UWZGLĘDNIENIE KWESTII BEZPIECZEŃSTWA I HIGIENY PRACY W OCENIE RYZYKA W CYBERPRZESTRZENI

Abstrakt

W niniejszym dokumencie omówiono nową perspektywę, badając związek między zagrożeniami cyberbezpieczeństwa a zdrowiem i bezpieczeństwem pracowników. Wymaga to odejścia od tradycyjnego postrzegania cyberbezpieczeństwa, skupiającego się wyłącznie na aspektach technicznych, i rozszerzenia zakresu dyskusji na konsekwencje cyberataków dla ludzi i całych społeczeństw.

Biorąc pod uwagę coraz powszechniejsze stosowanie technologii cyfrowej we wszystkich organizacjach oraz wzrost liczby ataków na systemy i sieci komputerowe tych organizacji, należy rozważyć nowe, pojawiające się zagrożenia dla zdrowia i bezpieczeństwa pracowników. Bezpieczeństwo i higiena pracy (BHP) musi być dostosowane do nowych potrzeb i wyzwań w nadchodzących latach.

Sytuacja dotycząca cyberbezpieczeństwa

W ciągu ostatnich kilku lat kwestia cyberbezpieczeństwa stała się głównym tematem dyskusji wszystkich przedsiębiorstw we wszystkich sektorach. Cyberprzestępczość staje się coraz bardziej wyrafinowana, a cyberprzestępcy wykorzystują do swoich ataków wszystkie rodzaje luk w zabezpieczeniach – fizyczne, techniczne i dotyczące człowieka.

W słowniku Cambridge Dictionary cyberatak zdefiniowano jako „nielegalną próbę uszkodzenia czyjegoś systemu komputerowego lub znajdujących się w nim informacji przy użyciu internetu”[1]. Dokładniej rzecz ujmując, według NIST (Narodowego Instytutu Standaryzacji i Technologii) cyberatak to „atak, za pośrednictwem cyberprzestrzeni, ukierunkowany na wykorzystanie cyberprzestrzeni przez przedsiębiorstwo w celu zakłócenia, wyłączenia, zniszczenia lub kontrolowania w złej wierze środowiska komputerowego/infrastruktury bądź zniszczenia integralności danych lub kradzieży informacji kontrolowanych”[2].

W coraz bardziej cyfrowym świecie każde przedsiębiorstwo narażone jest na ryzyko cyberataku. W szczególności rok 2020 stanowił przełomowy moment zarówno w kwestii cyfryzacji, jak i cyberbezpieczeństwa. Przedsiębiorstwa coraz częściej stosują podejścia organizacyjne oparte na elastyczności i technologii umożliwiające pracę zdalną, głównie ze względu na pandemię COVID-19, ale stanowi to również żyzny grunt dla cyberprzestępców, do tego stopnia, że 78% organizacji doświadczyło wzrostu liczby cyberataków z powodu przejścia na pracę zdalną[3].

87% organizacji na całym świecie zostało narażonych na próbę wykorzystania istniejącej luki w zabezpieczeniach, a 71% specjalistów ds. bezpieczeństwa odnotowało wzrost liczby zagrożeń cyberbezpieczeństwa (phishing, złośliwe oprogramowanie, oprogramowanie szantażujące) od wybuchu pandemii COVID-19[4].

Ogólnie rzecz biorąc, cyberataki stale się nasilają, nie tylko pod względem liczby, ale także pod względem skutków (ENISA, 2021a), a poszczególne państwa dysponują różnymi zasobami i narzędziami służącymi do zarządzania kwestią cyberbezpieczeństwa. Na przykład na podstawie konkretnych czynników, takich jak zaangażowanie w kwestię cyberbezpieczeństwa i przepisy, trzy państwa europejskie (Portugalia, Litwa i Słowacja) sklasyfikowano jako posiadające najwyższy wskaźnik cyberbezpieczeństwa[5].

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/
[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/

Rozszerzający się krajobraz zagrożeń sprawił, że Komisja Europejska musi pilnie wdrożyć skuteczną strategię UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[6], aby zagwarantować bezpieczną cyfryzację poprzez zwiększenie odporności, budowanie zdolności w zakresie zapobiegania cyberincydentom i reagowania na nie oraz określenie spójnej międzynarodowej polityki w dziedzinie cyberbezpieczeństwa. Ponadto w strategii tej podkreślono znaczenie programu mającego na celu zwiększenie świadomości wszystkich instytucji, organów i agencji UE w zakresie cyberbezpieczeństwa, aby stworzyć skuteczną kulturę cyberbezpieczeństwa.

Obecne i przyszłe zagrożenia

Przewiduje się, że do 2025 r. koszty związane z cyberprzestępczością na świecie osiągną 10,5 bln USD rocznie[7]. W rzeczywistości cyberprzestrzeń jest wykorzystywana przez różne podmioty do szkodliwych celów i z różnych pobudek – od cyberprzestępców, których główną motywacją jest zysk finansowy, po cyberterrorystów, którzy kierują się celami politycznymi i ideologicznymi. Przestępczość w internecie jest bardzo zróżnicowana i obejmuje wiele nielegalnych działań – znanych już w świecie fizycznym – takich jak kradzież tożsamości, nadużycia finansowe, szpiegostwo, przestępstwa związane z własnością intelektualną, a także różne formy cyberprzemocy (np. uporczywe nękanie (stalking) lub nękanie). Działania te mogą opierać się na potężnych zasobach, jakie zapewnia kontekst cyfrowy, a ze względu na coraz większą liczbę wzajemnych połączeń na świecie cyberprzestępczość będzie stanowiła jedno z głównych zagrożeń w ciągu następnych dwóch dziesięcioleci[8].

Cyberbezpieczeństwo stanowi priorytet dla każdej organizacji i dla każdego państwa ze względu na różnorodność i dotkliwość konsekwencji: od utraty cennych informacji po paraliż systemów komputerowych i związanych z nimi usług, a także poważne zagrożenia dla zdrowia i bezpieczeństwa ludzi.

Mimo że o niektórych rodzajach zagrożeń cyberbezpieczeństwa (tabela 1), takich jak phishing i oprogramowanie szantażujące, wiadomo od lat, ich liczba wciąż rośnie[9]. W rzeczywistości są one bardzo opłacalne dla cyberprzestępców, a koszt ich wykonania jest bardzo niski w porównaniu z ryzykiem złapania sprawców ataku (Hernandez-Castro i in., 2020). Phishing pozostaje jedną z głównych taktyk naruszania bezpieczeństwa (Verizon, 2021), ale różne formy cyberataków uwidaczniają złożoność krajobrazu zagrożeń cyberbezpieczeństwa. Na przykład ataki w ramach łańcucha dostaw są coraz częstsze i w przyszłości będą stanowiły poważny problem dla organizacji (ENISA, 2021b)[10].

Tabela 1: Rodzaje najczęstszych zagrożeń cyberbezpieczeństwa[11]

Rodzaj	Opis
Phishing i spear phishing (phishing ukierunkowany)	Phishing to praktyka polegająca na wysyłaniu oszukańczych wiadomości, które wydają się pochodzić z wiarygodnego źródła, zazwyczaj za pośrednictwem poczty elektronicznej. Ich celem jest kradzież danych wrażliwych, takich jak dane dotyczące kart kredytowych i logowania, lub zainstalowanie złośliwego oprogramowania na komputerze ofiary. Istnieją różne formy phishingu, np. spear phishing, czyli bardziej wyrafinowana odmiana phishingu ukierunkowana na konkretną osobę lub organizację.

[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/
[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] Łańcuch dostaw to „połączenie ekosystemu zasobów niezbędnych do zaprojektowania, wyprodukowania i dystrybucji produktu". W obszarze cyberbezpieczeństwa łańcuch dostaw obejmuje sprzęt i oprogramowanie, przechowywanie w chmurze lub lokalnie oraz mechanizmy dystrybucji https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Są to jedne z najczęstszych zagrożeń cyberbezpieczeństwa zgłaszanych przez ENISA (2020; 2021). Opis zagrożeń można znaleźć również w https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Rodzaj	Opis
Złośliwe oprogramowanie i oprogramowanie szantażujące	Złośliwe oprogramowanie to szeroki termin określający oprogramowanie szpiegujące, oprogramowanie szantażujące, wirusy i robaki komputerowe. Na przykład oprogramowanie szantażujące to forma złośliwego oprogramowania, które szyfruje informacje dotyczące ofiary i żąda zapłaty w zamian za klucz deszyfrujący. Jest ono jednym z najbardziej lukratywnych rodzajów cyberataków.
Inżynieria społeczna	Inżynieria społeczna to technika stosowana do oszukiwania ludzi i manipulowania nimi w celu uzyskania informacji poufnych lub dostępu do ich komputerów. Phishing jest przykładem inżynierii społecznej.
Odmowa usługi (DoS)	Ten rodzaj ataku przeciąża systemy, serwery lub sieci, zapełniając je tak dużą liczbą plików, że system nie jest w stanie spełnić uzasadnionych żądań. Sprawcy ataku mogą również wykorzystać wiele zainfekowanych urządzeń do przeprowadzenia tego ataku (DDos, rozproszony atak typu „odmowa usługi").
Naruszenie ochrony danych	Naruszenie ochrony danych to cyberincydent, w trakcie którego informacje zostają skradzione, pobrane z systemu lub wykorzystane bez upoważnienia.
Cyberszpiegostwo	Celem cyberszpiegostwa jest kradzież wrażliwych lub niejawnych danych albo własności intelektualnej w celu uzyskania przewagi nad konkurencyjnym przedsiębiorstwem lub podmiotem rządowym.
Dezinformacja i kampanie przekazywania informacji wprowadzających w błąd	Dezinformacja polega na celowym tworzeniu i rozpowszechnianiu nieprawdziwych informacji w celu wyrządzenia szkody. Przekazywanie informacji wprowadzających w błąd polega na rozpowszechnianiu nieprawdziwych lub niedokładnych informacji w sposób przypadkowy. Mogą one stanowić etap przygotowujący do przeprowadzenia innych ataków (takich jak inżynieria społeczna i phishing) i być wykorzystywane razem z innymi zagrożeniami cyberbezpieczeństwa.

Paradoks polega na tym, że z jednej strony innowacyjne technologie mogą być wykorzystywane do tworzenia nowych rozwiązań służących poprawie cyberbezpieczeństwa; z drugiej strony te same technologie stwarzają dalsze możliwości dla samych cyberprzestępców. Dlatego oprócz pozytywnego wykorzystania sztucznej inteligencji, np. do wykrywania włamań i identyfikacji złośliwego oprogramowania (Truong i in., 2020), pojawiają się nowe zagrożenia, a znane zagrożenia stają się coraz poważniejsze (Brundage i in., 2018). Na przykład technologie sztucznej inteligencji mogą być wykorzystywane do automatyzacji ataków w ramach inżynierii społecznej, a także do zwiększania skuteczności złośliwego oprogramowania. Ponadto rozpowszechnienie urządzeń wykorzystujących koncepcję internetu rzeczy tworzy kolejne luki w zabezpieczeniach, z którymi trzeba się zmierzyć, ponieważ mają one mniejsze możliwości przetwarzania i przechowywania danych, co ogranicza zabezpieczenia niezbędne do ich ochrony[12].

Szczególne sytuacje związane z pracą zwiększają możliwości działania cyberprzestępców. Na przykład praca zdalna, powszechnie przyjęta w 2020 r. ze względu na pandemię COVID-19, spowodowała powstanie nowych wyzwań w zakresie bezpieczeństwa dla przedsiębiorstw, na przykład powstanie większej liczby punktów końcowych, które mogą być podatne na naruszenia bezpieczeństwa, oraz

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/

wykorzystywanie urządzeń osobistych do działań związanych z pracą (BYOD – posługiwanie się własnym sprzętem)[13]. W rzeczywistości łatwość znalezienia wszystkiego na jednym urządzeniu wiąże się ze znacznymi zagrożeniami dla bezpieczeństwa, gdy na przykład nierozważne zachowania związane z prywatnym użytkowaniem urządzeń cyfrowych mają również zastosowanie w sytuacji służbowej (Disterer i Kleiner, 2013). Nie wspominając o tym, że utrata urządzenia cyfrowego oznacza narażenie na ryzyko nie tylko danych osobistych, lecz również danych dotyczących przedsiębiorstwa. Praca zdalna stanowi zatem wyzwanie w zakresie bezpieczeństwa dla przedsiębiorstw, które muszą zmienić swoje strategie korporacyjne i zainwestować w solidne szkolenia dla telepracowników (Borkovich i Skovira, 2020).

Interesujące jest również to, że sami pracownicy korzystający z urządzeń do noszenia na ciele (takich jak bezprzewodowe słuchawki douszne lub inteligentne zegarki) mogą być nieświadomymi wektorami dla cyberprzestępców. W rzeczywistości technologie ubieralne stwarzają pewne zagrożenia dla cyberbezpieczeństwa, np. w przypadku urządzeń podłączonych do służbowego laptopa, które mogą wprowadzać wirusy do systemu przedsiębiorstwa, a także zagrożenia dla prywatności spowodowane nieuprawnionym dostępem (Heembrock, 2015).

Inne pojawiające się zagrożenia cyberbezpieczeństwa stanowią dodatkowe źródło obaw zarówno dla osób prywatnych, jak i przedsiębiorstw, ze względu na efekt wzmocnienia, jaki zapewniają media społecznościowe. Deepfake to na przykład cyfrowo zmienione nagranie wideo lub plik audio przedstawiające konkretne osoby – często celebrytów lub polityków – przygotowane do złych celów, takich jak rozpowszechnianie nieprawdziwych informacji i narażanie na szwank ich reputacji. Jednak obawy związane z tymi zagrożeniami wykraczają poza propagandę i wybory polityczne, ponieważ mogą one również wpływać na przedsiębiorstwa poprzez manipulację na rynku, sabotaż marki, szantaż i cyfrowe podszywanie się pod członka zarządu (Westerlund, 2019).

Wreszcie, biorąc pod uwagę imponujący rozwój innowacji technologicznych, szacuje się, że jeszcze przed 2025 r. informatyka kwantowa, w ramach której można przetwarzać informacje znacznie wydajniej niż przy zastosowaniu tradycyjnych metod, może być łatwo dostępna[14]. Teoretycznie komputery te mogłyby złamać wiele dzisiejszych systemów szyfrowania zabezpieczeń, ale aby technologia ta mogła mieć praktyczne zastosowanie, konieczny jest znaczny postęp technologiczny[15].

Z opisanego przed chwilą scenariusza jasno wynika, dlaczego ryzyko w cyberprzestrzeni zajmuje wysoką pozycję wśród innych globalnych zagrożeń (WEF, 2021).

Wpływ cyberataków na BHP

Cyberataki na przedsiębiorstwa i instytucje zawsze były analizowane z technologicznego punktu widzenia, mimo że czynnik ludzki stanowi równie ważną część kwestii cyberbezpieczeństwa (Corradini i in., 2020). Podobnie, analizując wpływ cyberataków, koncentrujemy się przede wszystkim na aspektach ekonomicznych (Cashell i in., 2004; Anderson i in., 2013), a rzadko na zdrowiu i bezpieczeństwie pracowników. W rzeczywistości wpływ ten mierzy się głównie w kategoriach kosztów materialnych, takich jak utrata danych i przerwa w działalności gospodarczej, oraz kosztów niematerialnych, takich jak utrata przewagi konkurencyjnej związana z utratą własności intelektualnej oraz uszczerbek na reputacji marki[16].

W rzeczywistości cyberataki mogą potencjalnie prowadzić do urazów, problemów psychologicznych lub utraty życia: jest zatem jasne, że ocena ryzyka w cyberprzestrzeni i ocena ryzyka w zakresie BHP w miejscu pracy nie mogą być traktowane jako odrębne działania, ale muszą być wykonywane razem (Izuakor, 2016). W związku z tym przedsiębiorstwa powinny brać pod uwagę różne skutki związane z zagrożeniami cyberbezpieczeństwa i przyjąć bardziej kompleksowe podejście do optymalizacji zarządzania ryzykiem związanym z cyberbezpieczeństwem (Couce-Vieira i in., 2020), jak na przykład opisano w tabeli 2.

[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/
[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution
[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html

Tabela 2: Różne skutki dla zarządzania ryzykiem związanym z cyberbezpieczeństwem

Kategorie	Skutki
Organizacja	Szkody ekonomiczne (takie jak mniejsza produkcja związana z niedostępnością usługi, utrata udziału w rynku lub utrata przewagi konkurencyjnej)
	Uszczerbek na reputacji (spadek zaufania zainteresowanych stron)
	Inne aspekty ekonomiczne (np. ubezpieczenie na wypadek cyberataków)
Pracownicy	Uszczerbek na zdrowiu (np. utrata życia w wyniku awarii systemu cyberfizycznego)
	Uszczerbek na zdrowiu psychicznym (np. lęk lub frustracja)
	Wpływ na prawa osobiste (naruszenie prywatności wynikające z naruszenia ochrony danych)
	Osobiste szkody ekonomiczne
Inne powiązane organizacje	Szkody wynikające z zakłóceń w powiązaniach w ramach globalnego łańcucha dostaw
Środowisko	Wpływ na środowisko naturalne (np. zanieczyszczenie terenu w wyniku cyberincydentu)

Źródło: Couce-Vieira i in., 2020

Skutki te mogą być związane z kosztami mierzalnymi w ujęciu pieniężnym, takimi jak utrata udziału w rynku, oraz niepieniężnym, takimi jak uszczerbek na zdrowiu fizycznym lub psychicznym.

W dalszej części omówione zostanie znaczenie ewentualnego fizycznego i psychologicznego wpływu na zdrowie i bezpieczeństwo pracowników.

Aspekty związane z cyberbezpieczeństwem

Niewystarczające uwzględnienie aspektów związanych z cyberbezpieczeństwem można przypisać postrzeganiu zagrożeń cyberbezpieczeństwa jako zagrożeń zewnętrznych, podczas gdy kwestie zdrowia i bezpieczeństwa rozwiązywane są w ramach organizacji[17]. Jednak rozwój zagrożeń cyberbezpieczeństwa i coraz większe narażenie organizacji na cyberataki wymaga przyjęcia holistycznego podejścia do skutecznego zarządzania nimi, obejmującego także ochronę zdrowia i bezpieczeństwa pracowników.

Cyberataki mogą zagrozić nie tylko zasobom informacyjnym organizacji, lecz również zdrowiu fizycznemu i psychicznemu pracowników, gdy hakerzy zaatakują infrastrukturę krytyczną[18] lub przejmą kontrolę nad ich urządzeniami technicznymi. Manipulowanie urządzeniem może na przykład wyrządzić fizyczną krzywdę osobom fizycznym i narazić na szwank bezpieczeństwo danych osobowych (Loukas, 2019).

Kwestię tę można wyjaśnić na podstawie kilku przykładów. W 2014 r. w Niemczech włamano się do huty stali, a sprawcom ataku udało się wyłączyć piec[19]. Ryzyko przekształcenia cyberataku w zdarzenie krytyczne dotyczące bezpieczeństwa pracowników było bardzo wysokie ze względu na charakter materiałów, których dotyczył atak.

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/
[18] Infrastruktura krytyczna ma zasadnicze znaczenie dla funkcjonowania danego państwa, ponieważ obejmuje takie sektory, jak energetyka, zdrowie publiczne, telekomunikacja, bankowość i finanse.
[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

W 2017 r. amerykański Urząd ds. Żywności i Leków (FDA) wycofał z rynku około 465 tys. rozruszników serca z powodu luk w zabezpieczeniach. Urządzenia te były narażone na hakowanie, co zagrażało życiu pacjentów[20].

Cyberataki na przemysłowe systemy sterowania (ICS), które obejmują zarówno elementy cybernetyczne, jak i fizyczne, stanowią znaczne zagrożenie dla życia ludzkiego. Przykładem może być Stuxnet[21], robak komputerowy stworzony w 2010 r. w celu przejęcia kontroli nad irańskimi wirówkami służącymi do wzbogacania uranu, lub złośliwe oprogramowanie Triton[22], które w 2017 r. zostało wykorzystane w zakładach petrochemicznych na Bliskim Wschodzie, co na szczęście zakończyło się niepowodzeniem. Tego typu ataki mogą mieć również poważne skutki dla środowiska.

Zdalne korzystanie ze sprzętu w niebezpiecznych sytuacjach może zagrażać bezpieczeństwu pracowników, np. w przypadku pojazdów lub maszyn działających poza kontrolą z powodu zakłóceń sygnałów bezprzewodowych lub ataków hakerów (Steijn i in., 2016).

W sektorze produkcji, w którym ludzie i roboty współpracują ze sobą na liniach produkcyjnych, cyberataki mogą zakłócać fizyczne procesy przemysłowe i narażać pracowników na obrażenia (Perales Gómez i in., 2020).

Według przedsiębiorstwa Gartner do 2025 r. sprawcy cyberataku mogą wykorzystać technologię operacyjną i inne systemy cyberfizyczne, aby skutecznie szkodzić ludziom lub ich zabijać[23].

Przeprowadzając cyberatak na szpitale, hakerzy mogą uzyskać dostęp do wszystkich informacji szczególnie chronionych dotyczących pacjentów i pracowników, ale tym, co może zostać poważnie zagrożone, jest możliwość zapewnienia pacjentom właściwej opieki i wykonywania niezbędnych operacji medycznych (Argaw i in., 2020)[24]. Analiza globalnego ataku „WannaCry" z użyciem oprogramowania szantażującego w maju 2017 r. wykazała znaczące negatywne skutki dla brytyjskiej krajowej służby zdrowia (Ghafur i in., 2019).

Podczas pandemii COVID-19 amerykańskie szpitale stały się celem fali ataków z użyciem oprogramowania szantażującego, które spowodowały przerwanie opieki zdrowotnej w kilku z nich, co wiązało się z poważnym zagrożeniem życia pacjentów[25]. Badania, których głównym przedmiotem jest wykorzystanie oprogramowania szantażującego przeciwko organizacjom opieki zdrowotnej, wskazują, że te zagrożenia cyberbezpieczeństwa mogą mieć konsekwencje zagrażające życiu lub powodujące śmierć (Ponemon, 2021).

Skutki społeczne i psychologiczne

Cyberataki mogą wywoływać skutki społeczne, takie jak utrata zaufania do technologii cyfrowych, oraz psychologiczne, takie jak lęk, gniew i depresja (Bada i Nurse, 2020). Pracownicy będący ofiarami cyberataków mogą również czuć się zawstydzeni, winni, zdezorientowani lub sfrustrowani, zwłaszcza w przypadku wycieku informacji cyfrowych, a znaczenie tych skutków zależy od środowiska związanego z cyberatakiem (Agrafiotis i in., 2018). Na przykład w instytucji finansowej, gdzie konsekwencje naruszenia ochrony danych są prawdopodobnie bardziej dotkliwe niż w innej instytucji świadczącej usługi, szkody psychologiczne pracowników mogą być większe. W bardziej ekstremalnych przypadkach konsekwencją wycieku danych może być samobójstwo poszkodowanych osób –

[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362
[21] https://spectrum.ieee.org/the-real-story-of-stuxnet
[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/
[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece
[24] W 2020 r. niemiecki szpital padł ofiarą cyberataku, który uniemożliwił przyjmowanie pacjentów. Kobieta, która została tam przewieziona na leczenie, zmarła w drodze do następnego szpitala oddalonego o ponad 30 km. Po przeprowadzeniu dochodzenia prokuratorzy uznali, że dowody są niewystarczające, ale wiadomo, że szpitalny oddział ratunkowy został zamknięty z powodu ataku z użyciem oprogramowania szantażującego. https://www.wired.co.uk/article/ransomware-hospital-death-germany
25 https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

ponieważ publiczne ujawnienie informacji na ich temat jest odczuwane jako tak haniebne[26], że obciążenie psychiczne odczuwane przez pracowników może być bardzo trudne do zniesienia.

Dlatego też prywatność i bezpieczeństwo są coraz bardziej ze sobą powiązane; podczas gdy prywatność odnosi się do gromadzenia i wykorzystywania danych osobowych, bezpieczeństwo ma na celu zagwarantowanie ochrony tych danych[27]. W ogólnym rozporządzeniu o ochronie danych (RODO), które weszło w życie 25 maja 2018 r., na organizacje nakłada się obowiązek ochrony danych i prywatności w UE[28], a w przypadku naruszenia ochrony danych, które stwarza ryzyko dla praw i wolności użytkowników, przedsiębiorstwa mają maksymalnie 72 godziny na powiadomienie osób dotkniętych naruszeniem.

Interesująca jest obserwacja, w jaki sposób naruszenie prywatności może mieć negatywny wpływ na zdrowie psychiczne poszczególnych osób. Prywatność jest w istocie potrzebą psychologiczną ściśle związaną z rozwojem tożsamości osobistej (Aboujaoude, 2019).

Badania dotyczące wiktymizacji w wyniku cyberprzestępczości podkreślają negatywne doświadczenia zarówno przedsiębiorstw, jak i poszczególnych osób (na przykład Augustina, 2015 oraz McGuire i Dowling, 2013). Szczególnie w przypadku ataków z użyciem oprogramowania szantażującego zespoły informatyczne odczuwają skutki w postaci spadku zaufania zawodowego i utraty wysokiego uznania dla wykwalifikowanych pracowników[29]. Ponadto ataki z użyciem oprogramowania szantażującego mogą mieć większy wpływ psychologiczny na emocje pracowników niż inne cyberincydenty, ponieważ płacąc okup, przedsiębiorstwa „nagradzają" sprawców ataku, zamiast inwestować pieniądze w rozwój swojego personelu[30].

Dalsze rozważania można poczynić w odniesieniu do błędu ludzkiego, uważanego za główną przyczynę 90% przypadków naruszenia cyberbezpieczeństwa[31]. Błędy te, takie jak otwieranie wiadomości phishingowych lub zaniedbywanie zarządzania hasłami, mogą narazić organizacje na poważne konsekwencje, takie jak przypadkowe zainstalowanie złośliwego oprogramowania w sieci przedsiębiorstwa. Łatwo można sobie wyobrazić uczucie porażki, jakiego doświadczają pracownicy odpowiedzialni za to, co się stało, co może ich także powstrzymywać przed zgłoszeniem błędu organizacji.

Jeśli chodzi o błędy ludzkie, ważne jest, aby wziąć pod uwagę czynniki psychologiczne związane z cyberincydentami: 52% pracowników popełnia błędy, gdy są zestresowani, 43% – gdy są zmęczeni, a 26% – gdy czują się wypaleni[32]. Nie wspominając o tym, że specjaliści ds. cyberbezpieczeństwa doświadczają wysokiego poziomu stresu lub wypalenia zawodowego w związku z pracą nad zapobieganiem skutkom cyberataków i ich ograniczaniem [33]..

Wreszcie, nawiasem mówiąc, warto obserwować, jak wymiar cybernetyczny wpływa również na zjawiska przemocy. Na przykład cyberprzemoc jest najbardziej znaną formą nękania w sieci (Notar i in., 2013), której celem jest upokorzenie, prześladowanie i kontrolowanie danej osoby przy użyciu środków cyfrowych. Mimo że zjawisko to nie jest ściśle związane z cyberbezpieczeństwem, ataki takie jak te z użyciem złośliwego oprogramowania i kradzież tożsamości mogą być wykorzystywane do szkodzenia ludziom. Nękanie w sieci może wywołać poważne skutki psychosomatyczne, społeczne i psychiczne (Dressing i in., 2014; Betts, 2016). Dlatego, biorąc pod uwagę, że cyberprzemoc w miejscu pracy (Corradini, 2019; Farley i in., 2021) może zagrażać zdrowiu i bezpieczeństwu pracowników, należy odpowiednio zająć się tą kwestią.

Cel cyberataków

[26] Ashley Madison, serwis randkowy, do którego włamano się w lipcu 2015 r., to dramatyczny przypadek, jeśli chodzi o konsekwencje. Dane ujawnione przez hakerów obejmowały nazwiska, hasła, adresy, a także informacje o pragnieniach seksualnych klientów. Po tym naruszeniu ochrony danych doszło do rezygnacji z pracy, rozwodów i samobójstw. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

[28] https://gdpr.eu/tag/gdpr/

[29] https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

[30] https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

[31] https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

[32] https://www.tessian.com/research/the-psychology-of-human-error/

[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021

Technologia innowacyjna jest obecna w każdym sektorze działalności. Wszystkie organizacje – zarówno mikro, małe i średnie przedsiębiorstwa (MŚP), jak i duże przedsiębiorstwa – mogą być celem cyberprzestępców, a tym samym są narażone na cyberataki. Wiele mikro- i małych przedsiębiorstw nie dysponuje zasobami niezbędnymi do ich ochrony, o czym świadczy fakt, że 43% wszystkich przypadków naruszenia ochrony danych dotyczy mikro- i małych przedsiębiorstw (Verizon, 2019).

Jest oczywiste, że w coraz bardziej cyfrowym świecie przedsiębiorstwa są coraz bardziej połączone ze sobą, co zwiększa powierzchnię ataku.

Jeśli chodzi o sektory najbardziej narażone na cyberataki, według raportu IBM Security 2021 w 2020 r. najbardziej atakowanymi branżami były finanse i ubezpieczenia (23% ataków), a następnie produkcja (17,7%), energetyka (11,1%), handel detaliczny (10,2%), zawody regulowane (8,7%), administracja rządowa (7,9%), opieka zdrowotna (6,6%), media (5,7%), transport (5,1%) i edukacja (4,0%).

Obserwując rozwój sektorów padających ofiarą cyberataków, w badaniach podkreśla się, że sektor opieki zdrowotnej staje się bardzo atrakcyjnym celem dla cyberprzestępców[34], zwłaszcza ze względu na informacje szczególnie wrażliwe przechowywane w dokumentacji medycznej (Martin i in., 2017). Pandemia COVID-19 pogorszyła sytuację, w związku z czym cyberprzestępcy zwrócili uwagę na własność intelektualną wykorzystywaną do opracowywania szczepionek (Muthuppalaniappan i Stevenson, 2021) i zaczęli wykorzystywać wiadomości phishingowe o tematyce związanej z COVID-19[35]. Sektor opieki zdrowotnej uległ jednak znacznym zmianom w wyniku walki z pandemią i zgodnie z perspektywami na przyszłość musi wzmocnić swoje zabezpieczenia[36].

Nawet organizacje edukacyjne stają się atrakcyjnym celem dla cyberprzestępców, biorąc pod uwagę, że w 2020 r. 44% z nich zostało zaatakowanych z użyciem oprogramowania szantażującego, a 35% z nich zapłaciło okup, aby odzyskać swoje dane[37]. Przyczyn takiego stanu rzeczy należy upatrywać w ograniczonych budżetach przeznaczonych na zapewnienie cyberbezpieczeństwa oraz w dużej liczbie użytkowników, takich jak studenci i pracownicy, którzy mogą być bardziej narażeni na ataki. Co więcej, brak świadomości cyfrowej wśród nauczycieli i uczniów wymaga wprowadzenia programów szkoleniowych w zakresie odpowiedzialnego korzystania z technologii cyfrowych (Corradini i Nardelli, 2020).

Bieżąca sytuacja w zakresie cyberataków stale się zmienia, dlatego konieczne jest monitorowanie zmian z roku na rok. W tym czasie zarysowuje się bardziej niepokojący obraz. Podmioty produkujące oprogramowanie szantażujące testują nowe metody wymuszania okupu, co skłania organizacje do współpracy i wymiany informacji w celu reagowania na zagrożenia[38].

Czynniki ryzyka wiktymizacji

Cyberprzestępcy są bardziej zainteresowani atakami na przedsiębiorstwa z wykorzystaniem skradzionych haseł niż przeprowadzaniem masowych ataków w poszukiwaniu informacji dotyczących konsumentów[39]. Jednak w 2020 r. 330 mln osób dorosłych w 10 państwach padło ofiarą cyberprzestępczości[40], nie wspominając o tym, że działania ukierunkowane na konkretnych pracowników, na przykład poprzez spear phishing, mogą być skuteczną strategią uzyskania dostępu do ich organizacji.

Ryzyko stania się ofiarą różnych form cyberprzestępczości zależy zarówno od czynników osobistych, jak i środowiskowych (Jansen i in., 2017), a badania profili ofiar mogą pomóc w jak najlepszym zrozumieniu związku między cyberatakami a pochodzeniem ofiar.

Na przykład analizując ofiary cyberprzestępstw z różnych pokoleń, wydaje się, że młodzi dorośli (poniżej 25 roku życia) i najstarsi (75 lat i więcej) są bardziej narażeni na cyberataki[41]. Płeć stanowi ważny czynnik wpływający na zachowania związane z cyberbezpieczeństwem (Anwar i in., 2017),

[34] https://cybersecurityguide.org/industries/healthcare/
[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home
[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective
[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/
[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021
[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport
[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report

chociaż dalsze badania w tym obszarze – i badania dotyczące cech demograficznych – mogą być bardzo interesujące z punktu widzenia działań zapobiegawczych. Niektóre badania wykazały, że kobiety są bardziej narażone na ataki typu phishing (Darwish i in., 2012), podczas gdy inne ujawniają, że kobiety bardziej niż mężczyźni obawiają się o swoją prywatność w serwisach społecznościowych (Tifferet, 2019).

Wreszcie, biorąc pod uwagę potrzebę zwiększania odporności środowiska miejsca pracy na zagrożenia cyberbezpieczeństwa, interesujące wydaje się przeanalizowanie, w jaki sposób czynniki organizacyjne, takie jak normy i rutyny, wpływają na podatność pracowników na wiadomości phishingowe i spear phishingowe (Williams i in., 2018). Taka szeroka analiza mogłaby dostarczyć przydatnych spostrzeżeń w celu udoskonalenia projektowania interfejsów i programów podnoszenia świadomości pracowników.

Kompleksowe podejście do kwestii cyberbezpieczeństwa: rola świadomości

Związek między zagrożeniami cyberbezpieczeństwa a zdrowiem i bezpieczeństwem stanowi wysoce dynamiczne wyzwanie dla organizacji, które muszą wykorzystać wszystkie niezbędne środki w ramach ogólnego podejścia korporacyjnego do kwestii cyberbezpieczeństwa[42].

Perspektywa ta wymaga połączenia aspektów dotyczących bezpieczeństwa i ochrony, które zwykle traktowane są jako odrębne pojęcia, ze względu na różne granice prawne, interesy i kwestie praktyczne (Boustras i Waring, 2020).

Dla osiągnięcia tego celu kluczową kwestią jest świadomość różnych zainteresowanych stron, którą należy rozwijać z punktu widzenia ściśle ze sobą powiązanych cyberbezpieczeństwa i BHP.

Jeśli chodzi o zagadnienia dotyczące cyberbezpieczeństwa, w badaniach podkreśla się, że mała zgodność z zasadami bezpieczeństwa i inne czynniki organizacyjne, takie jak niewystarczające środki reagowania, sprawiają, że organizacje są narażone na cyberataki (Hart, 2019). Ponadto, niezależnie od różnorodności sektorów pracy, brak świadomości pracowników w zakresie cyberbezpieczeństwa jest przyczyną wielu cyberincydentów[43]. W związku z tym programy podnoszenia świadomości w zakresie cyberbezpieczeństwa mogą odegrać ważną rolę w rozwijaniu skutecznej kultury cyberbezpieczeństwa w organizacjach (Corradini, 2020) i zapobieganiu cyberatakom (Aldawood i Skinner, 2018).

Rozwijanie świadomości możliwych konsekwencji cyberataków w obszarze BHP wymaga rozszerzenia uwagi na źródła ryzyka, które tradycyjnie nie są brane pod uwagę w odniesieniu do zdrowia i bezpieczeństwa pracowników. Pozytywne doświadczenia związane z zarządzaniem ryzykiem w zakresie BHP mogą również stanowić doskonałe źródło inspiracji, biorąc pod uwagę fakt, że w porównaniu z cyberbezpieczeństwem tematyka bezpieczeństwa i higieny pracy w organizacjach opiera się na wieloletnim doświadczeniu, a wiele aplikacji i programów służących tworzeniu bezpieczniejszych środowisk pracy jest nadal z powodzeniem wdrażanych. Ponadto zarządzanie błędami ludzkimi jest uważane za kluczowe dla zapobiegania wypadkom w dziedzinie BHP.

Co więcej, biorąc pod uwagę, że służby/departamenty/eksperci ds. bezpieczeństwa informatycznego zazwyczaj nie mają wiedzy na temat BHP, a społeczność BHP nie ma wiedzy na temat zagrożeń cyberbezpieczeństwa, współpraca między tymi dwoma obszarami ma zasadnicze znaczenie. Na przykład, o ile to możliwe, współpraca między działami ds. bezpieczeństwa w zakresie BHP, zasobów ludzkich i IT w organizacji może umożliwić spojrzenie na kwestię zagrożeń cyberbezpieczeństwa z różnych perspektyw i wdrożenie skuteczniejszych, bardziej innowacyjnych rozwiązań w zakresie zapobiegania.

Podnoszenie świadomości wśród zainteresowanych stron

Biorąc pod uwagę powyższe rozważania, pierwszym krokiem jest uwrażliwienie różnych zainteresowanych stron na zagrożenia w zakresie BHP wynikające z zagrożeń cyberbezpieczeństwa, tak aby skłonić te zainteresowane strony do odpowiedzialnego działania.

[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511
[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

Programy podnoszenia świadomości mogą być niezwykle przydatne, ale aby były skuteczne, muszą być dobrze opracowane i dostosowane do konkretnych sytuacji, a także odpowiednie dla różnych zainteresowanych stron. Powinny one także obejmować zestaw narzędzi i metod, takich jak kampanie, warsztaty, konferencje, materiały edukacyjne i inne działania informacyjne. Ponadto, biorąc pod uwagę specyfikę mikroprzedsiębiorstw i MŚP oraz ich ograniczone zasoby, należy wprowadzić specjalne inicjatywy, aby im pomóc.

W programach podnoszenia świadomości powinny uczestniczyć co najmniej następujące wewnętrzne i zewnętrzne zainteresowane strony.

- **Pracodawcy**, którzy są prawnie odpowiedzialni za bezpieczeństwo i zdrowie swoich pracowników, a także **kadra kierownicza**, odgrywają pierwszoplanową rolę w organizacjach. Zgodnie z prawem dotyczącym BHP pracodawcy mają wiele obowiązków w zakresie ochrony swoich pracowników przed wszelkimi zagrożeniami związanymi z pracą oraz skutecznego zarządzania tymi zagrożeniami. Ponieważ zagrożenia cyberbezpieczeństwa mogą mieć wpływ na zdrowie i bezpieczeństwo pracowników, należy je wyraźnie uwzględnić w działaniach związanych z zapobieganiem ryzyku w zakresie BHP i zarządzaniem nim.
- **Pracownicy** muszą być informowani o wszelkich zagrożeniach dla ich bezpieczeństwa i zdrowia, na jakie mogą być narażeni podczas wykonywania pracy, a ryzyko w cyberprzestrzeni powinno zaliczać się do tych zagrożeń: oczywiste jest zatem, że zapewnienie pracownikom informacji i szkoleń w tym zakresie jest podstawowym środkiem zapobiegawczym.
- **Specjaliści ds. BHP** powinni być zaangażowani w inicjatywy mające na celu podnoszenie świadomości, ponieważ na ogół nie mają wiedzy na temat cyberbezpieczeństwa. Mogą oni odgrywać kluczową rolę w zapobieganiu wpływowi cyberataków na zdrowie i bezpieczeństwo pracowników i powinni być na bieżąco informowani o zmianach organizacyjnych i względnych zagrożeniach cyberbezpieczeństwa.
- **Inspektoraty pracy.** Nowe wyzwania związane z zagrożeniami cyberbezpieczeństwa w zakresie BHP będą prawdopodobnie wymagały nowych metod i narzędzi związanych z funkcjami pełnionymi przez inspektoraty pracy. Świadomość zagrożeń w zakresie BHP związanych z cyberbezpieczeństwem ma zatem zasadnicze znaczenie zarówno ze względu na ich rolę w kontroli, jak i zapobieganiu.
- **Kierownicy ds. bezpieczeństwa informatycznego.** Często nie mają oni wiedzy na temat zagadnień związanych z cyberbezpieczeństwem, ponieważ ze względu na charakter swojej pracy koncentrują się głównie na bezpieczeństwie sieci i danych oraz na projektowaniu skutecznej polityki informatycznej swojej organizacji i zarządzaniu nią. Podniesienie ich świadomości na ten temat może pomóc w zachęceniu do współpracy z ekspertami ds. BHP oraz uwzględnieniu dodatkowej perspektywy w określaniu przepisów i praktyk dotyczących bezpieczeństwa w organizacjach.

Biorąc pod uwagę przyszłe rozszerzenie zagrożeń cyberbezpieczeństwa na bezpieczeństwo w miejscu pracy, inne zainteresowane strony powinny być świadome wpływu cyberbezpieczeństwa na BHP oraz wnieść wkład w strategie zapobiegania. Wśród nich są na przykład eksperci w dziedzinie interakcji człowiek-komputer (HCI) oraz twórcy oprogramowania.

HCI to multidyscyplinarna dziedzina nauki, początkowo skupiona na interakcji między użytkownikami a komputerami, a obecnie obejmująca wiele form projektowania technologii informacyjnych[44]. Biorąc pod uwagę, że sprzęt roboczy będzie w coraz większym stopniu połączony w sieć, właściwe zaprojektowanie interfejsu HCI przez ekspertów w tej dziedzinie będzie miało kluczowe znaczenie dla zminimalizowania wpływu na cyberbezpieczeństwo i BHP (Korfmacher, 2019).

Podobnie ważną rolę mogą odegrać **twórcy oprogramowania**, zważywszy, że coraz większa część osób pracujących, zarówno w domu, jak i zdalnie, wykonuje swoje obowiązki za pomocą systemów oprogramowania. Dlatego ważne jest, aby zwiększyć świadomość twórców oprogramowania na temat wpływu cyberataków na bezpieczeństwo i zdrowie pracowników, aby zapewnić staranne projektowanie i realizację tych systemów pod kątem ich zdolności do ochrony przed zagrożeniami

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction

cyberbezpieczeństwa, co będzie miało pozytywny wpływ na dobrostan pracowników, którzy będą czuć się chronieni przed atakami.

Podsumowując, najważniejszym zaleceniem jest zaangażowanie **ekspertów w dziedzinie zachowań ludzkich** w opracowywanie i wdrażanie programów podnoszenia świadomości w zakresie cyberbezpieczeństwa. W rzeczywistości pomyślność takich inicjatyw zależy od motywacji uczestników, a także od metod i narzędzi wykorzystywanych do ich realizacji. Potrzebne są zatem odpowiednie kompetencje i wiedza na temat zachowań ludzkich.

Wreszcie, cyberbezpieczeństwo jest przede wszystkim kwestią dotyczącą człowieka. Dlatego do skutecznego zarządzania tą kwestią coraz bardziej potrzebne będą zespoły interdyscyplinarne dysponujące umiejętnościami technicznymi oraz ludzkimi i społecznymi.

Kolejne kroki

Przyszłe badania powinny dotyczyć przede wszystkim wzajemnych powiązań między dwoma omawianymi obszarami – cyberbezpieczeństwem i BHP. Określenie potrzeb i luk pomoże zidentyfikować potencjalne zagrożenia dla pracowników związane z cyberatakami, a także określić odpowiednie strategie polityczne i strategie zapobiegania w organizacjach. W literaturze omówiono już interesujące powiązania między bezpieczeństwem a ochroną, na przykład pozytywny związek między kulturą bezpieczeństwa, satysfakcją z pracy i zgodnymi z przepisami zachowaniami w zakresie bezpieczeństwa (Green i D'Arcy, 2010).

Istniejące badania dotyczące związku między cyberbezpieczeństwem a zagrożeniami cyberbezpieczeństwa dotyczą zasadniczo sektora opieki zdrowotnej (na przykład Martin i in., 2017) oraz pojazdów autonomicznych (na przykład Taeihagh i Lim, 2019), trzeba natomiast przeprowadzić więcej badań, aby wyjaśnić wszystkie możliwe skutki cyberataków dla zdrowia i bezpieczeństwa pracowników w każdym sektorze pracy.

Ponadto, biorąc pod uwagę fakt, że systemy wbudowane będą w przyszłości coraz powszechniejsze, konieczne będzie zapewnienie odpowiedniej integracji między bezpieczeństwem a ochroną. W rzeczywistości systemy te można zaprojektować tak, aby zarówno reagowały na cele związane z bezpieczeństwem (takie jak ataki hakerów), jak i gwarantowały funkcje bezpieczeństwa, zapobiegając szkodom dla użytkowników (pracowników). Integracja bezpieczeństwa i ochrony jest głównym tematem związanym z rozwojem systemów o znaczeniu krytycznym[45], a normy międzynarodowe mogą stanowić użyteczne wsparcie dla organizacji[46].

Na koniec można przyjąć, że w przyszłości jeszcze bardziej rozpowszechnione będą hybrydowe formy pracy – łączące pracę w domu z pracą biurową – oraz inteligentne środowiska pracy oparte na technologiach internetu rzeczy i systemach cyberfizycznych (Podgórski i in., 2017). W związku z tym organizacje będą musiały aktualizować swoją ocenę ryzyka, aby zidentyfikować wszelkie potencjalne zagrożenia dla pracowników i podjąć odpowiednie działania. W tym celu konieczne będzie wdrożenie nowych metod i narzędzi.

Wnioski

Transformacja cyfrowa to proces, którego nie da się powstrzymać. Towarzyszy mu kilka wyzwań, z którymi każde państwo musi się zmierzyć. Obecnie cyberbezpieczeństwo stanowi ogromny problem dla przedsiębiorstw i instytucji niezależnie od ich wielkości i sektora, w którym działają, a w przyszłości problem ten będzie narastał.

Zarządzania cyberbezpieczeństwem nie można jednak sprowadzać do samej tylko technologicznej ochrony systemów i informacji. Ponieważ cyberataki mogą mieć również wpływ na zdrowie i bezpieczeństwo pracowników, organizacje powinny przyjąć holistyczne podejście do cyberbezpieczeństwa. Osiągnięcie tego celu wymaga **przyjęcia multidyscyplinarnej wizji łączącej kompetencje techniczne i społeczne** w celu radzenia sobie z różnymi skutkami zagrożeń cyberbezpieczeństwa.

[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/

[46] Zob. np. ISO/TR 22100-4, Bezpieczeństwo maszyn – Związek z ISO 12100 – Część 4: Wytyczne dla producentów maszyn dotyczące uwzględnienia powiązanych aspektów bezpieczeństwa informatycznego (cyberbezpieczeństwa); IEC TR 63074:2019 „Bezpieczeństwo maszyn – aspekty dotyczące bezpieczeństwa związane z bezpieczeństwem funkcjonalnym systemów sterowania związanych z bezpieczeństwem”.

W przypadku dużych organizacji współpraca między działami ds. bezpieczeństwa informatycznego i BHP jest wysoce zalecana w celu określenia innowacyjnego procesu oceny ryzyka, aby chronić aktywa materialne i niematerialne, a przede wszystkim ludzi. Jednocześnie jednym z głównych tematów jest sposób wdrażania skutecznych strategii dla mikroprzedsiębiorstw i MŚP, które często nie dysponują specjalnymi wewnętrznymi zasobami[47], a mimo to są narażone na skutki zagrożeń cyberbezpieczeńswa.

To bardzo trudne wyzwanie na przyszłość. Na dobry początek należy najpierw opracować solidny i szeroko zakrojony program mający na celu podniesienie świadomości w tych tematach, aby przygotować pracodawców, pracowników i społeczność BHP, a także kierowników ds. bezpieczeństwa informatycznego i inne odpowiednie podmioty – takie jak eksperci w dziedzinie HCI, twórcy oprogramowania i eksperci w dziedzinie zachowań ludzkich – na coraz bardziej cyfrowy scenariusz i rozwój zagrożeń cyberbezpieczeństwa.

Autorzy: Isabella Corradini, dyrektor naukowy Centrum Badawczego Themis (Włochy),

Zarządzanie projektem: Emmanuelle Brun, Annick Starren, we współpracy z Aną Cayuelą, Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy (EU-OSHA).

Niniejszy dokument do dyskusji przygotowano na zlecenie Europejskiej Agencji Bezpieczeństwa i Zdrowia w Pracy (EU-OSHA). Za jego treść, w tym za wszelkie wyrażone w nim opinie lub wnioski, odpowiadają wyłącznie autorzy, a streszczenie niekoniecznie odzwierciedla poglądy EU-OSHA.

Tłumaczenie wykonane przez Centrum Tłumaczeń (CdT, Luksemburg), na podstawie oryginału w języku angielskim.

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

Bibliografia

Aboujaoude, E. (2019), Protecting privacy to protect mental health: The new ethical imperative [Ochrona prywatności w trosce o zdrowie psychiczne: nowy imperatyw etyczny], *Journal of Medical Ethics*, *45*(9), s. 604–607.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. i Upton, D. (2018), A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate [Taksonomia zagrożeń cyberbezpieczeństwa: określenie skutków cyberataków i zrozumienie sposobu ich rozprzestrzeniania się], *Journal of Cybersecurity*, *4*(1).

Aldawood, H. i Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review [Edukacja i podnoszenie świadomości na temat inżynierii społecznej w zakresie cyberbezpieczeństwa: przegląd literatury], [w:] Międzynarodowa Konferencja IEEE poświęcona Nauczaniu, Ocenie i Uczeniu Się do celów Inżynierii (TALE), IEEE, s. 62–68.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. i Savage, S. (2013), Measuring the cost of cybercrime [Pomiar kosztów cyberprzestępczości], [w:] R. Böhme (red.), *The economics of information security and privacy [Ekonomia bezpieczeństwa i prywatności informacji],* (s. 265–300), Springer-Verlag.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. i Xu, L. (2017), Gender difference and employees' cybersecurity behaviors [Różnice w traktowaniu kobiet i mężczyzn a zachowania pracowników w zakresie cyberbezpieczeństwa], *Computers in Human Behavior*, 69, s. 437–443.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. i Flahault, A. (2020), Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks [Cyberbezpieczeństwo szpitali: omówienie wyzwań i działanie na rzecz ograniczenia ryzyka], *BMC Medical Informatics and Decision Making, 20*(146).

Augustina, J. R. (2015), Understanding cyber victimization: Digital architectures and the disinhibition effect [Zrozumienie wiktymizacji w cyberprzestrzeni: architektury cyfrowe i efekt zahamowania], *International Journal of Cyber Criminology*, *9*(1), s. 35–54.

Bada, M. i Nurse, J. R. C. (2020), The social and psychological impact of cyber-attacks, psychology [Społeczny i psychologiczny wpływ cyberataków, psychologia], [w:] V. Benson i J. Mcalaney (red.), *Emerging cyber threats and cognitive vulnerabilities [Nowe zagrożenia cybernetyczne i luki poznawcze],* (s. 73–92), Academic Press.

Betts, L. R. (2016), Cyberbullying: Approaches, consequences, and interventions [Cyberprzemoc: podejścia, konsekwencje i interwencje], [w:] J. Binder (red.), *Palgrave studies in Cyberpsychology* [Studia Palgrave w dziedzinie cyberpsychologii], Palgrave Macmillan.

Borkovich, D. J. i Skovira, R. J. (2020), Working from home: Cybersecurity in the age of covid-19 [Praca z domu: cyberbezpieczeństwo w dobie pandemii COVID-19], *Issues in Information Systems*, *21*(4), s. 234–236.

Boustras, G. i Waring, A. (2020), Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context [W kierunku ponownej konceptualizacji kwestii bezpieczeństwa i ochrony, ich wzajemnych oddziaływań oraz wymogów polityki w kontekście XXI wieku], *Safety Science*, s. 132.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. i in. (2018), *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation* [Złośliwe wykorzystanie sztucznej inteligencji: prognozowanie, zapobieganie i łagodzenie skutków], https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Cashell, B., Jackson, W. D., Jickling, M. i Webel, B. (2004), The Economic Impact of Cyber-Attacks [Wpływ cyberataków na gospodarkę], *CRS Report for Congress [Raport CRS dla Kongresu]*.

Corradini, I. (2020), *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology [Budowanie kultury cyberbezpieczeństwa w organizacjach: jak zmniejszyć przepaść między ludźmi a technologią cyfrową],* Springer.

Corradini, I. (2019), *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking,* Themis.

Corradini, I., Nardelli, E. i Ahram, T. (red.) (2020), *Advances in human factors in cybersecurity* [Postępy w stosowaniu czynników ludzkich w cyberbezpieczeństwie], AHFE 2020, Advances in Intelligent Systems and Computing [Postępy w zakresie inteligentnych systemów i informatyki kwantowej], tom 1219, Springer.

Corradini, I. i Nardelli, E. (2020), Developing digital awareness at school: A fundamental step for cybersecurity education [Rozwijanie świadomości cyfrowej w szkole: podstawowy krok w edukacji w zakresie cyberbezpieczeństwa], [w:] I. Corradini, E. Nardelli i T. Ahram (red.), *Advances in human factors in cybersecurity* [Postępy w stosowaniu czynników ludzkich w cyberbezpieczeństwie], AHFE 2020, Advances in intelligent systems and computing [Postępy w zakresie inteligentnych systemów i informatyki kwantowej], tom 1219, Springer.

Couce-Vieira, A., Insua, D. R. i Kosgodagan, A. (2020), Assessing and forecasting cybersecurity impacts [Ocena i prognozowanie skutków w zakresie cyberbezpieczeństwa], *Decision Analysis, 17*(4), s. 356–374.

Darwish, A., El Zarka, A. i Aloul, F. (2012), Towards understanding phishing victims' profile [W kierunku zrozumienia profilu ofiar phishingu], *International Conference on Computer Systems and Industrial Informatics* [Międzynarodowa Konferencja poświęconaSystemom Komputerowym i Informatyce Przemysłowej], s. 1–5.

Disterer, G. i Kleiner, C. (2013), BYOD – Bring Your Own Device [BYOD – posługiwanie się własnym sprzętem], *HMD*, 50, s. 92–100.

Dressing, H., Bailer, J., Anders, A., Wagner, A. i Gallas, C. (2014), Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims [Cyberstalking w dużej próbie użytkowników portali społecznościowych: częstość występowania, charakterystyka i wpływ na ofiary], *Cyberpsychology, Behavior, and Social Networking,* 17: s. 61–67.

ENISA (2020), *Threat Landscape 2020 [Krajobraz zagrożeń 2020]*. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA (2021a), Threat Landscape 2021 [Krajobraz zagrożeń 2021], 27 października 2021 r. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b), Threat Landscape for Supply Chain Attacks [Krajobraz zagrożeń w przypadku ataków w ramach łańcucha dostaw], 29 lipca 2021 r. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Farley, S., Coyne, I. i D'Cruz, P. (2021), Cyberbullying at Work: Understanding the influence of technology [Cyberprzemoc w miejscu pracy: zrozumienie wpływu technologii], [w:] P. D'Cruz, E. Noronha, G. Notelaers i C. Rayner (red.), *Handbooks of workplace bullying, emotional abuse and harassment [Podręczniki dotyczące nękania w miejscu pracy, niegodziwego traktowania w sferze emocjonalnej i nękania]*, tom 1, Springer.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. i Aylin, P. (2019), A retrospective impact analysis of the WannaCry cyberattack on the NHS [Retrospektywna analiza wpływu cyberataku WannaCry na krajową służbę zdrowia], *NPJ Digital Medicine*, *2*(98).

Hamlyn-Harris, J. H. (2017), *Three reasons why pacemakers are vulnerable to hacking [Trzy powody, dla których rozruszniki serca są narażone na ataki hakerów],* The Conversation, http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

Hart, D. V. (2019), Factors influencing the adoption of cybersecurity situational awareness programs [Czynniki wpływające na przyjęcie programów świadomości sytuacyjnej w zakresie cyberbezpieczeństwa], *Isaca Journal*, https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

Heembrock, M. (2015), The risks of wearable tech in the workplace [Zagrożenia związane z technologią ubieralną w miejscu pracy], *Risk Management Magazine,* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

Hernandez-Castro, J., Cartwright, A. i Cartwright, E. (2020), An economic analysis of ransomware and its welfare consequences [Ekonomiczna analiza oprogramowania szantażującego i jego skutków dla dobrostanu], Royal Society Open Science, 7(3), 190023.

Izuakor, C. (2016), Understanding the impact of cyber security risks on safety [Zrozumienie wpływu zagrożeń cyberbezpieczeństwa na bezpieczeństwo], ICISSP 2016 – II Międzynarodowa Konferencja poświęcona Systemom Informacyjnym, Bezpieczeństwu i Prywatności.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. i van der Zee, S. (2017), Victims [Ofiary], [w:] R. Leukfeldt (red.), *Research agenda. The human factor in cybercrime and cybersecurity [Program badań. Czynnik ludzki w cyberprzestępczości i cyberbezpieczeństwie]*, Eleven International Publishing.

Kavallieratos, G., Katsikas, S. i Gkioulos, V. (2020), Cybersecurity and Safety Co-Engineering of Cyberphysical Systems-A Comprehensive Survey [Współinżynieria systemów cyberfizycznych w zakresie cyberbezpieczeństwa i bezpieczeństwa – kompleksowe badanie], *Future Internet*, *12*(4), s. 65.

Korfmacher, S. (2019), The relevance of cybersecurity for functional safety and HCI [Znaczenie cyberbezpieczeństwa dla bezpieczeństwa funkcjonalnego i HCI], [w:] V. Duffy (red.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science [Cyfrowe modelowanie ludzkie i zastosowania w dziedzinie zdrowia, bezpieczeństwa, ergonomii i zarządzania ryzykiem – ciało ludzkie i ruch HCII 2019, notatki z wykładu* z informatyki*]*, 11581, Springer.

Loukas, G. (2019, listopad), Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0 [Cyberfizyczne zagrożenia bezpieczeństwa dotyczące bezpieczeństwa i higieny pracy (BHP) w Przemyśle 4.0], https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A. i Kinross, J. (2017), Cybersecurity and healthcare: How safe are we? [Cyberbezpieczeństwo i opieka zdrowotna: Jak bardzo jesteśmy bezpieczni?], *British Medical Journal* (red. Clinical research), 358, j3179.

McGuire, M. i Dowling, S. (2013), Cybercrime: A review of the evidence. Summary of key findings and implications [Cyberprzestępczość: przegląd dowodów. Podsumowanie kluczowych ustaleń i skutków] (Home Office Research Report, s. 75), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Muthuppalaniappan, M. i Stevenson, K. (2021), Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health [Cyberataki w służbie zdrowia i pandemia COVID-19: poważne zagrożenie dla zdrowia na świecie], *International Journal for Quality in Health Care*, *33*(1).

Notar, C. E., Padgett, S. i Roden, J. (2013), Cyberbullying: A review of the literature [Cyberprzemoc: przegląd literatury], *Universal Journal of Educational Research, 1*(1), s. 1–9.

Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., García Clemente, F.J., Gil Pérez, M. i Martínez Pérez, G. (2020), SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry [SafeMan: ujednolicone ramy zarządzania cyberbezpieczeństwem i bezpieczeństwem w przemyśle wytwórczym], *Software: Practice and Experience*, *51(3),* s. 607–627.

Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G. i Okrasa, M. (2017), Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies [W kierunku ram koncepcyjnych zarządzania ryzykiem w zakresie BHP w inteligentnych środowiskach pracy w

oparciu o inteligentne ŚOI, inteligentne otoczenie i technologie internetu rzeczy], *International Journal of Occupational Safety and Ergonomics*, *23*(1), s. 1–20.

Ponemon (2021), The impact of ransomware on healthcare during covid-19 and beyond [Wpływ oprogramowania szantażującego na opiekę zdrowotną w okresie pandemii COVID-19 i później], https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

Stacey, N., Ellwood, P., Bradbrook, S., Reynolds, J., Williams, H. i David, L. (2018), *Key trends and drivers of change in information and communication technologies and work location. Foresight on new and emerging risks in OSH [Kluczowe tendencje i czynniki stymulujące zmiany w technologiach informacyjno-komunikacyjnych i miejscu pracy. Prognozowanie nowych i pojawiających się zagrożeń w zakresie BHP],* Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy, https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

Steijn, W., van der Vorm, J., Luiijf, E., Gallis, R. i van der Beek, D. (2016, 6 września), Emergent risks to workplace safety as a result of IT connections of and between work equipment [Pojawiające się zagrożenia dla bezpieczeństwa w miejscu pracy wynikające z połączeń informatycznych w sprzęcie roboczym i pomiędzy nim], *TNO report*.

Taeihagh, A. i Lim, H. S. M. (2019), Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks [Zarządzanie pojazdami autonomicznymi: nowe rozwiązania w zakresie bezpieczeństwa, odpowiedzialności, prywatności, cyberbezpieczeństwa i zagrożeń branżowych], *Transport Reviews*, 39, s. 103–128.

Tifferet, S. (2019), Gender differences in privacy tendencies on social network sites: A meta-analysis [Różnice w traktowaniu kobiet i mężczyzn w zakresie skłonności do zachowania prywatności w serwisach społecznościowych: metaanaliza], *Computers in Human Behavior*, 93: s. 1–12.

Truong, T. C., Diep, Q. B. i Zelinka, I. (2020), Artificial Intelligence in the Cyber Domain: Offense and Defense [Sztuczna inteligencja w domenie cyberprzestrzeni: atak i obrona], *Symmetry, 12*(3), s. 410.

Verizon (2019), Sprawozdanie z dochodzeń w sprawie naruszeń ochrony danych z 2019 r., https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon (2021), Sprawozdanie z dochodzeń w sprawie naruszeń ochrony danych z 2021 r., https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

WEF (2021), These are the top cybersecurity challenges of 2021. [Oto najważniejsze wyzwania związane z cyberbezpieczeństwem w 2021 r.], https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Westerlund, M. (2019), The emergence of deepfake technology: A review [Pojawienie się technologii deepfake: przegląd], *Technology Innovation Management Review, 9*(11), s. 40–53.

Williams, E. J., Hinds, J. i Joinson, A. N. (2018), Exploring susceptibility to phishing in the workplace [Badanie podatności na phishing w miejscu pracy], *International Journal of Human-Computer Studies*, 120, s. 1–13.