Paweł KOBIS
ORCID: 0000-0003-0714-1888

Politechnika Częstochowska
Wydział Zarządzania

Rola czynnika ludzkiego w procesach zarządzania bezpieczeństwem zasobów informacyjnych przedsiębiorstw

Streszczenie: Zarządzanie bezpieczeństwem informacji poza głównym obszarem działalności przedsiębiorstwa jest obecnie jedną z przestrzeni funkcjonowania każdego podmiotu gospodarczego. Ilość przetwarzanych i magazynowanych informacji rośnie eksponencjalnie. Informacje stanowią obecnie jeden z głównych zasobów przedsiębiorstw, kreując poziom ich konkurencyjności. Szeroko rozumiane zasoby informacyjne warunkujące istnienie podmiotu gospodarczego na rynku, będące nośnikiem jego know-how są postrzegane jako wartość, którą należy odpowiednio chronić, zabezpieczać przed przypadkową utratą lub celowymi, nielegalnymi próbami pozyskania lub zniszczenia. Obecnie możemy wyróżnić ochronę informacji na dwóch płaszczyznach: technicznej, obejmującej oprogramowanie i sprzęt, oraz czynnika ludzkiego, obejmującego zachowania osób zarządzających informacją, których działania i popełniane błędy powodują zwiększenie ryzyka utraty zasobów niematerialnych. W rozdziale przedstawiono zagadnienia dotyczące drugiej z wymienionych płaszczyzn. Celem rozdziału jest scharakteryzowanie pojęcia czynnika ludzkiego w bezpieczeństwie informacji oraz zaprezentowanie wyników badań dotyczących aspektów związanych z czynnikiem ludzkim w procesach zarządzania bezpieczeństwem informacji.
Słowa kluczowe: *bezpieczeństwo informacji, czynnik ludzki, błąd ludzki, system informacyjny, przedsiębiorstwo*

Role of human factor in processes of managing information resources security in enterprises

Summary: Information management security, in addition to the main area of activity of the company, is currently one of the functions of the functioning of the dimensions of every economic entity's functioning. The number of processes and stored information is growing exponentially. Currently, information constitutes one of the primary resources of the company, shaping the level of its competitiveness. Widely understood information resources that condition the existence of an economic entity on the market, being the carrier of its know-how, are perceived as a value that needs to be appropriately protected, secured against an accidental loss or deliberate, illegal attempts aimed at acquiring or destroying them. Today, two dimensions of information protection can be distinguished. The first dimension is the technical one and it includes software and hardware. The second dimension is the human factor, which comprises the behaviours of persons that manage information, whose actions, mistakes they make, increase the risk of loss of immaterial resources. The paper presents the issues pertaining to the latter dimension. The objective of the paper is to characterise the notion of human factors in information

security and present the results of the research on aspects related to human factors in information security management processes.
Keywords: *information security, human factor, human error, information system, enterprise*

Wstęp

Zasoby informacyjne współczesnych przedsiębiorstw stanowią jeden z kluczowych zasobów dających przewagę konkurencyjną na rynku gospodarczym. W większości przypadków informacja przechowywana i przetwarzana jest w sposób cyfrowy w postaci ciągu bitów reprezentowanych przez pliki (tekstowe, binarne) oraz jako zapisy w bazach danych. Papierowe oraz analogowe nośniki informacji (taśmy audio, video) są obecnie skutecznie wypierane lub stanowią raczej postać wtórną jako wydruki, zestawienia, nagrania, infografiki generowane z określonych aplikacji i systemów informatycznych. Cyfrowa postać informacji posiada wiele zalet. Umożliwia przetwarzanie i magazynowanie jej w sposób relatywnie szybki, przesyłanie na duże odległości w czasie rzeczywistym, tworzenie w sposób automatyczny i półautomatyczny dowolnych zestawień. Umożliwia również pracę w dowolnym miejscu z użyciem odpowiednich technik komunikacyjnych poprzez sieć internet. Obserwacja współczesnego rynku gospodarczego pozwala zauważyć swoisty „wyścig" przedsiębiorstw w pozyskiwaniu informacji, najlepiej unikatowych, niosących dużą wartość dla samego podmiotu. Same podmioty gospodarcze również tworzą nowe zasoby informacyjne, chociażby poprzez działalność marketingową w sieci internet, tworzenie nowych zasobów w postaci blogów, stron www, poczty elektronicznej i innych. Informacje tworzone są również przez same urządzenia (IoT – Internet Rzeczy). Zasobów informacyjnych jest coraz więcej, zarówno tych przydatnych dla działalności gospodarczej, jak i informacji bezużytecznych lub zagrażających funkcjonowaniu podmiotu. Na przykład według raportu firmy IDC „Worldwide Global DataSphere Forecast" w 2025 roku na świecie będzie około 180 zettabajtów danych. To samo badanie wskazuje, że w ciągu roku średnio o 23% rośnie ilość gromadzonych danych, produkowanych przede wszystkim przez organizacje gospodarcze[1]. Autor ma świadomość, że

[1] Newseria Biznes, *W 2025 roku na świecie przechowywanych będzie 180 zettabajtów danych. Najszybciej produkują je firmy, ale wciąż mają problemy z ich gromadzeniem i wykorzystywaniem*, http://biznes.newseria.pl/news/w-2025-roku-na-swiecie,p1512315547, data dostępu: 28.06.2021.

przytoczone badanie dotyczy danych (jak większość tego typu raportów publikowanych na świecie), z kolei tematem opracowania są informacje – pojęcia odmienne. Należy jednak podkreślić, że tworzenie informacji według teorii pojęć poznawczych odbywa się przy wykorzystaniu określonych danych. Można więc przyjąć, że wzrost wymienionych pojęć poznawczych następuje proporcjonalnie.

Ilość generowanych i przetwarzanych na świecie informacji wymusza stosowanie coraz bardziej zaawansowanych rozwiązań informatycznych zarówno na płaszczyźnie ich agregacji, dezagregacji, wyszukiwania, selekcji, operacji arytmetycznych, statystycznych i innych, jak i na płaszczyźnie ich ochrony. Zarządzanie bezpieczeństwem informacji stało się więc kluczowe z punktu widzenia ciągłości działania podmiotów gospodarczych. Informacja, jako zasób kluczowy, musi podlegać najwyższym standardom ochrony – zarówno ze strony jej przypadkowego uszkodzenia, jak i ze strony prób nielegalnego pozyskania lub uszkodzenia przez osoby trzecie. Informacja stała się narzędziem walki konkurencyjnej, przez co inwestycje związane z jej zabezpieczeniem stają się kluczowe.

Możliwości i zaawansowanie techniczne współczesnych zabezpieczeń pozwalają uniknąć większości zagrożeń powodowanych przez złośliwe oprogramowanie. Między twórcami sprzętu i oprogramowania zabezpieczającego informacje a twórcami różnego rodzaju szkodliwego oprogramowania trwa swoisty „wyścig zbrojeń". W jego efekcie obserwuje się coraz mniej incydentów naruszenia bezpieczeństwa informacji mających podłoże czysto techniczne. Jest to bowiem coraz trudniejsze. Osoby, grupy chcące pozyskać nielegalnie informacje wykorzystują więc techniki pozwalające ominąć techniczne zabezpieczenia – wykorzystując człowieka jako najsłabszego „elementu" systemu bezpieczeństwa informacji. Tym samym można zaobserwować znaczny wzrost ataków wykorzystujących inżynierię społeczną, błędy człowieka oraz próby pozyskiwania pracowników jako szpiegów gospodarczych, przykładowo poprzez wykorzystanie ich szeroko rozumianego niezadowolenia z obecnej pracy.

Celem niniejszego rozdziału jest przybliżenie pojęcia czynnika ludzkiego jako głównej, współczesnej przyczyny utraty informacji w podmiotach gospodarczych oraz przedstawienie przykładowych badań dotyczących aspektów związanych z czynnikiem ludzkim w procesach zarządzania bezpieczeństwem informacji.

Zagrożenia bezpieczeństwa informacji powodowane przez człowieka – aspekt teoretyczny

Prowadzone współcześnie badania nad bezpieczeństwem zasobów informacyjnych w przedsiębiorstwach generalnie podkreślają, że ludzie są najważniejszym elementem bezpieczeństwa danych i informacji. Paradoksalnie jednak jest to obszar o najniższych nakładach inwestycyjnych pod względem cyberbezpieczeństwa[2]. W obszarze praktyki zabezpieczeń nacisk kładziony jest zwykle na technologicznym komponencie systemów informatycznych. Czynnik ludzki nadal jest obszarem, któremu nie poświęca się należytej uwagi. Analiza literatury przedmiotu pozwala na wysnucie hipotezy, że w wielu przypadkach przyjęto założenie, że ludzie będą postępować zgodnie z oczekiwanymi wzorcami bezpiecznego zachowania, a zatem oczekiwania dotyczące bezpieczeństwa systemu zostaną spełnione. Wszystkie ewentualne, przypadkowe błędy zostaną „wychwycone" i zneutralizowane przez zaimplementowany system bezpieczeństwa. Bezpieczeństwo nie jest jednak czymś, co można po prostu kupić[3]. Jak pisze B. Schneier, amerykański kryptograf i specjalista z zakresu bezpieczeństwa teleinformatycznego: „Ideologia, że dobre systemy technologiczne mogą rozwiązać problem bezpieczeństwa organizacji, jest oznaką braku zrozumienia problemu, a także braku zrozumienia technologii"[4].

Na podstawie analizy literatury przedmiotu[5] można stwierdzić, że niepowołany dostęp do zasobów informacyjnych przedsiębiorstw uzyskiwany

[2] U.D. Ani, H. He, A. Tiwari, *Human factor security: Evaluating the cybersecurity capacity of the industrial workforce*, „Journal of Systems and Information Technology" 2019, nr 21(1), s. 2-4; J. Jeimy, M. Cano, *The Human Factor in Information Security*, „ISACA Journal" 2019, nr 5, https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security, data dostępu: 28.06.2021.

[3] K. Hughes-Lartey, M. Li, F.E. Botchey, Z. Qin, *Human factor, a critical weak point in the information security of an organization's Internet of things*, „Heliyon" 2021, nr 7(3), s. 1-2.

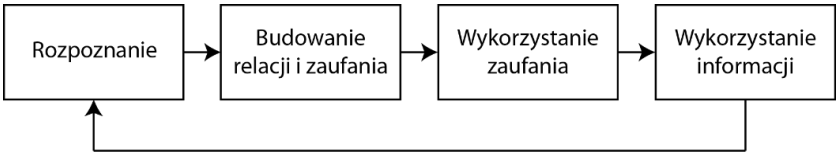
[4] B. Schneier, *Schneier on Security*. John Wiley & Sons, Hoboken, New Jersey 2009.

[5] I. Corradini, E. Nardelli, *Social Engineering and the Value of Data: The Need of Specific Awareness Programs*, [w:] *Advances in Human Factors in Cybersecurity*, T. Ahram, W. Karwowski (red.), Springer International Publishing, New York 2020, s. 59-65; G. Desolda, F. di Nocera, L. Ferro, R. Lanzilotti, P. Maggi, A. Marrella, *Alerting Users About Phishing Attacks*, [w:] *HCI for Cybersecurity, Privacy and Trust*, A. Moallem (red.), Springer International Publishing, New York 2019, s. 134-148; A.K. Jain, B.B. Gupta, *A survey of phishing attack techniques, defence mechanisms and open research challenges*, „Enterprise Information Systems" 2021, s. 1-39; Moraph, *Human Factors in Cyber Security*, 2020, http://34.234.138.24/human-factors-in-cyber-security/, data dostępu: 27.06.2021; I. Salihovic, H. Serdarevic, J. Kevric, *The Role of Feature Selection in Machine Learning for*

jest przez wykorzystanie czynnika ludzkiego przy użyciu: phishingu, socjotechnik, złośliwego oprogramowania, wadliwych polityk bezpieczeństwa oraz luk w systemach informatycznych. Scenariuszy ataków wykorzystujących czynnik ludzki jest bardzo wiele. W uproszczeniu sprowadzają się one do dwóch obszarów:

1) wykorzystania nieumyślnych działań pracownika;
2) wykorzystania luk systemu informacyjnego celowo spreparowanych przez pracownika.

W pierwszym przypadku mówimy najczęściej o działaniach mających charakter socjotechniczny, których schemat pokazano na rysunku 1.



Rysunek 1. Cykl ataków socjotechnicznych według Kevina Mitnicka
Źródło: K.D. Mitnick, W.L. Simon, *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, Hoboken 2003, cyt. za: I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar, T. Baker, *Security threats to critical infrastructure: The human factor*, „The Journal of Supercomputing" 2018, nr 74(10), s. 4990.

Działania wykorzystują podatność pracowników na zmanipulowanie przez osoby trzecie, celem np. nieumyślnego podania hasła, uruchomienia programu, otworzenia załącznika poczty elektronicznej. Cyberprzestępcy wykorzystują praktycznie wszystkie możliwe formy komunikacji z przyszłą „ofiarą" ataku: pocztę elektroniczną, komunikatory internetowe, portale społecznościowe, specjalnie spreparowane strony www, telefonię stacjonarną i komórkową przy uwzględnieniu większości dostępnych w niej usług. Posługują się technikami inżynierii społecznej, pozwalającymi kierować ludzkimi działaniami. Wśród najpopularniejszych technik można wymienić[6]:

- Tworzenie poczucia wiarygodności, np. generowanie fałszywych „polubień" na portalach społecznościowych oraz sztuczne zwiększanie liczby obserwujących osób celem wywołania wrażenia, że inne osoby wspierają dane zachowanie.

Detection of Spam and Phishing Attacks, [w:] *Advanced Technologies, Systems, and Applications III*, S. Avdaković (red.), Springer International Publishing, New York 2019, s. 476-483.
[6] K. Haycock, J.R. Matthews, *Persuasive Advocacy*, „Public Library Quarterly" 2016, nr 35(2), s. 126-135.

- Budowanie poczucia obowiązku odwzajemnienia się, np. oferowanie bezpłatnych usług i produktów i oczekiwanie w zamian dostępu do danych.
- Perswazja: przekonywanie do przekazania informacji w określonym celu, np. statystycznym.
- Podszywanie się pod specjalistów, np. poprzez kontakt telefoniczny, podawanie się za osobę z innego działu lub przełożonego (w przypadku dużych przedsiębiorstw lub korporacji) lub osobę z określonej instytucji.

Wymienione techniki stanowią przykłady z dużo szerszego spektrum możliwych scenariuszy. Szczególnie podatne mogą na nie być osoby dopiero rozpoczynające pracę, nieznające struktury przedsiębiorstwa lub osoby obawiające się jej utraty[7].

Obszar zawiera również wykorzystanie luk w systemie informacyjnym, które powstały poprzez nieumiejętne posługiwanie się narzędziami informatycznymi (brak kompetencji, doświadczenia) lub które powstały z powodu nieuwagi, lenistwa, zmęczenia, stresu lub pod wpływem cech psychofizycznych pracownika. W takich sytuacjach nawet bez stosowania socjotechnik może dojść do naruszenia bezpieczeństwa zasobów niematerialnych. Skala zjawiska jest duża: można tutaj przytoczyć badanie przeprowadzone przez firmę Proofpoint[8], z którego wynika, że:

- tylko 61% respondentów poprawnie wskazało definicję phishingu na tablicy wielokrotnego wyboru;
- tylko 31% poprawnie zdefiniowało oprogramowanie ransomware;
- 45% respondentów przyznaje się do wielokrotnego używania tego samego hasła w różnych usługach;
- ponad 50% respondentów nie chroni hasłem domowych sieci Wi-Fi (jest to szczególnie istotne w obecnym okresie pandemii COVID-19, kiedy znaczny odsetek pracowników pracuje zdalnie ze swojego miejsca zamieszkania);
- 32% respondentów nie wie, czym jest wirtualna sieć prywatna (VPN).

[7] R.A. Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar, *Review and insight on the behavioral aspects of cybersecurity*, „Cybersecurity" 2020, nr 3.
[8] Proofpoint Inc., *2020 User Risk Report. Exploring Vulnerability and Behaviour in a People-Centric Threat Landscape*, https://az659834.vo.msecnd.net/eventsairaueprod/production-aisa-public/442f8d3ebe7445049ca67e2e7d20f348, data dostępu: 27.06.2021.

Obszar drugi dotyczy działań celowych pracownika. Należy tutaj sprecyzować pojęcie „celowości". Może ono bowiem mieć wymiar złośliwy: handlu informacjami, współpracy z cyberprzestępcą, której motywacją jest niezadowolenie z obecnego stanowiska pracy lub chęć zemsty na pracodawcy. Może również wynikać z regularnego szpiegostwa gospodarczego, podyktowanego chęcią dodatkowego zysku, działalnością dywersyjną lub sabotażową. Może również dotyczyć działań, o których pracownik wie, że są ryzykowne i niebezpieczne, a mimo to im ulega (np. pracownik zapisze hasło na karteczce, a następnie umieści ją w pobliżu komputera z nadzieją, że nikt inny jej nie użyje)[9].

Zagrożenia dla informacji powodowane czynnikiem ludzkim są szczególnie widoczne w okresie obecnej pandemii. Praca zdalna, wykonywana z sieci prywatnych pracowników, brak nadzoru nad sprzętem komputerowym i zachowaniem osób wykorzystujących zasoby informacyjne przedsiębiorstw skutkuje zwiększeniem prób nielegalnego pozyskania informacji. Według raportu opublikowanego przez Sophos[10] wynika, że średnie, kwartalne wypłaty okupu za odszyfrowanie informacji po atakach typu Ransomware wzrosły w okresie od 4 kwartału 2019 roku do 3 kwartału 2020 roku trzykrotnie. W raporcie zatytułowanym „Global Security Insights Report 2021. Extended enterprise under threat"[11] ujawniono, że aż 78% globalnych specjalistów ds. cyberbezpieczeństwa stwierdziło, że liczba ataków wzrosła z powodu pracowników pracujących zdalnie, a 79% stwierdziło, że ataki stały się bardziej wyrafinowane.

Badania dotyczące bezpieczeństwa informacji, uwzględniające czynnik ludzki

Wiedza o cyberbezpieczeństwie i zrozumienie pracowników w organizacji gospodarczej jest tak samo ważne jak każda wprowadzana polityka

[9] R.A. Maalem Lahcen, B. Caulkins, R. Mohapatra, M. Kumar, *Review*…, dz. cyt.
[10] Sophos, *Sophos 2021 Threat Report: Navigating cybersecurity in an uncertain world*, s. 8, https://nakedsecurity.sophos.com/2020/11/18/sophos-threat-report-2021/, data dostępu: 27.06.2021.
[11] Vmware, Global Security Insights Report. Extended enterprise under threat 2021, https://www.carbonblack.com/resources/global-security-insights-report-2021/, data dostępu: 27.06.2021.

zabezpieczeń i przeprowadzana kontrola[12]. Według raportu firmy Proofpoint[13]:

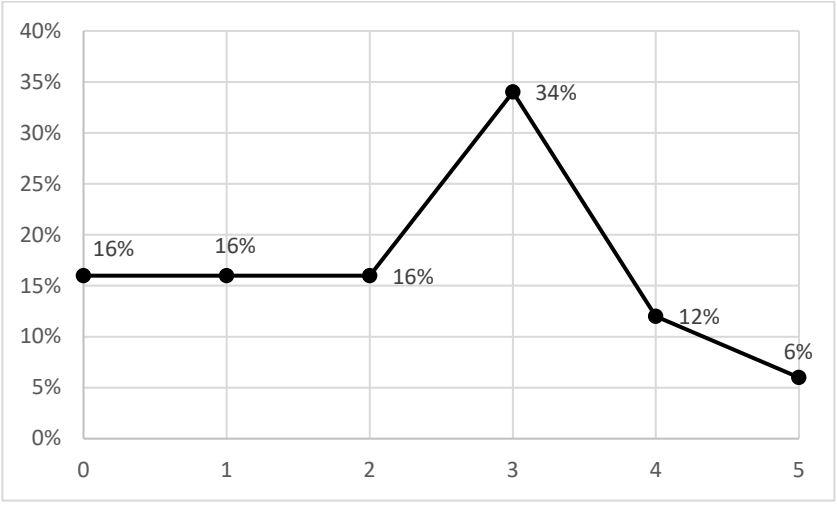
- ponad 99% zaobserwowanych zagrożeń wymagało interakcji człowieka – włączenia makra, otwarcia pliku, skorzystania z łącza lub otwarcia dokumentu;
- do ataków wykorzystywane są osoby, których wybrane dane są powszechnie dostępne na stronach organizacji, portalach społecznościowych lub łatwo odszukiwane za pomocą przeglądarki Google; są to osoby zajmujące zazwyczaj wysokie stanowiska, mające dostęp do określonych zasobów informacyjnych;
- oszuści internetowi naśladują prawdziwe procedury biznesowe, np. poprzez odzwierciedlanie legalnych wzorców ruchu poczty email: najwięcej wiadomości rozsyłanych jest w początkowych dniach tygodnia, a znikoma ich ilość w weekendy;
- oszuści dostosowują się do kultury pracy i zwyczajów panujących w określonych regionach świata. Preparują odpowiednio wiadomości e-mail i wysyłają je w określonych porach dnia; na przykład pracownicy z regionu Azji i Pacyfiku oraz Ameryki Północnej znacznie częściej czytają pocztę wcześnie rano, podczas gdy użytkownicy z Bliskiego Wschodu i Europy częściej odczytują wiadomości w środku dnia i po obiedzie;
- oszuści wykorzystują ludzką ciekawość i niepewność; działania phishingowe są zazwyczaj nakierowane na aktualne w danym okresie tematy, wzbudzają w użytkownikach chęć interakcji (klikania w linki, udzielania odpowiedzi).

Powyższe dane skłaniają do wysunięcia wniosku, że podmioty gospodarcze powinny zwracać szczególną uwagę na bezpieczeństwo swoich zasobów niematerialnych. Przy tym uwzględnić muszą przede wszystkim poziom kompetencji, doświadczenia i wyszkolenia swoich pracowników w zakresie ochrony informacji. Celem powinny być organizowane cykliczne szkolenia w zakresie cyberbezpieczeństwa, które w zamierzeniu mają na celu podnoszenie świadomości pracowników w kwestii aktualnych zagrożeń

[12] A. Cosgrove, *How Identifying your 'Very Attacked People' Can Bolster Your Cybersecurity Strategy*. 2020, Netherlands, https://orangecyberdefense.com/nl/blog/partner/how-identifying-your-very-attacked-people-can-bolster-your-cybersecurity-strategy/, data dostępu: 28.06.2021.
[13] Exclusive Networks, Proofpoint, *Human Factor Report 2019. Exclusive Networks*, Sweden, 2019, https://www.exclusive-networks.com/se/proofpoint-human-factor-report-2019/, data dostępu: 28.06.2021.

oraz stosowanych powszechnie działań socjotechnicznych. Niezbędne wydaje się wprowadzanie i udoskonalanie polityk bezpieczeństwa, których egzekwowaniem powinny zająć się specjalnie powołane w tym celu jednostki (korporacje, przedsiębiorstwa duże) lub określone osoby (przedsiębiorstwa średnie i małe).

Z badań przeprowadzonych przez firmę Norstat Polska na próbie 100 organizacji gospodarczych: małych, średnich i dużych (wykres 1), opublikowanych przez KPMG[14], wynika, że tylko 6% planuje znaczące, a 12% duże inwestycje w obszarze podnoszenia świadomości pracowników w zakresie bezpieczeństwa. Aż 16% nie planuje żadnych wydatków w tym zakresie, a małe lub bardzo małe wydatki planuje łącznie 32% (wskazania 1 i 2 w skali Likerta). Średniej wielkości wydatki zadeklarowało 34% respondentów.

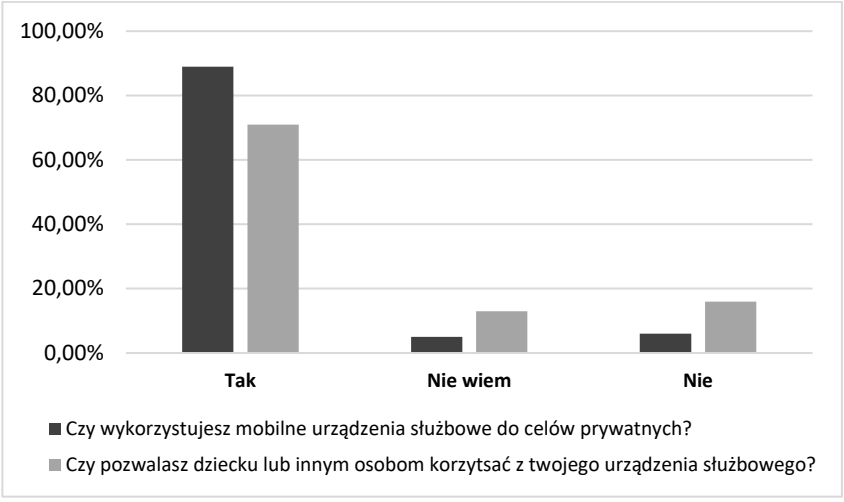


Wykres 1. Poziom planowanych inwestycji przedsiębiorstw w programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa, gdzie 5 oznacza znaczące inwestycje, a wartość 0 – brak inwestycji
Źródło: opracowanie własne na podstawie badań KPMG, *Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych*, 2020, s. 16, https://dl.ptwp.pl/4WmgWxNmNk/raport-kpmg-barometr-cyberbezpieczenstwa-2020.pdf, data dostępu: 28.06.2021.

Uzyskane wyniki świadczą o tym, że przedsiębiorstwa wciąż nie dostrzegają istniejącego ryzyka związanego z czynnikiem ludzkim. Tym

[14] KPMG, *Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych*, 2020, https://dl.ptwp.pl/4WmgWxNmNk/raport-kpmg-barometr-cyberbezpieczenstwa-2020.pdf, data dostępu: 28.06.2021.

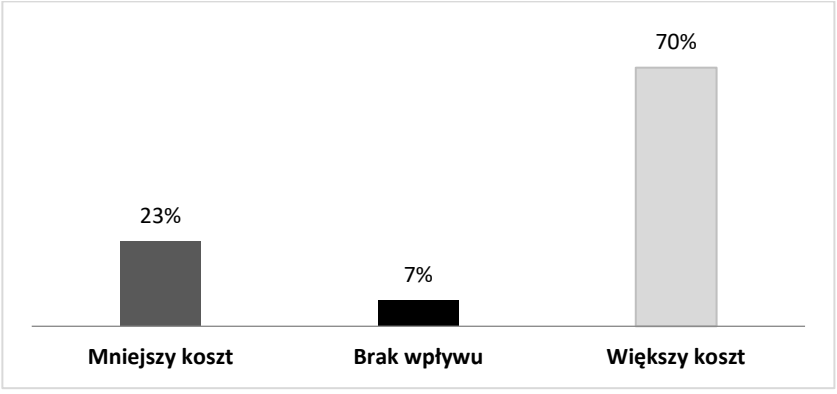
samym potwierdzają się wyniki analizy literaturowej, prezentowanej w poprzednim rozdziale, które stwierdzają, że czynnik ludzki nadal jest obszarem, któremu nie poświęca się należytej uwagi. Być może wynikiem takiego stanowiska podmiotów gospodarczych jest przeświadczenie o wysokich kompetencjach własnych pracowników lub zbytnie przecenianie posiadanej ochrony technologicznej. Niestety wyniki przedstawione przez KPMG nie udzielają odpowiedzi na to pytanie. Badanie zostało przeprowadzone w styczniu 2020 roku, a więc przed okresem wzmożonej pracy zdalnej. Być może nabyte przez przedsiębiorstwa w trakcie pandemii doświadczenia, zmienią stosunek do inwestycji w tym zakresie. Niestety w chwili pisania niniejszego tekstu autor nie dotarł do tego typu badań. Można jednak wspierać się badaniami, które powinny w pewnym zakresie wzbudzić zainteresowanie wśród decydentów planowanych inwestycji. Na wykresie 2 przedstawiono badania dotyczące zachowania użytkowników względem służbowych urządzeń komputerowych – wpisujących się więc w realia obszaru pracy zdalnej. Wynika z nich, że aż 89% osób wykorzystuje mobilne urządzenia służbowe do celów prywatnych, a 71% pozwala osobom trzecim na korzystanie z urządzeń służbowych. Są to wyniki, które powinny wzbudzić co najmniej obawy wśród właścicieli i mocodawców w podmiotach gospodarczych.



Wykres 2. Zachowania użytkowników względem służbowych urządzeń komputerowych
Źródło: opracowanie własne na podstawie K. Gawkowski, *Polski barometr cyberbezpieczeństwa społecznego 2019*, a&s Polska, https://aspolska.pl/polski-barometr-cybebezpieczenstwa-spolecznego-2019/, data dostępu: 28.06.2021.

Wykorzystanie urządzeń służbowych do celów prywatnych niesie ryzyko przypadkowego udostępnienia zasobów poprzez instalację nieznanego pod względem bezpieczeństwa oprogramowania lub zainfekowania urządzenia poprzez złośliwe oprogramowanie podczas korzystania z prywatnych kont social mediów, komunikatorów oraz przeglądania przypadkowych stron internetowych. Podobne zagrożenia istnieją przy udostępnianiu urządzeń osobom trzecim, które nieświadomie mogą przyczynić się do utraty lub udostępnienia poufnych informacji.

Przedstawione na wykresie 2 wyniki w pewnym stopniu korelują z badaniami dotyczącymi prognozowanych kosztów ponoszonych przez przedsiębiorstwa związane z naruszeniem ochrony danych podczas pracy zdalnej (wykres 3).



Wykres 3. Jak praca zdalna wpłynęłaby na koszty naruszenia ochrony danych
Źródło: opracowanie własne na podstawie: Ponemon Institute, *Raport z badania kosztów naruszeń ochrony danych 2020*, s. 65, https://www.ibm.com/pl-pl/security/data-breach, data dostępu: 28.06.2021.

Według badania opublikowanego w 2020 roku przez IBM Security[15] aż 70% respondentów stwierdziło, że koszty naruszenia ochrony informacji będą większe, 23% zadeklarowało spadek kosztów, a 7% nie widzi wpływu pracy zdalnej na wysokość szkód finansowych z powodu naruszenia bezpieczeństwa informacji. Przedsiębiorstwa wobec tego zdają sobie sprawę z wpływu czynnika ludzkiego (w tym przypadku za sprawą zmiany formy pracy) na bezpieczeństwo zasobów niematerialnych. Pozostaje wobec tego założyć, że wystąpienie potencjalnych strat finansowych zmusi podmioty

[15] Ponemon Institute, *Raport z badania kosztów naruszeń ochrony danych 2020*, s. 65, https://www.ibm.com/pl-pl/security/data-breach, data dostępu: 28.06.2021.

gospodarcze do bardziej wnikliwej analizy własnej polityki wobec eliminacji zagrożeń powodowanych przez człowieka.

Zakończenie

Poziom współczesnych zabezpieczeń technologicznych, wdrażanych zgodnie z ogólnie przyjętymi normami i procedurami, zapewnia podmiotom wysoki stopień bezpieczeństwa informacji. Osoby lub grupy osób (cyberprzestępcy), którzy chcą pozyskać nielegalnie określone zasoby niematerialne uciekają się więc do działań pozatechnicznych – wykorzystujących pracownika, określanego w literaturze przedmiotu jako najsłabszy „element" systemu bezpieczeństwa informacji. Poziom rozwoju inżynierii społecznej oraz coraz nowszych sposobów wykorzystywania człowieka do pozyskania informacji wymuszają na przedsiębiorstwach wdrażanie programów przeciwdziałających potencjalnym zagrożeniom i zwiększających kompetencje i doświadczenie własnych pracowników. Jak próbowano wykazać w rozdziale, brak działań w tym zakresie może doprowadzić do sytuacji, w których podmioty gospodarcze będą ponosiły duże koszty związane z usuwaniem skutków naruszeń lub sytuacji, w których działalność przedsiębiorstw po utracie kluczowych zasobów informacji oraz utracie reputacji nie będzie dalej możliwa. Czynnik ludzki odpowiada obecnie za większość istniejących naruszeń bezpieczeństwa. Po analizie publikacji naukowych, popularnonaukowych oraz raportów największych wywiadowni na świecie można przyjąć, że sytuacja ta nie ulegnie zmianie w najbliższej przyszłości.

Bibliografia

Ani U.D., He H., Tiwari A., *Human factor security: Evaluating the cybersecurity capacity of the industrial workforce*, „Journal of Systems and Information Technology" 2019, 21(1).

Corradini I., Nardelli E., *Social Engineering and the Value of Data: The Need of Specific Awareness Programs*, [w:] *Advances in Human Factors in Cybersecurity*, T. Ahram, W. Karwowski (red.), Springer International Publishing, New York 2020.

Cosgrove A., *How Identifying your 'Very Attacked People' Can Bolster Your Cybersecurity Strategy*. 2020, Netherlands, https://orangecyberdefense.com/nl/blog/partner/how-identifying-your-very-attacked-people-can-bolster-your-cybersecurity-strategy/, data dostępu: 28.06.2021.

Desolda G., Di Nocera F., Ferro L., Lanzilotti R., Maggi P., Marrella A., *Alerting Users About Phishing Attacks*, [w:] *HCI for Cybersecurity, Privacy and Trust*, A. Moallem (red.), Springer International Publishing, New York 2019.

Exclusive Networks, Proofpoint, *Human Factor Report 2019. Exclusive Networks*, Sweden 2019, https://www.exclusive-networks.com/se/proofpoint-human-factor-report-2019/, data dostępu: 28.06.2021.

Gawkowski K., *Polski Barometr Cyberbezpieczeństwa Społecznego 2019*, a&s Polska, https://aspolska.pl/polski-barometr-cybebezpieczenstwa-spolecznego-2019/, data dostępu: 28.06.2021.

Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S., Baker T., *Security threats to critical infrastructure: The human factor*, „The Journal of Supercomputing" 2018, 74(10).

Haycock K., Matthews J.R., *Persuasive Advocacy*, „Public Library Quarterly" 2016, 35(2).

Hughes-Lartey K., Li M., Botchey F.E., Qin Z., *Human factor, a critical weak point in the information security of an organization's Internet of things*, „Heliyon" 2021, 7(3).

Jain A.K., Gupta B.B., *A survey of phishing attack techniques, defence mechanisms and open research challenges*, „Enterprise Information Systems" 2021.

Jeimy J., Cano M., *The Human Factor in Information Security*, „ISACA Journal", 2019, nr 5, https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security, data dostępu: 28.06.2021.

KPMG, *Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych*, 2020, https://dl.ptwp.pl/4WmgWxNmNk/raport-kpmg-barometr-cyberbezpieczenstwa-2020.pdf, data dostępu: 28.06.2021.

Maalem Lahcen R.A., Caulkins B., Mohapatra R., Kumar M., *Review and insight on the behavioral aspects of cybersecurity*, „Cybersecurity" 2020.

Mitnick K.D., Simon W.L., *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, Hoboken 2003.

Moraph, *Human Factors in Cyber Security*, 2020, http://34.234.138.24/human-factors-in-cyber-security/, data dostępu: 27.06.2021.

Newseria Biznes, *W 2025 roku na świecie przechowywanych będzie 180 zettabajtów danych. Najszybciej produkują je firmy, ale wciąż mają problemy z ich gromadzeniem i wykorzystywaniem*, 2021, http://biznes.newseria.pl/news/w-2025-roku-na-swiecie,p1512315547, data dostępu: 28.06.2021.

Ponemon Institute, *Raport z badania kosztów naruszeń ochrony danych 2020,* https://www.ibm.com/pl-pl/security/data-breach, data dostępu: 28.06.2021.

Proofpoint, Inc., *2020 User Risk Report. Exploring Vulnerability and Behaviour in a People-Centric Threat Landscape*, https://az659834.vo.msecnd.net/ event sairaueprod/production-aisa-public/442f8d3ebe7445049ca67e2e7d20f348, data dostępu: 27.06.2021.

Salihovic I., Serdarevic H., Kevric J., *The Role of Feature Selection in Machine Learning for Detection of Spam and Phishing Attacks*, [w:] *Advanced Technologies, Systems, and Applications III*, S. Avdaković (red.), Springer International Publishing, New York 2019.

Schneier B., *Schneier on Security*. John Wiley & Sons, Hoboken, New Jersey 2009.

Sophos, *Sophos 2021 Threat Report: Navigating cybersecurity in an uncertain world*, https://nakedsecurity.sophos.com/2020/11/18/sophos-threat-report-2021/, data dostępu: 27.06.2021.

Vmware, *Global Security Insights Report. Extended enterprise under threat 2021*, https://www.carbonblack.com/resources/global-security-insights-report-2021/, data dostępu: 27.06.2021.