WYŻSZA SZKOŁA BANKOWA W POZNANIU
Wydział Finansów i Bankowości

Agnieszka Reguła

Ocena świadomości zagrożeń i problemów dotyczących cyberbezpieczeństwa w różnych grupach społecznych

Praca magisterska

Promotor
Dr Grzegorz Nowak

Poznań 2023

Streszczenie

Ocena świadomości zagrożeń i problemów dotyczących cyberbezpieczeństwa w różnych grupach społecznych

Wraz z rozwojem technologii stale rozwijane są nowe formy zagrożeń w cyberprzestrzeni, a ilość ataków w Polsce od wielu lat znacząco rośnie. Celem pracy była ocena czy i w jaki sposób wiek oraz obszar zatrudnienia lub studiowania ma wpływ na świadomość zagrożeń i problemów dotyczących cyberbezpieczeństwa w różnych grupach społecznych.

Do badań włączono 100 osób, w tym 41 studentów, 58 osób pracujących i jednej osoby nie pracującej i nie studiującej. Zastosowanym narzędziem badawczym był kwestionariusz ankietowy dotyczący bezpieczeństwa w sieci. Analiza statystyczna przeprowadzana została z wykorzystaniem testu Chi-kwadrat.

Wykazano, że wiek oraz obszar zatrudnienia ma wpływ na niektóre aspekty świadomości zagrożeń i problemów dotyczących cyberbezpieczeństwa. Analiza statystyczna wykazała również, że najmniejszą świadomość i wiedzę w obszarze cyberbezpieczeństwa mają ludzie młodzi (do 24 roku życia) studiujący lub uczący się oraz osoby pracujące w administracji państwowej lub samorządowej.

Słowa kluczowe: cyberbezpieczeństwo, bezpieczeństwo, kradzież danych, zagrożenia cyberbezpieczeństwa, ataki hakerskie, luka w zabezpieczeniach , ochrona danych

Spis treści

1. Wstęp

Wprost proporcjonalnie do rozwoju technologii, wzrostu popularności Internetu i rozwiania oprogramowania w siłę rośnie podziemie cybernetycznych przestępców. Coraz nowocześniejsze formy zagrożeń i ataków stają się nie tylko narzędziem do niszczenia konkurencji, a nawet bronią, która potrafi sparaliżować jednostkę, miasto czy nawet cały kraj na wiele dni. Według analityków Check Point Research ilość ataków z roku na rok znacząco wzrasta. W Polsce ilość ataków w 2022 roku wrosła o 35% w stosunku do roku poprzedniego. W europejskim rankingu państw pod względem ilości miesięczny ataków Polska jest zazwyczaj w górnej części tabeli (około miejsca 6). Tygodniowo w Polsce firmy mierzą się z 938 atakami. Największa ilość ataków przeprowadzana jest na sektor finansowy, jednostki rządowe i jednostki militarne, ale znacząco wrasta również ilość ataków na sektor opieki zdrowotnej.

Rozpoczęcie się wojny na Ukrainie znacznie wpłynęło na wzrost ilości cyberataków na świecie, co świadczyć może o tym, że coraz częściej w trakcie konfliktów państwowych cyberwojna będzie kolejnym filarem działań wojennych. Z tego powodu coraz więcej krajów powołuje specjalne jednostki rządowe i wojskowe, które mają dbać o rozwój i rozbudowę struktury cyberbezpieczeństwa. W Polsce kilka lat temu po szczycie NATO (2016 rok) został utworzony kolejny filar Wojska Polskiego, który zajmuje się cyberobroną. Wojska Obrony Cyberprzestrzeni zatrudniają wielu specjalistów cywilnych i wojskowych, których celem jest rozbudowa i rozwój struktury obrony oraz ochronę narodowego bezpieczeństwa w cyberprzestrzeni.

Oprócz bezpiecznych systemów i struktur w kraju jednym z najważniejszych elementów cyberbezpieczeństwa jest uświadamianie i uczenie użytkowników sieci o potencjalnych zagrożeniach, atakach i wyciekach danych. Nawet najbezpieczniejszy system na świecie może zostać zaatakowany, a jego zabezpieczenia złamane, jeśli użytkownicy nie stosują się do zasad bezpieczeństwa.

Celem pracy jest ocena świadomości osób z różnych grup społecznych dotyczącej aspektów bezpieczeństwa podczas korzystania z urządzeń elektronicznych oraz Internetu. Temat ten jest istotny ze względu na wciąż wzrastające i ewoluujące zagrożenia w sieci, które grożą zarówno poszczególnym użytkownikom, firmom i całej krajowej infrastrukturze.

Podstawą do napisania pracy magisterskiej jest badanie kwestionariuszowe oraz analiza dostępnej literatury na temat współczesnych zagrożeń w cyberprzestrzeni.

2. Część literaturowa

2.1 Cyberbezpieczeństwo – rozwinięcie pojęcia

„Cyberbezpieczeństwo to organizacja i zbiór zasobów, procesów i struktur wykorzystywanych do ochrony cyberprzestrzeni i systemów obsługujących cyberprzestrzeń przed wystąpieniem zdarzeń, które są niezgodne z faktycznymi prawami własności”(Craigen i in., 2014). Według polskiego Urzędu Dozoru Technicznego cyberbezpieczeństwo definiowane jest jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”(Urząd Dozoru Technicznego, 2018). Obie definicje wskazują, że istotą cyberbezpieczeństwa jest dostarczanie narzędzi i rozwiązań by zadbać o bezpieczeństwo w cyberprzestrzeni. Cyberbezpieczeństwo jest również ogromną dyscypliną naukową, przede wszystkim komputerową, ale zawiera również elementy prawa, polityki, etyki i wpływu czynnika ludzkiego. Dyscyplina tak skupia się na badaniu i rozwoju bezpieczeństwa danych, oprogramowania, komunikacji sieciowej, systemów, organizacji, społeczeństwa i użytkowników.

2.2 Cyberprzestępczość – definicja

Za jedną z pierwszych definicji cyberprzestępstwa uznajemy definicję R. von Zur Mühlena głoszącą, że cyberprzestępstwem nazywamy każdy akt przestępczy, którego narzędziem lub celem jest komputer (zur Mühlen, 1973). Definicja ta jednak jest bardzo ogólna i niejednoznaczna. Wraz z mijającymi latami, kolejnych definicji powstało wiele, jednak mimo to wiele krajów wciąż ma problem z prawnym uchwyceniem istoty czym jest cyberprzestępstwo. Najbardziej intuicyjnym jest skategoryzowanie cyberprzestępczości pod względem roli komputera w przestępstwie (Zhang i in., 2012):

- komputer jest wykorzystywany jako narzędzie działalności przestępczej (np. spamowanie, łamanie praw autorskich)
- komputer lub sieć jest celem aktywności przestępczej (np. Ataki DOS, Malware)
- komputer lub sieć jest miejscem wykonywania przestępstwa (np. łamanie zabezpieczeń sieci telefonicznych)
- tradycyjne przestępstwa są popełniane poprzez komputer (np. kradzież tożsamości, dziecięca pornografia, cybeterroryzm)
- inne przestępstwa informacyjne (np. wykradanie tajemnic handlowych).

Według A. Završnika możemy wyznaczyć trzy generacje przestępstw komputerowych. Pierwsza obejmowała zamachy na komputery, dane i sieci komputerowe. Z rozwojem sieci teleinformatycznych nadeszła druga generacja, niosąca za sobą ataki na integralność i dostępność owych sieci. Trzecią generacją nazywamy współczesną formę cyberataków, czyli wykorzystywanie oprogramowania by atakowanie stawało się jak najbardziej automatycznym procesem (Završnik, 2008). Według S. Gordona i R. Forda, by lepiej zrozumieć niuanse cyberprzestępstwa, a tym samym dokładniej zdefiniować całe zjawisko, warto podzielić je na dwa rodzaje (tabela 1).

Rodzaj 1

Przestępstwo tego rodzaju z perspektywy ofiary jest pojedyncze lub dyskretne, często odbywa się przy użyciu programów przestępczych takich jak Keystroke logger, Koń trojański, Rootkit czy wirusy i może być, ale nie musi, ułatwione przez luki w systemie.

Rodzaj 2

Przestępstwo tego rodzaju z perspektywy ofiary powtarza się często, zwykle odbywa się za pomocą programów które użytkownik uważa za bezpieczne, takich jak klienci IM (komunikacja natychmiastowa) lub za pomocą przesyłania plików poprzez protokół FTP (Gordon & Ford, 2006).

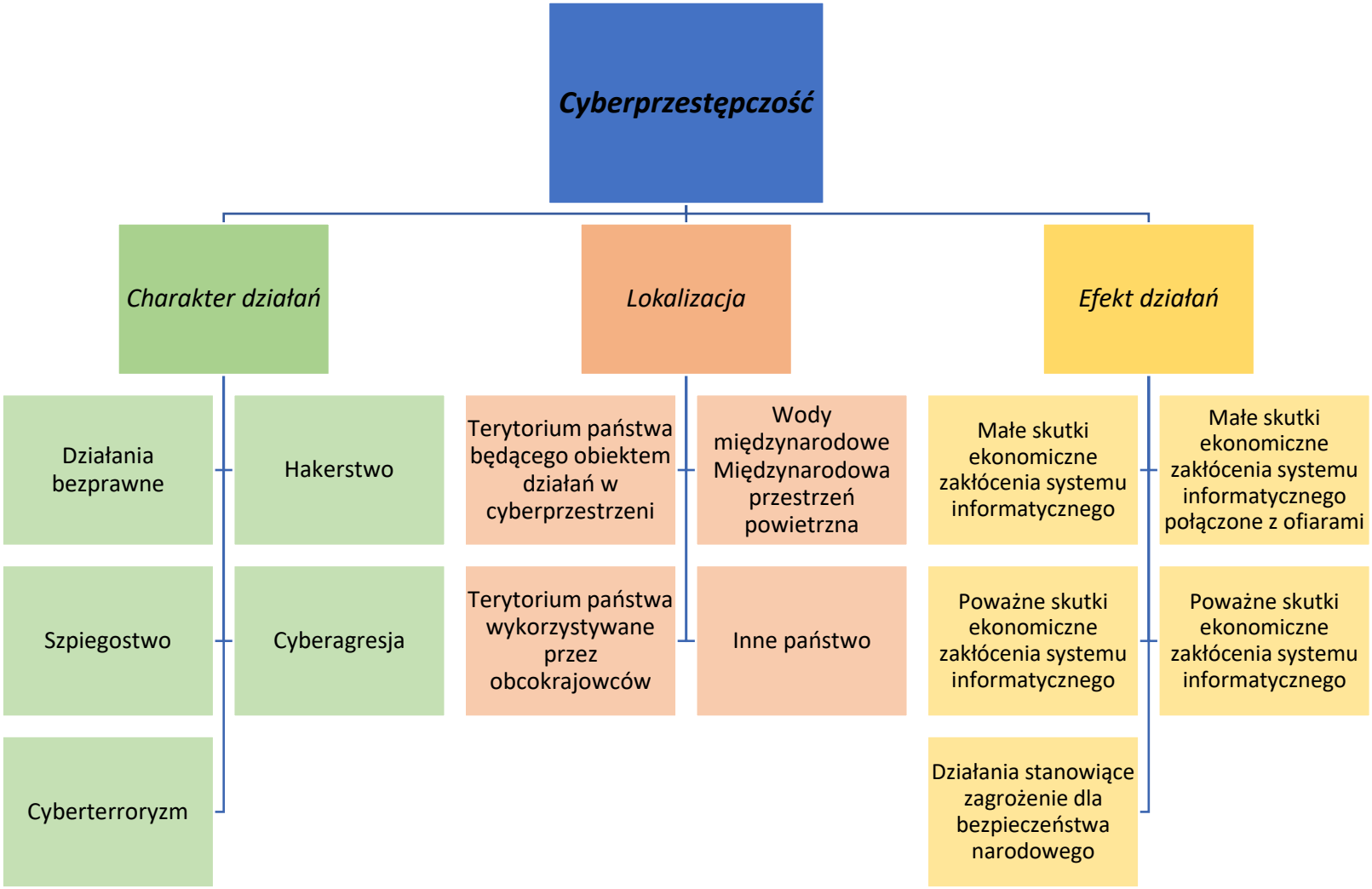
Tabela 1. Przykłady cyberprzestępstw według rodzaju z uwzględnieniem użytego oprogramowania

Przykład	Rodzaj	Oprogramowanie	Crimeware
Phishing	1	Klient pocztowy	Nie
Kradzież tożsamości	1	Keylogger, Trojan	Tak
Cyberstalking	2	Klient pocztowy, czaty	Nie
DDoS	1	Boty	Tak
Cyberterroryzm	2	Steganografia, szyfrowanie, czaty	Nie

Źródło: Cyberprzestępstwo według rodzajów (Gordon & Ford, 2006)

Z pespektywy bezpieczeństwa państwa cyberprzestępczość staje się jednym z największych zagrożeń dla jego poprawnego funkcjonowania. Szybki rozwój technologii sprawia, że coraz trudniej przewidywać potencjalne formy ataku. By jak najlepiej usystematyzować działania w cyberprzestrzeni warto jest rozpatrywać je w zależności od ich charakterystyki, lokalizacji przestępcza i efektu jaki wywołały. Taki rodzaj systematyki ułatwia rozeznanie niebezpieczeństwa jak i utworzenie odpowiedniego systemu karnego dla tego rodzaju wykroczeń (rysunek 1).

Rysunek 1. Systematyka działań przestępczych w cyberprzestrzeni



Źródło: Cyberterroryzm jako nowa forma zagrożenia terrorystycznego (Szubrycht, 2005)

2.3 Hakerstwo i crackerstwo – definicje i różnice

Hakerstwem nazywamy działania, które mają na celu wyszukiwanie dziur w oprogramowaniu w celach edukacyjnych, z ciekawości lub po prostu dla zabawy(Saini i in., 2012). Dla wielu „haker" kojarzy się z przestępcą, który regularnie łamie prawo dla własnych korzyści. W rzeczywistości jednak intencje hakerów są dobre i służą ogólnopojętemu bezpieczeństwie sieciowemu. Według J. Ericksona istotą hakowania jest „znalezienie przeoczonych lub niezamierzonych zastosowań dla praw i właściwości danej sytuacji, a następnie zastosowanie ich w nowy i pomysłowy sposób w celu rozwiązania problemu" (Erickson, 2010). Oryginalni, pierwsi hakerzy uważali programowanie za formę wyrazu, a komputer za narzędzie do tworzenia tej sztuki. Mieli również swoją etykę, która sformułowana została w książce „Hackers: Heroes of the Revolution" (Levy, 1984). Współcześnie hakerów możemy podzielić na trzy grupy (Caldwel, 2011):

- White Hat hackers testują zabezpieczenia w celu wyszukiwania dziur i robią to w sposób etyczny.
- Grey Hat hackers testują zabezpieczenia z dobrymi intencjami, ale przekraczają przy tym normy etyczne.
- Black Hat hackers, działają w sposób nielegalny i wykorzystują dziury w bezpieczeństwie np. w celach zarobkowych lub jako formę zastraszania.

Trzecia grupa kiedyś nazywana była crackerami. Pojęcie cracker powstało, by odróżnić tych dobrych hakerów, od tych złych i opisywało osoby, które bez skrupułów naruszały dobra informatyczne np. pobierały nielegalnie oprogramowanie czy niszczyły strony Internetowe.

2.4 Szpiegostwo – nieuprawnione pozyskiwanie informacji

Wraz z postępującą powszechną cybernetyzacją coraz częściej na ustach ludzi pojawia się temat podsłuchiwania i szpiegowania. Mimo świadomości części użytkowników o potencjalnym zagrożeniu, ich wiedza o bezpieczeństwie w sieci jest zbyt mała by przynosiła skutki. Szpiegostwem komputerowym nazywamy wszelkie działania polegające na zbieraniu informacji poprzez inne instytucje, przedsiębiorstwa czy kraje i wykorzystywanie ich by wyrządzić szkodę. W tabeli 2 przedstawiono różnice pomiędzy szpiegowaniem, a innym cyberprzestępstwem.

Tabela 2. Generalne różnice pomiędzy szpiegowaniem, a innym cyberprzestępstwem

	Szpiegostwo	**Cyberprzestępstwo**
Główne bodźce	Gromadzenie informacji	Zysk pieniężny, Wandalizm
Cele	Kilka	Wiele
Projektowanie szkodliwego oprogramowania	Dostosowane do potrzeb	Ogólne
Wymagana wiedza	Specyfika branży, Bezpieczeństwo IT, Kultura i język	Bezpieczeństwo IT
Niezbędne zasoby	Wiele	Kilka
Złożoność inżynierii	Wysoka	Niska

Źródło: Podsumowanie ogólnych różnic pomiędzy cyberszpiegostwem, a przestępczością (Wangen, 2015)

2.5 Cyberagresja – agresja w cyberprzestrzeni

Wraz z rozwojem dostępności do Internetu, rozwinęła się rosnąca w niepokojącym tempie cyberagresja (inaczej cybrenękanie, ang. cyberbullying). W stosunku do standardowej formy agresji dzięki poczuciu anonimowości w sieci zachwiana jest równowaga sił. Strona atakująca przy niewielkim wysiłku może stać się bardzo trudna do zidentyfikowania, a dzięki poszczególnym narzędziom może przeprowadzać ataki na wielu frontach i w masowej skali. Cyberagresja jest więc agresywnym, celowym, długotrwałym i wielokrotnym działaniem realizowanym przez grupę lub jednostkę, z wykorzystaniem elektronicznych form kontaktu, a ofiara ma trudności z obroną przed atakiem (Smith i in., 2008). Cybernękanie można podzielić na cztery grupy(Nocentini i in., 2010):

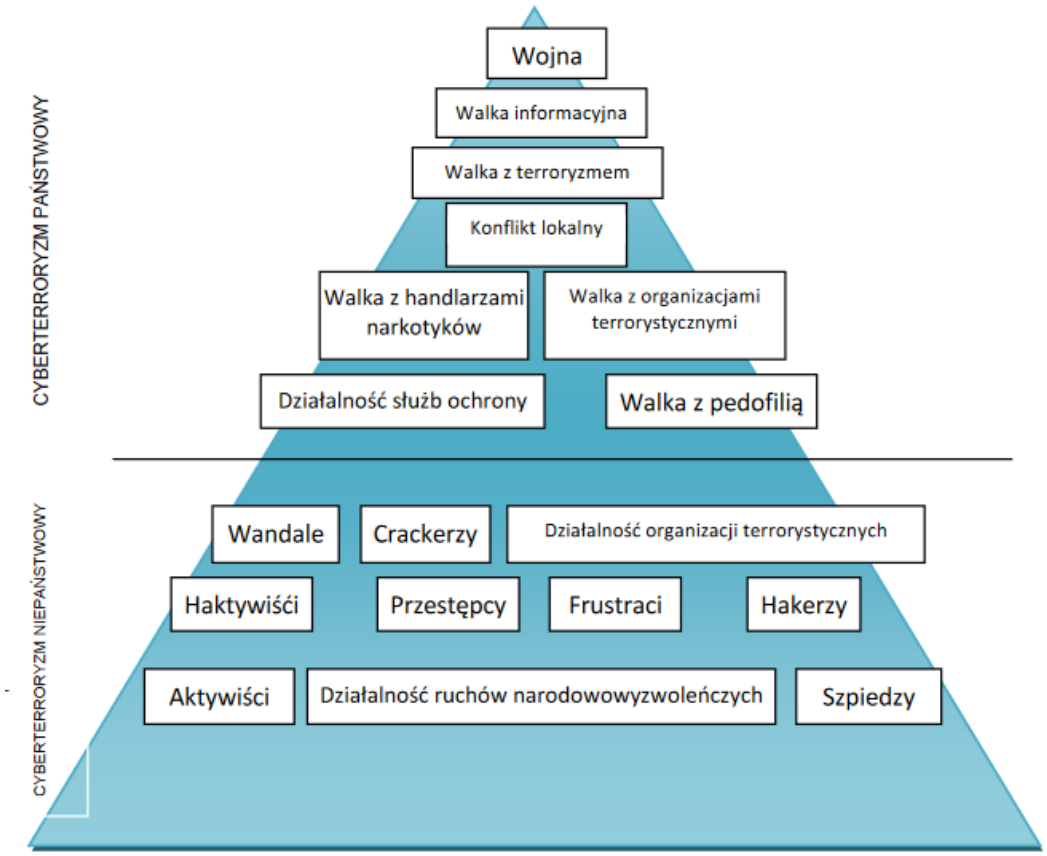
- zachowania pisemno-werbalne (rozmowy telefoniczne, rozmowy tekstowe, blogi. e-maile, media społecznościowe),
- zachowania wizualne (zamieszczanie, wysyłanie lub udostępnianie kompromitujących zdjęć i filmów przez telefon komórkowy lub Internet),
- wykluczenia (celowe wykluczanie osób w grup czy społeczności Internetowych),
- podszywanie się (wykradanie danych osobistych wykorzystywanie i upublicznianie ich przez inne konto).

2.6 Cyberterroryzm – atak w sieci

Cyberterroryzmem nazywamy terroryzm w cyberprzestrzeni. Według najczęściej przytaczanej w literaturze definicji oznacza to bezprawne ataki lub zagrożenia atakami na struktury informatyczne. Atak kwalifikuje się jako cyberterroryzm, gdy skutkuje przemocą wobec osób lub mienia, lub przynajmniej wykonuje wystarczającą szkodę by wywołać

strach(Weimann, 2004). Przykładem cyberterroryzmu będzie atak skutkujący katastrofą lotniczą, wybuchem, katastrofą transportu publicznego lub poważnymi stratami gospodarczymi. Federalne biuro śledcze (FBI) zaproponowało, by uznawać cyberterroryzm za celowy atak umotywowany politycznie wobec systemów komputerowych, oprogramowania, danych i informacji (Voicescu, 2012).

Rysunek 2. Cyberterroryzm państwowy i niepaństwowy



Źrodło: Cyberterroryzm jako zagrożenie bezpieczeństwa w społeczeństwie informacyjnym (Krztoń, 2012)

Podsumowując, cyberterroryzm oznacza konkretne działania terrorystyczne poprzez użycie komputera, które znacząco wpływają na funkcjonowanie obiektów i instytucji publicznych. Działania te również mają zwiększać negatywne emocje i panikę, a ich skutki mogą przyjmować wymiar fizyczny.

2.7 Strategia obrony przed cyberatakami - Defense in Depth

Stworzenie odpowiedniej strategii obrony umożliwia odpowiednie zabezpieczenia systemów. W cyberbezpieczeństwie najczęściej zalecane jest przyjęcie strategii głębokiej ochrony - Defense in Depth. Strategia ta zakłada wdrożenie niezależnych od siebie warstw

zabezpieczeń na wielu poziomach (Shamim i in., 2014). Dzięki takim założeniom systemy informatyczne są znacząco bardziej bezpieczne i w dużej mierze odporne na skutki błędów i ataków, ponieważ w sytuacji, gdy jedna warstwa zabezpieczeń zawiedzie kolejna powinna zatrzymać atak. Strategia Defense in Depth składa się z 6 kluczowych elementów (Rahman i in., 2019).

1. Polityki i procedury bezpieczeństwa

Pierwsza warstwa obrony polega na wdrożeniu odpowiednich polityk i procedur bezpieczeństwa oraz w niektórych przypadkach także regulacji prawnych. Istnieje wiele różnorodnych standardów dotyczących bezpieczeństwa informacji np. ISO (International Organization for Standardization), PCI (Payment Card Industry) lub DSS (Data Security Standard). Procedury i polityki te obejmują rozwój i ograniczenie ryzyka oraz metody przywracania systemów.

2. Separacja sieci

Drugim elementem jest separacja sieci. Najpopularniejszą metodą segmentacji sieci jest zastosowanie stref DMZ (demilitarized zones). Do ich utworzenia stosuje się zapory sieciowe i wszystkie połącznia powinny przez nie przechodzić. Takie rozwiązanie umożliwia ochronę systemów przed zagrożeniami napływającymi z sieci (Kuipers & Fabro, 2006).

3. Bezpieczeństwo granic sieci

Trzecią warstwą zabezpieczeń są zabezpieczenia sieci z wykorzystaniem zapór (firewall), mechanizmów wykrywania włamań, autoryzacji dostępu i blokowania złośliwego oprogramowania oraz filtracji ruchu sieciowego. Dzięki takim narzędziom można zablokować dostęp osobom bez uprawnień.

4. Segmentacja sieci

Tradycyjnie segmentacja była realizowana poprzez używanie wielu routerów. Polegała na dzieleniu sieci na podsieci i ograniczenie przepływu danych jedynie w obrębie podsieci. Najczęściej odbywa się to za pomocą przełączników sieciowych (switch) i umożliwia ograniczenie zasięgu potencjalnych naruszeń, np. ataków złośliwego oprogramowania, tylko do jednego z segmentów.

5. Bezpieczeństwo sprzętowe

Do piątej warstwy zabezpieczeń należą fizyczne zabezpieczenia serwerowni, ochrona sprzętu za pomocą haseł i profili użytkowników oraz ochrona czynników ludzkich.

6. Monitorowanie i rejestrowanie zdarzeń

Kolejną warstwą zabezpieczeń jest stała obserwacja i rejestrowanie zdarzeń. Wszelkie operacje sieciowe muszą być stale monitowane pod względem oznak potencjalnych włamań, dzięki temu można tworzyć i rozwijać skuteczny system alarmowania. Dodatkowo niezbędne jest regularne przeglądanie krytycznych logów w celu wykrywania zaawansowanych włamań i zagrożeń dla systemu oraz aktualizacje systemów i oprogramowania.

Utrzymywanie wielu warstw zabezpieczeń może wydawać się skomplikowane i kosztowne, jednak prawidłowo wdrożona wielowarstwowa strategia poprawia znacząco niezawodność systemu, a większość zabezpieczeń jest zrozumiała dla końcowych użytkowników systemów.

Strategię Defense in Depth można sprowadzić do pięciu ogólnych kroków (Ewing, 2010):

1. Zdefiniowanie i wdrożenie zatwierdzonych przez kierownictwo polityk i procedur
2. Zidentyfikowanie i udokumentowanie krytycznych zasobów i ścieżek komunikacyjnych.
3. Przeprowadzenie analizy ryzyka.
4. Testowanie, wdrażanie i dokumentowanie kontroli bezpieczeństwa.
5. Wykonywanie rutynowej analizy i aktualizowanie informacji.

2. 8 Największe znane cyberataki w historii

The Melissa Virus

„Wirus Melissa tworzy nowy rodzaj zagrożenia”(Garber, 1999). Tak brzmiał nagłówek artykułu z 1999 roku opisujących jeden z największych cyberataków w historii. Wirus ten zainfekował ogromną liczbę urządzeń w bardzo krótkim czasie dzięki wykorzystaniu poczty e-mail. Kluczowe w rozprzestrzenianiu się wirusa było zaufanie użytkowników do nadawców poczty, to spowodowało, że obiorcy bez namysłu otwierali zainfekowane załączniki, tym samym rozprzestrzeniając wirusa dalej. Wiadomość, którą otrzymywali użytkownicy składała się z tematu, treści i załącznika:

1. Temat: Ważna wiadomość od **xyz** - *XYZ* oznaczała poprzednią ofiarę ataku, która miała w książce adresowej dane odbiorcy.
2. Wiadomość: Oto ten dokument, o który prosiłeś... nie pokazuj nikomu innemu ;-)

3. Załącznik: list.doc, który teoretycznie zawierał listę nazw użytkowników i haseł do stron pornograficznych.

Jeśli odbiorca zainfekowanego e-maila używał klienta poczty Microsoft Outlook i edytora tekstu Word 97 lub Word 2000, po otwarciu załącznika wirus przesyłał wiadomość do pierwszych 50 kontaktów z książki adresowej. Kontakt w tym przypadku nie oznaczał jednak jedynie pojedynczego adresu e-mail, ale mogły być to też całe grupy odbiorów. Dodatkowo wirus infekował wzorzec „normal.dot", który standardowo służył do tworzenia nowych dokumentów w programie Word. W przypadku gdy obiorca zainfekowanej wiadomości używał innego klienta poczty, wirus jedynie infekował sam wzorzec programu Word, tym samym rozprzestrzeniał się wolniej, ponieważ użytkownik sam musiał załączyć dokument lub przenieść do za pomocą pamięci zewnętrznej (np. pendrive lub dyskietki). Ze strony technicznej zatrzymanie i usunięcie wirusa było dość proste. Wymusiło to jednak na firmach wyłączanie serwerów na kilka dni i skrupulatne usuwanie wirusa z każdego stanowiska. Szacuje się, że wirus zainfekował 1,2 miliona komputerów.

Cyberatak na NASA

Cyberatak na agencję kosmiczną NASA przeprowadzony został w 1999 przez 15-letniego Jamesa Jonathana. Skutkiem ataku było wyłączenie trzynastu komputerów w Marshall Space Flight Center w Huntsville na 21 dni. Koszt jaki NASA poniosło, by znaleźć dziury w zabezpieczeniach i naprawić komputery to 41 000 dolarów. Podczas pobytu na komputerach, James wykradł dane o wartości 1,7 miliona dolarów tym samym zostając najmłodszym skazanym za cyberprzestępczość (Wilson).

Estoński cyberatak

W 2007 roku w wyniku konfliktu między Estonią, a Rosją doszło do serii cyberataków trwających łącznie ponad miesiąc. Seria ataków rozpoczęła się od zapełnienia skrzynek poczty elektronicznej spamem i e-mailami phishingowymi estońskich organizacji. Strony obsługujące pocztę, strony WWW i inne usługi Internetowe zaczęły nagle zwalniać, albo się zatrzymywać przez nagły, niezwykle duży, ruch sieciowy. Estoński Parlament pod wpływem ataku musiał wyłączyć tymczasowo usługę poczty, a duży serwis informacyjny Postimes padł ofiarą ataku DDoS. Ponadto fora dyskusyjne Postimes Online były masowo spamowane przez boty które obrażały estońskiego premiera. Zmasowane działania były niepokojące, jednak najbardziej władze Estonii zaczęły się obawiać ataków DDoS ponieważ to one miały największy wpływ na poprawne funkcjonowanie państwa. Obawy te były jak

najbardziej słuszne, ponieważ po kilkunastu dniach przyszła najpoważniejsza fala ataków, która trwała 22 dni. Polegała na stałym atakowaniu DDoS stron Internetowych, systemów DNS, stron rządowych, usług finansowych, systemów policyjnych i banków. Ataki te były wykonywane z różną częstotliwością w stosunku do różnych celów z wykorzystaniem różnorodnych narzędzi by nie dawać możliwości łatwej obrony (Schmidt, 2013). Z perspektywy czasu jednoznacznie można określić, że Estonia padła ofiarą cyberterroryzmu.

Cyberatak na sieć PlayStation (SONY)

Sony jest jedną z najbardziej rozpoznawalnych firm na całym świecie. Dostarcza wielu różnorodnych usług, a na jedną z kluczowych w 2011 roku został przeprowadzony spektakularny cyberatak. Z PlayStation Network (PSN) w kilka godzin zostały wykradzione dane 77 milionów użytkowników. Nazwy użytkowników, hasła, dane personalne, adresy i numery kart płatniczych. Mimo stosunkowo szybkiej reakcji administratorów ilość wykradzionych danych była bezprecedensowe w swojej skali i zakresie. Według szacunków straty jakie Sony poniosło za ten wyciek to 171 milionów dolarów (Goode i in., 2017). Do tej pory nie ma pewności w jaki sposób doszło do ataku.

Cyberatak na firmę Adobe

W 2013 roku miał miejsce kolejny ogromny wyciek danych. Z firmy Adobe wykradzione zostało blisko 3 miliony numerów kart płatniczych 38 milionów użytkowników oraz część kodów źródłowych np. Adobe Photoshop i Adobre Acrobat PDF (Whitney, 2013). Atak nastąpił poprzez luki w oprogramowaniu ColdFusion. Według specjalisty od zabezpieczeń Alexa Holdena, luki te zostały wykorzystane do co najmniej kilku innych ataków na mniejsze firmy. Lista potencjalnych domen, którym groziło ryzyko ataku zawierała 1,2 miliona pozycji (Mimoso, 2013). Celem atakujących były trzy konkretne luki, które umożliwiały ominięcie schematów uwierzytelniania i zdalnego kontrolowania serwerów WWW. Mimo szybkiej reakcji firmy Adobe i wdrożenia potrzebnych łatek, doszło do kolejnego dużego wycieku danych z firmy hostingowej Linode, która również korzystała z oprogramowania ColdFusion (Bell, 2018).

Cyberatak na firmę Yahoo

Firma Yahoo w 2016 roku została wykupiona przez koncern Verizon Communications, realizacja umowy jednak znacząco się przesunęła, gdy ujawniono informacje o trzech ogromnych cyberatakach i wycieku danych. Pierwszy atak miał miejsce

w 2014 roku, wykradzione wtedy zostały dane 500 milionów użytkowników, adresy e-mail, numery telefonów, nazwiska, daty urodzenia, zaszyfrowane hasła oraz w niektórych przypadkach zaszyfrowane lub niezaszyfrowane pytania i odpowiedzi dotyczące bezpieczeństwa (Thielman, 2016). Najprawdopodobniej przechwycenie danych odbyło się za pomocą fałszywych ciasteczek, których kod powstał na podstawie prawdopodobnie wykradzionego kodu. Z czasem okazało się, że wyciek mógł być znacznie większy, w tej chwili spekuluje się, że mógł dotyczyć 3 miliardów użytkowników. Dane te jednak nigdy nie zostały potwierdzone przez firmę Yahoo, szczegółowe dane o powodzie wycieku również. Yahoo musiało zapłacić ogromną karę finansową, przede wszystkim za niepoinformowanie użytkowników na czas o wycieku ich danych.

Cyberatak na ukraińską firmę energetyczną

W 2015 firma energetyczna Kyivoblenergo zgłosiła przerwę w świadczeniu usług. Początkowo siedem podstacji zostało odłączonych na trzy godziny, następnie okazało się, że problem z zasilaniem dotknął większej części sieci. Problemy spowodowane zostały nielegalnym wejściem osoby trzeciej do komputera spółki i systemów zarządzania procesami (SCADA). Dodatkowo by utrudnić firmie odbudowę infrastruktury włamywacze wymazali serwery (Assante, 2016). Z czasem okazało się, że, ataków na firmy energetyczne zostało przeprowadzonych więcej, łącznie zasilanie utraciło 225 tysięcy klientów na różnych obszarach kraju (Electricity Information Sharing and Analysis Center (E-ISAC), 2016). Najprawdopodobniej za włamanie do systemów odpowiadały rosyjskie służby bezpieczeństwa, a sam atak miał miał na celu sterroryzowanie Ukrainy.

Seria ataków WannaCry

Ataki WannaCry były największymi atakami typu ransomware wszechczasów. W 2017 roku zainfekowane zostało 200 000 komputerów w wielu krajach. Jednorazowy atak polegał na infekowaniu plików, do których dostęp zostawał zablokowany. By odszyfrować pliki przestępcy żądali około 300 dolarów w kryptowalucie Bitcoin. Do ataku wykorzystane zostały luki w protokole Microsoft Server Message Block 1.0 (SMBv1), które umożliwiły zdalne wykonywanie kodu (Akbanova i in., 2019). Jedną z większych jednostek która padła ofiarą ataku była narodowa służba zdrowia w Wielkiej Brytanii. Zaatakowane zostało również wiele firm na całym świecie. Falę ataków udało się zatrzymać dzięki uzyskaniu próbki kodu wirusa, do tego czasu przestępcy otrzymali około 79 tysięcy dolarów.

2.9 Codzienna rzeczywistość zagrożeń w sieci

Portal „Niebezpiecznik” w dniu 20 stycznia 2023 roku opublikował serię postów dotyczących zagrożeń, ataków i wycieków danych, które zostały upublicznione w ciągu poprzednich 24 godzin.

Wyciek danych klientów T-Mobile

Firma T-mobile upubliczniła raport dotyczący ataku z 5 stycznia. Za pomocą API bez wymogu autoryzacji wykradzione zostało 37 milionów danych użytkowników. Firma zapewniła, że API którego użyto nie zapewniło dostępu do informacji o kartach płatniczych, numerów ubezpieczeń, praw jazdy, rządowych numerów identyfikacyjnych, haseł i PINów ani innych danych o kontach bankowych. Najprawdopodobniej wyciekły imiona i nazwiska klientów, adresy rozliczeniowe, adresy e-mail, numery telefonów, daty urodzeń oraz numery kont T-Mobile (*T-Mobile Report*, 2023).

Przejęcie danych klientów PayPal

Część użytkowników PayPal otrzymała e-mail z informacją o potencjalnym nieupoważnionym dostępie do kont użytkowników. Pomiędzy 6, a 8 grudnia miało miejsce nieautoryzowane działanie polegające na dostępie do kont za pomocą poświadczeń poszczególnych użytkowników. PayPal zapewnił, że nie doszło do jakichkolwiek kradzieży i wycieku danych oraz nie znalazł dowodów na to, że dane logowania zostały uzyskane z jakichkolwiek systemów PayPal (*PayPal Report*, 2023).

Złośliwe reklamy sponsorowane przez Google

Portal Bleeping Computer przeprowadził śledztwo dotyczące coraz popularniejszych złośliwych reklam, które wyświetlają się na 1 pozycji w Google. Pierwsza głośniejsza sytuacja dotyczyła popularnego fana kryptowalut, który stracił sporą część majątku poprzez kliknięcie w reklamę oprogramowania do edycji video wyświetlającą się na górze wyników wyszukiwania. Pobrany plik wykonywalny przechwycił jego loginy i podmienił szczegóły jego cyfrowego portfela. Najpopularniejszymi złośliwymi reklamami były reklamy VCL, OBS i Notepad++. Google zapewnił, że złośliwe reklamy zostały usunięte jednak najprawdopodobniej domeny z wirusami wciąż pozostały dostępne i mogą wyświetlać się w wynikach wyszukiwania na niższych pozycjach (Boyd, 2023).

Wyciek poufnych danych linii lotniczych („No Fly List")

19 stycznia na stronie autora maia arson crimew udostępniony został artykuł pod tytułem: „Jak w 3 prostych krokach całkowicie przejąć linię lotniczą - i złapać listę TSA nofly po drodze". Artykuł ten opisywał przechwyt danych linii lotniczych z publicznego serwera z nudów. Autor poszukiwał odkrytych serwerów Jenkins i tak natrafił na serwer CommuteAir. Bez większych problemów udało się uzyskać z baz danych linii dane wszystkich członków załogi, planów lotu, dane konserwacji samolotu i wiele innych. Przede wszystkim jednak udało się uzyskać listę osób, które mają zakaz wchodzenia na pokład, ponieważ mogą stwarzać poważne zagrożenie. Lista ta miała około 1,56 miliona wierszy i 90MB (maia arson crimew, 2023).

AirTagi przerabiane w celu śledzenia użytkowników

Popularny gadżet firmy Apple – AirTag zaczął budzić wiele kontrowersji. Z jednej strony gadżet w formie breloczku zdaje się być innowacyjnym rozwiązaniem w sytuacji potencjalnej kradzieży lub zgubienia przedmiotu jednak z drugiej strony może zostać wykorzystany do śledzenia użytkownika. 19 stycznia portal „Niebezpiecznik" (Niebezpiecznik, 2023) udostępnił link do aukcji w serwisie eBay gdzie można było zakupić zmodyfikowaną wersję AirTag z funkcją „cichego śledzenia". W niepowołanych rękach taki gadżet może stanowić ogromne zagrożenie (https://web.archive.org/web/20230119212120/https://www.ebay.com/itm/155353682052).

Taka częstotliwość zagrożeń z jakimi może spotkać się użytkownik nie jest niczym wyjątkowym. Regularnie portal „Niebezpiecznik" udostępnia informacje o naruszeniach bezpieczeństwa, atakach, wyciekach danych czy problemach z bankowością. W ciągu dnia takich powiadomień jest nawet kilka, a by zwiększyć czujność i bezpieczeństwo użytkowników, powstała aplikacja „Cyberalerty", która wysyła powiadomienia push o zagrożeniach, z którymi w Polsce użytkownik może się zetknąć.

2. Cel pracy

Celem pracy była ocena świadomości osób z różnych grup społecznych dotyczącej aspektów bezpieczeństwa podczas korzystania z urządzeń elektronicznych oraz Internetu. Celami szczegółowymi były:

1. Ocena wśród respondentów stosowania odpowiedniego oprogramowania do ochrony sprzętu
2. Analiza tworzenie i używanie bezpiecznych haseł przez respondentów
3. Ocena świadomości wśród ankietowanych osób zagrożeń związanych z potencjalnymi atakami i wyciekiem danych

Aby odpowiedzieć na cel główny postawiono hipotezy badawcze, które następnie zweryfikowano statystycznie:

1. Miejsce zatrudnienia lub studiowania ma wpływ na wiedzę dotyczącą zainstalowanej zapory sieciowej
2. Wiek badanych osób wpływa na wybór dodatkowych usług ochrony Internetu
3. Obszaru zatrudnienia lub studiowania respondentów wpływa na to czy badani zabezpieczają swoje dane i sprzęt by umożliwić zdalną blokadę lub usunięcie danych
4. Istnieje zależność między wiekiem, a zabezpieczaniem swoich danych i sprzętu by umożliwić zdalną blokadę lub usunięcie danych
5. Obszaru zatrudnienia lub studiowania wpływa na deklarację liczby znaków w bezpiecznym haśle
6. Korzystanie przez respondentów z menadżerów haseł na urządzeniach prywatnych i firmowych zależy od miejsca zatrudnienia lub studiowania badanych osób
7. Istnieje zależność między obszarem zatrudnienia lub studiowania, a odpowiedzią czy respondent uważa, że był ofiarą cyberataku
8. Istnieje zależność między obszarem zatrudnienia, a deklarowaniem śledzenia na bieżąco informacji o wyciekach danych
9. Wiek wpływa na deklarację śledzenia informacji o wyciekach danych
10. Istnieje zależność między śledzeniem informacji o wyciekach danych przez użytkownika, a deklaracją, że dane respondenta mogły kiedykolwiek wyciec z zabezpieczonych baz danych
11. Deklaracja respondentów o śledzeniu informacji o atakach hakerskich i innych zagrożeniach w sieci zależy od miejsca zatrudnienia lub studiowania

12. Wiek wpływa na śledzenie informacji w wyspecjalizowanych serwisach o atakach hakerskich i innych zagrożeniach w sieci
13. Istnieje zależność między grupą wiekową, a spotkaniem się z kampanią promującą bezpieczne zachowania w sieci.

3. Metody badawcze i materiał badawczy

3.1. Metody i techniki badawcze

Zastosowanym narzędziem badawczym był kwestionariusz ankietowy. Wybór ten umożliwił dotarcie do różnorodnych grup wiekowych i zawodowych.

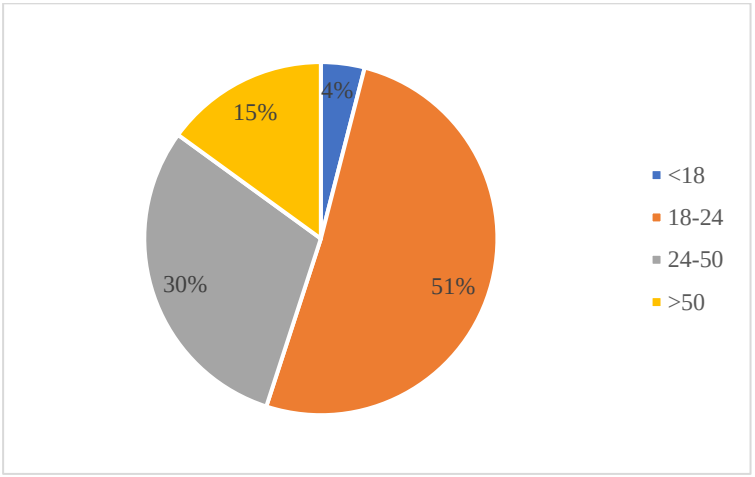
Ankieta została stworzona w narzędziu Arkusze Google i rozpowszechniona za pomocą portali społecznościowy, zawierała 38 pytań zamkniętych i trzy otwarte. Kwestionariusz podzielony został na 4 sekcje. Pierwsza sekcja zawierała pytania dotyczące metryczki respondentów oraz danych socjo-demograficznych, w drugiej zamieszczono pytania dotyczące sprzętów elektronicznych z których korzystają respondenci, trzecia część ankiety dotyczyła wiedzy o bezpieczeństwie w internecie, czwarta natomiast zawierała pytania dotyczące świadomości istniejących zagrożeń. Wszystkie wykorzystane w ankiecie pytania są pytaniami autorskimi.

Uzyskane od respondentów odpowiedzi wprowadzono do Arkusza Microsoft Office Excel i przeprowadzono ich analizę statystyczną z wykorzystaniem testu Chi-kwadrat. Różnice przy poziomie $p<0,05$ zostały uznane za istotne. Wyniki przedstawiono w formie graficznej.

3.2 Grupa badawcza i jej charakterystyka

Ankietę przeprowadzono u 100 osób. Największą grupę stanowiły osoby w wieku 18-24, natomiast najmniejszą - osoby powyżej 50 roku życia (rysunek 3).

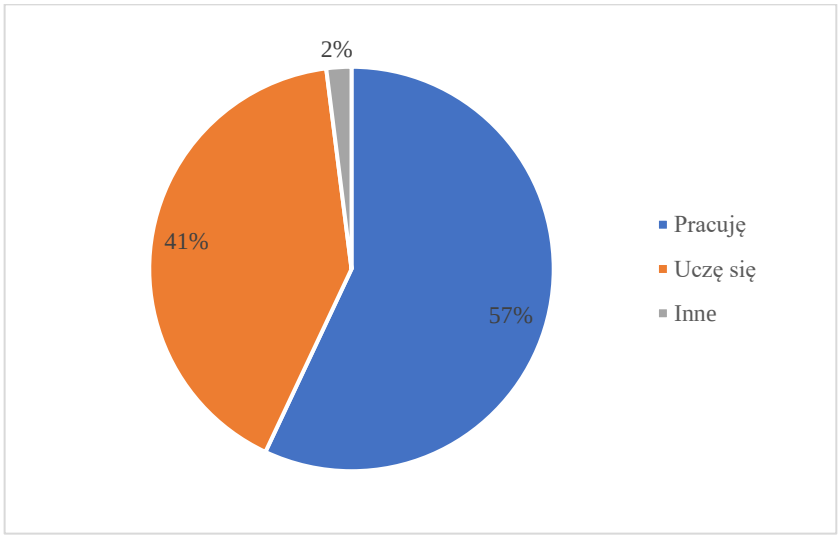
Rysunek 3. Rozkład wieku badanych respondentów



Źródło: opracowanie własne

Wśród badanych 57% to osoby pracujące, mniejszością są osoby na bezrobociu, rencie i emeryturze (rysunek 4).

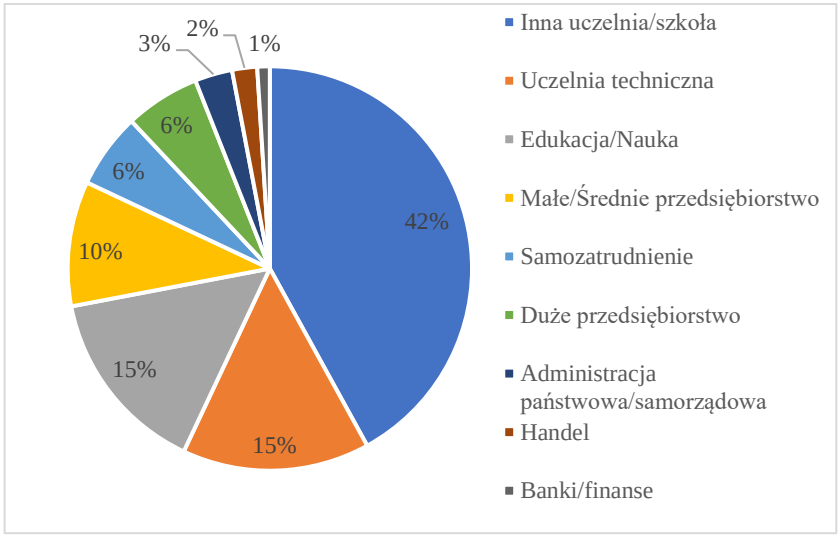
Rysunek 4. Sytuacja zawodowa badanych osób



Źródło: opracowanie własne

Na rysunku 5 przedstawiono miejsce pracy badanych respondentów. Największa część badanych osób studiowała na uczelni nietechnicznej, drugą pod względem liczności była grupa osób, które studiowały na uczelni technicznej i pracowały w dziedzinie edukacji lub nauki. Mniejszością były osoby zatrudnione w dziedzinie handlu i bankowości.

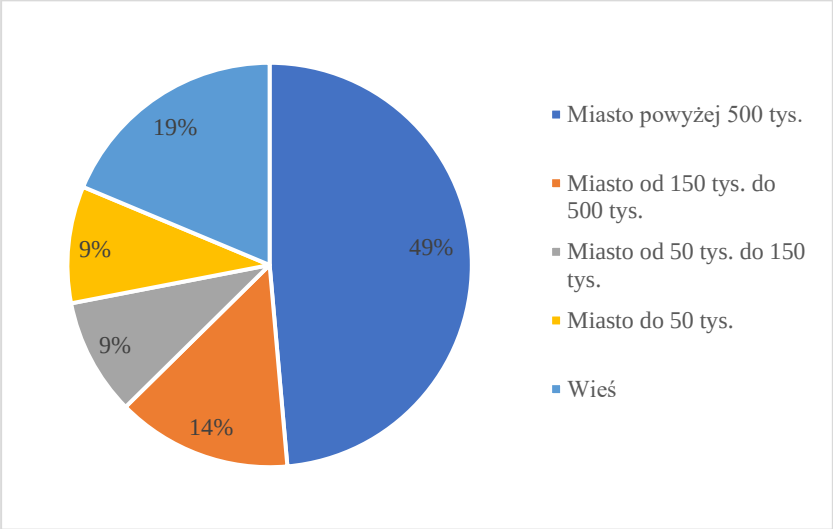
Rysunek 5. Miejsce pracy badanych respondentów



Źródło: opracowanie własne

Większość badanych mieszkała w mieście powyżej 500 tysięcy mieszkańców i na wsi. Najmniej osób mieszkało w mieście do 50 tysięcy i od 50 do 150 tysięcy mieszkańców (rysunek 6).

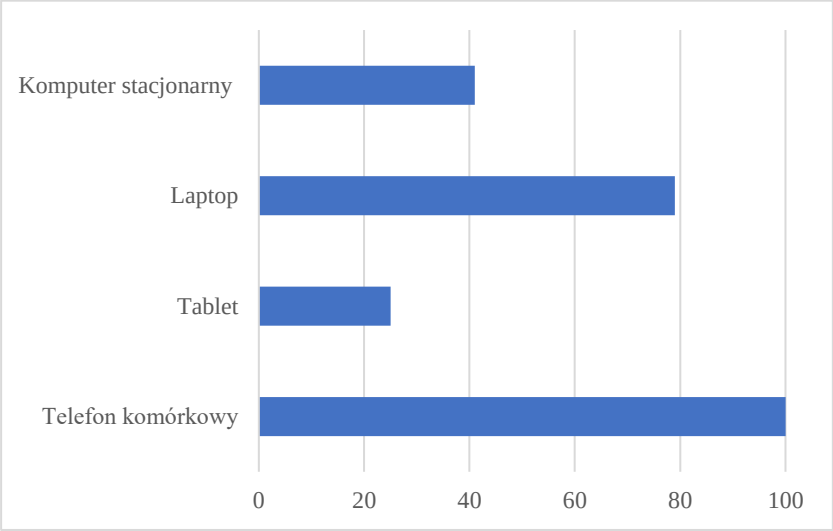
Rysunek 6. Miejsce zamieszkania badanych osób



Źródło: opracowanie własne

Wśród badanych najbardziej popularnym urządzeniem, z którego korzystali na co dzień był telefon (rysunek 7). Drugim popularnym urządzeniem był laptop, najczęściej ankietowani wybierali do codzienne pracy telefon komórkowy jak i laptop.

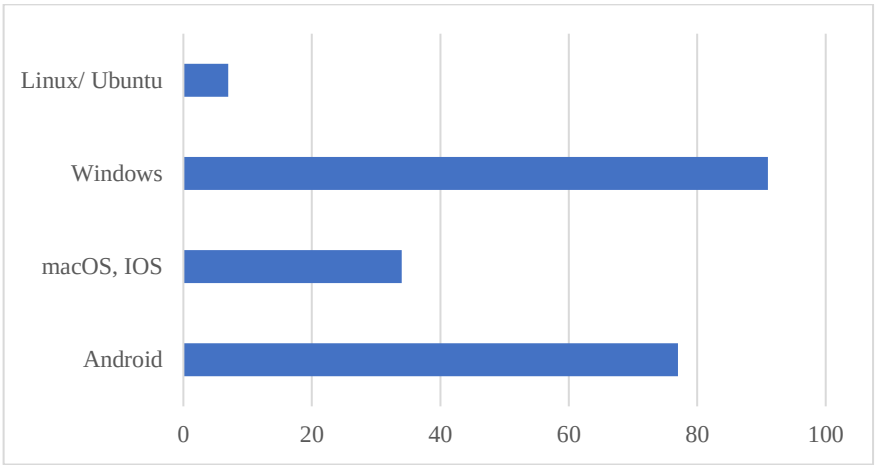
Rysunek 7. Narzędzia elektroniczne z jakich korzystają respondenci



Źródło: opracowanie własne

Respondenci korzystali na co dzień najczęściej z systemu Windows i Android. Najmniej osób korzystało z systemów Linux/Ubuntu (rysunek 8).

Rysunek 8. Systemy z jakich korzystają respondenci



Źródło: opracowanie własne

4. Wyniki badań

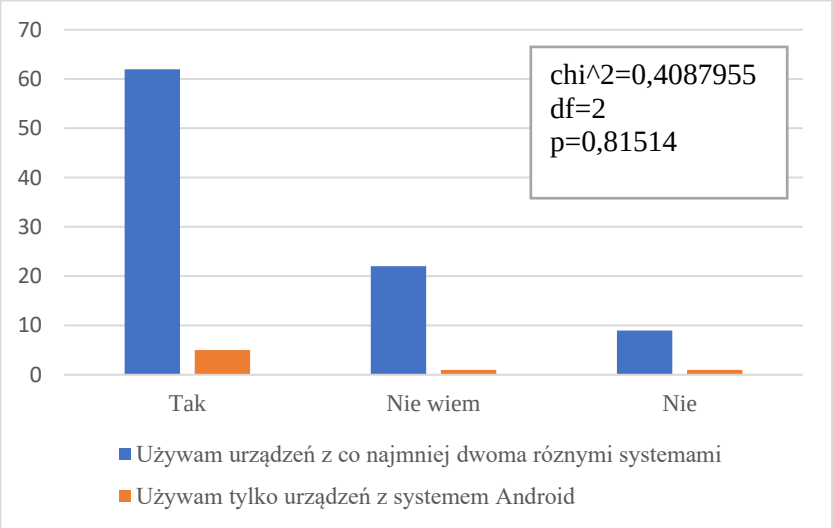
4.1. Ochrona sprzętu odpowiednim oprogramowaniem

Wiedza na temat posiadania zapory sieciowej na swoim sprzęcie elektronicznym

Zaporę sieciową posiadają prawie wszystkie popularne systemy na komputery, laptopy i urządzenia mobilne. Jedynym systemem, który nie posiada wbudowanej zapory sieciowej jest system Android. W przypadku innych systemów są one wbudowane i działają w tle bez jakiejkolwiek ingerencji użytkownika.

Na podstawie uzyskanych wyników z kwestionariusza ankietowego zaobserwowano, że większość respondentów (67%) uważało, że ma zainstalowaną zaporę sieciową na sprzęcie elektronicznym którego używa, 10% stwierdziło, że takowej nie posiada, a 23% nie miało wiedzy na ten temat (rysunek 9).

Rysunek 9. Posiadanie zapory sieciowej na sprzęcie elektronicznym

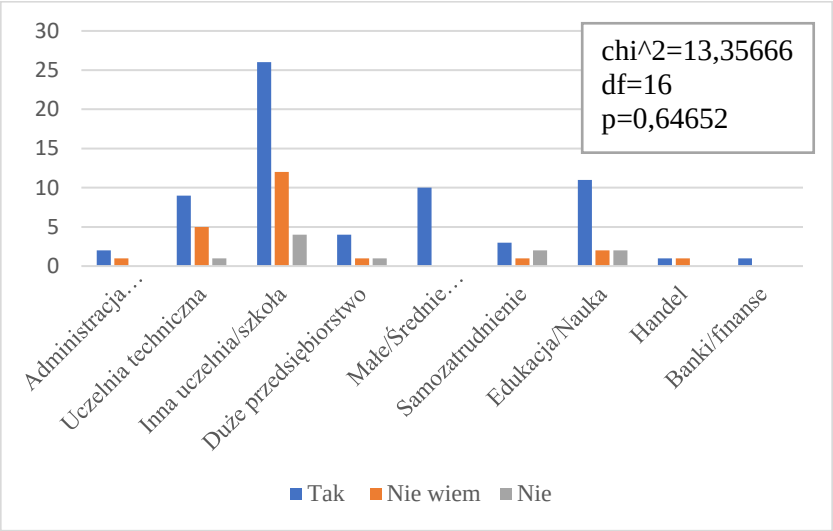


Źródło: opracowanie własne

W wyniku analizy statystycznej nie stwierdzono zależności pomiędzy korzystaniem z zapory sieciowej, a używaniem jedynie systemu Android (rysunek 9).

Najwięcej osób, które nie miało wiedzy na temat posiadana zapory lub uważało, że jej nie posiada (40%) uczyło się na uczelni technicznej. Drugą grupą byli pracownicy lub studenci uczelni nietechnicznych (38%) (rysunek 10).

Rysunek 10. Wiedza dotyczącą zainstalowanej zapory sieciowej w zależności od miejsca zatrudnienia lub studiowania



Źródło: opracowanie własne

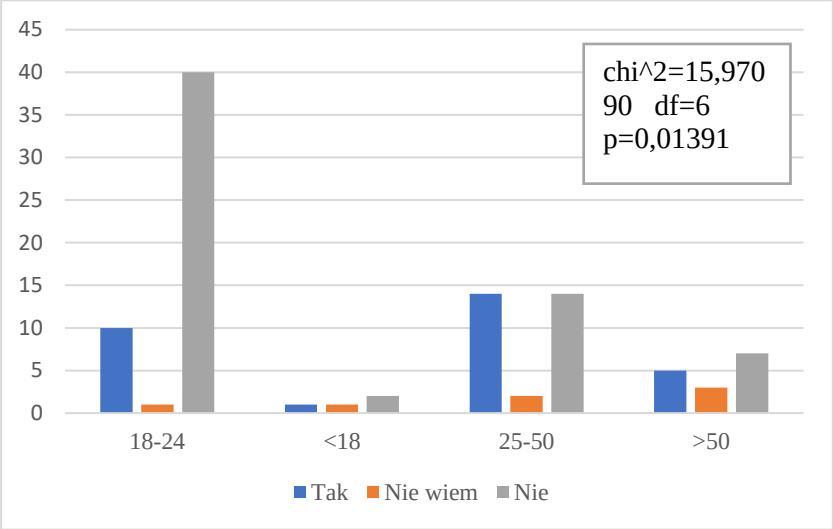
Nie znaleziono zależności pomiędzy obszarem zatrudnienia lub studiowania, a wiedzą dotyczącą zainstalowanej zapory sieciowej (rysunek 10).

Wybór płatnych usług ochrony Internetu

Różnorodne usługi ochrony Internetu są proponowane przez dostawców i sieci komórkowe. Zazwyczaj usługi takie są dostępne w pakietach z ochroną rodzicielską i działają podobnie do standardowego antywirusa. Każdy usługodawca zaleca pobranie odpowiedniej aplikacji, która działa w tle i chroni urządzenia przed zagrożeniami pochodzącymi z Internetu. Na podstawie uzyskanych wyników z autorskiej ankiety stwierdzono, że większość ankietowanych (63%) nie korzystała z płatnych usług ochrony Internetu w domu. 7% osób nie wiedziało, czy ma wykupione takie usługi, natomiast 30% taką usługę posiadało.

Wykupowanie usług ochrony Internetu najbardziej popularne było w grupie wiekowej 25-50 lat (47%). Na drugim miejscu znajdowała się grupa wiekowa powyżej 50 roku życia (33%) natomiast najwięcej osób, które nie korzystają z takich usług to grupa 18-24 lat i było to aż 78% ankietowanych (rysunek 11).

Rysunek 11. Zależność pomiędzy wiekiem badanych osób a wybór dodatkowych usług



Źródło: opracowanie własne

Analiza statystyczna wykazała istotny wpływ wieku ankietowanych na wybór dodatkowych usług ochrony Internetu (rysunek 11).

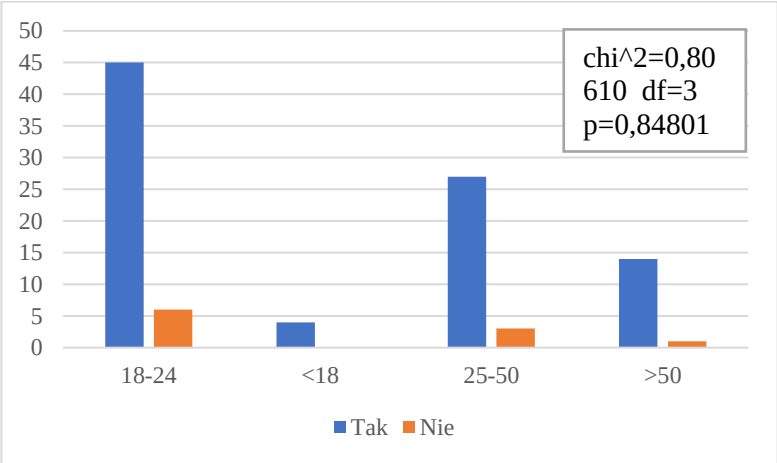
Posiadanie programów antywirusowych i antyszpiegowskich

Wiele systemów ma wbudowanego antywirusa, który bez wiedzy użytkownika pracuje w tle i blokuje niepożądane pliki. Coraz częściej jednak wybierane są dodatkowe programy antywirusowe i szpiegowskie, a ich popularność wciąż wzrasta.

W wyniku analizy otrzymanych odpowiedzi od respondentów stwierdzono, że znacząca większość respondentów (90%) uważała, że posiada na swoich urządzaniach elektronicznych pogramy antywirusowe lub antyszpiegowskie, a tylko 10% zadeklarowało, że takowych nie posiada.

Największy procent osób, które uważają, że nie posiadają oprogramowania antywirusowego lub antyszpiegowskiego znajduje się w grupie wiekowej 18-24 lat (88%) (rysunek 12).

Rysunek 12. Zależność między wiekiem respondentów, a posiadaniem programów antywirusowych lub antyszpiegowskich

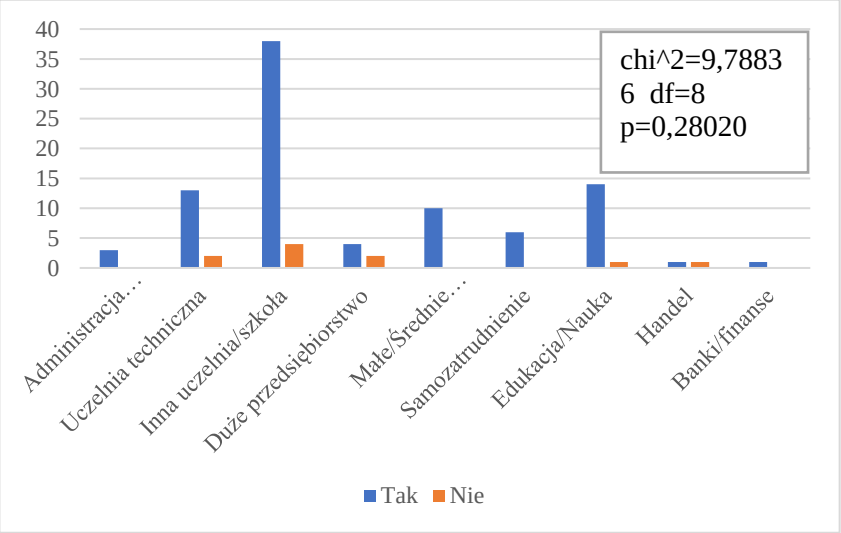


Źródło: opracowanie własne

Analizując zależność pomiędzy wiekiem respondentów, a posiadaniem programów antywirusowych lub antyszpiegowskich nie stwierdzono wpływu wieku na popularność stosowania tych programów (rysunek 12).

Wśród osób zatrudnionych w handlu tylko 50% uważa, że posiada takie oprogramowanie, druga w kolejności rosnącej jest grupa studiujących na uczelni technicznej (67%) (rysunek 13).

Rysunek 13. Zależność między obszarem zatrudnienia lub studiowania, a posiadaniem programów antywirusowych lub antyszpiegowskich



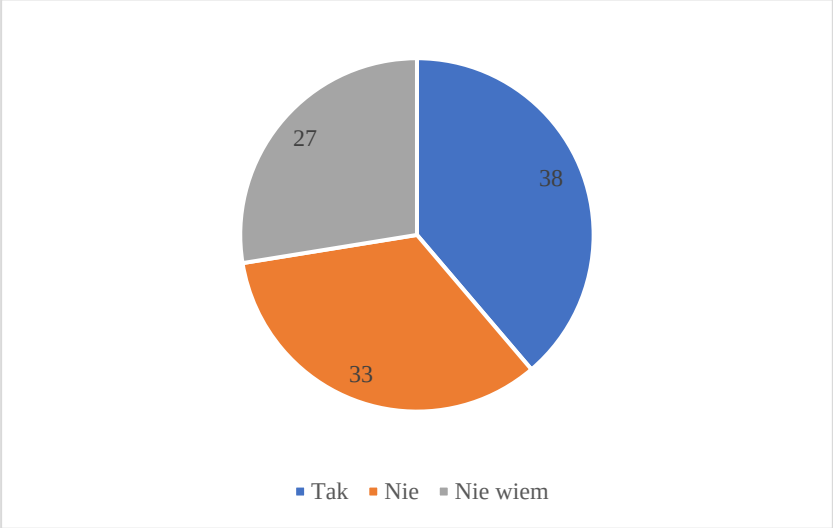
Źródło: opracowanie własne

Nie zanotowano również zależności między obszarem zatrudnienia lub studiowania, a posiadaniem programów antywirusowych lub antyszpiegowskich (rysunek 13).

Mechanizmy szyfrowania danych

Wśród respondentów większość uważała, że używa mechanizmów szyfrowania danych (38%). Nie używa tych mechanizmów aż 33%, natomiast 27% nie wiedziała czy takowej używa (rysunek 14).

Rysunek 14. Popularność stosowania mechanizmów szyfrowania danych



Źródło: opracowanie własne

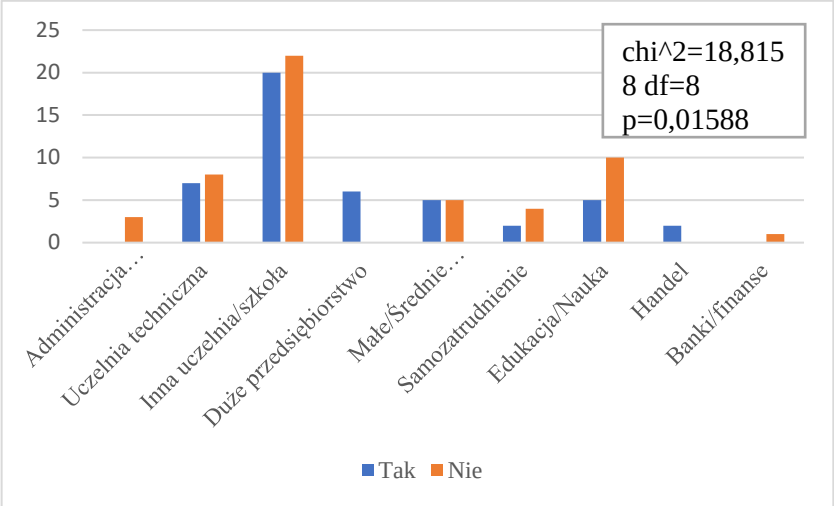
Znajomość funkcji zdalnej blokady urządzenia lub usunięcia danych

Wszystkie urządzenia mobilne oparte o system iOS bądź Android posiadają możliwość zdalnego wyczyszczenia danych z telefonu w razie kradzieży bądź zgubienia urządzenia. Urządzenia z systemem macOS i Windows również posiadają taką możliwość, jeśli tylko mamy podłączone urządzenia do kont wymaganych przez danych twórców.

Na podstawie wyników z autorskiego kwestionariusza zanotowano, że 53% respondentów nie zabezpiecza danych i urządzeń by umożliwić zdalną blokadę urządzenia lub usunięcie danych.

Zaobserwowano również, że wśród osób pracujący w administracji państwowej/ samorządowej i bankowości 100% osób uważało, że nie zabezpiecza danych i urządzeń by umożliwić zdalną blokadę urządzenia lub usunięcie danych, natomiast wśród osób pracujących w dużych przedsiębiorstwach 100% osób stwierdziło, że używa takich funkcji (rysunek 15).

Rysunek 15. Zależność między obszarem zatrudnienia lub studiowania, a zabezpieczaniem swoich danych i sprzętu by umożliwić zdalną blokadę lub usunięcie danych

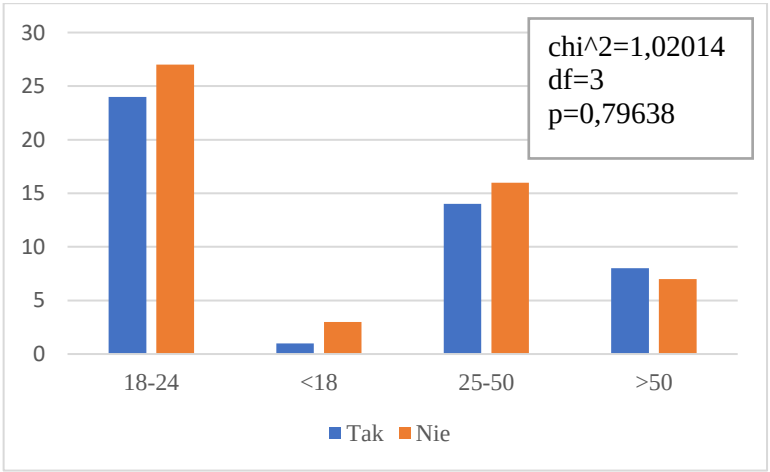


Źródło: opracowanie własne

W wyniku analizy statystycznej stwierdzono, że istnieje zależność między obszarem zatrudnienia lub studiowania, a zabezpieczaniem swoich danych i sprzętu by umożliwić zdalną blokadę lub usunięcie danych (rysunek 15).

W grupie powyżej 50 roku życia najczęściej respondenci deklarowali korzystanie z opcji zabezpieczania danych by umożliwić zdalne blokowanie urządzenia lub usuwanie danych (53%). Najrzadziej korzystanie z tej opcji deklarowały osób poniżej 18 roku życia (25%) (rysunek 16).

Rysunek 16. Zależność między wiekiem, a zabezpieczaniem swoich danych i sprzętu by umożliwić zdalną blokadę lub usunięcie danych



Źródło: opracowanie własne

Analiza statystyczna wykazała, że nie ma zależności między wiekiem, a zabezpieczaniem swoich danych i sprzętu by umożliwić zdalną blokadę lub usunięcie danych (rysunek 16).

4.2 Tworzenie i używanie bezpiecznych haseł

Wybór bezpiecznego hasła z przygotowanej listy

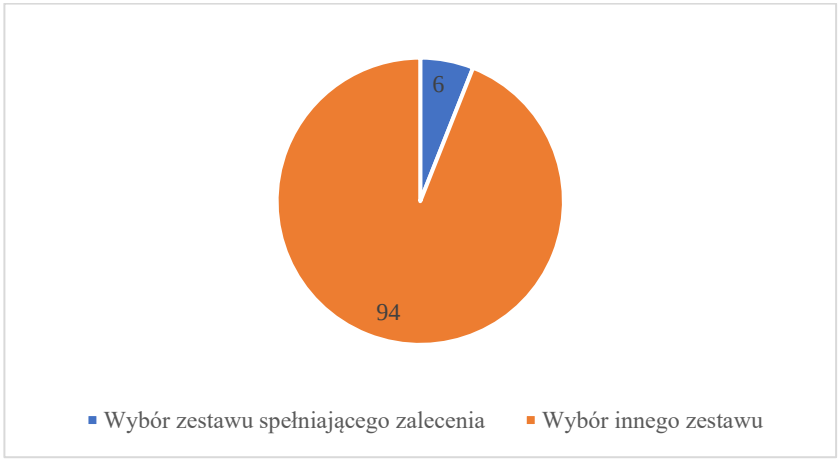
Właściwe hasła to podstawa bezpiecznego sprzętu oraz swoich danych w sieci. Większość firm posiada swoją prywatną politykę tworzenia haseł oceniając za pomocą administratorów potencjalne ryzyka. Popularna opinia brzmi „im hasło dłuższe tym lepsze" i faktycznie hasło powinno być jak najdłuższe, ale również jak najbardziej skomplikowane. Nie powinno zawierać słów słownikowych, powinno zawierać kombinacje dużych i małych liter, cyfr i znaków specjalnych.

a) Zalecenia firmy Microsoft (https://support.microsoft.com/pl-pl/windows/tworzenie-i-u%C5%BCywanie-silnych-hase%C5%82-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb)

Firma Microsoft zaleca stosowanie haseł z co najmniej 12 znakami, najlepiej 14, kombinacją wielkich liter, małych liter, cyfr i symboli, niestosowanie słów słownikowych, nazw użytkowników, nazw produktu czy organizacji, indywidualne dla tej platformy i przede wszystkim łatwych do zapamiętania, ale trudnych do odgadnięcia.

Według powyższych wytycznych tylko 6% respondentów wybrało poprawny zestaw haseł z listy wielokrotnego wyboru (rysunek 15). Hasłami spełniającymi powyższą politykę były hasła: „R@dosnyM*rs2022" i „T*talnaM@sakracja50%" (rysunek 17).

Rysunek 17. Ilość respondentów deklarujących wybór haseł zgodnie z zaleceniami firmy Microsoft



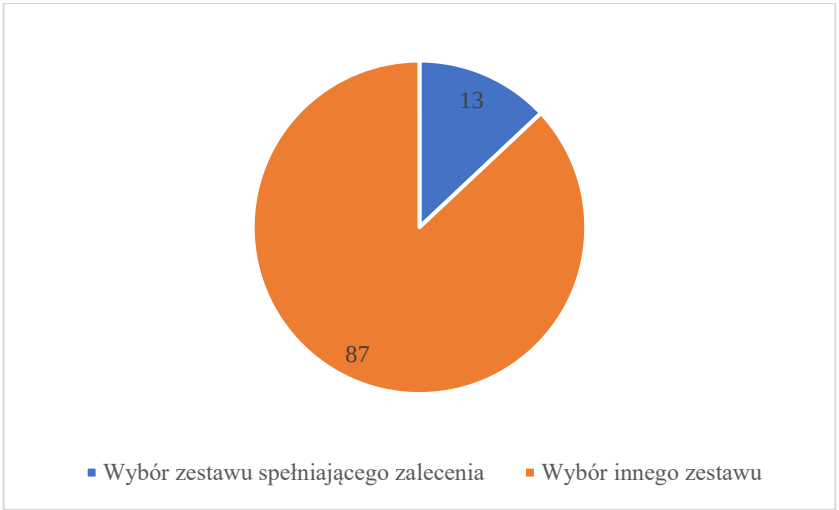
Źródło: opracowanie własne

b) Zalecenia mBank (https://www.mbank.pl/mbank-news/co-nowego/sposoby-na-tworzenie-mocnych-hasel.html)

Instytucja finansowa mBank sugeruje by hasło miało co najmniej 8 znaków w tym wielkich i małych liter, cyfr i znaków specjalnych, było wyjątkowe dla tej platformy i by nie zawierało imion członów rodziny, peseli i dat urodzeń.

Powyższe wytyczne spełniają trzy hasła użyte w ankiecie: „R@dosnyM*rs2022", „T*talnaM@sakracja50%" i „soK8%6Af". Taki zestaw haseł wybrało 13% respondentów (rysunek 18).

Rysunek 18. Ilość respondentów deklarujących wybór haseł zgodnie z zaleceniami mBank



Źródło: opracowanie własne

c) Zalecenia firmy Meta dla portalu Facebook (https://www.facebook.com/help/124904560921566)

Firma Meta zaleca by dla portalu Facebook hasła były wyjątkowe dla tej platformy, łatwe do zapamiętania, ale trudne do zgadnięcia oraz nie powinny zawierać popularnych słów, e-maili, numerów telefonów i dat urodzenia. Konglomerat Meta sugeruje również, że dłuższe hasła są bezpieczniejsze jednak nie podaje minimalnej liczny znaków.

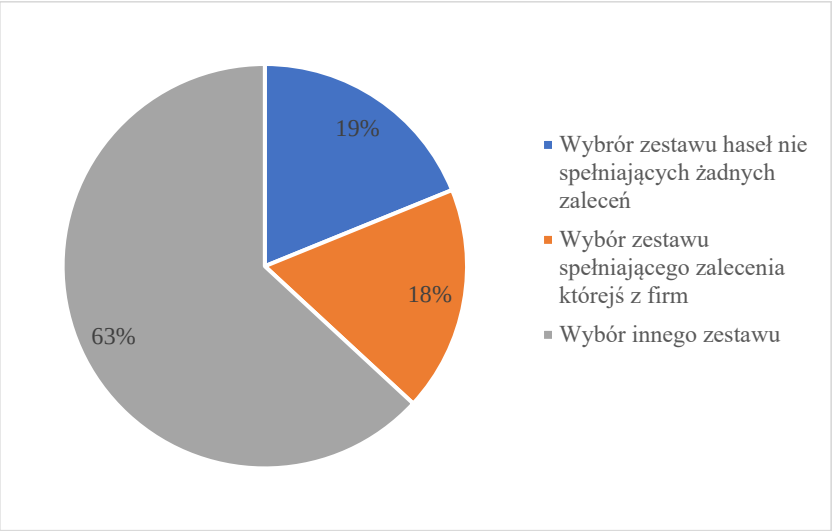
Zalecenia te są stosunkowo niekonkretne co zmusza użytkownika do własnej interpretacji, na przykład czy dane słowo użyte w haśle jest popularne lub ile znaków to dłuższe hasło. Pośród podanych w ankiecie haseł, aż 6 haseł spełnia te zalecenia: „R@dosnyM*rs2022", „a6YzgpKYhd", „T*talnaM@sakracja50%", „V6Bmt", „soK8%6Af", „njeniuod". Taki zestaw odpowiedzi wybrało 3% respondentów (rysunek 19).

Rysunek 19. Ilość respondentów deklarujących wybór haseł zgodnie z zaleceniami firmy Meta

Źródło: opracowanie własne

Wśród respondentów aż 23% wybrało zestawy haseł, które nie spełniły zaleceń którejkolwiek z firm. Pozostałe 77% osób wybrało niepełne pakiety poprawnych haseł (np. 2 z 3 poprawnych według konkretnego zalecenia) (rysunek 20).

Rysunek 20. Ilość respondentów deklarujących wybór zestawu haseł spełniających lub niespełniających zalecenia jakichkolwiek firm

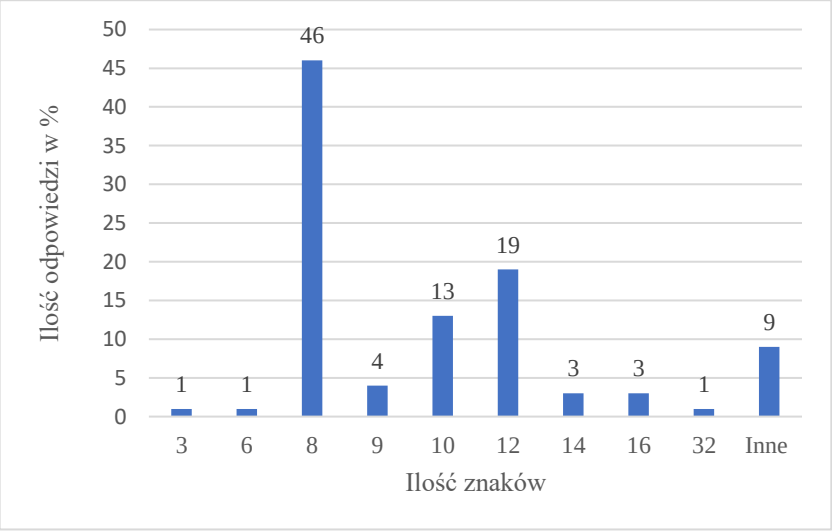


Źródło: opracowanie własne

Ilość znaków w bezpiecznym haśle

Największa część osób biorących udział w ankiecie wskazała, że bezpieczne hasło powinno posiadać co najmniej 8 znaków (46%). Najmniej osób uznało, że bezpieczne hasło powinno składać się z 3 (1%), 6 (1%) i 32 znaków (1%). 9% osób podało odpowiedzi niejednoznaczne (rysunek 21).

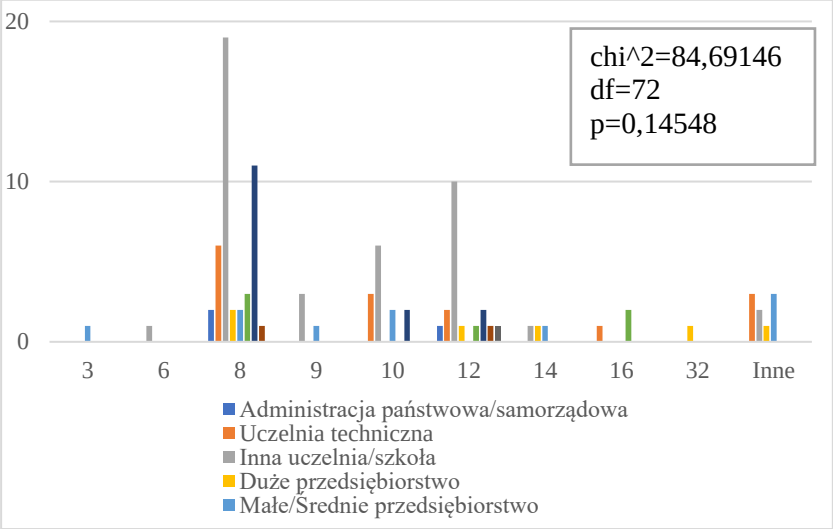
Rysunek 21. Odpowiedź respondentów dotycząca ilości znaków w haśle



Źródło: opracowanie własne

W grupie osób pracujących w administracji państwowej/ samorządowej (2%), edukacji (11%), dużych przedsiębiorstwach (2%) i na samozatrudnieniu (3%) większość wskazała, że bezpieczne hasło powinno mieć co najmniej 8 znaków. Taką odpowiedź wskazała też większość osób studiujących na uczelniach technicznych (6%) i nietechnicznych (19%). Wśród osób pracujących w banku najpopularniejszą odpowiedzią było 12 znaków (1%), a w handlu równie popularnymi odpowiedziami było 8 i 12 znaków. W grupie pracującej w małych i średnich przedsiębiorstwach respondenci w większości wybrali odpowiedź „inne" (rysunek 22).

Rysunek 22. Wpływ obszaru zatrudnienia lub studiowania na deklarację liczby znaków w bezpiecznym haśle



Źródło: opracowanie własne

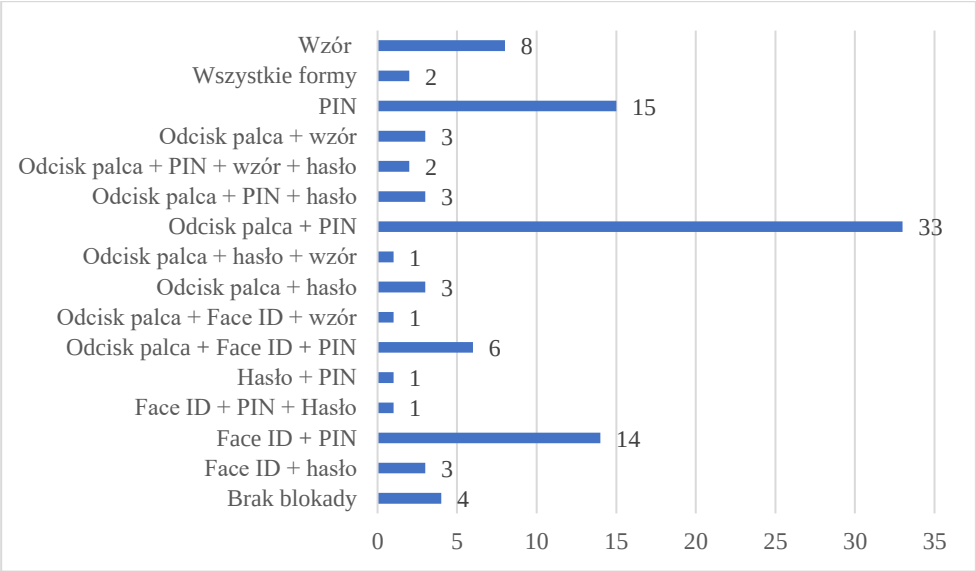
Analiza statystyczna nie wykazała wpływu między obszarem zatrudnienia lub studiowania, a wskazywaną liczbą znaków w bezpiecznym haśle (rysunek 19).

Hasło ekranu blokady

Telefony z systemem Android i iOS oferują kilka różnych form odblokowywania ekranu. Najbardziej popularną formą jest PIN i wzór, a mniej popularną formą jest hasło. W zależności od modelu telefonu, producenci oferują dodatkowo możliwość odblokowywania ekranu odciskiem palca lub Face ID.

Wśród respondentów najczęściej wybieraną formą odblokowywania ekranu był odcisk palca i PIN (33%) oraz Face ID i PIN (14%). Aż 4 % respondentów deklaruje, że nie używa hasła ekranu blokady (rysunek 23).

Rysunek 23. Deklaracja przez respondentów metody blokady ekranu



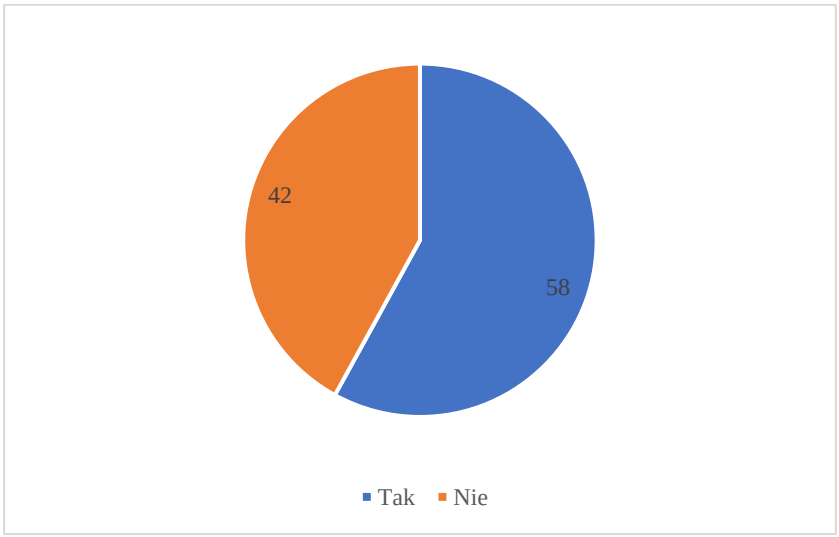
Źródło: opracowanie własne

Menadżery haseł

Używanie menadżera haseł jest jednym z najpopularniejszych zaleceń by jeszcze lepiej zabezpieczać swoje dane osobowe, konta e-mailowe czy konta na różnorodnych portalach. Dzięki takiemu narzędziu użytkownik może bezpiecznie przechowywać swoje hasła i sięgać do nich w razie potrzeby, ale nie musi ich pamiętać. To znacząco odciąża użytkownika i sprawia, że przestaje mieć opory przed stosowaniem wyjątkowych haseł do platform, a same hasła są bardziej skomplikowane i dłuższe.

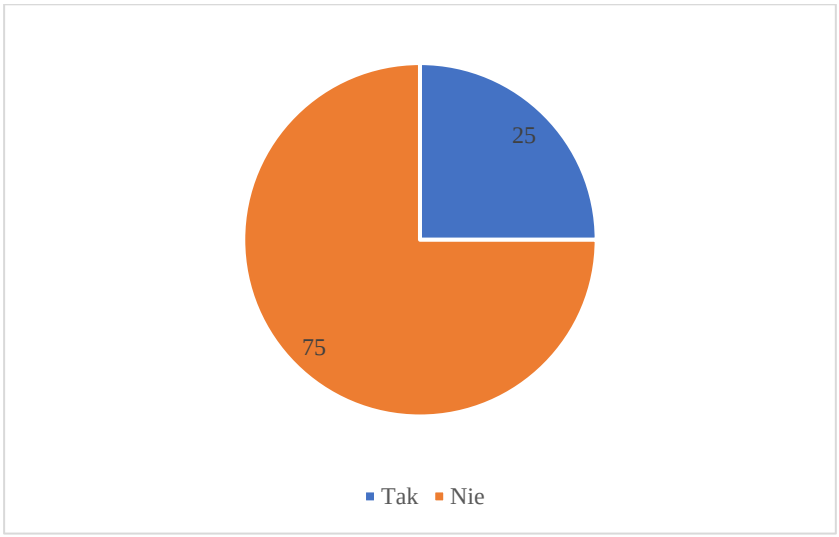
Na urządzeniach prywatnych korzysta z menadżerów haseł 58% respondentów (rysunek 24), natomiast na sprzęcie firmowym, korzystanie z menadżera urządzeń zdeklarowało już tylko 25% (rysunek 25).

Rysunek 24. Korzystanie przez respondentów z menadżerów haseł na urządzeniach prywatnych



Źródło: opracowanie własne

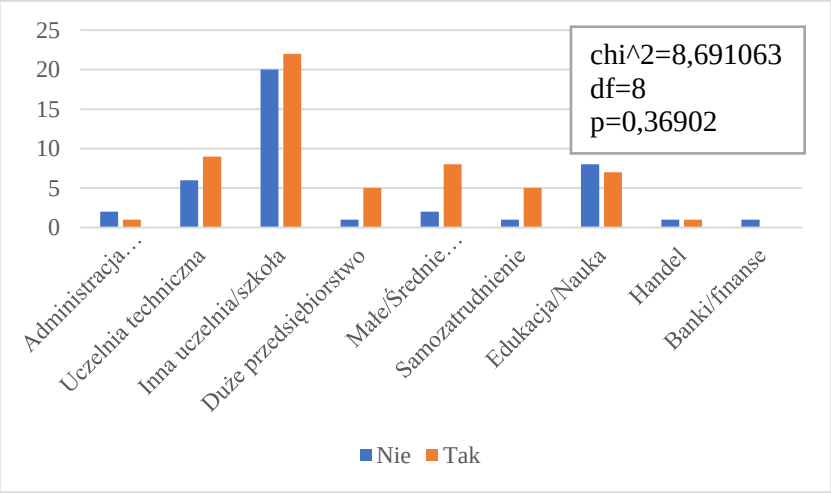
Rysunek 25. Korzystanie przez respondentów z menadżerów haseł na urządzeniach firmowych



Źródło: opracowanie własne

Stosowanie menadżera haseł na urządzeniach domowych najczęściej deklarowane było przez osoby na samozatrudnieniu (83%) i pracujących w dużych przedsiębiorstwach (83%). Najrzadziej używanie tego narzędzia deklarowały osoby pracujące w administracji państwowej/ samorządowej (33%) (rysunek 26).

Rysunek 26. Korzystanie przez respondentów z menadżerów haseł na urządzeniach prywatnych w zależności od obszaru zatrudnienia lub studiowania

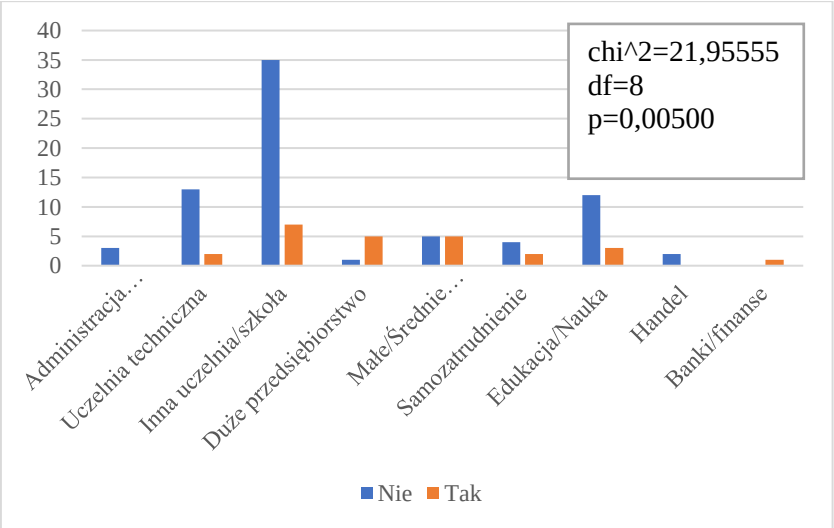


Źródło: opracowanie własne

Nie stwierdzono zależności pomiędzy obszarem zatrudnienia/ studiowania, a używaniem menadżera urządzeń na prywatnych urządzeniach (rysunek 26).

Korzystanie z menadżera haseł na urządzeniach firmowych najpopularniejsze było wśród osób pracujących w dużych przedsiębiorstwach (83%). Wszystkie osoby pracujące w administracji państwowej/ samorządowej i handlu zadeklarowały, że nie używają menadżera haseł na urządzeniach firmowych (rysunek 27).

Rysunek 27. Korzystanie przez respondentów z menadżerów haseł na urządzeniach firmowych w zależności od obszaru zatrudnienia lub studiowania



Źródło: opracowanie własne

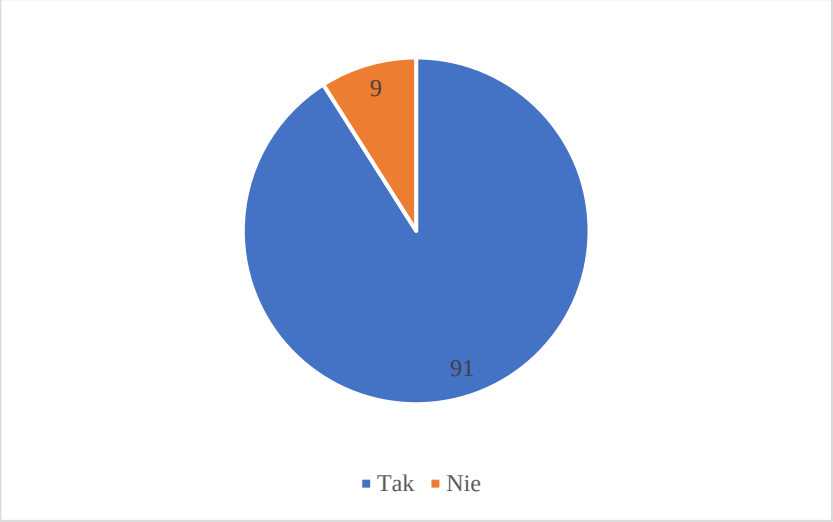
Analiza statystyczna wykazała wysoko istotny wpływ ($p<0.01$) obszaru zatrudnienia/ studiowania na korzystanie z menadżera haseł na urządzeniach firmowych (rysunek 27).

Nawyk zmiany hasła

Niektóre firmy mają w swojej polityce haseł wymóg regularnego zmieniania hasła. Taka cykliczna zmiana hasła może zapobiegać wielu zagrożeniom, szczególnie w sytuacji, gdy z innej firmy zostaną nielegalnie pozyskane dane użytkowników i hasła. Podobną politykę posiada wiele portali Internetowych, użytkownik zostaje co pewien czas poproszony o zmianę hasła. Powodem takich działań jest również to, że użytkownicy bardzo rzadko zmieniają hasła do portali Internetowych.

Wśród respondentów aż 91% deklaruje, że stosuje indywidualne hasła do różnych portali (rysunek 28).

Rysunek 28. Stosowanie różnych haseł do różnorodnych portali



Źródło: opracowanie własne

Respondenci najczęściej deklarowali, że zmieniają hasło w przypadku, kiedy zapomną dotychczasowego hasła, kiedy z kontem dzieje się coś nie typowego, albo po uzyskaniu informacji od serwisu o możliwym wycieku danych (33%). Duża część ankietowanych zdeklarowała, że zmienia hasło tylko w przypadku, gdy nie pamięta hasła, albo gdy otrzyma informacje o wycieku danych (15%) oraz że zmienia hasło jedynie w wypadku, gdy nie pamięta hasła (12%). Tylko 1% osób odpowiedziało, że zmienia hasło we wszystkich podanych przypadkach, kiedy zapomni hasła, kiedy z kontem dzieje się coś nietypowego, po informacji o wycieku danych, od czasu do czasu bez powodu i regularnie kilka razy w roku (tabela 3).

Tabela 3. Przyczyny zmiany hasła deklarowane przez respondentów

Powody zmiany haseł	Ilość respondetnów
Kiedy z kontem dzieje się coś nietypowego	3
Kiedy z kontem dzieje się coś nietypowego, od czasu do czasu bez powodu	1
Kiedy z kontem dzieje się coś nietypowego, po informacjach o wycieku	3
Kiedy z kontem dzieje się coś nietypowego, regularnie kilka razy do roku	1
Od czasu do czasu bez powodu	8
Po informacjach od serwisu o możliwym wycieku danych	2
Regularnie kilka razy w roku	2
Wszystkie poza regularną zmianą hasła	5
Wszystkie poza zmianą od czasu do czasu	2
Wszystkie przypadki	1
Z kontem dzieje się coś nietypowego, po informacji o możliwym wycieku, od czasu do czasu	2
Z kontem dzieje się coś nietypowego, po informacji o możliwym wycieku, regularnie kilka razy w roku	1
Zapomnienie hasła	12
Zapomnienie hasła, kiedy z kontem dzieje się coś nietypowego	15
Zapomnienie hasła, od czasu do czasu bez powodu	3
Zapomnienie hasła, po informacji o potencjalnym wycieku	3
Zapomnienie hasła, po informacji o potencjalnym wycieku, od czasu do czasu	1
Zapomnienie hasła, po informacji o potencjalnym wycieku, regularnie kilka razy w roku	1
Zapomnienie hasła, z kontem dzieje się coś nietypowego, od czasu do czasu	1
Zapomnienie hasła, z kontem dzieje się coś nietypowego, po informacji o potencjalnym wycieku	33

Źródło: opracowanie własne

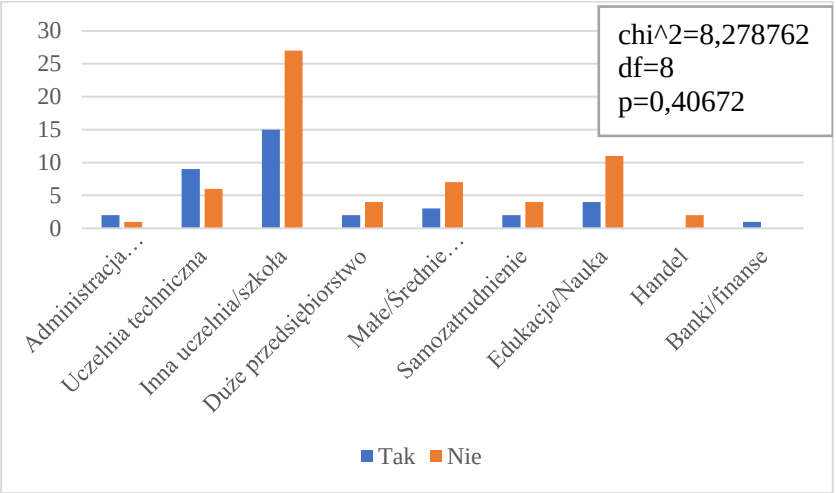
4.3 Świadomość zagrożeń związanych z potencjalnymi atakami i wyciekiem danych

Świadomość cyberataków i wycieków danych w przeszłości

Wycieki danych czy cyberataki mają miejsce na tyle często, że powoli niemożliwym jest uchowanie swoich danych przed wyciekiem czy kradzieżą. Kupując w sklepach Internetowych, zapisując się do różnorodnych newsletterów lub podając dane na portalach aukcyjnych użytkownik powinien mieć świadomość, że najprawdopodobniej jego dane chociaż raz w życiu wyciekły. Coraz popularniejsze robią się też próby ataków, w szczególności wyłudzenia pieniędzy poprzez oszustwa.

Wśród respondentów 62% wskazało, że nigdy nie zostało ofiarą cyberataku. Odpowiedź, że respondent został kiedyś ofiarą ataku najbardziej popularna była w grupie osób pracujących w bankowości (100%), administracji państwowej/ samorządowej (67%) lub studiujących na uczelni technicznej (60%), najmniej popularna była natomiast wśród osób pracujących w handlu (rysunek 29).

Rysunek 29. Zależność między obszarem zatrudnienia lub studiowania, a odpowiedzią czy respondent uważa, że był ofiarą cyberataku

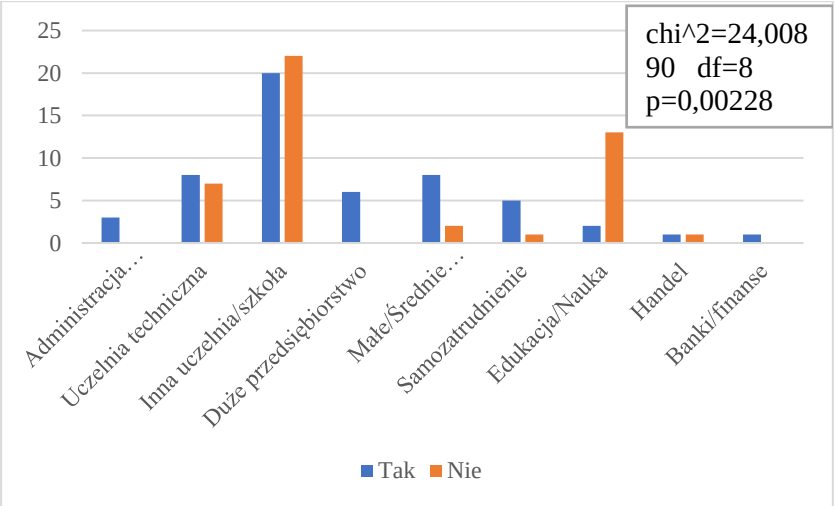


Źródło: opracowanie własne

Nie stwierdzono zależności pomiędzy obszarem zatrudnienia lub studiowania, a odpowiedzią czy respondent uważa, że był ofiarą cyberataku (rysunek 29).

Aż 54% ankietowanych uważało, że kiedyś ich dane mogły wycieknąć. Ta odpowiedź najmniej popularna była w grupie osób pracujących w edukacji/ nauce (13%) i studiujących na uczelniach nietechnicznych (48%). Najczęściej natomiast taką odpowiedź wybrały osoby pracujące w dużym przedsiębiorstwie (100%), administracji państwowej/ samorządowej (100%) i bankowości (100%) (rysunek 30).

Rysunek 30. Zależność między obszarem zatrudnienia lub studiowania, a odpowiedzią czy respondent uważa, że jego dane wyciekły z zabezpieczonych baz danych.



Źródło: opracowanie własne

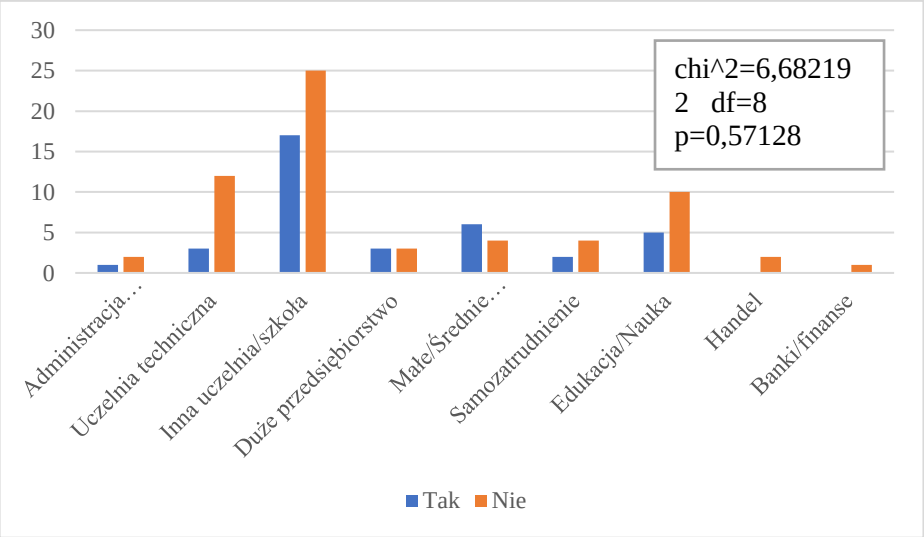
Analiza statystyczna wykazała wysoko istotny wpływ obszaru zatrudnienia lub studiowania na odpowiedź czy respondent uważa, że jego dane wyciekły z zabezpieczonych baz danych (rysunek 30).

Śledzenie informacji o wyciekach danych i atakach hakerskich

Stosowanie aplikacji z cyberalertami, śledzenie na bieżąco wycieków danych i aktualnych trendów pośród oszustów może znacząc zwiększyć bezpieczeństwo użytkowników w sieci i zapobiec wielu problemom i czasami nawet życiowym tragediom.

Większość respondentów zdeklarował, że nie śledzi na bieżąco informacji o wyciekach danych (63%). Najczęściej deklaracja śledzenia na bieżąco takich informacji padała wśród osób pracujących w dużych przedsiębiorstwach (60%) oraz w małych i średnich przedsiębiorstwach (50%). Takiej odpowiedzi nie zdeklarowała żadna osoba pracująca w handlu i bankowości (rysunek 31).

Rysunek 31. Zależność między obszarem zatrudnienia, a deklarowaniem śledzenia na bieżąco informacji o wyciekach danych

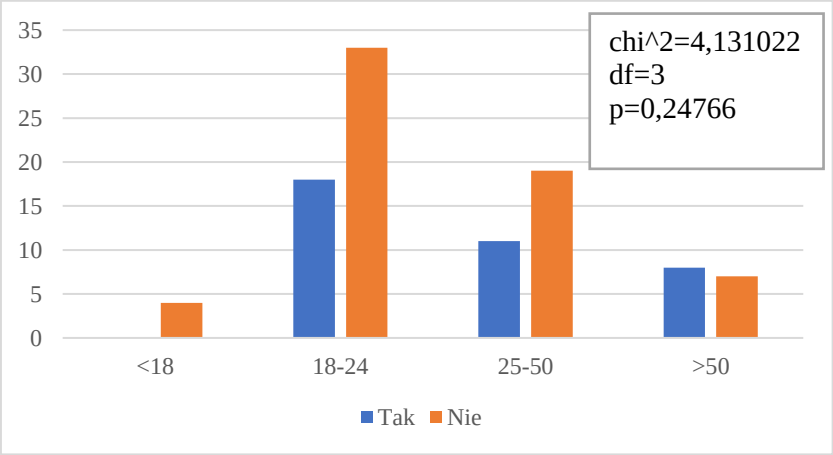


Źródło: opracowanie własne

Nie stwierdzono zależności pomiędzy obszarem zatrudnienia, a deklarowaniem śledzenia na bieżąco informacji o wyciekach danych (rysunek 31).

Informacje o wyciekach danych najczęściej śledziły osoby w grupie wiekowej powyżej 50 roku życia (53%). W grupie wiekowej poniżej 18 roku życia natomiast nikt nie zdeklarował takiej odpowiedzi (rysunek 32).

Rysunek 32. Zależność między grupą wiekową, a deklaracją śledzenia informacji o wyciekach danych

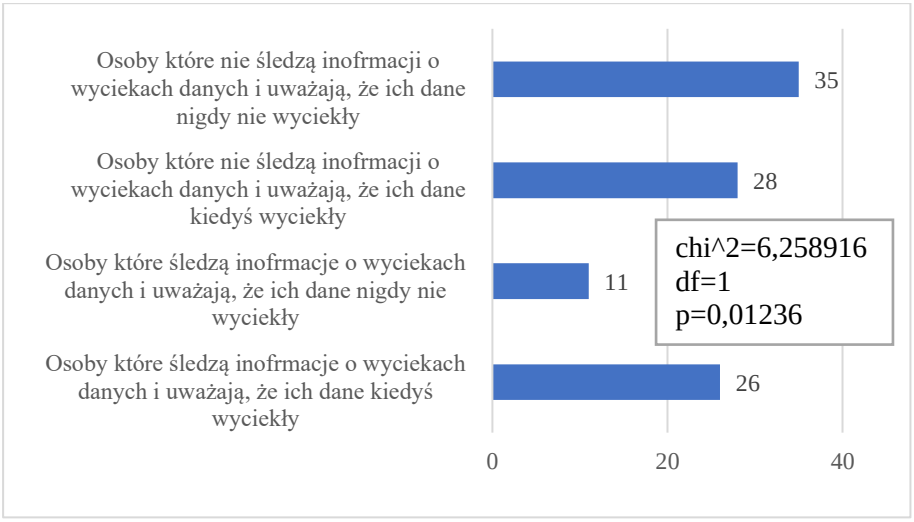


Źródło: opracowanie własne

Analiza statystyczna nie wykazała wpływu wieku grupy na deklarację śledzenia informacji o wyciekach danych (rysunek 32).

Dodatkowa analiza wykazała istotny wpływ śledzenia informacji o wyciekach danych na deklarację, że dane respondentów mogły kiedykolwiek wyciec z zabezpieczonych baz danych. 35% ankietowanych nie śledziła danych o wyciekach zarazem uważając, że ich dane nigdy nie wyciekły (rysunek 33).

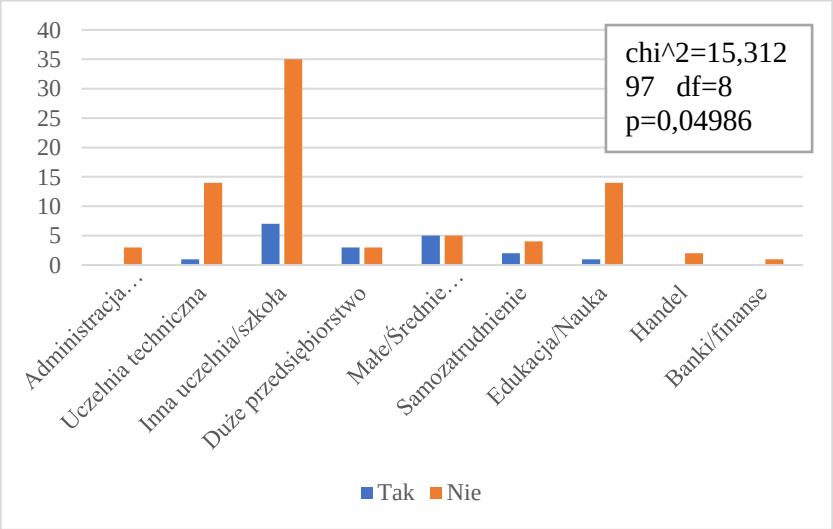
Rysunek 33. Zależność między śledzeniem informacji o wyciekach danych przez użytkownika, a deklaracją, że dane respondenta mogły kiedykolwiek wyciec z zabezpieczonych baz danych



Źródło: opracowanie własne

Wśród respondentów tylko 19% zdeklarowało, że na bieżąco śledzi informacje w wyspecjalizowanych serwisach o atakach hakerskich i innych zagrożeniach w sieci. Najczęściej taka deklaracja padała wśród osób pracujących w dużych (50%) oraz w średnich i małych (50%) przedsiębiorstwach. Wśród osób pracujących w administracji państwowej/ samorządowej, bankowości i handlu żaden ankietowany nie zadeklarował śledzenia takich informacji (rysunek 34).

Rysunek 34. Zależność między dziedziną zatrudnienia lub studiowania, a deklaracją śledzenia informacji o atakach hakerskich i innych zagrożeniach w sieci

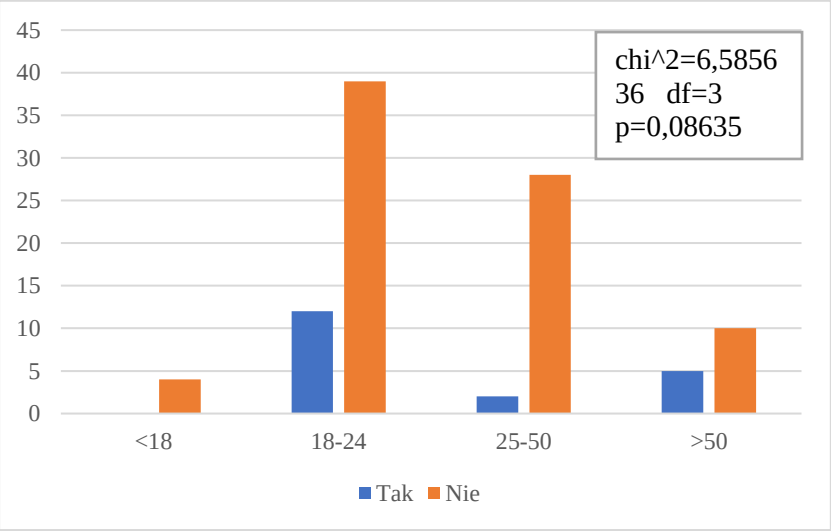


Źródło: opracowanie własne

Analiza statystyczna wykazała istotny wpływ miejsca zatrudnienia lub studiowania na deklarację śledzenia informacji o atakach hakerskich i innych zagrożeniach w sieci (rysunek 34).

Najczęściej informacje o zagrożeniach w sieci i atakach hakerskich śledzą osoby powyżej 50 roku życia (33%), najrzadziej natomiast osoby poniżej 18 roku życia (rysunek 35).

Rysunek 35. Zależność między grupą wiekową, a śledzeniem informacji w wyspecjalizowanych serwisach o atakach hakerskich i innych zagrożeniach w sieci



Źródło: opracowanie własne

Nie stwierdzono zależności między grupą wiekową, a śledzeniem informacji w wyspecjalizowanych serwisach o atakach hakerskich i innych zagrożeniach w sieci (rysunek 35).

Dane osobowe, których wyciek jest niebezpieczny

Najczęściej respondenci pośród 9 danych osobowych (PESEL, numer dowodu osobistego, imię i nazwisko, e-mail, numer telefonu, adres zamieszkania, adres IP, dane o medycznym stanie pacjenta) uznali, że najniebezpieczniejszy jest wyciek numeru PESEL, numeru dowodu osobistego, imienia i nazwiska, e-maila, numeru telefonu, adresu zamieszkania, adresu IP i danych o medycznym stanie pacjenta (10%) oraz numeru PESEL, numeru dowodu osobistego, adresu zamieszkania, adresu IP, danych o lokalizacji i danych o medycznym stanie pacjenta (10%).

Tabela 4. Wybór danych osobowych, których wyciek jest niebezpieczny

Dane osobowe których wyciek jest niebezpieczny	Ilość respondentów
PESEL, Numer dowodu osobistego, Imię i nazwisko, E-mail, Numer telefonu, Adres zamieszkania, Adres IP, Dane o medycznym stanie pacjenta	10
PESEL, Numer dowodu osobistego, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	10
PESEL, Numer dowodu osobistego, Imię i nazwisko, E-mail, Numer telefonu, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	6
PESEL, Numer dowodu osobistego, Imię i nazwisko, E-mail, Numer telefonu, Adres IP, Dane o lokalizacji	6
PESEL, Numer dowodu osobistego, Imię i nazwisko, Adres zamieszkania, Adres IP, Dane o lokalizacji	6
PESEL, Numer dowodu osobistego, E-mail, Adres zamieszkania, Adres IP, Dane o medycznym stanie pacjenta	4

Numer dowodu osobistego, E-mail, Numer telefonu, Adres zamieszkania, Dane o lokalizacji, Dane o medycznym stanie pacjenta	4
Numer dowodu osobistego, Adres zamieszkania, Adres IP, Dane o medycznym stanie pacjenta	4
PESEL, Numer dowodu osobistego, Imię i nazwisko, Numer telefonu, Adres IP, Dane o medycznym stanie pacjenta	3
PESEL, Numer dowodu osobistego, Imię i nazwisko	3
PESEL, Numer dowodu osobistego, E-mail, Numer telefonu, Dane o medycznym stanie pacjenta	3
PESEL, Numer dowodu osobistego, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	3
PESEL, Adres IP	3
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania	2
PESEL, Numer dowodu osobistego, Numer telefonu	2
PESEL, Numer dowodu osobistego, Dane o lokalizacji, Dane o medycznym stanie pacjenta	2
Dane o medycznym stanie pacjenta	2
PESEL, Numer dowodu osobistego, Numer telefonu, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Dane o lokalizacji	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Adres IP, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Numer telefonu, Adres zamieszkania, Adres IP	1
PESEL, Numer dowodu osobistego, Imię i nazwisko, Numer telefonu, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Imię i nazwisko, E-mail, Numer telefonu, Adres zamieszkania, Dane o lokalizacji	1
PESEL, Numer dowodu osobistego, Imię i nazwisko, Adres zamieszkania, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Imię i nazwisko, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Imię i nazwisko, Adres zamieszkania, Adres IP	1
PESEL, Numer dowodu osobistego, E-mail, Numer telefonu, Adres zamieszkania, Adres IP, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Dane o lokalizacji	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Dane o lokalizacji, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Dane o lokalizacji	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Adres IP, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Adres IP, Dane o lokalizacji	1
PESEL, Numer dowodu osobistego, Adres zamieszkania, Adres IP	1
PESEL, Numer dowodu osobistego, Adres IP, Dane o medycznym stanie pacjenta	1
PESEL, Numer dowodu osobistego, Adres IP	1
PESEL, Numer dowodu osobistego	1
PESEL, Imię i nazwisko, Numer telefonu, Adres zamieszkania, Adres IP	1
Numer dowodu osobistego, Dane o medycznym stanie pacjenta	1
Imię i nazwisko, Dane o lokalizacji	1

Źródło: opracowanie własne

Jednostki narażone na potencjalny cyberatak

Najczęściej respondenci wskazali, że jednostką najbardziej narażoną na cyberatak są zwykli użytkownicy nie stosujący zasad bezpieczeństwa (8%). Drugą najpopularniejszą odpowiedzią wskazywaną przez ankietowanych były wszystkie jednostki (banki, jednostki wojskowe, urzędy państwowe, prywatne firmy, organizacje non-profit, politycy, pracownicy zajmujący odpowiedzialne stanowiska w firmach, zwykli użytkownicy nie stosujący zasad bezpieczeństwa) wskazane w ankiecie (5%).

Tabela 5. Wybór jednostek najbardziej narażonych na potencjalny cyberatak

Jednostki narażone na potencjalny cyberatak	Ilość respondentów
Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	8
Banki, Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	5
Banki, Urzędy państwowe, Prywatne firmy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	4
Banki, Urzędy państwowe, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	4
Banki, Jednostki wojskowe, Urzędy państwowe, Politycy	3
Banki, Jednostki wojskowe, Urzędy państwowe, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	3
Banki, Prywatne firmy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	3
Prywatne firmy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	3
Urzędy państwowe, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	3
Banki, Jednostki wojskowe, Urzędy państwowe, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	2
Banki, Jednostki wojskowe, Urzędy państwowe, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Politycy	2
Banki, Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Prywatne firmy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Urzędy państwowe, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Urzędy państwowe, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Urzędy państwowe, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	2
Banki, Urzędy państwowe, Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	2
Banki, Urzędy państwowe, Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Prywatne firmy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Urzędy państwowe, Organizacje non-profit, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	2
Banki, Jednostki wojskowe, Politycy	1
Banki, Jednostki wojskowe, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	1

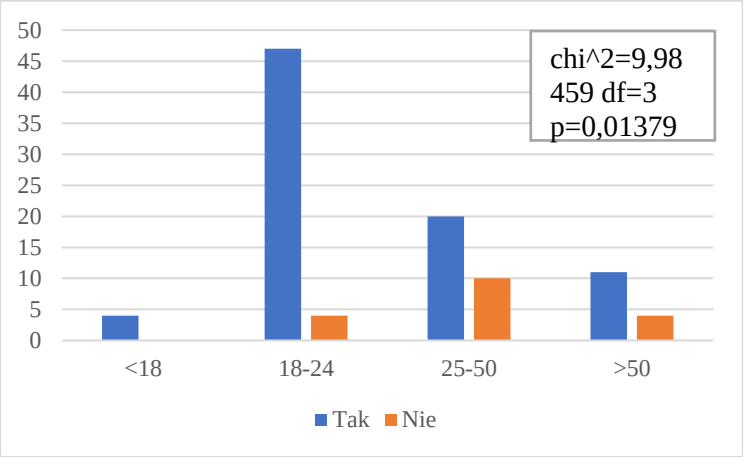
Banki, Jednostki wojskowe, Urzędy państwowe	1
Banki, Jednostki wojskowe, Urzędy państwowe, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Banki, Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	1
Banki, Prywatne firmy, Organizacje non-profit	1
Banki, Prywatne firmy, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Banki, Prywatne firmy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	1
Banki, Urzędy państwowe	1
Banki, Urzędy państwowe, Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Banki, Urzędy państwowe, Politycy	1
Banki, Urzędy państwowe, Prywatne firmy	1
Banki, Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Jednostki wojskowe, Prywatne firmy	1
Jednostki wojskowe, Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Jednostki wojskowe, Urzędy państwowe, Prywatne firmy	1
Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	1
Jednostki wojskowe, Urzędy państwowe, Prywatne firmy, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Organizacje non-profit, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach	1
Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Prywatne firmy, Organizacje non-profit	1
Prywatne firmy, Organizacje non-profit, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Prywatne firmy, Organizacje non-profit, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Prywatne firmy, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Urzędy państwowe, Politycy	1
Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Politycy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Politycy, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Urzędy państwowe, Prywatne firmy, Organizacje non-profit, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Urzędy państwowe, Prywatne firmy, Pracownicy zajmujący odpowiedzialne stanowiska w firmach, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1
Urzędy państwowe, Zwykli użytkownicy nie stosujący zasad bezpieczeństwa	1

Źródło: opracowanie własne

Kampanie promujące bezpieczeństwo

Kampanie promujące bezpieczne zachowania w sieci są coraz popularniejsze, przede wszystkim w szkołach. Większość respondentów (82%) spotkała się z takową kampanią, a w grupie wiekowej poniżej 18 roku życia taką odpowiedź udzieliło 100 % ankietowanych. Odpowiedź ta najmniej popularna była w grupie wiekowej 25-50 (67%) (rysunek 36).

Rysunek 36. Zależność między grupą wiekową, a spotkaniem się z kampanią promującą bezpieczne zachowania w sieci



Źródło: opracowanie własne

Analiza statystyczna wykazała istotny wpływ grupy wiekowej na spotkanie się z kampanią promującą bezpieczne zachowania w sieci (rysunek 36).

5. Podsumowanie, wnioski i zalecenia

Na podstawie przeprowadzonego badania można stwierdzić, że:

1. Duża część respondentów nie ma wiedzy na temat zaimplementowanych zabezpieczeń na swoich urządzeń.
2. Wiek ankietowanych ma istotny wpływ na korzystanie z dodatkowych usług ochrony Internetu.
3. Obszar zatrudnienia lub edukacji respondentów ma istotny wpływ na wiedzą o możliwościach zdalnej blokady urządzenia lub usunięcia danych.
4. Znacząca większość ankietowanych ma niepełną wiedzę dotyczącą zasad tworzenia bezpiecznych haseł. 23 % respondentów zupełnie nie zna zasad tworzenia bezpiecznych haseł.
5. Duża część osób uważa, że bezpieczne hasła muszą mieć co najmniej 8 znaków.
6. Wśród ankietowanych 4% nie używa żadnej formy blokady ekranu.
7. Większość ankietowanych używa menadżerów haseł na urządzeniach domowych, natomiast znacząca mniejszość używa menadżerów haseł na urządzeniach firmowych.
8. Obszar zatrudnienia lub edukacji wysoko istotnie wpływa na stosowanie przez respondentów menadżera haseł na urządzeniach firmowych.
9. Znacząca większość respondentów używa indywidualnych haseł do różnych serwisów, jednak zmienia je dość rzadko, najczęściej, kiedy zapomni hasła, z kontem dzieje się coś nietypowego lub gdy otrzyma informację o wycieku danych.
10. Większość ankietowanych uważa, że nigdy nie została ofiarą cyberataku.
11. Ponad połowa osób uważa, że ich dane mogły kiedyś wyciec z zabezpieczonych baz danych.
12. Obszar zatrudnienia lub edukacji wysoko istotnie wpływa na deklarację, że dane respondenta mogły kiedyś wyciec.
13. Większość respondentów nie śledzi na bieżąco informacji o wyciekach danych.
14. Większość ankietowanych, która uważa, że ich dane nigdy nie wyciekły nie śledzi na bieżąco informacji o wyciekach
15. Śledzenie informacji o wyciekach danych istotnie wpływa na deklarowanie przez respondentów, że ich dane wyciekły.

16. Zdecydowana większość ankietowanych nie śledzi na bieżąco informacji o cyberatakach i innych potencjalnych zagrożeniach w sieci.
17. Obszar zatrudnienia lub edukacji istotnie wpływa na śledzenie przez ankietowanych informacji o cyberatakach i innych potencjalnych zagrożeniach w sieci.
18. Większość respondentów spotkała się z kampanią promującą bezpieczeństwo w sieci.
19. Wiek ankietowanych ma istotny wpływ na to czy spotkali się z kampanią promującą bezpieczeństwo w sieci.

Autorskie badanie wykazało bardzo duże braki w wiedzy dotyczącej niektórych aspektów cyberbezpieczeństwa pośród poszczególnych grup. Osoby poniżej 24 roku życia, mimo że w większości spotkały się z kampaniami promującym bezpieczeństwo w sieci w dużej części mają znaczące braki w wiedzy dotyczącej haseł i zabezpieczeń urządzeń by jak najlepiej chronić swoje dane. Nie deklarują również śledzenia na bieżąco informacji dotyczących wycieków, ataków i innych zagrożeń w sieci. Pośród grup zawodowych największe braki w wiedzy dotyczącej cyberbezpieczeństwa mają osoby pracujące w administracji państwowej lub samorządowej i edukacji. Zdecydowanie największą wiedzę i świadomość posiadają osoby pracujące w dużych, średnich i małych przedsiębiorstwach.

Zalecenia dla szkół podstawowych i ponadpodstawowych

Cyberbezpieczeństwo staje się coraz obszerniejszą dziedziną wiedzy. W szkołach na tak obszerną dziedzinę Informatyki poświęcane jest tylko kilka godzin rocznie. W klasach 4-6 na tematy dotyczące cyberbezpieczeństwa według proponowanego programu przez WSiP (Wydawnictwa Szkolne i Pedagogiczne) przeznaczane są w sumie 4 z 96 godzin Informatyki, natomiast w klasach 7-8, nie ma przeznaczonej ani jednej godziny. W szkołach ponadpodstawowych na poziomie Informatyki podstawowej program zaproponowany przez WSiP zaleca poświęcenie jedynie jednej godziny lekcyjnej na zagadnienia związane z cyberbezpieczeństwem, a dokładniej na prawnych aspektach działań w sieci. Z 250 godzin Informatyki jedynie 5 w całej edukacji młodych osób jest przeznaczana na tak ważne aspekty jak bezpieczeństwo w sieci. Tym samym młode osoby wchodzące w dorosłość zakładając konta bankowo i robiąc pierwsze zakupy w sieci bardzo często stają się ofiarą oszustw i wyłudzeń. Odpowiednim rozwiązaniem by poprawić wiedzę i świadomość młodych ludzi byłoby stworzenie dodatkowego przedmiotu „Cyberbezpieczeństwo” dla szkół

podstawowych i ponadpodstawowych lub znaczne zmodyfikowanie aktualnego programu nauczania przedmiotu „Informatyka”.

Zalecenia dla administracji państwowych lub samorządowych i dziedziny nauki lub szkolnictwa

Jednym z podstawowych problemów bezpieczeństwa systemów jest świadomość i wiedza obsługujących ich użytkowników. Brak podstawowej wiedzy na temat potencjalnych zagrożeń, zasad bezpiecznego posługiwania się sprzętem i tworzenia haseł może być niebezpieczne nie tylko dla pojedynczego użytkownika, ale i dla całej firmy, w której użytkownik pracuje. Duża część osób nie śledzi na bieżąco nowości technologicznych, tym samym nie śledzi również rozwijających się metod potencjalnych ataków, nowych form oszustw i innych zagrożeń. To powoduje mniejszą motywację do odpowiedniego chronienia swoich danych osobowych, ponieważ użytkownicy nie mają świadomości w jakiej sytuacji mogą postawić siebie i swojego pracodawcę. Pracodawcy powinni regularnie organizować szkolenia dotyczące cyberbezpieczeństwa dla wszystkich pracowników, skupiające się na nowych formach zagrożenia, dobrych i bezpiecznych nawykach korzystania z sieci, a przede wszystkim na obrazowaniu rzeczywistego ryzyka nie stosowania się do zasad bezpieczeństw. To znacząco podniesie świadomość w firmie, a regularne kontrole sprzętu, zainstalowanych zabezpieczeń i wymuszanie dobrych praktyk na użytkownikach, poprzez przykładowo wymuszane oprogramowaniem zmiany haseł w serwisach, przez administratorów i informatyków pomoże minimalizować zagrożenia wycieków danych i włamań do informatycznej struktury firmy.

Zalecenia dla każdego użytkownika sieci – dobre praktyki

Najważniejszym elementem cyberbezpieczeństwa, które użytkownicy powinni wdrażać w swoim życiu jest stosowanie się do zasad bezpiecznego tworzenia i używania haseł, regularne aktualizowanie oprogramowania, odpowiednia ochrona sprzętów i stałe zwiększanie swojej świadomości. Dodatkowo warto jest obserwować różnego rodzaju wyspecjalizowane serwisy zajmujące się na bieżąco wykrywaniem niebezpieczeństw czyhających na użytkowników. Bardzo często wiele portali o tematyce cyberbezpieczeństwa organizuje ciekawe szkolenia dla zwykłych użytkowników niezwiązanych z dziedziną IT w pełni za darmo. Na części szkoleń można uzyskać konkretne rady jak się zabezpieczać przed potencjalnymi zagrożeniami, ale i ostrzeżenia przed niektórymi serwisami czy praktykami.

6. Bibliografia

1. Akbanova, M., Vassilakisa, V. G., & Logothetisb, M. D. (2019). Ransomware Detection and Mitigation using Software-Defined Networking: The Case of WannaCry. *Computers & Electrical Engineering*, *76*, 111–121. https://doi.org/10.1016/j.compeleceng.2019.03.012
2. Assante, M. (2016). Confirmation of a Coordinated Attack on the Ukrainian Power Grid. *SANS Industrial Control Systems*. https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
3. Bell, T. (2018). *Adobe's CSO talks security, the 2013 breach, and how he sets priorities.* CSO.
4. Boyd, C. (2023, styczeń 19). *MalwareBytes*.
5. Caldwel, T. (2011). Ethical hackers: putting on the white hat. *Network Security*, *2011*(7), 10–13. https://doi.org/10.1016/S1353-4858(11)70075-7
6. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review* , *4*(10). https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf
7. Electricity Information Sharing and Analysis Center (E-ISAC). (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, *388*, 1–29.
8. Erickson, J. (2010). *Hacking: The Art of Exploitation, 2nd Edition*.
9. Ewing, C. (2010). Engineering Defense-in-Depth Cybersecurity for the Modern Substation. W *12th Annual Western Power Delivery Automation Conference*.
10. Garber, L. (1999). Melissa Virus Creates a New Type of Threat. *Technology News*, *32*(6), 16–19.
11. Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). What to do when your clients' data is breached: The case of Sony Playstation. *LSE Business Review*.
12. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology* , *2*, 13–20. https://doi.org/10.1007/s11416-006-0015-z
13. Krztoń, W. (2012). Cyberterroryzm jako zagrożenie bezpieczeństwa w społeczeństwie informacyjnym. *Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej* , *4*, 89–100.

14. Kuipers, D., & Fabro, M. (2006). Control Systems Cyber Security: Defense in Depth Strategies. W *U.S. Department of Homeland Security Under DOE Idaho Operations Office*.
15. Levy, S. (1984). *Hackers: Heroes of the Revolution*.
16. maia arson crimew. (2023, styczeń 19). *Google sponsored ads lead to rogue imitation sites*.
17. Mimoso, M. (2013). *Gang Behind Adobe Hack Hit Other Unnamed Companies*. ThreatPost.
18. Niebezpiecznik. (2023, styczeń 19). *Przerobione AirTagi*.
19. Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, Behaviours and Definition in Three European Countries. *Journal of Psychologists and Counsellors in Schools*, *20*(2), 129–142. https://doi.org/10.1375/ajgc.20.2.129
20. *PayPal Report*. (2023).
21. Rahman, T., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Asadizanjani, N., & Tehranipoor, M. (2019). Defense-in-Depth: A Recipe for Logic Locking to Prevail. *Integration*, *72*, 39–57.
22. Saini, H., Rao, Y. S., & Panda T.C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications*, *2*(2), 202–209.
23. Schmidt, A. (2013). The Estonian Cyberattacks. *The fierce domain – conflicts in cyberspace*, 174–193.
24. Shamim, A., Fayyaz, B., & Balakrishnan, V. (2014). Layered Defense in Depth Model for IT Organizations. W *2nd International Conference on Innovations in Engineering and Technology* (s. 21–23).
25. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). *Cyberbullying: its nature and impact in secondary school pupils.* .
26. Szubrycht, T. (2005). Cyberterroryzm jako nowa forma zagrożenia terrorystycznego. *ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ*, *1*(160).
27. Thielman, S. (2016). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*.
28. *T-Mobile Report*. (2023).
29. Urząd Dozoru Technicznego. (2018). *Ustawa o krajowym systemie cyberbezpieczeństwa*.

30. Voicescu, M. (2012). Cyber terrorism and bioterrorism-new forms of terrorists action. Size, effects and countermeasures. *International Scientific Conference" Strategies XXI*, *3*, 313.
31. Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, *6*(2), 183–211. https://doi.org/10.3390/info6020183
32. Weimann, G. (2004). *Cyberterrorism: How real is the threat?* (T. 31).
33. Whitney, L. (2013). *Adobe hack attack affected 38 million accounts*. CNET.
34. Wilson, C. (b.d.). *15-Year-Old Admits Hacking NASA Computers*. abcNews.
35. Završnik, A. (2008). Cybercrime definitional challenges and criminological particularities. *Masaryk University Journal of Law and Technology*, *2*(2), 1–29.
36. Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. (2012). A survey of cyber crimes. *Security and Communication Networks*, *5*(4), 422–437. https://doi.org/10.1002/sec.331
37. zur Mühlen, R. von. (1973). Computer-Kriminalität: Gefahren und Abwehrmassnahmen, ang. Computer crime: threats and defenses. *Luchterhand*, *15*.

Spis tabel

Spis rysunków

Załączniki

Załącznik 1. Ankieta „Bezpieczeństwo w sieci”

Bezpieczeństwo w sieci

Badanie realizowane jest w ramach pracy magisterskiej na kierunku Informatyka.

*Wymagane

Twój wiek?*

- <18
- 18-24
- 25-50
- >50

Twój status zawodowy?*

- Pracuję
- Uczę się
- Inne

Miejsce nauki/zatrudnienia?*

- Uczelnia techniczna
- Inna uczelnia/szkoła
- Samozatrudnienie
- Banki/finanse
- Edukacja/Nauka
- Administracja państwowa/samorządowa
- Handel
- Małe/Średnie przedsiębiorstwo
- Duże przedsiębiorstwo

Miejsce zamieszkania?*

- Wieś
- Miasto do 50 tys.
- Miasto od 50 tys. do 150 tys.
- Miasto od 150 tys. do 500 tys.
- Miasto powyżej 500 tys.

Z jakiego sprzętu elektronicznego korzystasz na co dzień? Możesz wybrać kilka odpowiedzi. *

- Telefon komórkowy
- Tablet
- Laptop
- Komputer stacjonarny
- Z jakich systemów operacyjnych korzystasz? Możesz wybrać kilka odpowiedzi. *
- Android
- macOS, IOS
- Windows
- Linux/ Ubuntu

Jaką wersję systemu masz zainstalowaną na telefonie? Jeśli nie wiesz pozostaw pustą odpowiedź.

Czy interesuje Cię tematyka bezpieczeństwa sieciowego?*

- Tak
- Nie

Czy na swoim urządzeniu masz zainstalowaną zaporę sieciową? *

- Tak
- Nie
- Nie wiem

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) na swoim urządzeniu mają zainstalowaną zaporę sieciową? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy korzystasz z płatnych usług ochrony Internetu?*

- Tak
- Nie
- Nie wiem

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) korzystają z płatnych usług ochrony Internetu? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy korzystasz z programów antywirusowych lub antyszpiegowskich?*

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) korzystają z programów antywirusowych lub antyszpiegowskich? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy korzystasz z mechanizmów szyfrowania danych?

- Tak
- Nie
- Nie wiem

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) korzystają z mechanizmów szyfrowania danych? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy zabezpieczasz dane / urządzenia w taki sposób by umożliwić zdalną blokadę urządzenia lub usunięcie wszystkich danych osobowych? *

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) zabezpieczają dane / urządzenia w taki sposób by umożliwić zdalną blokadę urządzenia lub usunięcie wszystkich danych osobowych? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy znane są Tobie zasady tworzenia bezpiecznego hasła?*

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) znane są zasady tworzenia bezpiecznego hasła?*

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Które z poniższych haseł uważasz za bezpieczne? Możesz wybrać kilka odpowiedzi. *

- CzerwoneGitary1978*
- R@dosnyM*rs2022
- a6YzgpKYhd
- Olunia2022!
- T*talnaM@sakracja50%
- V6Bmt
- 12Marzec1970
- soK8%6Af
- njeniuod
- OlaJanek0409
- 95Wenecja

Ile w sumie liter, znaków specjalnych, cyfr powinno mieć bezpieczne hasło?*

Jakiej blokady telefonu używasz? Możesz wybrać kilka odpowiedzi.*

- Hasło
- PIN
- Wzór
- Face ID
- Odcisk palca
- Nie używam blokady telefonu

Czy stosujesz różne hasła do poszczególnych serwisów Internetowych? *

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) stosują różne hasła do poszczególnych serwisów? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy na prywatnych urządzeniach używasz menadżera haseł?*

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) na prywatnych urządzeniach używają menadżera haseł? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy na sprzęcie firmowym używasz menadżera haseł?*

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) na sprzęcie firmowym używają menadżera haseł?*

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Kiedy zmieniasz hasła do serwisów Internetowych / kont pocztowych? Możesz wybrać kilka odpowiedzi. *

- Jak zapomnę dotychczasowego hasła
- Kiedy z kontem dzieje się coś nietypowego
- Po informacjach od serwisu o możliwym wycieku danych
- Od czasu do czasu bez powodu
- Regularnie kilka razy w roku

Czy uważasz, że kiedykolwiek zostałeś ofiarą cyberataku?*

- Tak
- Nie

Czy ktoś z Twojego najbliższego otoczenia (rodzina/znajomi) został ofiarą cyberataku? *

- Tak
- Nie
- Nie wiem

Czu uważasz, że kiedykolwiek Twoje dane wyciekły z zabezpieczonych baz danych?*

- Tak
- Nie

Czy śledzisz informacje dotyczące wycieków danych z witryn Internetowych?*

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) śledzą informacje dotyczące wycieków danych z witryn Internetowych? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Czy posiadasz aplikacje lub na bieżąco śledzisz informacje w wyspecjalizowanych serwisach (np. Niebezpiecznik) o atakach hakerskich i innych zagrożeniach w sieci? *

- Tak
- Nie

Czy osoby z Twojego najbliższego otoczenia (rodzina/znajomi) posiadają aplikacje lub na bieżąco śledzą informacje w wyspecjalizowanych serwisach (np. Niebezpiecznik) o atakach hakerskich i innych zagrożeniach w sieci? *

- Tak
- Raczej tak
- Raczej nie
- Nie
- Nie wiem

Wyciek których danych osobowych uważasz za niebezpieczny? Możesz wybrać kilka odpowiedzi. *

- PESEL
- Numer dowodu osobistego
- Imię i nazwisko
- E-mail
- Numer telefonu
- Adres zamieszkania
- Adres IP
- Dane o lokalizacji
- Dane o medycznym stanie pacjenta

Kto / jakie jednostki według Ciebie są najbardziej podatne na cyberatak? Możesz wybrać kilka odpowiedzi. *

- Banki
- Jednostki wojskowe
- Urzędy państwowe
- Prywatne firmy
- Organizacje non-profit
- Politycy
- Pracownicy zajmujący odpowiedzialne stanowiska w firmach
- Zwykli użytkownicy nie stosujący zasad bezpieczeństwa

Czy spotkałeś się z kampanią promującą bezpieczeństwo w sieci?*

- Tak
- Nie