenstein, Rossouw von Solms, Combatting phishing: A holistic human approach, https://digifors.cs.up.ac.za/issa/2014/Proceedings/Full/103_Paper.pdf (dostęp: 08.06.2024).

26 Bytom korporacyjnym poświęcone zostało wiele prac skrupulatnie opisujących ich złożone struktury wewnętrzne i mechanizmy działania wspólne dla setek przedsiębiorstw na całym świecie. Do jednych z takich opracowań należy praca Barbary Fryzeł: Barbara Fryzeł, Kultura korporacyjna: poglądy, teorie, zarządzanie (Kraków: Wydawnictwo UJ, 2005).

27 Adele Martins, Jan Elofe, „Information Security Culture", w: Security in the Information Society. IFIP Advances in Information and Communication Technology 86, red. M. Adeb Ghonaimy, Mahmud T. El-Hadidi, Heba Aslan (New York: Springer, 2022), 204–205.

z infrastrukturą technologiczną miejsca pracy, założeń tworzonych na miarę konkretnego bytu firmowego oraz konkretnych jego pracowników i ich grup[28].

Na najbardziej podstawowym poziomie jeden z głównych elementów budowy kultury bezpieczeństwa stanowi, czy też stanowić powinna, wspólna, w pewien sposób współdzielona między pracownikami świadomość zestawu zagrożeń mogących dotknąć dany kolektyw pracowniczy[29]. Odpowiedzialni za tworzenie tego rodzaju świadomości w większości przypadków okazują się edukatorzy stojący po stronie danej korporacji czy też firmy zewnętrznej realizującej szkolenia mające na celu obniżenie współczynnika podatności pracowników danej spółki na różne kategorie cyberzagrożeń opartych na prostych metodach inżynierii społecznej[30]. Często w zakresie mniejszych przedsiębiorstw, idee tego rodzaju wprowadzane są w życie przy niskim stopniu świadomości osób zarządzających firmą, bez większego przywiązania do właściwego planowania czy strukturyzacji działań albo unikalnej specyfiki danej grupy pracowniczej. Inne, także niezwykle istotne, elementy kultury bezpieczeństwa to odgórne przywiązanie wagi do równomiernej edukacji wszystkich pracowników, zwrócenie uwagi na systematyczne monitorowanie, rozwijanie i aktualizowanie wybranych stosowanych metod edukacyjnych i treningowych oraz stała weryfikacja działań połączona ze śledzeniem postępów każdej z zatrudnionych osób zaangażowanych w szkolenie. Bardzo istotnym elementem okazuje się tutaj także, podobnie zresztą jak w przypadku podejmowania jakichkolwiek działań związanych z ingerencją w bytowanie, świadomość oraz zwyczaje danej grupy pracowników, unikalna wyjściowa kultura danego kolektywu korporacyjnego i jej szczególne wyróżniki, takie jak rodzaj zwyczajowych stosunków międzypracowniczych, utarte sposoby komunikacji wewnętrznej i zewnętrznej, przyjęte metodologie pracy zespołowej, jak również szeroko pojęta sfera symboliczna otaczająca, spajająca i jednocześnie tworząca dane środowisko firmowe, także w pewien sposób wbrew pozorom niepowtarzalna i trudna

28 AlHogail Areej, „Design and validation of information security culture framework", Computers in Human Behavior 49 (2015): 567.

29 Areej AlHogail, Abdulrahman Mirza, „Information security culture: A definition and a literature review", 2014 World Congress on Computer Applications and Information Systems (WCCAIS): 1–7, https://www.researchgate.net/publication/282754259_Information_Security_Culture_A_Definition_and_A_Literature_Review (dostęp: 20.02.2024).

30 Norhafizah Abu Bakar, Masnizah Mohd, Rossilawati Sulaiman, „Information leakage preventive training", 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI): 1–6, https://ieeexplore.ieee.org/document/8312403 (dostęp: 15.03.2024).

do uchwycenia dla zewnętrznego czy mniej uważnego obserwatora[31]. Pomimo iż współcześnie istnieje wiele metod opisu tego rodzaju zjawisk, nigdy nie należy zapominać o unikalnej charakterystyce danego miejsca pracy czy jego wycinka, która nigdy nie ma charakteru neutralnego, gdy bierzemy pod uwagę tworzenie, kształtowanie czy rewizję zwyczajów pracowników stanowiących jego główny i najważniejszy element, i zawsze powinna być brana pod uwagę, zanim planować będziemy jakiekolwiek działania dotyczące tej kategorii[32]. Oprócz tego bardzo istotny podczas planowania ingerencji w kulturę bezpieczeństwa danego miejsca pracy poprzez wdrażanie rozmaitych systemów szkoleniowych jest także właściwy balans między podejściem całościowym a indywidualnym, co w przypadku nowoczesnych form programowej edukacji pracowniczej często stanowi problem z uwagi na osobliwy charakter wielu ofert proponowanych przez rozmaite zewnętrzne firmy szkoleniowe[33].

Właściwe określenie misji spółki, położenie nacisku na istotną rolę rozwijania kompetencji każdego z pracowników, podkreślenie rangi szczególnego rodzaju odpowiedzialności indywidualnej przy jednoczesnym zmiękczeniu poczucia zbiorowej, rozmytej odpowiedzialności za ewentualne incydenty, a także wprowadzenie elementów idei rywalizacji międzypracowniczej oraz międzyfirmowej do schematu działań edukacyjnych i treningowych w zakresie najlepszych praktyk dotyczących bezpieczeństwa – to tylko niektóre komplementarne działania, które można podjąć odgórnie, by kulturę bezpieczeństwa danego miejsca pracy budować świadomie, a nie tylko incydentalnie, podejmując nieustrukturyzowane działania, czy w sposób reakcyjny, po odnotowaniu zaistniałego incydentu[34]. Do innych praktyk czy też kierunków rozwoju, które – gdy zostaną podjęte – mogą relatywnie łatwo przyczynić się do kształtowania się zdrowej, naturalnie rozwijającej się kultury bezpieczeństwa środowiska firmowego, należą chociażby: kładzenie nacisku na odbywanie szkoleń tematycznych w grupach „na żywo" aniżeli zaledwie online, podkreślanie przez edukatorów szczególnej wartości

31 Marko Cabric, Corporate security management: Challenges, risks, and strategies (Oxford: Butterworth-Heinemann, 2015), 35–36.

32 Kathryn Parsons, Agata McCormac, Marcus Butavicius, Lael Ferguson, Human factors and information security: individual, culture and security environment, https://apps.dtic.mil/sti/pdfs/ADA535944.pdf (dostęp: 09.04.2024).

33 Przykładowo, przez firmę KnowBe4: The Ultimate Guide to Security Awareness Training, https://www.knowbe4.com/security-awareness-training (dostęp: 15.02.2024).

34 Jean Emmanuel Ntsama, Claude Fachkha, Philippe Brice Owomo, „A Gamification Architecture to Enhance Phishing Awareness", w: Safe, Secure, Ethical, Responsible Technologies and Emerging Applications. SAFER-TEA 2023, red. Franklin Tchakounte, Marcellin Atemkeng, Rajeswari Pillai Rajagopalan (New York: Springer, 2024), 40.

przedstawianej wiedzy oraz jej użyteczności poza miejscem pracy, atrakcyjna edukacja seminegatywna, odkrywająca pozornie utajone techniki działania cyberkryminalistów czy też zachęcanie do przekazywania zdobytej wiedzy dalej, w środowisku domowym, oraz do stania się lokalnym autorytetem mogącym zapobiegać incydentom nie tylko w godzinach pracy, chroniąc kolektyw firmowy, ale także poza nimi, chroniąc swoją rodzinę oraz najbliższych znajomych przed rozmaitymi rodzajami nowo poznanych cyberzagrożeń.

Rola programowej edukacji pracowniczej

Pomimo iż edukacja w zakresie bezpieczeństwa w wielu firmach prowadzona jest nadal w sposób wypracowany *stricte* przez dane środowisko korporacyjne, zaprojektowany i zunifikowany jedynie w jej zakresie, współcześnie istnieje już wiele mniej lub bardziej ustandaryzowanych programów o charakterze edukacyjnym czy symulacyjnym, mających na celu rozwijać wiedzę użytkowników końcowych (pracowników) na temat najpopularniejszych zagrożeń oraz metod stosowanych przez cyberprzestępców. Do takich rozwiązań należą chociażby programy firm KnowBe4, Cofense czy Hoxhunt, łączących w swoich ofertach edukacyjnych kierowanych do korporacji programy edukacji pracowniczej w zakresie cyberbezpieczeństwa, z programami symulacji incydentów, oraz systemami weryfikacji wyników prowadzonych działań[35]. Szkolenia takie składają się w większości przypadków z odgórnie ustalonych, choć możliwych do spersonalizowania w ograniczonym stopniu zbiorów materiałów treningowych przekazywanych pracownikom w formie szkoleń w formacie wideo, narzędzi pozwalających administrującym treningiem na weryfikację postępów w zapoznawaniu się z materiałem osób biorących udział w szkoleniu oraz narzędzi umożliwiających przeprowadzanie próbnych testów polegających na rozsyłaniu spreparowanych maili phishingowych uczestnikom procesu edukacyjnego w celu weryfikacji ich nowo nabytych zdolności identyfikacji prób manipulacji w komunikacji online, a co za tym idzie – ich odporności na phishing czy metody inżynierii społecznej w ogóle[36]. Łatwo jednak daje się zauważyć,

35 Asangi Jayatilaka et al., Evaluation of security training and awareness programs: Review of current practices and guideline, https://arxiv.org/abs/2112.06356 (dostęp: 20.06.2024).

36 Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, Julia Downs, „Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", Proceedings of CHI 2010: Privacy Behaviors: 374.

że pomimo pozytywnych wyników raportowanych przez wspomniane firmy w zakresie zmniejszania współczynnika podatności użytkowników końcowych na zagrożenia powiązane z phishingiem udział pracownika w przeznaczonych dla niego szkoleniach zasadniczo nie jest w stanie sam w sobie przyczynić się w znaczący sposób do utworzenia wydajnego organicznego systemu ochrony przedsiębiorstwa przed zagrożeniami zewnętrznymi[37]. Dodatkowo istnieje wiele problemów pośrednich, ostatecznie powodujących często suboptymalny poziom skuteczności wielu tego rodzaju rozwiązań. Brak faktycznej gwarancji zapoznania się pracownika z treścią szkolenia, techniczne niedoskonałości formy wiadomości symulacyjnych dających się często łatwo rozpoznać bez zbytniego namysłu, niewystarczający poziom personalizacji zawartych w nich komunikatów czy też całkowite porzucenie w zasadzie jakiejkolwiek formy podejścia personalnego z uwagi na przystosowanie tego rodzaju programów do masowych wdrożeń w grupach liczących setki pracowników to zaledwie kilka z nich[38].

Zakończenie

Pomimo iż z prostych przyczyn nigdy nie możemy marzyć o programie edukacyjnym, który byłby w stu procentach skuteczny, nie należy z tego względu odrzucać możliwości ulepszenia istniejących już i szeroko stosowanych rozwiązań czy podjęcia prób rewizji w celu uzyskania ich większej wydajności, lepszej kompatybilności z ideami przewodnimi danej korporacji i jej specyficzną kulturą pracowniczą, oraz – co za tym idzie – często podniesienia opłacalności implementacji takiego rozwiązania dla docelowej spółki. Wciąż jednak należy pamiętać, iż – parafrazując słowa Kevina Mitnicka – łańcuch jest tylko tak silny, jak jego najsłabsze ogniwo[39]. Kulturę bezpieczeństwa firmy tworzą z zasady przede wszystkim jej pracownicy w mniejszym lub większym stopniu kierowani przez misję danej korporacji i odgórnie narzucony zestaw zasad, i to oni winni być na pierwszym miejscu podmiotami procesów mających za zadanie podnieść współczynnik odporności kolektywu

37 Alex Sumner, Xiaohong Yuan, Mohd Anwar, Maranda McBride, „Examining factors impacting the effectiveness of anti-phishing trainings", Journal of Computer Information Systems 62/5 (2022): 990.

38 Phishing attacks: defending your organisation, https://www.ncsc.gov.uk/guidance/phishing (dostęp: 20.01.2024).

39 Kevin Mitnick, Robert Vamossi, The Art of Invisibility (Boston: Little, Brown and Company, 2017), 57.

firmowego na cyberataki z użyciem technik inżynierii społecznej oraz zarazem pierwszymi respondentami w razie zaistniałego incydentu, mogącymi uchronić spółkę przed znacznymi stratami. Właściwe formowanie kultury bezpieczeństwa zakładać powinno partycypację wszystkich członków grupy pracowniczej zaangażowanych w komunikację sieciową czy korzystających podczas pracy z technicznej infrastruktury firmowej, bez względu na stanowisko, poziom doświadczenia czy zastane zdolności. Całościowe podejście do kreowania struktury wewnętrznie spójnej, samoweryfikującej się w sposób organiczny oraz odznaczającej się silnym poczuciem współodpowiedzialności za dobro kolektywu po stronie jednostki, a także stale rozwijającej swoje sumaryczne kompetencje w zakresie bezpieczeństwa wewnętrznego spółki oraz bezpieczeństwa indywidualnego, stanowić powinno priorytet podczas planowania, organizacji i wdrażania wszelkiego rodzaju rozwiązań mających na celu podniesienie poziomu odporności danego środowiska firmowego na negatywne działania zewnętrzne[40]. W ten sposób budować można organizm, u którego podstaw leżeć będzie poszanowanie dla jego unikalnej specyfiki oraz cech szczególnych, który wzmocniony przez właściwie projektowane i zarządzane działania w zakresie edukacji pracowniczej odznaczać się może ponadprzeciętnymi wynikami w zakresie odporności na działania cyberprzestępców przy jednoczesnej korzyści indywidualnej dla wszystkich pracowników, którzy posiedli zdolności potrzebne im do osiągnięcia tego celu.

Bibliografia

Książki i monografie

Antonucci Domenic, *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities* (Hoboken: Wiley, 2017).

Cabric Marko, *Corporate security management: Challenges, risks, and strategies* (Oxford: Butterworth-Heinemann, 2015).

Cialdini Robert B., *Influence: The Psychology of Persuasion* (New York City: Harper Business, 2006).

Fryzeł Barbara, *Kultura korporacyjna: poglądy, teorie, zarządzanie* (Kraków: Wydawnictwo UJ, 2005).

Hadnagy Christopher, *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails* (Indianapolis: John Wiley & Sons, 2015).

Hadnagy Christopher, *Social Engineering: The Art of Human Hacking* (Indianapolis: Wiley, 2015).

40 Frauenstein, Combatting phishing: A holistic human approach.

Hadnagy Christopher, *Unmasking the social engineer: The human element of security* (Hoboken: Wiley, 2014).
Jakobsson Markus, Myers Steven, *Phishing and Countermeasures* (Hoboken: Wiley-Interscience, 2006).
Lance James, *Phishing Exposed* (Burlington: Syngress Publishing, Inc., 2005).
Li Quing, Clark Gregory, *Security Intelligence: A Practitioner's Guide to Solving Enterprise Security Challenges* (Hoboken: Wiley, 2015).
Mitnick Kevin, *Art of Deception* (Indianapolis: Wiley, 2002).
Mitnick Kevin, Vamossi Robert, *The Art of Invisibility* (Boston: Little, Brown and Company, 2017).
Seligman Adam B., *The Problem of Trust* (Oxford: Princeton University Press, 2021).

Czasopisma

Areej AlHogail, „Design and validation of information security culture framework", *Computers in Human Behavior* 49 (2015): 567–575.
Aleroud Ahmed, Zhou Lina, „Phishing environments, techniques, and countermeasures: A survey", *Computers & Security* 68 (2017): 160–196.
Bendovschi Andreea, „Cyber-attacks – trends, patterns and security countermeasures", *Procedia Economics and Finance* 28 (2015): 24–31.
Biju Jibi Mariam, Neethu Gopal, Anju J. Prakash, „Cyber attacks and its different types", *International Research Journal of Engineering and Technology* 6/3 (2019): 4849–4852.
Guo Ken H., Yuan Yufei, Archer Norman P., Connelly Catherine E., „Understanding nonmalicious security violations in the workplace: A composite behavior model", *Journal of Management Information Systems* 28/2 (2011): 203–236.
Jeffrey Hunker, Christian W. Probst, „Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques", *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2 (2011), 4–27.
Iovan Stefan, Alina-Anabela Iovan, „From cyber threats to cyber-crime", *Journal of Information Systems & Operations Management* 10/2 (2016): 425–434.
Leroy Iryna, „The relationship between cyber-attacks and dynamics of company stock: the role of reputation management", *International Journal of Electronic Security and Digital Forensics* 14/4 (2022): 309–317.
Li Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, Xiaohong Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management* 45 (2019): 13–24.
M. Uma, Padmavathi Ganapathi, „A survey on various cyber attacks and their classification", *International Journal of Network Security* 15/5 (2013): 390–396.

Mihelic Anze, Bernik Igor, Jevšček Matej, Vrhovec Simon, „Testing the Human Backdoor: Organizational Response to a Phishing Campaign", *Journal of Universal Computer Science* 25/11 (2019): 1458–1477.

Sheng Steve, Holbrook Mandy, Kumaraguru Ponnurangam, Cranor Lorrie, Downs Julia, „Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", *Proceedings of CHI 2010: Privacy Behaviors*: 373–382.

Srinath Perera, Xiaohua Jin, Alana Maurushat, De-Graft Joe Opoku, „Factors affecting reputational damage to organisations due to cyberattacks", *Informatics* 9/28 (2022): 1–24.

Sumner Alex, Yuan Xiaohong, Anwar Moht, McBride Maranda, „Examining factors impacting the effectiveness of anti-phishing trainings", *Journal of Computer Information Systems* 62/5 (2022): 975–997.

van Niekerk Johan F., von Solms Rossouw, „Information security culture: A management perspective", *Computers & Security* 29/4 (2010): 476–486.

Rozdziały w monografiach

Martins Adele, Elofe Jan, „Information Security Culture", w: *Security in the Information Society. IFIP Advances in Information and Communication Technology 86*, red. M. Adeb Ghonaimy, Mahmud T. El-Hadidi, Heba Aslan (New York: Springer, 2022), 203–214.

Ntsama Jean Emmanuel, Fachkha Claude, Philippe Brice Owomo, „A Gamification Architecture to Enhance Phishing Awareness", w: *Safe, Secure, Ethical, Responsible Technologies and Emerging Applications. SAFER-TEA 2023*, red. Franklin Tchakounte, Marcellin Atemkeng, Rajeswari Pillai Rajagopalan (New York: Springer, 2024), 37–57.

Netografia

Abu Bakar Norhafizah, Mohd Masnizah, Sulaiman Rossilawati, „Information leakage preventive training", *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*: 1–6, https://ieeexplore.ieee.org/document/8312403 (dostęp: 15.03.2024).

AlHogail Areej, Abdulrahman Mirza, „Information security culture: A definition and a literature review", *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*: 1–7, https://www.researchgate.net/publication/282754259_Information_Security_Culture_A_Definition_and_A_Literature_Review (dostęp: 20.02.2024).

APWG, *Phishing Attack Trends Report – 3Q 2023*, https://docs.apwg.org/reports/apwg_trends_report_ q4_2023.pdf (dostęp: 20.05.2024).

Bakar Norhafizah Abu, Mohd Masnizah, Sulaiman Rossilawati, „Information leakage preventive training", *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*: 1–6, https://ieeexplore.ieee.org/document/8312403 (dostęp: 15.03.2024).

Frauenstein Edwin D., Rossouw von Solms, *Combatting phishing: A holistic human approach*, https://digifors.cs.up.ac.za/issa/2014/Proceedings/Full/103_Paper.pdf (dostęp: 08.06.2024).

Fruhlinger Josh, *Marriott data breach FAQ: How did it happen and what was the impact?*, https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (dostęp: 01.07.2024).

Heiligenstein Michael X., *Uber Data Breaches: Full Timeline Through 2023*, https://firewalltimes.com/ uber-data-breach-timeline/ (dostęp: 01.07.2024).

Jayatilaka Asangi, Beu Nathan, Baetu Irina, Zahedi Mansooreh, Babar M. Ali, Hartley Laura, Lewinsmith Winston, *Evaluation of security training and awareness programs: Review of current practices and guideline*, https://arxiv.org/abs/2112.06356 (dostęp: 20.06.2024).

Lineberry Stephen, *The human element: The weakest link in information security*, https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html (dostęp: 01.06.2024).

Parsons Kathryn, Agata McCormac, Marcus Butavicius, Lael Ferguson, *Human factors and information security: individual, culture and security environment*, https://apps.dtic.mil/sti/pdfs/ADA535944.pdf (dostęp: 09.04.2024).

Phishing attacks: defending your organisation, https://www.ncsc.gov.uk/guidance/phishing (dostęp: 20.01.2024).

Raport Roczny z Działalności CERT Polska 2022, https://cert.pl/posts/2023/05/krajobraz-bezpieczenstwa polskiego-internetu-w-2022-roku/ (dostęp: 20.05.2024).

The Ultimate Guide to Security Awareness Training, https://www.knowbe4.com/security-awareness-training (dostęp: 15.02.2024).

Verizon Data Breach Investigations Report 2023, https://www.verizon.com/business/resources/reports/dbir/ (dostęp: 05.05.2024).