**Nowoczesne Systemy Zarządzania**
Zeszyt 17 (2022), nr 3 (lipiec-wrzesień)
ISSN 1896-9380, s. 81-98
DOI: 10.37055/nsz/155323

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

**Modern Management Systems**
Volume 17 (2022), No. 3 (July-September)
ISSN 1896-9380, pp. 81-98
DOI: 10.37055/nsz/155323

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

# Cyberbezpieczeństwo systemów teleinformatycznych w dobie powszechnej cyfryzacji

# Cybersecurity of ict systems in the era of widespread digitization

**Joanna Antczak**
Wojskowa Akademia Techniczna
Wydział Bezpieczeństwa, Logistyki i Zarządzania
joanna.antczak@wat.edu.pl; ORCID:0000-0001-5691-2525

**Marcin Kos**
Wyższa Szkoła Informatyki Stosowanej i Zarządzania w Warszawie
marcin.a380@gmail.com

**Abstrakt.** Okres XXI wieku jest bezprecedensowy, jeżeli chodzi o rozwój w obszarze technologii. Użytkownicy cyberprzestrzeni muszą proaktywnie korzystać z praktyk związanych zachowaniem bezpieczeństwa, aby były one realnie skuteczne i odczuwalne. Celem artykułu było zbadanie wpływu dynamicznie postępującej cyfryzacji na cyberbezpieczeństwo systemów teleinformatycznych oraz świadomości ich użytkowników w tym zakresie. Przeprowadzone badania jednoznacznie wskazują, iż istnieje kilka obszarów cyberbezpieczeństwa, w których należałoby poczynić kroki mające na celu zwiększenie świadomości społeczeństwa. Główny obszar stanowi uświadomienie, że każdy użytkownik Internetu może być potencjalnym celem ataku cybernetycznego. Kolejnym istotnym obszarem, który został uwidoczniony podczas analizy odpowiedzi na pytania ankietowe, jest rażąca polityka zarządzania hasłami praktykowana przez użytkowników Internetu. W artykule wykorzystano następujące metody i techniki badawcze: metody ankietowe, metody indukcji jako formy przechodzenia od szczegółu do ogółu, metodę dedukcji jako formę uogólniającą i wnioskową, analizę literatury oraz danych statystycznych. Poruszana tematyka w opracowaniu wskazuje na konieczność prowadzenia oraz rozwoju badań nad sposobem, w jaki społeczeństwo reaguje na zmiany zachodzące w cyberprzestrzeni.
**Słowa kluczowe:** cyberbezpieczeństwo, systemy teleinformatyczne, cyberatak

**Abstract.** The period of the 21st century is unprecedented in terms of developments in technology. Users of cyberspace must proactively use security preservation practices to be realistically effective and noticeable. The purpose of the article was to study the impact of rapidly advancing digitization on the cyber security

of ICT systems and the awareness of their users in this regard. From the research, it was clear that there are several areas of cyber security in which steps should be taken to increase public awareness. The main area is awareness that any Internet user can be a potential target of a cyber attack. Another important area that was highlighted during the analysis of survey responses is the blatant password management policies practiced by Internet users. The following research methods and techniques were used in the article: survey method, induction method as a form of going from the particular to the general, deduction method as a form of generalization and inference, analysis of literature and statistical data. The topics discussed in the article indicate the need to conduct and develop research on how society responds to changes in cyberspace.
**Keywords:** cyber security, ICT systems, cyber attack

## Wstęp

Cyberprzestrzeń w XXI wieku jest jednym z najbardziej rozwijających się, a zarazem zmieniających się obszarów zagrożeń, przynoszącym coraz większe straty zarówno gospodarkom narodowym, przedsiębiorstwom, jak i indywidualnym obywatelom. Zagrożenia cybernetyczne nabrały charakteru strategicznego, obejmującego całokształt działalności państwa łącznie z jego systemem bezpieczeństwa i obrony. Dostęp do Internetu czy korzystanie z jego zasobów stało się codziennością wraz z wiążącymi się z tym konsekwencjami (Antczak, 2020, s. 16).

Ogromny potencjał Internetu doprowadził do zmiany znaczenia granic geograficznych, w wyniku czego odległość geograficzna przestała odgrywać taką rolę, jaką pełniła w poprzednich dekadach. Posiadanie komputera oraz dostęp do Internetu umożliwił sprawniejsze prowadzenie większości działań administracyjnych, politycznych i biznesowych bez wymogu obecności w miejscu pracy. Każda osoba z komputerem osobistym może stać się nadawcą treści. Współcześnie nie jest niczym nadzwyczajnym zjawisko pobierania, przesyłania i zapisywania wiadomości za pomocą jednego ruchu myszy komputerowej czy kliknięcia klawisza (Górka, 2017, s. 73).

Wypadkową szybkiego rozwoju systemów teleinformatycznych i konieczności dopasowania się do wymagań rynku, który to stawia między innymi na cyfryzację, jest rosnące ryzyko z zakresu cyberbezpieczeństwa. Równolegle z postępem transformacji cyfrowej rozwija się również działalność przestępcza, która przeniosła swój obszar aktywności do Internetu.

Celem artykułu było zbadanie wpływu dynamicznie postępującej cyfryzacji na cyberbezpieczeństwo systemów teleinformatycznych oraz świadomości ich użytkowników w tym zakresie.

W publikacji wykorzystano następujące metody i techniki badawcze: metody ankietowe, metody indukcji jako formy przechodzenia od szczegółu do ogółu, metodę dedukcji jako formę uogólniającą i wnioskową, analizę literatury oraz danych statystycznych.

Poruszana tematyka w opracowaniu wskazuje na konieczność prowadzenia oraz rozwoju badań nad sposobem, w jaki społeczeństwo reaguje na zmiany zachodzące w cyberprzestrzeni.

## Istota i motywy transformacji cyfrowej

Hasło, jakim jest „transformacja cyfrowa" lub w określeniu synonimicznym „cyfryzacja", ostatnimi laty zagościło na stałe w światowej kulturze i tematyce szeroko pojętego rozwoju technologicznego. Interpretacja tego sformułowania niestety jest niejednoznaczna, dla jednych bowiem może ono oznaczać instalację pojedynczych stacji komputerowych w przedsiębiorstwie, a dla innych korzystanie z całej gamy różnorakich urządzeń infrastruktury informatycznej realizujących określone cele (Rojek, 2016).

Przyglądając się dokładniej genezie tego określenia, można jednak wysnuć pewne prawidłowości z nim związane. Zdecydowana większość dostępnych definicji sprowadza się do tego, że jest to rodzaj integracji sfery cyfrowej z różnymi formami aktywności firmy. Na transformację cyfrową składają się w głównej mierze wszelkiego rodzaju rozwiązania informatyczne mogące podnieść sprawność funkcjonowania przedsiębiorstwa (Kowalska, 2021). Doskonałymi przykładami technologii informatycznych XXI wieku, wpisujących się w trend cyfryzacji, są sztuczna inteligencja, Internet rzeczy, zautomatyzowane przetwarzanie i analizowanie danych oraz potocznie zwana chmura danych.

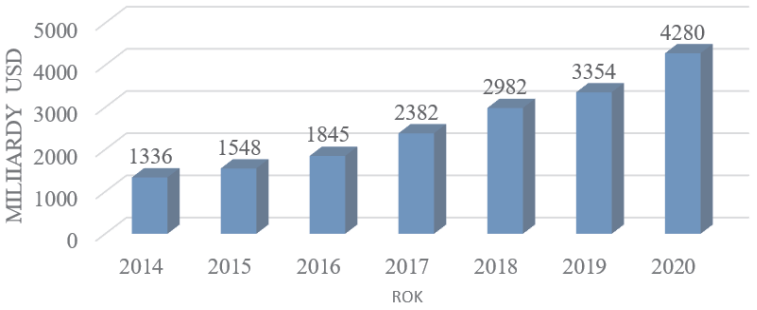
Warto przy tym zagadnieniu się zatrzymać i nadmienić, iż rozwój w tych dziedzinach spowodowany jest w głównej mierze przez bezprecedensowy postęp i powstanie nowych możliwości przesyłu dużych wolumenów danych w skali lokalnej oraz globalnej. Firmy, widząc zalety takiego stanu rzeczy, stopniowo zaczęły eliminować przetwarzanie danych w tradycyjny sposób z wykorzystaniem papierowych arkuszy (Kowalska, 2021).

Cyfryzacja to jednak nie tylko technologia, lecz w dużej mierze sposób myślenia lub, mówiąc szerzej, część kultury organizacyjnej przedsiębiorstwa. Nie wystarczy wprowadzenie samych nowinek technologicznych, aby proces transformacji się udał, musi też nastąpić zmiana sposobu funkcjonowania firmy na każdym z jej szczebli. Wbrew pozorom to może okazać się jednym z większych wyzwań stojących przed organizacją, do modernizacji aspektów sprzętowych bowiem wystarczy w dużej mierze tylko odpowiednia ilość zasobów finansowych, a zmiana kultury organizacyjnej, przekonanie pracowników do nowej rzeczywistości, sposobu pracy i myślenia to niekiedy proces czasochłonny i obarczony wieloma problemami (SpotData, 2019).

Analizując przebieg kształtowania się transformacji cyfrowej w przedsiębiorstwach, warto zacząć od handlu, który zalicza się do sektora gospodarczego usług. Przedsiębiorcy zajmujący się wymianą towarowo-pieniężną w stosunkowo niedługim czasie musieli zmierzyć się ze zmianami wynikającymi z rosnącego udziału w życiu gospodarczym tak zwanego pokolenia cyfrowego ludzi. Konieczna była również zmiana sposobu myślenia i przyzwyczajeń utartych przez lata pracy. Jako przykładem można posłużyć się rynkiem handlu internetowego (ang. e-commerce) w Polsce, który według raportu Statista DigitalMarket Outlook plasuje się na trzynastym

miejscu wśród najszybciej rosnących rynków na świecie. Zważywszy na fakt, że e-commerce nie powinno być traktowane jako alternatywne do sprzedaży tradycyjnej, lecz raczej jej uzupełnienie, polski rynek odpowiednio zareagował na zmiany w trendzie rynkowym wynikającym między innymi z postępu pokoleniowego.

Na rysunku 1 przedstawiono globalną skłonność sprzedażową w części rynku określanej jako handel internetowy.




Rys. 1. Sprzedaż globalna e-commerce

Źródło: opracowanie własne na podstawie danych ze strony www.statista.com

W ciągu niespełna jednej dekady, w latach 2014-2020, wartość sprzedaży globalnej e-commerce zwiększyła się trzykrotnie. Nie jest to dziełem przypadku, rosnący bowiem trend sprzedażowy e-commerce utrzymywał się nieprzerwanie.

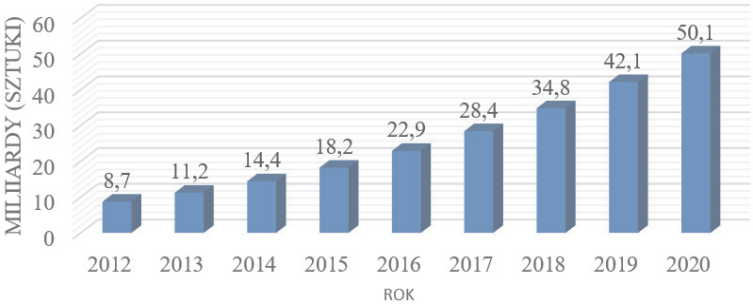
Skłonności ludzkie do poprawiania komfortu życia codziennego, zarówno w obszarze prywatnym, jak i zawodowym, na przestrzeni lat miały również kluczowy wpływ na kształtowanie się procesu transformacji cyfrowej. Koncepcja Internetu rzeczy (ang. Internet of Things – IoT), mająca swoje początki w ubiegłym wieku, w dużej mierze wychodzi naprzeciw takim oczekiwaniom konsumenckim. Czym zatem jest wspomniany Internet rzeczy? Z technicznego punktu widzenia IoT to wzajemne połączenie różnego rodzaju urządzeń, nie tylko komputerów, lecz również całego wachlarza czujników. W swojej istocie oferuje również zwiększoną liczbę usług, których zautomatyzowanie oraz inteligencja są na zdecydowanie wyższym poziomie, a to wszystko z minimalnym bieżącym udziałem człowieka (Miller, 2016, s. 10).

Technologia Internetu rzeczy w ostatnim dziesięcioleciu znacząco się rozpowszechniła, co można zaobserwować na rysunku 2 przedstawiającym liczbę działających urządzeń IoT w ciągu dziewięciu lat.

W 2012 roku uwidoczniła się już skala IoT, liczba urządzeń bowiem w tamtym czasie była większa od liczby ludności na świecie. W prezentowanych latach 2012-2020 średni wzrost globalnej liczby urządzeń IoT plasował się na poziomie 25%, w wyniku czego ostatecznie w 2020 roku liczba urządzeń Internetu rzeczy ponad sześciokrotnie przekroczyła liczbę ludności.

Większość urządzeń podłączonych do IoT często określana jest mianem inteligentnych, ale wydźwięk tego określenia może być rozumiany różnorako. W rzeczywistości są to proste urządzenia, które same w sobie nie są inteligentne, a które stają się takimi w połączeniu z innymi, tworząc sieć. W ramach Internetu rzeczy wszystkie połączone urządzenia stają się czymś więcej niż tylko zbiorem pojedynczych części. Urządzenia w danym otoczeniu komunikują się ze sobą i wymieniają informacjami, a zjawisko to określane jest przez ekspertów mianem „inteligentnego otoczenia" (Miller, 2016, s. 10).

Jeszcze dwie dekady temu mało kto był w stanie uwierzyć, że na porządku dziennym będzie wszczepianie ludziom inteligentnych rozruszników serca czy implantów monitorujących jego pracę. Sprzęty domowe, takie jak pralki, lodówki, telewizory, ze względu na swoje niestandardowe funkcje zawierają znamiona Internetu rzeczy.




Rys. 2. Globalna liczba urządzeń IoT na przestrzeni lat
Źródło: opracowanie własne na podstawie danych ze strony www.researchgate.net

## Znaczenie oraz kształtowanie cyberbezpieczeństwa

Cyberprzestępczość w skali gospodarek krajowych oraz poszczególnych przedsiębiorstw jest generatorem olbrzymich strat między innymi w aspekcie finansowym oraz w ujęciu niematerialnym. Wobec tempa rozwoju cyfryzacji w wymiarze globalnym idealnym scenariuszem byłoby rozpatrywanie nakładów na systemy zapewniające bezpieczeństwo infrastruktury informatycznej jako inwestycję o charakterze strategicznym. Stosowanie takiego podejścia znacząco wpłynęłoby na zmniejszenie ryzyka utraty pozycji konkurencyjnej i wiarygodności biznesowej (Gajewski, Paprocki, Pieriegud, 2016, s. 25). Wysiłki skierowane na zapobieganie incydentom w cyberprzestrzeni nie mogą polegać wyłącznie na podstawowej ochronie danych osobowych, jest ona bowiem niewystarczająca do pełnego zabezpieczenia wartości cyfrowych firm. Konsekwencje cyberataków mogą być fatalne

w skutkach, a straty finansowe to jedynie początek. Niepoprawne zabezpieczenie systemów teleinformatycznych może również powodować szkody wizerunkowe, a w skrajnych przypadkach nawet zagrożenie życia.

Ze względu na swoją złożoność, zarówno pod względem politycznym, jak i technologicznym, cyberbezpieczeństwo jest jednym z głównych wyzwań współczesnego świata. Warto więc zwrócić szczególną uwagę na sposób kształtowania się tego procesu.

Początki cyberbezpieczeństwa określane są na lata 70. XX wieku, wówczas powstał program komputerowy o nazwie Creeper, który mógł poruszać się po sieci ARPANET, zostawiając pod sobie komunikat „Jestem creeperem: złap mnie, jeśli potrafisz" (ang. I'm the creeper: catch me if you can) (History of cybersecurity, 2022). Wywołało to wówczas nie lada zainteresowanie oraz obawy w związku z tym, że oprogramowanie mogło swobodnie wędrować po sieci. W wyniku rosnącej uwagi skierowanej w stronę programu Creeper powstał program, którego zadaniem było wyszukiwanie oraz usuwanie Creepera. Ten czas można określić jako powstanie pierwszego oprogramowania antywirusowego, idea kryjąca się bowiem za nim przetrwała do dzisiaj w popularnych systemach antywirusowych.

Po 2000 roku rozwój technologiczny nie zwalniał, komputery znajdowały się w większości biur i domów, co jednocześnie implikowało więcej zagrożeń i możliwości dla cyberprzestępców. Ataki hakerskie rosły na popularności, a ich szkodliwość gospodarcza liczona była w setkach milionów dolarów. Obszar cyberbezpieczeństwa nie pozostawał jednak bez odzewu, powołane zostało wiele inicjatyw, w których skład wchodzą między innymi (Cadd, 2020):

- **uwierzytelnianie wieloskładnikowe** (ang. MFA – Multi-Factor Authentication) – jeden ze sposobów ochrony cyfrowych zasobów, polegający na dodaniu kolejnych kroków lub czynników do sekwencji logowania. MFA ma za zadanie utrudnić atakującym pozyskanie dostępu do usług. Najprostszymi dodatkowymi sekwencjami służącymi do wieloskładnikowego logowania są kody wysyłane za pomocą usługi SMS lub odcisk palca. W przypadku usług i systemów o kluczowym znaczeniu dla działalności organizacji priorytetem powinno okazać się stosowanie uwierzytelniania wieloskładnikowego (Stallings, 2019, s. 863);
- **piaskownica** (ang. sandboxing) – technika odnosząca się między innymi do izolowania potencjalnie niebezpiecznych plików lub programów. Daje to możliwość ochrony sieci biznesowych przed potencjalnymi zagrożeniami. Hasło to odnosi się również do procesu wytwarzania oprogramowania i ma na celu utworzenie środowiska do testowania aplikacji, które jak najlepiej odzwierciedla docelową konfigurację. Dzięki temu rośnie szansa wykrycia błędów lub usterek, zanim produkt zostanie dostarczony do środowiska produkcyjnego;

- **tworzenie kopii i dublowanie** (ang. backup and mirroring) – okresowe tworzenie kopii zapasowych systemu jest podstawową czynnością, którą administratorzy systemów teleinformatycznych powinni mieć na uwadze. Zasadną praktyką jest zautomatyzowanie procesu tworzącego kopie oraz okresowe testowanie awaryjnych strategii ich wykorzystywania w celu ponownego uruchomienia środowiska po potencjalnym ataku. Ponadto często stosowany jest zabieg tworzenia środowiska będącego niejako lustrem głównej aplikacji, które w przypadku awarii może zostać w krótkim czasie podmienione, dzięki czemu ciągłość pracy systemu nie powinna zostać znacząco naruszona;
- **zapory sieciowe** (ang. firewall) – funkcjonują jako pierwsza linia obrony w zakresie bezpieczeństwa sieci komputerowych. Z technicznego punktu widzenia zapora to zestawienie ochrony sprzętowej oraz programowej, które monitoruje przychodzący i wychodzący ruch sieciowy.

Na przestrzeni lat ranga cyberbezpieczeństwa w funkcjonowaniu przedsiębiorstw wzrastała. Fakt ten można zaobserwować również ze względu na kwestie finansowe, wydatki bowiem na ten segment branży teleinformatycznej stopniowo rosną.

## Metody cyberataków oraz sposoby ich zapobiegania

Rozwój technologiczny zrewolucjonizował wymianę informacji między ludźmi, stając się w ten sposób podstawowym filarem nowoczesnego społeczeństwa. Przyglądając się jednak temu, należy stwierdzić, że powstały również nowe problemy i zagrożenia w kwestiach bezpieczeństwa (Górka, 2017, s. 3). Świadomość użytkowników cyberprzestrzeni z zakresu możliwych zagrożeń z roku na rok jest coraz wyższa, ale w dalszym ciągu mimo rosnącego nacisku na zapewnienie wysokich standardów cyberbezpieczeństwa ataki cybernetyczne oraz działalność cyberprzestępcza rosną w siłę. W tabeli 1 scharakteryzowano wybrane metody cyberataków.

Tabela 1. Wybrane metody cyberataków

| Metody cyberataku | Charakterystyka cyberataku |
|---|---|
| Boty oraz wirus | To automatycznie instalujące się lub nieumyślnie instalowane przez pracownika złośliwe oprogramowania mające na celu przejęcie kontroli nad systemem lub kradzieżą danych. Mogą one zostać aktywowane, np. w momencie otworzenia wiadomości e-mail lub załącznika do niej lub kliknięcia w link pochodzący z niezweryfikowanego źródła. Cyberprzestępcy „maskują" również złośliwe programy, przygotowując pliki udające znane i popularne aplikacje. Hakerzy do osiągnięcia swoich celów coraz częściej wykorzystują też zewnętrzne nośniki, takie jak dyski, pendrive czy inne urządzenia typu USB. |

*cd. tab. 1*

| | |
|---|---|
| Wyłudzanie danych uwierzytelniających (phishing i pharming) | To w praktyce podszywanie się pod zaufane źródło, np. znaną instytucję lub osobę w celu wyłudzenia poufnych informacji. Phishing wykorzystuje pocztę elektroniczną – cyberprzestępcy rozsyłają maile zachęcające do kliknięcia w link i zalogowania się na podstawionej przez nich stronie, łudząco podobnej do prawdziwej, np. banku, a w efekcie mogą uzyskać dostęp do danych i pieniędzy użytkownika. Tak samo groźny pharming wykorzystuje przekierowania na fałszywe strony i serwery internetowe, na które jesteśmy kierowani np. poprzez zainstalowane na urządzeniu wirusy i złośliwe oprogramowania. |
| Ransomware | To oprogramowanie, które najpierw blokuje dostęp do systemu komputerowego oraz uniemożliwia odczytanie danych, a następnie żąda od użytkownika okupu za przywrócenie stanu pierwotnego. Hakerzy instalują takie oprogramowanie za pomocą załącznika w e-mailu lub przeglądarki internetowej w momencie odwiedzenia strony, która jest zainfekowana złośliwym oprogramowaniem tego typu. |
| Juice Jacking | To sposób na wykradanie danych ze smartfonów za pomocą „fałszywych" ładowarek do telefonów instalowanych przez hakerów w miejscach publicznych. Tym sposobem cyberprzestępcy z tak podłączonego telefonu mogą nie tylko pobrać dane (zdjęcia, wiadomości, e-maile), ale też wgrać do niego złośliwe oprogramowanie. |
| Clickjacking | To metoda polegająca na instalowaniu przez hakera złośliwego oprogramowania w określonej aplikacji lub na stronie internetowej (wykorzystując luki w ich zabezpieczeniach). Cyberprzestępcy w niezauważalny dla użytkowników sposób uzyskują dostęp do ważnych przycisków menu na określonej witrynie, przypisują im własne funkcje i odsyłają na strony przez nich zaprogramowane (gdzie np. znajduje się złośliwe oprogramowanie). |
| Podsłuchiwanie ruchu i ataki Man-in-the-Middle (MitM) | Sposób wykorzystywany przez hakerów na podsłuchiwanie i modyfikowanie ruchu sieciowego z urządzenia. Możliwe jest to, np. w sytuacji, gdy użytkownik połączy się z niezaufanym punktem dostępowym do Internetu zarządzanym przez hakera. Sposób ten umożliwia m.in. wykradanie danych i haseł. |
| SPAM | To niechciane lub niepotrzebne wiadomości elektroniczne, które są wysyłane za pomocą poczty elektronicznej lub publikowane na różnego typu grupach dyskusyjnych i forach internetowych. Standardowo wiadomości tego typu są wysyłane masowo, zawierają jednakową treść i są skierowane do nieznanych osób. |
| Zaawansowane ukierunkowane ataki (APT) | Oznacza zaawansowane trwałe zagrożenie. Jest to ukryty, ukierunkowany atak na sieć komputerową, w którym osoba lub grupa uzyskuje nieautoryzowany dostęp do sieci i pozostaje niewykryta przez dłuższy czas. Taki rodzaj ataków często prowadzony był przez rządy państw i miał na celu uszkodzenie lub kradzież poufnych danych. Jedną i znaczącą cechą szczególną takich ataków jest to, że są one trudne do zdefiniowania i mogą być przez lata niezauważone. |
| Ataki typu odmowa usługi (DoS/DDoS) | Zdarzenie, które pojawia się, gdy atakujący uniemożliwia uprawnionemu użytkownikowi na dostęp do określonych systemów komputerowych, urządzeń, usług lub innych zasobów IT. Ataki typu DoS zalewają serwery, systemy lub sieci, aby utrudnić lub uniemożliwić uprawnionym użytkownikom dostęp do tych zasobów. |
| Wycieki danych za pośrednictwem złośliwego oprogramowania (malware) | Oprogramowanie, które w swoim działaniu powoduje szkodę dla użytkownika, sprzętu komputerowego lub sieci internetowej. Głównym celem cyberprzestępców jest atak na osoby prywatne lub duże instytucje, które są w stanie zapłacić okup w zamian za odzyskanie zawłaszczonych danych. |

Źródło: Antczak, 2020, s. 32-33

Wczesne analizowanie potencjalnych zagrożeń oraz przygotowywanie zabezpieczeń systemów teleinformatycznych w taki sposób, aby były gotowe odeprzeć podstawowe ataki cybernetyczne, jest prostsze i mniej kosztowne aniżeli późniejsze likwidowanie skutków aktywności przestępców internetowych. Potencjalne straty wizerunkowe, finansowe oraz rzeczowe znacznie przewyższają nakłady, które powinny zostać poniesione na cele zabezpieczenia infrastruktury cyfrowej.

Audyt systemów informatycznych jest jednym z ważniejszych elementów zwiększających bezpieczeństwo i stabilność funkcjonowania przedsiębiorstw. Pozwala on na zaprojektowanie bezpiecznego środowiska teleinformatycznego, wcześniejsze wykrycie niedoskonałości procesowych i może wpłynąć na zwiększenie efektywności pracy. W celu przeprowadzenia efektywnego procesu audytorskiego ważne jest, aby zastosować do tego właściwą metodykę i podejście. Ścisła integracja systemów informatycznych wraz z procesami biznesowymi sprawia, że niemal każdy element środowiska może stać się przedmiotem pracy audytorów (Molski, Łacheta, 2006, s. 11).

Istnieje wiele technologii mogących zminimalizować ryzyko dokonania pomyślnego ataku cybernetycznego na przedsiębiorstwa, ale ostatecznie i tak większość zależy od świadomości i wykształcenia pracowników, którzy na co dzień obcują z systemami. Częste szkolenia i zwiększenie świadomości powinny być jednymi z bardziej priorytetowych zabiegów, które mogą ustrzec firmy przed stratami wynikającymi z działań hakerów.

Skuteczny system uświadamiający pracowników na temat potencjalnie otaczających ich zagrożeń powinien uzupełniać sposób pracy, a nie tworzyć zasady, które będą ją utrudniały. Nikt nie jest odporny na błędy ani nie ma wpływu na pojawienie się w zainteresowaniu cyberprzestępców, z tego też względu pracownicy na każdym szczeblu organizacji powinni przechodzić okresowe szkolenia.

Znaczna część ataków występujących w obecnych czasach opiera się na wykorzystywaniu zabiegów socjotechnicznych, mających wpłynąć bezpośrednio na użytkownika i skłonić go do popełnienia błędu umożliwiającego przeprowadzenie pomyślnego ataku. Różnego rodzaju badania wykazują, że niemal 90% wycieków danych spowodowanych jest błędami ludzkimi, co wzmacnia potrzebę ciągłej edukacji pracowników w zakresie cyberbezpieczeństwa (Ramachandran, 2019).

## Ocena świadomości użytkowników cyberprzestrzeni z zakresu cyberbezpieczeństwa (badania własne)

Popularne stwierdzenie z branży teleinformatycznej głosi, iż wszelkiego rodzaju systemy teleinformatyczne i ich bezpieczeństwo są tak silne, jak ich użytkownik z najmniejszą świadomością oraz poczuciem odpowiedzialności za ten aspekt. Incydenty związane z naruszeniem bezpieczeństwa danych są często wynikiem ludzkiego zachowania, w którym brak odpowiedniej wiedzy z zakresu bezpiecznego

poruszania się w cyberprzestrzeni. Tocząca się transformacja cyfrowa nie ułatwia tego zadania, istnieje bowiem pewna część użytkowników, którzy nie są w stanie nadążyć za coraz to nowo powstającymi atakami i metodami socjotechnicznymi ze strony cyberprzestępców.

Badania miały charakter pilotażowy, a ich celem było sprawdzenie, w jaki sposób społeczeństwo reaguje na zmiany zachodzące w otoczeniu cyberprzestrzeni. Ponadto szczególna uwaga została zwrócona na świadomość potencjalnych zagrożeń wynikających z aktywności cyberprzestępczej oraz metod zapobiegania atakom. Świadomość cyberbezpieczeństwa polega na uważnemu przyjrzeniu się bezpieczeństwu cyberprzestrzeni w codziennych sytuacjach. Użytkownicy muszą dobrowolnie i proaktywnie korzystać z praktyk związanych z cyberbezpieczeństwem, zarówno zawodowo, jak i osobiście, aby były one realnie skuteczne i odczuwalne.

Metoda badawcza, która została zastosowana, jest metodą pomiaru bezpośredniego za pomocą elektronicznego kwestionariusza przekazywanego respondentom. Ankieta została sporządzona za pomocą narzędzia firmy Google, dającego możliwość wygenerowania arkusza oraz udostępnienia go w sieci dowolnej liczbie osób. Głównym celem było zebranie doświadczeń i praktyk od pełnoletnich osób mających jakiekolwiek doświadczenie zawodowe. Fakt konieczności posiadania stażu pracy podyktowany był zamiarem zebrania informacji na temat niektórych praktyk stosowanych w przedsiębiorstwach.

Analizie zostały podane odpowiedzi 50 respondentów, którzy dobrowolnie wypełnili kwestionariusz. W badaniu udział wzięli przedstawiciele obu płci. Głosy ze względu na aspekt płci badanych rozłożyły się stosunkowo równomiernie, z niewielką przewagą frekwencyjną mężczyzn, których było 26 i stanowili wówczas 52% całości ankietowanych. Liczba kobiet biorących udział w badaniu stanowiła 45% całości i liczba ta przekładała się bezpośrednio na 24 badane.

Biorąc pod uwagę wiek ankietowanych, to udział osób w przedziale między 18. a 25. rokiem życia uzyskał taką samą wartość procentową jak osób w wieku od 26 lat do 35 lat. Do każdej z grup przynależało po 18 osób, stanowiąc z osobna po 38% całości. Z pięćdziesięciu badanych tylko 7 należało do grupy wiekowej od 36. do 45. roku życia, stanowiąc 14% badanych. Najmniej liczną grupą okazały się osoby powyżej 45. roku życia, których było 5, co przełożyło się na 10% pokrycia tej grupy wiekowej.

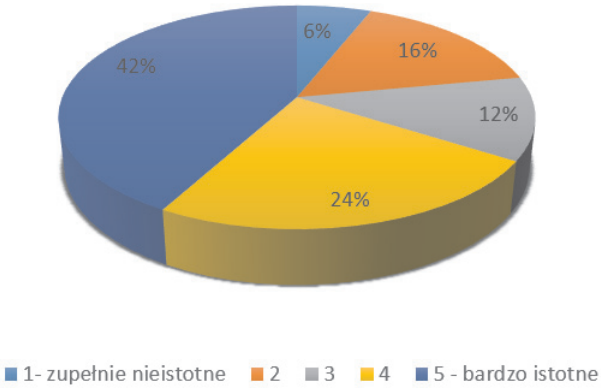
Główna część badania i analiza z tym związana opierała się na 19 pytaniach, które zostały zadane respondentom. Pytania były przekrojowe, co w praktyce oznaczało, że weryfikowały kilka obszarów świadomości ankietowanych w kontekście cyberprzestrzeni. Zagadnienia przedstawione badanym sprawdzały między innymi:

- prywatne poczucie istotności cyberprzestępstw w XXI wieku;
- samoocenę świadomości z zakresu cyberbezpieczeństwa;
- stopień wykorzystywania głównych tworów procesu transformacji cyfrowej,
- prywatną politykę związaną z bezpieczeństwem uwierzytelniania;

– znajomość najpopularniejszych ataków w cyberprzestrzeni;
– politykę cyberbezpieczeństwa przedsiębiorstwa.

Wyniki przeprowadzonej analizy przedstawione zostały w postaci wykresowej oraz tabelarycznej, ponadto do omawianych pytań dołączona została interpretacja oraz wnioski.

W pierwszym pytaniu ankietowani zostali poproszeni o określenie w pięciostopniowej skali istoty zagrożeń płynących z cyberprzestępstw w obecnych czasach, tj. w XXI wieku. Wybranie jedynki oznaczało, że zagrożenia są zupełnie nieistotne, a wybranie odpowiedzi numer pięć świadczyło o wysokiej istocie tego problemu. Na wykresie słupkowym (zob. rysunek 3) pokazany został podział odpowiedzi respondentów.

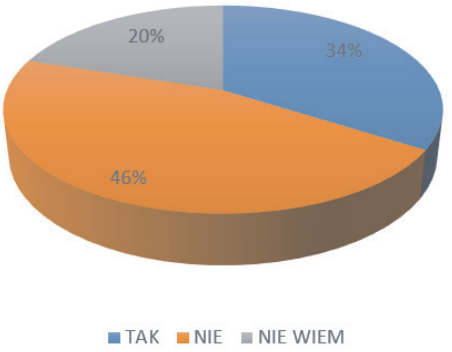



Rys. 3. Odpowiedzi na pytanie: w jakim stopniu uważa Pan/Pani, że cyberprzestępstwa są istotnym zagrożeniem w obecnych czasach?

Źródło: opracowanie własne na podstawie badań ankietowych

Ponad połowa, bo aż 33 osoby, co stanowiło 66% całości ankietowanych, przez wybranie czwartej i piątej odpowiedzi, jednoznacznie stwierdziło, że cyberprzestępstwa są istotnym zagrożeniem. Sześć osób, co stanowiło 12% badanych, miało neutralny stosunek do zagrożeń wynikających z aspektu wykroczeń popełnianych przez przestępców internetowych. Pozostałe 22% osób nie określiło tego zjawiska, jakoby miało ono wyjątkowe znaczenie w rzeczywistości opisywanego zakresu czasowego. Mając na uwadze rosnące trendy – inwestycyjny oraz rozwojowy branży teleinformatycznej – przedstawione wyniki pozwalają stwierdzić, że mimo to nie wszyscy ludzie podchodzą do opisywanego zjawiska z należytą uwagą. Zaprezentowana statystyka nie powinna powodować niepokoju, ale istnieje znaczące pole komunikacyjne, które powinno zostać wykorzystane oraz skierowane ściśle do osób niedostrzegających zagrożeń płynących z działań cyberprzestępców.

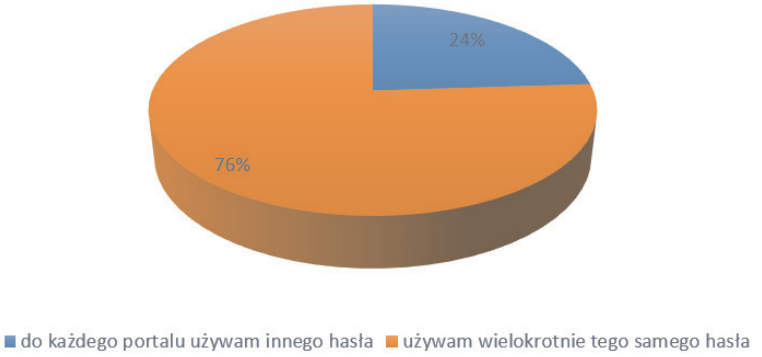
Istotnym zagadnieniem w kontekście cyberbezpieczeństwa są prywatne doświadczenia ankietowanych, dlatego też kolejne pytanie sprawdzało, czy w stronę badanych skierowane były kiedykolwiek ataki cyberprzestępcze. Na rysunku 4 przedstawione zostały udzielone odpowiedzi.




Rys. 4. Odpowiedzi na pytanie: czy kiedykolwiek w Pana/Pani stronę były skierowane ataki cyberprzestępcze?
Źródło: opracowanie własne na podstawie badań ankietowych

Siedemnaście osób, co stanowiło 34% grupy, odpowiedziało, iż było przedmiotem ataku cyberprzestępczego. Jeżeli skorelujemy to z pytaniem o możliwość bycia celem ataku w przyszłości, wówczas otrzymamy zbliżone wyniki, tj. liczba osób uważająca, że w przyszłości może być celem, jest zbliżona wielkościowo do grupy, która była już przedmiotem ataku. Ma to istotne znaczenie, ponieważ osoby, które doświadczyły na sobie cyberprzestępstwa, zazwyczaj zmieniają podejście do tego aspektu i są bardziej ostrożni oraz czujni w przyszłości. Na uwagę zasługuje również grupa osób, która określiła, iż nie wie, czy była przedmiotem cyberataku. Te osoby stanowią 20% wszystkich badanych. Biorąc pod uwagę, że w przypadku bycia nieostrożnym w sieci można pobrać na swój komputer oprogramowanie, takie jak np. keylogger, które dla zwykłych użytkowników może przez bardzo długi czas pozostać niewykryte, taki sposób odpowiedzi może sugerować nieco większą niż podstawową świadomość na temat cyberbezpieczeństwa. Pozostałe 23 osoby uznały, że nigdy w ich stronę nie były skierowane ataki cyberprzestępcze. Taka odpowiedź nie jest niczym nadzwyczajnym, jednostki mające ponadprzeciętną świadomość na temat tego obszaru funkcjonowania w sieci zazwyczaj są w stanie oszacować na podstawie swojego zachowania, czy mogły być przedmiotem aktywności cyberprzestępców.

Polityka związana z zarządzaniem hasłami dostępowymi do różnego rodzaju serwisów internetowych odgrywa bardzo istotną rolę w całym procesie bezpiecznego korzystania z cyberprzestrzeni. Kolejne pytanie (zob. rysunek 5) sprawdzało, czy użytkownicy stosują bezpieczną zasadę używania do każdego serwisu innego hasła.

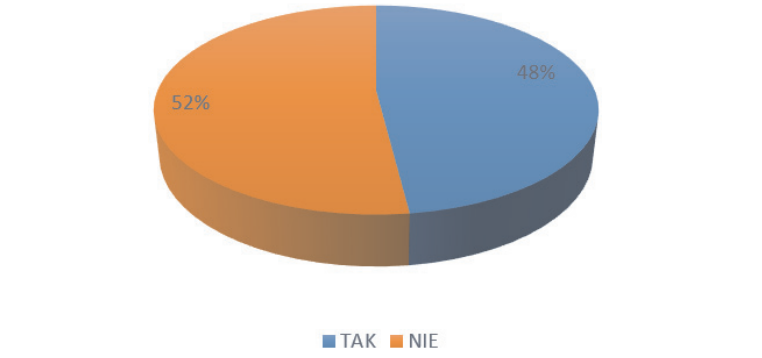



Rys. 5. Odpowiedzi na pytanie: jaka jest Pana/Pani osobista polityka związana z zarządzaniem hasłami?

Źródło: opracowanie własne na podstawie badań ankietowych

Odpowiedzi przedstawione na rysunku 5 są bardzo niepokojące. Ponad 70% osób zadeklarowało, że używa wielokrotnie tego samego hasła dostępowego w wielu miejscach w sieci. Biorąc pod uwagę ilość rozległych wycieków danych z serwisów internetowych, używanie tego samego hasła dla kilku witryn jest niezwykle niebezpieczną praktyką. Potencjalny wyciek danych logowania z jednej witryny może dać cyberprzestępcom dostęp do wielu innych.

W kontekście haseł oprócz unikalności istotna jest również ich poufność. Praktyki związane z przekazywaniem haseł osobom postronnym zostały zbadane w następnym pytaniu i odpowiedzi przedstawione zostały na wykresie (zob. rysunek 6).

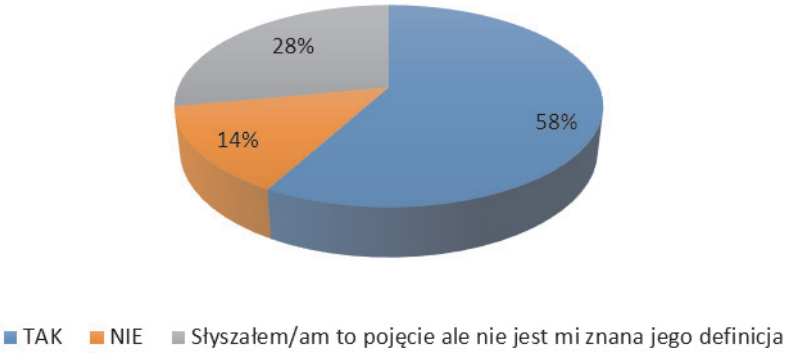



Rys. 6. Odpowiedzi na pytanie: czy kiedykolwiek zdarzyło się Panu/Pani przekazywać prywatne hasła dostępowe osobom postronnym?

Źródło: opracowanie własne na podstawie badań ankietowych

Wyniki rozłożyły się równomiernie, 48% osób przyznało się, że przynajmniej raz przekazało prywatne hasła osobom postronnym. Podobnie jak w przypadku wielokrotnego wykorzystywania tych samych haseł, przekazywanie danych logowania osobom postronnym również nie powinno mieć miejsca. Ze względów bezpieczeństwa dane dostępowe powinny zostać osobistą własnością osób je wykorzystujących.

Kolejna grupa trzech pytań zawarta w kwestionariuszu służyła do zweryfikowania wiedzy na temat jednych z bardziej szkodliwych sposobów działania wybieranych przez cyberprzestępców. Pierwsze pytanie sprawdzało, czy badani zaznajomieni są z pojęciem phishingu. Wyniki zostały przedstawione na rysunku 7.



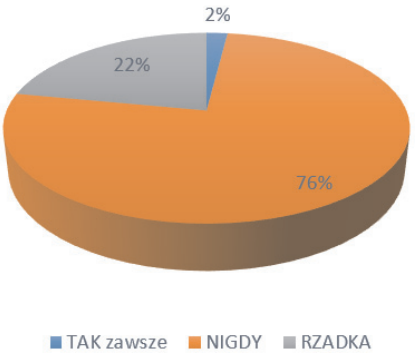

Rys. 7. Odpowiedzi na pytanie: czy wie Pan/Pani, czym jest phishing?
Źródło: opracowanie własne na podstawie badań ankietowych

Niewątpliwie pozytywną informacją jest fakt, iż prawie 60% osób potwierdziło znajomość określenia *phishing*. Jedna na trzy osoby oznajmiła, że słyszała o tym pojęciu, ale nie jest jej znana jego definicja. Pozostałe 14% osób, co przełożyło się na 7 osób, nie było świadomych znaczenia podanego terminu. Co do zasady idealną sytuacją byłaby stuprocentowa znajomość tego pojęcia przez ankietowanych, niemniej jednak przedstawione wyniki można uznać za akceptowalne.

Każda strona internetowa, która przetrzymuje i przetwarza dane użytkowników, powinna udostępniać wszelkiego rodzaju informacje na temat sposobu oraz celu wykorzystywania gromadzonych danych. Tego typu zbiór informacji często określany jest jako polityka prywatności serwisu. W kolejnym pytaniu ankietowani zostali poproszeni o udzielenie informacji, czy przed rejestracją konta w serwisie internetowym czytają wspomnianą politykę prywatności. Na rysunku 8 przedstawione zostały udzielone odpowiedzi.

Niestety ponad 75% osób stwierdziło, że nigdy nie czyta polityki prywatności, co jest wysoce niepokojącą informacją. Tylko jedna osoba zadeklarowała zapoznawanie się z zasadami przetwarzania danych w każdym przypadku, pozostałe 22%

osób zaś stwierdziło, że czyta politykę prywatności, ale nie w każdym przypadku. Mimo że odpowiedzi powinny budzić niepokój, takie podejście nie jest niestety niczym zaskakującym. Serwisy internetowe w znacznej części przypadków oferują użytkownikom do przeczytania dziesiątki stron regulaminu, pisanego często trudnym do zrozumienia dla zwykłych użytkowników językiem. Fakt ten w większości przypadków powoduje u użytkowników niechęć i zaakceptowanie polityki prywatności bez zapoznania się z jej zapisami.

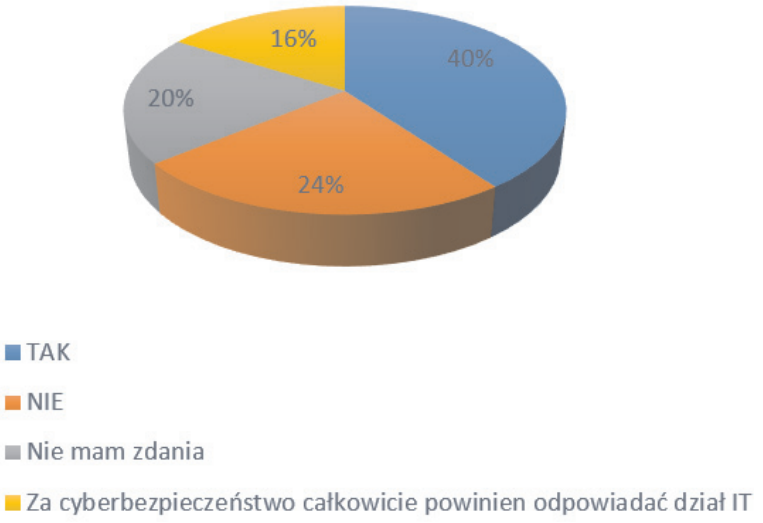



Rys. 8. Odpowiedzi na pytanie: czy przed rejestracją w serwisie internetowym czyta Pan/Pani politykę prywatności?

Źródło: opracowanie własne na podstawie badań ankietowych

W całym procesie utrzymywania wysokiego poziomu cyberbezpieczeństwa w przedsiębiorstwie istotne jest uświadamianie pracowników, że mają realny wpływ na powodzenie tego przedsięwzięcia. Pracownicy muszą czuć się częścią tego systemu i w pewnym stopniu sami nakładać na siebie odpowiedzialność za przestrzeganie wszelkiego rodzaju zasad związanych z bezpiecznym poruszaniem się w cyberprzestrzeni. Ankietowani w ostatnim pytaniu badania zostali poproszeni o określenie poczucia, że mają realny wpływ na cyberbezpieczeństwo w ich przedsiębiorstwie (zob. rysunek 9).

Odpowiedzi zaprezentowane na rysunku 9 niestety nie okazały się obiecujące, tylko 40% badanych bowiem potwierdziło, że czują, iż mają realny wpływ na cyberbezpieczeństwo w ich przedsiębiorstwie. Niespełna 1/4 grupy zaprzeczyła temu stwierdzeniu, 20% osób stwierdziło brak sprecyzowanego zdania w omawianej materii, a pozostałe 16% uznało, iż za ten obszar całkowicie powinien odpowiadać dział IT. Wyniki pokazują, że osoby odpowiedzialne za ten jeden z istotniejszych obszarów funkcjonowania firmy powinny przykładać znacznie większą wagę do uświadamiania pracowników, że to w głównej mierze od nich zależy powodzenie działań skierowanych w tym kierunku.




Rys. 9. Odpowiedzi na pytanie: czy czuje Pan/Pani, że ma realny wpływ na cyberbezpieczeństwo w przedsiębiorstwie?

Źródło: opracowanie własne na podstawie badań ankietowych

## Wnioski

Zapoczątkowanie ery szeroko pojętego Internetu było niezwykłym bodźcem do stopniowo zwiększającego się na przestrzeni lat trendu transformacji cyfrowej. Trzydzieści lat temu mało kto wyobrażał sobie, że Internet będzie dobrem powszechnym, a nie tylko przywilejem elit. W ciągu tego okresu znacząco zmienił się też sposób myślenia społeczeństwa.

Tocząca się transformacja cyfrowa jest to cykl, który ewoluował na przestrzeni lat i który z biegiem czasu dotykał innych aspektów życia codziennego. Jedne ze sztandarowych elementów, które są wynikiem transformacji cyfrowej, to między innymi rynek handlu internetowego oraz Internet rzeczy. Bez wątpienia wynik pracy osób zaangażowanych w powstanie tych technologii jest dostrzegany w życiu codziennym ludzi na całym świecie. Okres XXI wieku okazał się bezprecedensowy w kontekście rozwoju technologicznego, który bezpośrednio przekłada się na komfort życia społeczeństwa.

Cyberbezpieczeństwo oraz zagrożenia obecne w cyberprzestrzeni kształtowały się równolegle z transformacją cyfrową na przestrzeni wielu lat. Cyberprzestępcy na bieżąco rozwijają swoje umiejętności, aby przełamywać zabezpieczenia wypracowywane w celu ochrony danych. Przyczyny aktywności cyberprzestępczej są mocno

zróżnicowane, niemniej jednak bez względu na to, czym kierują się przestępcy, należy dokładać wszelkich starań, aby tego typu sytuacjom zapobiegać. Przeprowadzanie audytów, szkoleń oraz odpowiednia polityka haseł to tylko jedne z podstawowych sposobów obrony przed atakami.

Użytkownicy cyberprzestrzeni muszą proaktywnie korzystać z praktyk związanych z zachowaniem bezpieczeństwa, aby były realnie skuteczne i odczuwalne. Z badania świadomości użytkowników cyberprzestrzeni jednoznacznie wynika, iż istnieje kilka obszarów cyberbezpieczeństwa, w których należałoby poczynić kroki mające na celu zwiększenie świadomości społeczeństwa.

Zasadniczą kwestią jest uświadomienie sobie, że każdy może być potencjalnym celem ataku cybernetycznego. Coraz częściej można zaobserwować w życiu codziennym masowe kampanie hakerskie skierowane w strony zwykłych użytkowników.

Kolejnym istotnym aspektem, który został uwidoczniony podczas analizy odpowiedzi ankietowanych, jest rażąca polityka zarządzania hasłami praktykowana przez znaczną część osób. W tym zakresie istnieje duże pole do poprawy, ponieważ z danych wynika, iż ponad połowa osób ignoruje dobre praktyki związane z tym obszarem.

Warto również podkreślić zjawisko związane ze stosunkiem do polityki prywatności serwisów internetowych. Zdecydowana większość osób przed założeniem konta w serwisie zwyczajnie nie zapoznaje się z zasadami przetwarzania danych stosowanych przez konkretny portal. Nie jest to całkowicie wina użytkowników, ponieważ praktyka pokazuje, iż spora część stron internetowych posiada kilkudziesięciostronicowe regulaminy napisane trudnym do zrozumienia językiem.

Jeżeli chodzi o kontekst cyberbezpieczeństwa w przedsiębiorstwach, sytuacja wygląda obiecująco, ponieważ większa część firm, w których pracowali badani, stosuje podstawowe zasady związane z zachowaniem bezpieczeństwa cyberprzestrzeni.

## BIBLIOGRAFIA

[1] Antczak, J., 2020. *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*, Warszawa: Akademia Sztuki Wojennej.

[2] Gajewski, J., Paprocki, W., Pieriegud, J., 2016. *Cyfryzacja gospodarki i społeczeństwa. Szanse i wyzwania dla sektorów infrastrukturalnych*, Gdańsk: Europejski Kongres Finansowy.

[3] Górka, M., 2017. Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa, *Systemy Wspomagania w Inżynierii Produkcji*, t. 6, s. 73-89.

[4] Górka, M., 2017. *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*, Koszalin: Politechnika Koszalińska.

[5] Miller, M., 2016. *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa: PWN.

[6] Molski, M., Łacheta, M., 2019. *Przewodnik audytora systemów informatycznych*, Gliwice: Helion.

[7] Stallings, W., 2019. *Effective Cybersecurity Understanding and Using Standards and Best Practises*, USA: Addison-Wesley.

NETOGRAFIA

[1] Cadd, K., 2020. *Avast Blog History of Cyber Security*, https://blog.avast.com/history-of-cyber-security-avast (22.07.2022).

[2] History of Cybersecurity, 2022. *History of Cyber Security. Find an online cyber security degree*, https://cyber-security.degree/resources/history-of-cyber-security/ (22.07.2022).

[3] Kowalska, M., 2021. *Transformacja cyfrowa – czy nie ma od niej odwrotu?*, https://www.politykabezpieczenstwa.pl/pl/a/transformacja-cyfrowa-czy-nie-ma-od-niej-odwrotu (17.06.2022).

[4] Ramachandran, R., 2019. *The importance of Training: Cybersecurity Awareness like a Human Firewall*, https://www.entrepreneur.com/article/340838 (23.07.2022).

[5] Rojek, M., 2016. *Czym jest cyfryzacja?*, https://ceo.com.pl/marcin-rojek-czym-jest-cyfryzacja-79635 (17.06.2022).

[6] SpotData, 2019. *Cyfryzacja to więcej niż technologia*, https://raporty.spotdata.pl/cyfryzacja (17.06.2022).

[7] Strona internetowa researchgate.net – www.researchgate.net (23.06.2022).

[8] Strona internetowa statista.com – www.statista.com (23.06.2022).