ISSN 2720-2569

Współczesne Problemy Zarządzania • Volume 10 • Number 1 (20) • 2022 • 29–44

DOI: https://doi.org/10.52934/wpz.173

Katarzyna Kupińska

Studentka Państwowej Wyższej Szkoły Techniczno-Ekonomicznej
im. ks. B. Markiewicza w Jarosławiu
kasia12kupinska@gmail.com https://orcid.org/0000-0002-8235-5707

Zagrożenia cybernetyczne w funkcjonowaniu administracji publicznej powiatu jarosławskiego

Wprowadzenie

Cyberprzestrzeń to obszar szczególny, który wymaga dokonywania ciągłych zmian w wymiarze organizacyjnym, prawnym, systemowym i edukacyjnym. Istotne jest uświadomienie, że dynamika całego środowiska stawia przed użytkownikiem dostosowanie procedur i narzędzi, by w maksymalny sposób minimalizować ryzyko cyberataku na zasoby danych informacji.

Niestety należy podkreślić, że nie ma na świecie takiego rozwiązania, które by w 100% zapewniło stan bezpieczeństwa w cyberprzestrzeni. Rozwijająca się cyfryzacja całkowicie zmieniła świat, mając wpływ na to, jak żyjemy, uczymy się czy pracujemy. Każda organizacja, która świadczy lub będzie świadczyć usługi, odpowiadające potrzebom swoich klientów i pracowników, musi chronić swoją sieć.

Okazuje się, że dość często nie sprzęt, lecz człowiek jest tym najsłabszym ogniwem w cyberbezpieczeństwie. Człowiek jest nieodporny na różnego rodzaju bodźce czy to niezadowolonego klienta, czy niedocenionego pracownika. Poziom bezpieczeństwa powinien iść na równi ze świadomością w całym przedsiębiorstwie.

Zagadnienia teoretyczne bezpieczeństwa cybernetycznego

Cyberbezpieczeństwo nazywane również bezpieczeństwem sieci i systemów teleinformatycznych to wytrzymałość systemów teleinformatycznych na zagrożenia, które naruszają podstawowe cechy bezpieczeństwa informacji związane z przetwarzaniem informacji przez systemy informatyczne (Krawiec, 2019).

Cyberbezpieczeństwo polega na zagwarantowaniu bezpieczeństwa naszych danych. Każda duża instytucja zarówno państwowa, jak i prywatna zatrudniają specjalistów do spraw cyberbezpieczeństwa, by chronić firmę i użytkowników przed takim ryzykiem (Skórka, Skórka, Kaim, 2020).

Punktem docelowym tego bezpieczeństwa jest zagwarantowanie podstawowych cech informacji: integralności, dostępności i poufności.

Obok cyberbezpieczeństwa istnieje także cyberprzestrzeń, czyli przestrzeń do przetwarzania i wymiany informacji przez systemy informatyczne, urządzenia informatyczne i programy służące przetwarzaniu, przechowywaniu, wysyłaniu i odbieraniu informacji czy danych przez sieci telekomunikacyjne za pomocą telekomunikacyjnego urządzenia końcowego (Krawiec, 2019).

Z uwagi na wzrost znaczenia systemów IT, wykorzystywane obecnie przez społeczeństwa na całym świecie, także wchodzące w skład państwowej infrastruktury krytycznej, rozpoczęto interesować się legalnym definiowaniem cyberprzestrzeni (Wasilewski, 2013).

Definicja cyberprzestrzeni zapisana w polskiej ustawie z dnia 30 sierpnia 2011 r. definiuje cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (Ustawa, 2005).

Podsumowując, cyberprzestrzeń jest nowym wymiarem ludzkich działań, jednak z uwagi na sposób budowy jest sferą, która wysuwa się objaśnieniu za pomocą fizycznych kryteriów. Z uwagi na wciąż zwiększającą się dostępność nowych technologii oraz praktycznie bezgraniczny dostęp do Internetu, użytkownicy cyberprzestrzeni codziennie są aktywni w „cyfrowej domenie" za pośrednictwem urządzeń podłączonych do Internetu (Wasilewski, 2013).

Regulacje prawne dotyczące bezpieczeństwa cybernetycznego

Z upływem lat kraje rozpoczęły dostrzegać potrzebę zabezpieczenia sieci teleinformatycznych. Rozpoczęciem rozmów w tej kwestii był atak w 2007 r. rosyjskich hakerów na estońską cyberprzestrzeń. To właśnie Estonia padła pierwszą ofiarą ataku na swoją wirtualną przestrzeń. Po tym zdarzeniu państwa wysokorozwinięte rozpoczęły opracowywanie strategii bezpieczeństwa w zupełnie nowej formie zagrożenia w cyberprzestrzeni (Worona, 2017).

Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa została przyjęta 6 lipca 2016 r. Nakłada na państwa członkowskie szereg obowiązków, zobowiązuje je do powoływania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy.

Rozwój cyfryzacji w Unii Europejskiej był tak dynamiczny na przestrzeni lat, że środki zapewnione dyrektywą NIS okazały się być niewystarczające dla zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w krajach członkowskich. Dlatego w grudniu 2020 r. opublikowany został projekt nowej dyrektywy NIS2, który zastąpił poprzednią dyrektywę NIS. Wprowadzenie nowej dyrektywy uzasadnia konieczność wprowadzenia zmian w unijnych przepisach spowodowanych pandemią COVID-19, która w znacznym stopniu przyśpieszyła transformację cyfrową oraz wywołała większą liczbę incydentów cybernetycznych. Dyrektywa NIS2 ma doprowadzić do zwiększenia bezpieczeństwa usług cyfrowych świadczonych na terenie Unii Europejskiej (Wachowska, Elmerych, 2021).

W skali międzynarodowej podstawy prawne tworzy przede wszystkim Konwencja Rady Europy o cyberprzestępczości sporządzona 23 listopada 2001 r. w Budapeszcie. Dokument jest podsumowaniem i kontynuacją prac Rady Europy nad stworzeniem międzynarodowych standardów ukierunkowanych na zwalczanie przestępstw komputerowych. Powyższy dokument stanowi narzędzie międzynarodowej ochrony podmiotów wykorzystujących technologie komputerowe oraz podmioty, wobec których technologie ułatwiają popełnienie przestępstw (Banasiński, 2018).

Podstawy prawne cyberbezpieczeństwa zawarte w przepisach prawa powszechnie obowiązującego stanowi ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. To pierwszy akt prawny w tym zakresie w Polsce. Celem ustawy jest określenie organizacji i sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa oraz metod sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy (Ustawa, 2018). Zgodnie z ustawą incydenty polegają różnicowaniu w zależności od ich stopnia oddziaływania na systemy IT (Banasiński, Rojszczak, 2020).

Kolejnym dokumentem prawnym regulującym bezpieczeństwo cybernetyczne jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Jest to kontynuacja i poszerzenie działań podejmowanych przez administrację rządową, mającą na celu podniesienie poziomu cyberbezpieczeństwa w Polsce (Polska Izba Informatyki i Telekomunikacji, 2019). Głównym celem Strategii jest podniesienie poziomu ochrony na cyberzagrożenia oraz poziomu ochrony informacji w sektorze militarnym, publicznym oraz prywatnym (Ministerstwo Cyfryzacji, 2019).

Następnym krajowym dokumentem w zapewnieniu bezpieczeństwa cybernetycznego jest Dokument „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych". Został opracowany w ramach celu szczegółowego 2 przywołanego w strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (Ministerstwo Cyfryzacji, 2020). Chmurę obliczeniową definiuje się jako sposób dostępu poprzez sieć komputerową współdzielonych i łatwo konfigurowanych zasobów obliczeniowych (sieci, serwery, magazyny danych) przy minimalnym angażowaniu serwisu technicznego (Bartkiewicz, Czerwonka, Pamuła, 2020). Zakres usług oferowanych przez modele Chmur Obliczeniowych obejmuje cały zakres technologii informacyjnych – szczególnie infrastrukturę, platformy aplikacyjne, usługi bezpieczeństwa i oprogramowanie (Uchwała nr 97, 2019).

Regulacje prawne zarówno te na poziomie krajowym, jak i międzynarodowym ulegają ciągłym zmianom. Ze względu na szybki rozwój technologii „złoty środek" z wczoraj może być już nieaktualny dzisiaj.

Sposoby obrony przed zagrożeniami cybernetycznymi

Systemy informatyczne, bez względu od miejsca zainstalowania, szczególnie te podłączone do Internetu, są podatne na zagrożenia, które pochodzą z wielu różnych źródeł, zarówno wewnętrznych, jak i zewnętrznych (Grzelak, Liedel, 2012). Cyberatak

jest w stanie uniemożliwić działanie wszystkich sektorów gospodarki. W obliczu tych poważnych zagrożeń dynamiczny postęp cyfrowego świata wymaga podjęcia działań (Albrycht i in., 2019).

Jak się bronić przed tego typu zagrożeniami? Ważne jest odpowiednie zabezpieczenie każdego elementu. Jednym prostym przykładem może być np. obycie pracowników danej organizacji czy firmy o nieużywaniu prywatnej poczty czy urządzeń zewnętrznych na służbowym sprzęcie. To właśnie brak tak podstawowej wiedzy doprowadza do otwarcia furtki dla cyberprzestępców na dane klientów, tajemnic firmowych, handlowych czy środków finansowych firmy.

Kolejnym sposobem ochrony są kompleksowe zabezpieczenia sieci teleinformatycznej. Takim rozwiązaniem są urządzenia UTM (ang. Unified Threat Management), które w zintegrowany sposób zarządzają siecią i jej bezpieczeństwem. Poza atakami zewnętrznymi urządzenia UTM pozwalają na określenie ruchu wychodzącego np. poprzez filtrację stron internetowych, które może odwiedzać pracownik (Sykom, 2022).

Bezpieczeństwo sieci bezprzewodowej, nieprawidłowe zabezpieczenie jej można spotkać coraz częściej. Tworzona sieci Wi-Fi często swoim zasięgiem wykracza poza obszar firmy, domu. Poprawą bezpieczeństwa rozwiązań bezprzewodowych jest szyfrowanie danych sieciowych przy użyciu klucza. Korzystając z szyfrowania, koduje się wiadomość tak, aby była ona zaszyfrowana i niezrozumiała dla innej osoby, która zobaczy ją w zakodowanej formie (experience.dropbox.com/pl).

Uwierzytelnianie sieci bezprzewodowej określa tożsamość wszystkich korzystających z sieci oraz przyznaje im odpowiedni poziom dostępu. Przykład to stworzenie sieci produkcyjnej oraz sieci dla gości.

Przeciwdziałanie negatywnym skutkom przestępstw komputerowych wymaga nie tylko zwiększenia skuteczności działań organów ścigania, ale także podejmowania regularnych działań związanych z realizacją przedsięwzięć uświadamiających podstawowe zagrożenia i ryzyka związane z korzystaniem z coraz nowocześniejszych technologii informatycznych w całym społeczeństwie.

Charakterystyka powiatu jarosławskiego. Pojęcie administracji publicznej

Powiat jarosławski usytuowany jest na wschodniej ścianie województwa podkarpackiego. Terytorialnie podzielony jest na miasta: Jarosław i Radymno, gminę miejsko-wiejską Pruchnik oraz osiem gmin wiejskich: Chłopice, Jarosław, Laszki, Pawłosiów, Radymno, Rokietnica, Roźwienica i Wiązownica.

Powiat jarosławski został utworzony na mocy ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (experience.dropbox.com/pl), siedzibą powiatu jest miasto Jarosław, przy ul. Jana Pawła II 17 (Statut Powiatu Jarosławskiego, 2019). Terytorium powiatu obejmuje obszar o powierzchni 1029 km kwadratowych. Posiada swój herb, flagę i logo (mfiles.pl/pl/index.php).

Pojęcie ,,administracja" narodziło się w starożytnym Rzymie, połączenie z łacińskiego czasownika *ministrare – służyć,* z naciskiem na element służebności czy charakteru wykonawczego z przedrostkiem *ad- administrare,* mogło znaczyć obsługiwać, z biegiem lat zarządzać, a nawet kierować, ale nigdy rządzić. Administracja ma zatem charakter obsługowy, wykonawczy, służący określonemu czynnikowi decyzyjnemu (Izdebski, 2005).

Administracja publiczna to przejęte przez państwo i realizowane przez organy, w tym organy samorządu terytorialnego działania, które mają na celu zaspokoić zbiorowe i indywidualne potrzeby obywateli (Zimmermann, 2020). Posługując się pojęciem administracji publicznej, można przyjąć założenie, iż na poziomie powiatu funkcjonują w jej ramach równolegle dwie administracje – rządowa i samorządowa. Każda z nich ma swoje kompetencje, które się przenikają, uzupełniają i razem stanowią o skuteczności funkcjonowania administracji publicznej. Dlatego też w aspekcie administracji publicznej, funkcjonującej na trenie powiatu jarosławskiego, możemy mówić o administracji rządowej, powiatowej i gminnej.

Podmioty odpowiedzialne w największym stopniu za bezpieczeństwo w powiecie jarosławskim, które reprezentują administrację rządową, to:

1. Komenda Powiatowa Policji w Jarosławiu;
2. Komenda Powiatowa Państwowej Straży Pożarnej w Jarosławiu;
3. Powiatowy Inspektorat Weterynarii w Jarosławiu;
4. Powiatowy Inspektorat Nadzoru Budowlanego w Jarosławiu;
5. Powiatowa Stacja Sanitarno-Epidemiologiczna w Jarosławiu.

Ze względu na potrzebę wykonywania zadań publicznych na określonym terenie tworzy się zasadniczy podział państwa (Zimmermann, 2020). Na mocy ustawy o samorządzie powiatowym powiat jest pośrednią jednostką zasadniczego podziału terytorialnego (Ustawa, 1998).

Starosta jest kierownikiem starostwa powiatowego i zwierzchnikiem służbowym pracowników starostwa oraz kierowników jednostek organizacyjnych powiatu (Ustawa, 1998). Kompetencje mają charakter kontrolno-koordynacyjny i są znacząco dalekie od koncepcji zwierzchnictwa (Zimmermann, 2020).

Mieszkańcy powiatu tworzą z mocy prawa lokalną wspólnotę samorządową, powiat ma osobowość prawną, wykonuje zadnia publiczne o charakterze ponadgminnym we własnym imieniu i w swojej odpowiedzialności. Powstał, aby razem z gminami realizował zadania publiczne o charakterze lokalnym (Ustawa, 1998).

Strukturę organizacyjną samorządu powiatowego w Jarosławiu tworzy:

1. Rada Powiatu jest przede wszystkim organem stanowiącym i kontrolnym powiatu (Statut Powiatu Jarosławskiego, 2019).
2. Zarząd Powiatu jako organ wykonawczy powiatu.
3. Starosta wybierany przez Radę Powiatu sprawuje zwierzchnictwo w stosunku do powiatowych służb, inspekcji i straży (Ustawa, 1998).

Powiat jarosławski, działając na podstawie Statutu powiatu jarosławskiego z dnia 18 marca 2019 r., będący lokalną wspólnotą samorządową, obejmuje wszystkich mieszkańców oraz terytorium gmin.

Gmina jako podstawowa jednostka samorządu terytorialnego odpowiada za wszystkie sprawy o zasięgu lokalnym, które zgodnie z założeniami ustawy o samorządzie gminnym mogą się przysłużyć „zaspokojeniu zbiorowych potrzeb wspólnoty" (Ustawa, 1990). Organami gminy są rada gminy oraz wójt, burmistrz, prezydent miasta. Organem wykonawczym w gminie jest wójt (gmina wiejska) (www.mszana.finn.pl), burmistrz (gmina miejsko-wiejska, miejska) (Ustawa, 1990). Zadania wójta, burmistrza określa art. 30 ustawy o samorządzie gminnym. Zadania te, jak w przypadku samorządu powiatowego, są zadaniami własnymi i zleconymi.

Przestępczość cybernetyczna w powiecie jarosławskim. Charakterystyka przestępstw cybernetycznych

Ostatnie lata cechują się niebywałym tempem rozwoju środowiska informacyjnego oraz coraz to nowszych technologii. Postęp technologiczny, a wraz z nim współzależność życia codziennego od Internetu doprowadził do powstania nowych wyzwań i zagrożeń w cyberprzestrzeni (Wyrębek, 2021).

Cyberprzestępczość nazywana również przestępczością komputerową jest związana z Internetem. To zespół czynników polegających na wykorzystaniu sieci informatycznych lub systemów do naruszenia w dobra prawnie chronione. Przestępstwa komputerowe są obecnie traktowane jak przestępstwa tradycyjne – z tą różnicą, że przy użyciu innego narzędzia w przypadku przestępstw komputerowych jest to komputer oraz sieć teleinformatyczna (Fischer, 2000).

Cechami charakterystycznymi dla przestępczości komputerowej są przede wszystkim: anonimowość sprawcy, duży zasięg – niekiedy międzynarodowy, krótki okres potrzebny do popełnienia przestępstwa, poniesione niskie koszty, a duże korzyści, łatwa w obsłudze najnowsza technologia, nieświadomość ofiary o tym, że jej system został zaatakowany (Kowalczyk, 2016).

Przyłączenie komputera do sieci oznacza wystawienie go jako możliwy cel hakerów, jak również na infekcje różnego rodzaju wirusów. Najlepszym sposobem na rozpowszechnienie wirusów jest Internet. Na wielu stronach internetowych umieszczane są darmowe programy, z których bardzo często korzysta użytkownik.

Analiza statystyczna przestępczości cybernetycznej w powiecie jarosławskim w latach 2018–2021

Przestępstwo cybernetyczne w polskim prawie nie posiada legalnej czy jednolitej przyjętej przez prawo definicji. Można więc posłużyć się definicją intuicyjnie, rozumiejąc, że jest to przestępstwo popełniane przy lub za pomocą komputera oraz Internetu (Rabka, 2021).

Do obowiązujących w Polsce przepisów kodeksu karnego opisujących przestępstwa komputerowe zalicza się (Ustawa, 1997):

- art. 267 kk – nieuprawnione uzyskanie informacji tzw. hacking;
- art. 268 kk – udaremnienie uzyskania informacji;
- art. 268a kk – udaremnienie dostępu do danych informatycznych;

– art. 269 kk – sabotaż komputerowy;
– art. 269a kk – rozpowszechnianie złośliwych programów oraz cracking;
– art. 269b kk – tzw. „narzędzia hacker'skie";
– art. 287 kk – wyłudzanie danych i informacji, tzw. Phising (podlaska.policja.gov.pl).

Na podstawie danych statystycznych Komendy Powiatowej Policji w Jarosławiu problematyka cyberprzestępstw w latach 2018–2021 przedstawia się następująco:

Tabela 1. Przestępstwa cybernetyczne na terenie powiatu jarosławskiego w latach 2018–2021

	Postępowania wszczęte				Postępowania stwierdzone				Przestępstwa wykryte				Sprawca: P – pełnoletni N – nieletni				Wartość strat (w zł.)			
	2018	2019	2020	2021	2018	2019	2020	2021	**2018**	**2019**	**2020**	**2021**	**2018**	**2019**	**2020**	**2021**	**2018**	**2019**	**2020**	**2021**
Art. 267 kk	3	3	2	1	1	1	1	1	0	0	0	0	-	-	-	-	-	-	-	-
Art. 268 kk	1	1	0	0	1	1	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Art. 268a kk	0	0	1	4	0	0	1	4	0	0	0	0	-	-	-	-	-	-	-	18220
Art. 269 kk	0	0	0	0	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Art. 269a kk	0	0	0	0	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Art. 269b kk	0	0	0	0	0	0	0	0	0	0	0	0	-	-	-	-	-	-	-	-
Art. 287 kk	15	15	16	31	14	14	12	30	2	2	1	1	P	P	P	P	98936	98936	24233	295310

Źródło: opracowanie własne na podstawie danych Komendy Powiatowej Policji w Jarosławiu (stan na dzień: 25.02.2022).

Przestępstwami cybernetycznymi, które zasługują na uwagę i poddanie analizie są przestępstwa wyłudzania danych i informacji, tzw. Phising z art. 287 kk. Jak wynika z danych Komendy Powiatowej Policji, liczba tych przestępstw wzrasta, a co za tym idzie – niesie za sobą straty finansowe poniesione przez ofiary cyberprzestępcy.

Przestępstwo z art. 268 kk, dotyczące udaremnienia uzyskania informacji jest znikome, odnotowane w 2019 roku, w następnych latach nie zarejestrowano.

Jeśli chodzi o przestępstwo udaremnienia dostępu do danych informatycznych art. 268a kk, można zauważyć pojedyncze, stwierdzone przypadki (2020 – 1, 2021 – 4), przestępstwa na przestrzeni lat. Straty finansowe spowodowane tym rodzajem przestępczości oszacowano na 18 220 zł.

Kolejne przestępstwo polegające na nieuprawnionym uzyskaniu informacji (hacking) art. 267 kk, zostało odnotowane w 2019 roku trzykrotnie, przez kolejne lata natomiast można dostrzec spadek tego typu przestępczości.

Przestępstwa określone w art. 269, 269a, 269b kk nie zostały popełnione na terenie powiatu jarosławskiego w latach 2018–2021.

Analiza badań ankietowych w zakresie cyberzagrożeń

Celem niniejszego artykułu jest przybliżenie pojęć i definicji związanych z cyberbezpieczeństwem i związanym z tym środowiskiem sieciowym. Przedstawienie norm prawnych, które stanowią odpowiedź państwa na szybkie reagowanie w czasie cyberzagrożeń. Sieć w wymiarze technologicznym i społecznym oraz związane z tym konsekwencje stanowią jedno z nowych problemów bezpieczeństwa państwa na szczeblu krajowym i międzynarodowym. W pracy przedstawione zostały podstawowe sposoby obrony przed cyberzagrożeniami, określone zostały przestępstwa cybernetyczne.

Przeprowadzając badania ankietowe, zdefiniowano hipotezę badawczą, sprowadzającą się do twierdzenia, iż przygotowanie merytoryczne pracowników oraz podejmowane działania w jednostkach administracji publicznej powiatu jarosławskiego zapewniają bezpieczeństwo cybernetyczne tych instytucji.

Zdefiniowano również pytania badawcze, które sprowadzają się do:

1. Czy wybrani pracownicy administracji publicznej powiatu jarosławskiego są przygotowani do przeciwdziałania atakom cybernetycznym kierowanym w ich instytucjach?
2. Jak świadomość i wiedza pracowników organizacji może wpłynąć na zapobieganie ataków cybernetycznych?
3. Czy organizacje administracji publicznej powiatu jarosławskiego są przygotowane na możliwe ataki cybernetyczne?

W realizacji badań wykorzystano kwestionariusz ankiety składający się z pytań zamkniętych.

Za przedmiotowy obszar badawczy zostało przyjętych 11 urzędów gmin powiatu jarosławskiego, miasta: Jarosław i Radymno, gmina miejsko-wiejska

Pruchnik, osiem gmin wiejskich: Chłopice, Jarosław, Laszki, Pawłosiów, Radymno, Rokietnica, Roźwienica i Wiązownica oraz administrację samorządową powiatu jarosławskiego. Starostwo Powiatowe, organy administracji rządowej w powiecie: Komenda Powiatowej Państwowej Straży Pożarnej, Powiatowy Inspektorat Weterynarii, Powiatowy Inspektor Nadzoru Budowlanego w Jarosławiu. Podmiotowym obszarem objęto osoby w wymienionych organizacjach zatrudnione na stanowisku informatyka, administratora danych oraz osoby zajmującej się sprawami dotyczącymi systemów informatycznych.

Badania przeprowadzone zostały w kwietniu i maju 2022 r. w instytucjach administracji publicznej powiatu jarosławskiego. W badanej grupie znalazło się 15 osób, których zawodowe zainteresowanie badanym obszarem wynikało z realizowanych przez nie zadań zdefiniowanych w opisach ich stanowisk pracy. Jedyną instytucją, która odmówiła wzięcia udziału w badaniu, była Powiatowa Stacja Sanitarno-Epidemiologiczna w Jarosławiu ze względu na obowiązywanie trzeciego stopnia alarmowego CRP oraz drugiego stopnia alarmowego BRAVO ogłoszonymi przez Prezesa Rady Ministrów.

Ankietowani udzielili odpowiedzi na 20 zamkniętych pytań. Pierwsze z nich dotyczyło stażu pracy na stanowisku specjalisty od sieci informatycznych; 13 osób zadeklarowało, że pracuje na stanowisku informatyka powyżej 5 lat, jedna osoba odpowiedziała, że staż pracy to od 3–5 lat oraz mniej niż 1 rok.

Drugie i trzecie pytanie dotyczyło wykształcenia tych osób, a dokładnie, czy ukończony kierunek studiów odpowiada zajmowanemu stanowisku oraz o poziom wykształcenia. Z udzielonych odpowiedzi wynika, że większość osób ukończyła studia, które pozwalają im zajmować stanowiska informatyka i inne. Tym samym większa część badanych ukończyła studia II stopnia (8 osób), 3 osoby studia inżynierskie, 2 osoby studia I stopnia oraz 2 osoby posiada inne wykształcenie i jest to kurs informatyczny oraz wykształcenie średnie o kierunku informatycznym.

Czwarte pytanie dotyczyło odbycia dodatkowych kursów i szkoleń w ramach zwiększenia swoich umiejętności i wiedzy, piąte pytanie odnosiło się do informacji, z czyjej inicjatywy pracownicy wzięli udział w takich kursach i szkoleniach. Wynika, że aż 13 osób wzięło udział w takim kursie lub szkoleniu, a tylko 2 osoby nie korzystało z takiej możliwości. Spośród osób, które wzięły udział w szkoleniu, 7 osób odpowiada, że były to szkolenia z inicjatywy pracodawcy oraz 6 osób, które skorzystało ze szkolenia z własnej inicjatywy.

Szóste pytanie miało związek z kursami przeprowadzonymi przez renomowane firmy informatyczne i zdobyte przez to uprawnienia. Z uzyskanych odpowiedzi wynika, że 14 badanych osób nie brało udziału w kursie organizowanym przez renomowane firmy, a tylko 1 osoba wzięła udział i odpowiedziała, że ukończyła taki kurs. Zadeklarowała, że skorzystała z dwóch kursów: Cisco Certified Network Associate (CCNA) oraz Microsoft Certified IT Professional Server Administrator on Windows Server 2008 (MCITP). Pierwsze szkolenie pozwala usystematyzować wiedzę dotyczącą podstaw sieci komputerowych, jak i rozwija kompetencje zaawansowanych technik przełączania, routingu, bezpieczeństwa i automatyzacji (www.politechnet.

pl), drugie szkolenie przeznaczone jest dla osób, które chcą administrować systemem *Windows,* sprawnego zarządzania serwerami.

Kolejne pytanie skierowane do badanych obejmowało, z jakich źródeł wiedzy korzystają najczęściej. Ankietowani mogli wybrać więcej niż jedną odpowiedź. Mieli do wyboru Internet – strony internetowe poświęcone tematyce informatycznej, czasopisma – poświęcone nowościom technologicznym i informatycznym oraz specjalistyczne książki, wydawane w Polsce, jak i za granicą. Z odpowiedzi wynika, że większość odpowiedziała, że korzysta z Internetu – 13, odpowiedzi na podobnym poziomie, otrzymują czasopisma – 8 odpowiedzi, oraz książki – 7 odpowiedzi.

Kolejne pytania w ankiecie dotyczyły instytucji, w których pracują badane osoby oraz pozostałych pracowników administracyjnych.

Ósme pytanie dotyczyło wystąpienia ataków cybernetycznych w latach 2018–2021 na te instytucje oraz jeśli nastąpił atak, to jakiego rodzaju był. Odpowiedzi przedstawią, że spośród wszystkich instytucji, w których przeprowadzono ankietę, tylko w jednej wystąpił atak cybernetyczny i było to związane z zainfekowaniem systemów informatycznych, pozostałe instytucje nie doświadczyły ataku cybernetycznego na przestrzeni tych lat.

Kolejne pytania w ankiecie 10 i 11 odnosiły się do uzyskania informacji na temat wiedzy pozostałych pracowników, jeśli chodzi o bezpieczeństwo w sieci. W rezultacie w większości organizacji w ostatnim czasie odbyły się szkolenia dla pracowników. W ocenie badanych szkolenia te „raczej" podniosły wiedzę pracowników – 4 odpowiedzi, 5 osób zadeklarowało, że tak podniosły wiedzę, a 6 osób (w tym 3 odpowiedzi, które równoważą się z odpowiedzią, że nie przeprowadzono szkolenia) stwierdziło, że szkolenia nie wniosły dodatkowej wiedzy dla pracowników.

Pytania 12, 13 i 14, zawarte w ankiecie, odnosiły się do zachowań i czujności pracowników instytucji, którzy mają dostęp do sieci. Pytanie 12. dotyczyło częstotliwości zmiany haseł przez pracowników, 13 badanych możliwości korzystania przez pracowników z prywatnych urządzeń przenośnych z siecią w instytucji, 14. pytanie obejmowało świadomość pracownika, który podczas zauważenia wystąpienia podejrzanego incydentu wiedzą, do kogo powinni zgłosić problem.

Z odpowiedzi na pytanie nr 11 wynika, że pracownicy raz w miesiącu mają obowiązek zmieniać swoje hasła lub kilka razy w miesiącu tylko w jednej organizacji następuje to dopiero po ukazaniu się informacji o takiej potrzebie.

W większość instytucji (11 odpowiedzi) pracownicy mają także zakaz podłączania swoich prywatnych urządzeń do sieci i komputerów służbowych, jednak w 4 organizacjach mają taką możliwość.

Na podstawie analizy odpowiedzi na pytanie 13. można przyjąć, że we wszystkich instytucjach pracownicy wiedzą, do kogo mają zgłosić podejrzane, zagrażające incydenty w swojej organizacji.

Informacje zawarte w odpowiedzi na pytanie 14., dotyczące częstotliwości aktualizowania oprogramowania pokazuje, że w większości organizacji następuje to dopiero po ukazaniu się powiadomienia, a w czterech instytucjach odbywa się to raz w miesiącu, w trzech organizacjach raz w tygodniu, a w jednej kilka razy w miesiącu.

Pytanie 16. dotyczyło zagrożenia, które – wg badanych – stanowi największy problem dla ich instytucji. Ankietowani mogli wybrać więcej niż jedną odpowiedź. Większość badanych stwierdziła, że to zainfekowanie systemów (10 odpowiedzi) jest największym zagrożeniem, które mogłoby stanowić największy problem, złośliwe oprogramowanie (8 odpowiedzi) jako kolejne zagrożenie. Ankietowani uważają, że włamanie hakerów stanowi najmniejsze zagrożenie dla ich organizacji – 4 odpowiedzi.

Następne pytania w ankiecie (17. i 18.) dotyczyły przeprowadzenia sprawdzenia sprawności systemów ochrony i zabezpieczenia przed ewentualnym zagrożeniem cybernetycznym, wdrożonym zmianom oraz czasu przeprowadzonych usprawnień.

Odpowiedź na pytanie 15. pozwala stwierdzić, że sprawność systemów zabezpieczenia i ochrony systemów przed zagrożeniami przeprowadzono w 8 instytucjach. Zmiany po przeprowadzeniu sprawności systemów zostały wdrożone w 2 organizacjach, w pozostałych 6 nie wdrożono żadnych zmian. W 7 organizacjach w ostatnim czasie nie zostało przeprowadzone sprawdzenie sprawności systemów zabezpieczenia przed zagrożeniami cybernetycznymi.

We wskazanych 8 instytucjach takich sprawności dokonano stosunkowo niedawno, gdyż stało się to na przestrzeni ostatniego miesiąca do około pół roku temu.

Dwa ostatnie pytania w ankiecie – 19 i 20 to opinia specjalistów od sieci informatycznych w instytucjach o przygotowaniu ich organizacji na ewentualne wystąpienie ataków oraz o sposobach poprawienia i ulepszenia bezpieczeństwa informatycznego. Większość respondentów uważa, że ich instytucje są przygotowane na wystąpienie ewentualnych ataków cybernetycznych, tylko 3 osoby sądzą, że organizacja nie jest przygotowana.

W opinii badanych, aby polepszyć bezpieczeństwo sieci informatycznej w swoich instytucjach, w większości ankietowani odpowiedzieli o częstszych szkoleniach pracowników (12 odpowiedzi) oraz ulepszeniu zabezpieczeń sieci (10 odpowiedzi). Kolejnym ulepszeniem według ankietowanych byłoby okresowe sprawdzanie wiedzy wszystkich pracowników dotyczących bezpiecznego użytkowania sieci (5 odpowiedzi). Na równi były odpowiedzi, aby robić częstsze przeglądy i aktualizacje systemów (3 odpowiedzi) oraz zwiększyć liczbę etatów na stanowiskach odpowiedzialnych za bezpieczeństwo informatyczne w organizacjach (3 odpowiedzi). Za wyposażeniem stanowisk pracy w nowoczesny sprzęt uzyskałam najmniej – 2 odpowiedzi.

Podsumowanie

Wiedza i świadomość na temat bezpieczeństwa sieci jest współcześnie bardzo ważna. Wkraczając na drogę udoskonaleń technicznych i informatycznych, konieczne jest, aby użytkownik od początku był świadomy swoich działań.

Analizując wyniki przeprowadzonych badań wśród wybranej grupy, można zauważyć, że osoby te, odpowiedzialne za bezpieczeństwo sieciowe w instytucjach administracji publicznej, w których pracują, posiadają odpowiednie wykształcenie. Z przeprowadzonych badań wynika również, że respondenci ciągle podnoszą swoje

kompetencje poprzez uczestnictwo w dodatkowych szkoleniach i kursach organizowanych nie tylko przez pracodawcę, ale również ze swojej inicjatywy.

Obawę wzbudza informacja, że w pojedynczych instytucjach pracownicy mogą podłączać swoje prywatne urządzenia do sieci i służbowych komputerów. Analiza odpowiedzi przywodzi na myśl ryzyko związane z prawdopodobieństwem wystąpienia nieprzewidzianych skutków takiego działania oraz możliwości stworzenia zagrożenia dla całej instytucji.

Reasumując, przygotowanie merytoryczne pracowników i podejmowane działania zapewniają bezpieczeństwo cybernetyczne instytucjom administracji publicznej powiatu jarosławskiego. Głównym i nieustannym celem każdej wspomnianej instytucji, jeśli chodzi o cyberbezpieczeństwo, powinno być zatrudnianie specjalistów, którzy będą posiadali odpowiednie wykształcenie, uaktualniali swoją wiedze i będą potrafili wykorzystać to w zapewnieniu bezpieczeństwa w swoich organizacjach. Respondenci podkreślają, że częstsze szkolenia pozostałych pracowników stanowią podstawę poprawy bezpieczeństwa sieci.

Organizacje administracji rządowej i samorządowej powiatu jarosławskiego w większości są przygotowane na ataki cybernetyczne. Dokonując analizy przeprowadzonych badań w powiecie jarosławskim, w latach 2018–2021, doszło do jednego ataku cybernetycznego i doprowadziło do zainfekowania systemów informatycznych.

Abstrakt

Zagrożenia cybernetyczne w funkcjonowaniu administracji publicznej powiatu jarosławskiego

W czasach coraz powszechnej i ogólnodostępnej cyfryzacji i jednocześnie porozumiewania się za pośrednictwem sieci teleinformatycznych sprawa bezpieczeństwa systemów IT przestaje być tylko przedmiotem zainteresowania małej grupy ekspertów i specjalistów w tej dziedzinie. Bezpieczeństwo cybernetyczne ma szczególne znaczenie w prawidłowym funkcjonowaniu administracji publicznej na poziomie gminnym i powiatowym, gdzie istnieje potrzeba nieustannego podnoszenia kompetencji przez pracowników tych instytucji, co potwierdziły przeprowadzone badania w powiecie jarosławskim.

Słowa kluczowe: bezpieczeństwo systemów, cyfryzacja, użytkownik sieci, cyberbezpieczeństwo, administracja publiczna, powiat jarosławski

Abstract

Cyber threats in the functioning of the public administration of the Jarosław County

In times of widespread, commonly available digitization and at the same time, communication via teleinformatic networks, the issue of IT systems security is no longer of interest to only a small group of experts and specialists in this field. Cyber security

is also of wider importance in the proper functioning of public administration at the commune and county level. In such an environment, there is a need for continuous improvement of related competences in the employees of related institutions. This fact was confirmed by research carried out in the Jarosław County.

Keywords: systems security, digitization, network user, cybersecurity, public administration, Jarosław County

References

Albrycht, I., Autolitano, S., Gęborys, P., Krawczyk, M., Marczuk, P., Mednis, A., Siudak, R., Świątkowska, J. (2019). *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje*. Instytut Kościuszki. https://ik.org.pl/wp-content/uploads/wyzwania-w-cyberprzestrzeni.-przyklady-rozwiazan-zagrozenia-regulacje.pdf (dostęp: 29.01.2022).

Banasiński, C. (2018). *Cyberbezpieczeństwo. Zarys wykładu*. Wydawnictwo Wolters Kluwer.

Banasiński, C., Rojszczak, M., (2020). *Cyberbezpieczeństwo*. Wydawnictwo Wolters Kluwer.

Bartkiewicz, W., Czerwonka, P., Pamuła, A. (2020). *Współczesne narzędzia cyfryzacji organizacji*. Wydawnictwo Uniwersytetu Łódzkiego.

Fischer, B. (2000). *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno -kryminalistyczne*. Wydawnictwo Zakamycze.

Grzelak, M., Liedel, K. (2012). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu. *Bezpieczeństwo Narodowe, 22*(2), 124.

https://experience.dropbox.com/pl/resources/what-is-encryption (dostęp: 29.01.2022).

https://mfiles.pl/pl/index.php/Starostwo_powiatowe (dostęp: 29.01.2022).

https://podlaska.policja.gov.pl/pod/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-iii/rodzaje-i-kwalifikacja/28410,Rodzaje-i-kwalifikacja-przestepstw-komputerowych.html (dostęp: 28.02.2022).

https://www.mszana.finn.pl/bipkod/002/003 (dostęp: 10.02.2022).

https://www.politechnet.pl/akademia-sieci-cisco/ccna/ (dostęp: 16.05.2022).

Izdebski, H. (2005). Badania nad administracją publiczną. W: J. Hausner (red.), *Administracja publiczna* (s. 13). Wydawnictwo Naukowe PWN.

Kowalczyk, P. (2016). *Przestępstwa komputerowe – cechy charakterystyczne*. Mindly.pl. https://mindly.pl/kryminalistyka,ac232/przestepstwa-komputerowe-cechy-charakterystyczne,3709 (dostęp: 01.02.2022).

Krawiec, J. (2019). *Cyberbezpieczeństwo. Podejście systemowe*. Oficyna Wydawnicza Politechniki Warszawskiej.

Ministerstwo Cyfryzacji. (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://www.gov.pl/web/cyfryzacja/

strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 29.01.2022).

Ministerstwo Cyfryzacji. (2020). *Narodowe Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)*. https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf (dostęp: 29.01.2022).

Polska Izba Informatyki i Telekomunikacji. (2019). *MC- projekt uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://www.piit.org.pl/o-nas/komitety/komitet-grot2/dokumenty-grot/mc-projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 29.01.2022).

Rabka, M. (2021). Zwalczanie przestępczości i wymiar sprawiedliwości w powiecie jarosławskim. W: B. Szczypta-Kłak, K. Pobuta, K. Rejman (red.), *Wybrane wymiary bezpieczeństwa społecznego w powiecie jarosławskim w latach 2018–2020* (ss. 231–232). Wydawnictwo Państwowej Wyższej Szkoły Techniczno-Ekonomicznej w Jarosławiu.

Skórka, J., Skórka, K., Kaim, K. (2020). *Bezpieczeństwo w sieci. Jak skutecznie chronić się przed atakami*. Wydawnictwo ITSt@rt.

Statut Powiatu Jarosławskiego z dnia 18 marca 2019 r. (Załącznik do obwieszczenie nr 1/2019 poz. 1816).

Sykom Sp. z o.o. (2022). *Zabezpieczenie sieci – UTM*. https://sykom.pl/sprzet-uslugi-it/bezpieczenstwo/rozwiazania-utm-unified-threat-management/ (dostęp: 29.01.2022).

Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa".

Ustawa z 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372, 1834).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570, z 2018 r. poz. 1000, 1544, 1669, z 2019 r. poz. 60, 534).

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2020 r. poz. 920, z 2021 r. poz. 1038, 1834).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020. 1369). 2013, 5(9): 225–234.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2021 r. poz. 2345, 2447).

Wachowska, A., Elmerych, A. (2021). Dyrektywa NIS 2: jakie zmiany wprowadzi dla cyberbezpieczeństwa na rynku wewnętrznym UE? *Biuletyn Euro Info, 4*(207), 13–17.

Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego, 5*(9), 227, 230–232.

Worona, J. (2017). *Cyberprzestrzeń a prawo międzynarodowe*. Uniwersytet w Białymstoku.

Wyrębek, H. (2021). *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*. Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.

Zimmermann, J. (2020). *Prawo administracyjne*. Wydawnictwo Wolters Kluwer Polska.