dr Robert Zakrzewski
Wydział Zarządzania i Dowodzenia
Akademia Sztuki Wojennej
ORCID 0000-0002-4019-9048

ZAGROŻENIA W CYBERPRZESTRZENI

THREATS IN CYBER SPACE

Streszczenie
Praca przedstawia zagadnienia dotyczące cyberbezpieczeństwa i rozwiązań, przy pomocy których można je systematycznie zwiększać. Celem opracowania jest przedstawienie tych narzędzi i mechanizmów, które pomagają w tworzeniu systemu skutecznego i maksymalnie podnoszącego ogólny poziom bezpieczeństwa użytkowników sieci.
Wskazano również na konieczność poprawy poziomu wiedzy na temat bezpiecznego użytkowania Internetu i ochrony swoich danych czy też wszelkich informacji, które udostępnia się w sieci, a które mogą stanowić cel cyberprzestępców. Poruszono tutaj kwestie związane zarówno z bezpieczeństwem firm i innych podmiotów jak również prywatnych użytkowników.

Słowa kluczowe: bezpieczeństwo, cyberprzestępcy, identyfikacja, system, zagrożenia

Abstract
This paper discusses issues related to cybersecurity and solutions with the help of which it can be systematically increased. The goal is to present the things and mechanisms that help create a system which is effective and maximizes the overall level of security for network users. There was also pointed out the need to improve the level of knowledge about the safe use of the Internet and the protection of your data or any information that is shared on the network and which may be the target of cybercriminals. Issues related to both the security of companies and other entities as well as private users were raised here.

Key words: security, cyber criminals, identification, system, threats

Wstęp

Zapewnienie odpowiedniego poziomu bezpieczeństwa informacyjnego jest obecnie jednym z ważniejszych zadań, które stoją przed współczesnym państwem i poszczególnymi jego instytucjami. Ważne jest także, aby zapewnić obywatelom dostęp do odpowiedniej edukacji w tym zakresie, by sami mieli świadomość tego, w jak dużym stopniu poziom tego bezpieczeństwa jest uzależniony od działań, które podejmują na co dzień.

Celem opracowania jest wskazanie, jakie rozwiązania są podejmowane obecnie i jakie są ich założenia i rola w tworzeniu całego systemu zapewniającego bezpieczeństwo w cyberprzestrzeni.

1. Istota cyberbezpieczeństwa

Cyberbezpieczeństwo jest postrzegane jako zapobieganie uszkodzeniom, ochronie jak i perspektywie przywrócenia pełnej zdolności do właściwego funkcjonowania komputerów, a także systemów łączności elektronicznej lub określonych usług komunikacji, która ma miejsce w cyberprzestrzeni. Z drugiej strony jest to również ochrona wszystkich informacji, które uwzględnione są w przestrzeni komunikacji elektronicznej, a która zapewnia poufność przy jednoczesnym uwierzytelnieniu osób, które są do tego upoważnione[1]. Zwykle odnosi się ono do trzech, zupełnie niezależnych poziomów[2]:

- ochrona komputerów, nośników pamięci oraz wszystkich informacji, które są w nich zawarte;
- zdolność zapewnienia odpowiedniej ochrony przed atakami, które wynikają z wewnętrznych regulacji jak i z zabezpieczeń cybernetycznych;
- proces edukacji oraz ciągłe szkolenia podnoszące poziom posiadanych umiejętności i wiedzy – ważne jest, by dopasowane były one do dynamicznie zmieniającego się otoczenia.

Najważniejszym celem i założeniem cyberbezpieczeństwa jest ochrona cyberprzestrzeni, a także wszystkich jej zasobów. Odnosi się, zatem do działań powiązanych z komputerem, systemem komunikacji elektronicznej oraz do usług, które są realizowane przy ich pomocy jak i przy użyciu łączności elektronicznej oraz bezpieczeństwa informacji. Obejmuje ona zarówno ochronę sieci komputerowych, reagowania na ataki jak i koordynowanie gotowości do podejmowania ataków, monitorowania sieci oraz wykrywania czy też zapobiegania występującym atakom[3].

[1] K. Midor, Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa, Systemy Wspomagania w Inżynierii Produkcji, 6/2017, s. 75-80.
[2] Ibidem., s. 75-80
[3] Ibidem., s. 75-80.

Projektując działania z zakresu bezpieczeństwa informacyjnego konieczne jest uwzględnienie szeregu dodatkowych uwarunkowań. Zalicza się do nich następujące założenia[4]:

- informacja jest zasobem o charakterze strategicznym dla każdego państwa;
- Informacja oraz wynikająca z niej wiedza czy technologie informatyczne będą podstawowym czynnikiem wytwórczym;
- szeroko rozumiany sektor informacyjny odpowiada za tworzenie znacznej części dochodu narodowego;
- wszystkie procesy decyzyjne w pozostałych sektorach gospodarki oraz życia społeczne są o wiele bardziej uzależnione od systemu przetwarzania oraz przesyłania poszczególnych informacji;
- wszelkie zakłócenia prawidłowości działania poszczególnych systemów informacyjno- sterujących nie wiąże się z koniecznością ponoszenia większych nakładów materialnych;
- rywalizowanie między poszczególnymi przeciwnikami przenosi się coraz częściej na płaszczyznę walki mającej charakter informacyjny;
- technologie informatyczne są ważnym elementem działania bezpieczeństwa państwa, w tym również sił zbrojnych;
- media masowe mogą być stosowane, jako narzędzia skutecznego zakłócania informacyjnego.

2. Zagrożenia i ich źródła

Postęp technologiczny pozwala na to, by systemy informatyczne gromadziły niemal nieograniczone ilości danych. W efekcie tego konieczne jest podejmowanie bardziej zintensyfikowanych działań, które zwiększą poziom bezpieczeństwa[5]. Jest to szczególnie ważne, ze względu na zwiększająca się systematycznie liczbę incydentów naruszających bezpieczeństwo. Tylko w latach 2013-2014 ich liczba zwiększyła się nawet o 48%[6]. Mimo to wiele organizacji nadal nie zdaje sobie sprawy z tego, kto stanowi zagrożenie i jak często jest na to narażona[7]. Statystyki na temat liczby zainfekowanych komputerów w 2018 roku wynosił łącznie 940.079 unikalnych adresów IP.

[4] T. Aleksandrowicz, Bezpieczeństwo w cyberprzestrzeni ze stanowiska praw międzynarodowego, Przegląd Bezpieczeństwa Wewnętrznego, 15/2016, s. 14-17.
[5] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).
[6] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).
[7] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).

Tabela 1. Liczba zainfekowanych komputerów w polskich sieciach w 2018 roku

rodzina	rozmiar
Andromeda	6059
Conficker	4529
Mirai	1969
Sality	1531
Necurs	1502
Isfb	1412
Gamut	1392
Stealrat	1312
Nymaim	1261
Pushdo	1008

Źródło: Krajobraz bezpieczeństwa polskiego internetu. Raport Roczny z działalności CERT Polska, 2018, s.107-111.

Powyższe dane pokazują, że liczba ataków na komputery, każdego dnia jest bardzo wysoka. Dlatego też konieczne jest podjęcie szeregu działań pozwalających na zwiększenie poziomu bezpieczeństwa w zakresie użytkowania sieci.

Kolejna tabela pokazuje liczbę zgłoszeń phishingu, który występował w polskiej sieci.

Tabela 2. Zgłoszenia phishingu w 2018 roku

numer AS	nazwa AS	liczba IP	liczba domen
12824	Home.pl	553	930
15967	Nazwa AS	260	439
16276	OVH	113	306
205727	Aruba	92	321
41079	H88	90	296
5617	Orange	71	14
29522	KEI	66	95
198414	H88	48	110
197226	Sprint	43	1852
8308	NASK	36	63

Źródło: Krajobraz bezpieczeństwa polskiego internetu. Raport Roczny z działalności CERT Polska, 2018, s.107-111.

Jak wynika z powyższych zestawień, w 2018 roku otrzymano łącznie 77.536 wszystkich zgłoszeń. Odnosiły się one do 5566 domen prowadzących do stron rozwiązujących na 1885 unikatowych adresów IP.

Okazuje się, że największym zagrożeniem dla bezpieczeństwa danych są sami pracownicy – głównie ci obecni, ale również byli pracownicy czy też

partnerzy biznesowi i dostawcy, konsultanci czy dostawcy. Sporym źródłem zagrożenia są też zachowania klientów.

Większość z tych zagrożeń wynika z braku świadomości, że dana osoba zachowuje się w sposób nieodpowiedzialny. Potwierdza to fakt, że firmy, które zdecydowały się na wprowadzenie u siebie programów budowania świadomości w zakresie bezpieczeństwa, najczęściej zgłaszają zdecydowanie mniejsze straty finansowe ponoszone z tytułu nieodpowiedzialnej działalności pracowników czy innych podmiotów w Internecie[8].

Jest to o tyle ważne, że żadne zabezpieczenie nie będzie wystarczająco skuteczne, jeśli użytkownik nie będzie zachowywał się ostrożnie i nie będzie przestrzegał ustalonych zasad[9].

Jednocześnie, poza wdrażaniem coraz bardziej nowoczesnych rozwiązań, odnosi się również do tych starych i wypróbowanych, które sprowadzają się do stosowania efektywnego programu antywirusowego (np. bezpłatny Comodo Firewall, posiadający wbudowany moduł HIPS chroniący system przed trojanami, keyloggerami oraz rootkityami, itp.)[10]

3. Rozwiązania zwiększające poziom bezpieczeństwa

Najprostszymi rozwiązaniami, które pozwalają na zwiększenie poziomu bezpieczeństwa są[11]:

- zobowiązania pracowników do utrzymania w tajemnicy wszystkich danych osobowych, z którymi muszą pracować w czasie wypełniania swoich obowiązków służbowych,
- zwiększenie poziomu świadomości dotyczącej bezpieczeństwa danych,
- ustawienie monitorów komputera w taki sposób, aby inne osoby nie miały wglądu,
- odpowiednie skonfigurowanie sieci Wi-Fi,
- przechowywanie w bezpiecznym miejscu wszystkich kopii zapasowych danych osobowych – można je przechowywać w innym pomieszczeniu lub poza siedzibą firmy,
- szyfrowanie danych na swoim komputerze,
- sformułowanie właściwego zakresu przetwarzania danych osobowych przez pracownika,

[8] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).
[9] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).
[10] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).
[11] Strona internetowa: https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia (dostęp: 30.09.2019).

- wdrożenie obowiązku noszenia identyfikatorów służbowych,
- niszczenie urządzeń, dysków oraz innych urządzeń elektronicznych w taki sposób, by niemożliwym było odzyskanie z nich danych,
- odpowiednia ochrona posiadanych urządzeń mobilnych.

Jak zostało wskazane wcześniej, najważniejsze jest zwiększanie poziomu świadomości pracowników w zakresie zapewnienia bezpieczeństwa cybernetycznego. Im bardziej dana organizacja jest uzależniona od cybertechnologii, tym większe jest zapotrzebowanie na pracowników specjalizujących się w zapewnieniu bezpieczeństwa w sieci, tak by chronić wszystkie newralgiczne punkty systemu[12].

Zapewnienie odpowiedniego poziomu bezpieczeństwa w sieci, konieczne jest podejmowanie szczegółowego planu działania. Został on przedstawiony w tabeli 1.

Tabela 3. Cyberbezpieczeństwo

ramy cyberbezpieczeństwa	**systematyczna analiza oraz plan**
identyfikacja – ocena ryzyka	Przeprowadzenie szczegółowej analizy ryzyka Wykrycie potencjalnych słabych punktów
ochrona – opracowanie zabezpieczeń	Opracowanie polityk i procedur Wdrożenie odpowiedniego mechanizmu kontroli dostępu i audytu
wykrywanie – wczesne ujawnienie	Stały monitoring w trybie całodobowym przez 365 dni w roku Umożliwienie czynności audytowych
reagowanie – podjęcie działań	Przyjęcie stabilnego planu reakcji Korelacja, analiza, selekcja i reakcja na wykryte zdarzenia
działania odtworzone – przywrócenie funkcjonalności	Wdrożenie planu awaryjnego Wprowadzenie ulepszeń w celu zapobieżenia atakom w przyszłości

Źródło: Strona internetowa: https://www.motorolasolutions.com/content/dam/msi/docs/pl_pl/services/cybersecurity_services_comprehensive_brochure_polish.pdf (dostęp: 30.09.2019).

Ochrona infrastruktury powinna sprowadzać się do pięciu etapów. Zalicza się do nich[13]:

- ocena środowiska poprzez wszystkich zewnętrznych ekspertów specjalizujących się w bezpieczeństwie, którzy posiadają kompleksową wiedzę dotyczącą cybernetycznych oraz fizycznych słabych punktów danego systemu bezpieczeństwa oraz zagrożeń,

[12] K. Midor... op.cit., s. 75-80.
[13] Strona internetowa: https://www.motorolasolutions.com/content/dam/msi/docs/pl_pl/services/cybersecurity_services_comprehensive_brochure_polish.pdf (dostęp: 30.09.2019).

- przygotowanie stabilnego planu zarządzania ogółem ryzyka oraz eliminacji wykrytych najsłabszych punktów,
- aktywne monitorowanie całego systemu z perspektywy potencjalnych zagrożeń – przez cały rok,
- maksymalizacja ciągłości podejmowanej działalności operacyjne, przez wdrożenie poprawek w systemach oraz aktualizację poszczególnych elementów oprogramowania, które są odpowiedzialne za utrzymanie bezpieczeństwa,
- ciągłe weryfikowanie planów cyberbezpieczeństwa celem ograniczenia pojawiających się zagrożeń.

Monitoring może być prowadzony na dwa sposoby. Z jednej strony możliwe jest zlecenie tego zadania specjalnym analitykom ds. cyberzabezpieczeń, którzy pracują dla firmy zewnętrznej. Ich zadaniem jest monitorowanie systemu klienta przy użyciu najnowszych narzędzi analitycznych. To również międzysystemowa korelacja zdarzeń oraz pozyskiwanie informacji niezbędnych do podejmowania kompleksowej reakcji. Ważne jest również regularne identyfikacja, analiza oraz rozwiązywanie potencjalnych incydentów cybernetycznych[14].

Z drugiej strony bezpieczeństwo można zapewnić poprzez prowadzenie monitorowanie na miejscu, przy użyciu narzędzi, które zostały dostarczone przez firmę zewnętrzną specjalizującą się w bezpieczeństwie. Do działań i rozwiązań, które są tutaj stosowane zalicza się przede wszystkim indywidualny zestaw narzędzi pozwalających na monitorowanie systemu w ramach wyszczególnionego środowiska sieci Klienta. Powinno sprowadzać się to także do regularnego aktualizowania pulpitów zawierających niezbędne informacje pozwalające zespołowi klienta na identyfikowanie kluczowych zdarzeń dotyczących bezpieczeństwa oraz podejmowanie właściwych działań – w tym również przeglądu stanu systemu z poziomu strony startowej. Jednocześnie, powinno się stosować narzędzia, które zapewniają całodobowy dostęp do zespołu certyfikowanych ekspertów dostępnych w firmie[15].

Najwyższym poziomem dojrzałości cechuje się wdrożenie programów zapewniających ochronę przed złośliwym oprogramowaniem, a także bezpieczeństwo styku z siecią Internet. Na dobrym poziomie jest także reagowanie na incydenty bezpieczeństwa czy też wdrożenie specjalnych planów, dzięki którym możliwe jest zapewnienie ciągłości działania[16].

Inne rozwiązania, które są wdrażane celem podniesienia poziomu bezpieczeństwa w firmie[17]:

[14] Strona internetowa: Strona internetowa: https://www.motorolasolutions.com/content/dam/msi/docs/pl_pl/services/cybersecurity_services_comprehensive_brochure_polish.pdf (dostęp: 30.09.2019).
[15] https://www.motorolasolutions.com/content/dam/msi/docs/pl_pl/services/cybersecurity_services_comprehensive_brochure_polish.pdf (dostęp: 30.09.2019).
[16] Strona internetowa: https://greywizard.com/tarcza/cdn (dostęp: 30.09.2019).
[17] Ibidem.

- zarządzanie tożsamością i dostępem;
- bezpieczeństwo sieci wewnętrznej;
- ochrona przed wyciekami danych (DLP);
- klasyfikacja i kontrola aktywów;
- programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa;
- zarządzanie podatnościami;
- bezpieczeństwo w procesach wytwarzania oprogramowania;
- zarządzanie bezpieczeństwem urządzeń mobilnych;
- zarządzanie bezpieczeństwem partnerów biznesowych.

4. Regulacje prawne

Rozwiązaniem, o którym należy tutaj wspomnieć jest wprowadzona Doktryna Cyberbezpieczeństwa RP. Uwzględnia ona zestaw strategicznych kierunków działań, które pozwalają na zagwarantowanie odpowiedniego poziomu bezpieczeństwa RP w sieci. Powinna być również traktowana jako podstawa koncepcyjna, która pozwala na zapewnienie spójnego oraz kompleksowego podejścia do wszystkich zagadnień związanych z cyberochroną. Jest swoistym punktem odniesienia dla działań prowadzonych przez podmioty administracji publicznej, służby bezpieczeństwa jak i porządku publicznego czy też siły zbrojne, sektor prywatny oraz wszystkich obywateli. W ten sposób zapewnia bazę wyjściową do tworzenia bardziej precyzyjnej ochrony wszystkich podmiotów[18].

Ciekawym rozwiązaniem wydaje się również wprowadzenie usług łowieckich – hunting. Jest to propozycja opierająca się na założeniu, które pojawia się często w wielu instytucjach – że prędzej czy później nastąpił włamanie. Chcąc mu przeciwdziałać należy nie tylko mu zapobiegać, ale również maksymalnie skrócić okno czasowe pozwalające na jego szybkie wykrycie i ograniczenie ewentualnych strat. Dlatego też konieczne jest tworzenie zupełnie nowych usług, w tym powołanie zespołów bezpieczeństwa mających za zadane regularne sprawdzanie sieci wybranego podmiotu celem wykrycia ewentualnych ataków czy zagrożeń[19]. Jest to również ważna wiedza nie tylko techniczna, ale i zdolność obywatelska. Z tego też względu zagadnienia związane z cyberbezpieczeństwem powinny być uwzględnione na wszystkich poziomach edukacji. Szkoła musi zapewniać młodym ludziom nie tylko zaznajomienie się z działaniem cyberprzestrzeni, ale również zrozumienie jej zagrożeń i możliwość

[18] System bezpieczeństwa cyberprzestrzeni RP, Warszawa, 2015, s. 34-38.
[19] Ibidem., s. 94-99.

właściwej profilaktyki i ochrony – nie tylko w aspekcie technologicznym, ale również społecznym[20].

Instytucją, która zajmuje się zapewnieniem odpowiedniego poziomu bezpieczeństwa w sieci jest CERT (Computer Emergency Response Team), czyli zespół reagowania na incydenty, który utworzono w 1996 roku[21]. Jego najważniejszym celem jest obsługa incydentów bezpieczeństwa oraz podejmowanie współpracy z identycznymi podmiotami zagranicznymi.

Do najważniejszych zadań zespołu zalicza się[22]:

- rejestrowanie oraz obsługa wszelkich zdarzeń, które mogą naruszać bezpieczeństwo w Internecie,
- wykrywanie oraz analizowanie zagrożeń, które są wymierzone w polskich internautów i które zagrażają domenie.pl,
- aktywne i szybkie reagowanie w przypadku kiedy pojawią się bezpośrednie zagrożenia dla polskich użytkowników – prywatnych jak i publicznych i różnego rodzaju podmiotów gospodarczych,
- uczestniczenie w krajowych oraz międzynarodowych projektach powiązanych z bezpieczeństwem teleinformatycznym,
- prowadzenie działań badawczych dotyczących wykorzystywanych metod wykrywania incydentów bezpieczeństwa, a także analizy złośliwego oprogramowania oraz systemów wymiany danych o zagrożeniach,
- rozwijanie swoich narzędzi do tego, by wykrywać, monitorować, analizować oraz testować wszelkie narzędzia pozwalające na zwiększenie poziomu ochrony bezpieczeństwa,
- regularne publikowanie raportów CERT Polska,
- prowadzenie działań o charakterze informacyjno – edukacyjnym, które mają podnosić poziom świadomości dotyczącej bezpieczeństwa teleinformatycznego.

Zadaniem edukacji jest pozytywne kształtowanie obecności jednostki w cyberprzestrzeni. Odbywa się to głównie poprzez wskazanie na dobry lub zły model stosowanego zachowania. Sprawozdawczość medialna dotycząca cyberprzestępczości może być zbyt eksponowana. Jednak to poziom wiedzy oddziałuje na zachowania pracowników. Odnosi się to nie tylko do wykorzystywania komputerów do wykonywania swoich obowiązków, ale równie do utrzymania odpowiedniego poziomu prywatności i umiejętności jej ochrony[23].

Okazuje się, że najmniej skutecznym rozwiązaniem i narzędziem pozwalającym na zwiększenie poziomu bezpieczeństwa są przepisy znowelizowanego kodeksu karnego. Nawet po dostosowaniu ich do reguł uwzględnionych w Konwencji Rady Europy o cyberprzestępczości (z 2001 roku) nie była ona

[20] K. Midor... op.cit., s. 75-80.
[21] Raport Roczny z działalności CERT Polska. 2017, s. 7-10.
[22] Raport Roczny z działalności CERT Polska. 2017, s. 7-10.
[23] K. Midor... op.cit., s. 75-80.

wystarczająca. Uwzględniała jedynie penalizację przestępstw komputerowych jak i przestępstw, które mogą godzić w bezpieczeństwo systemów informatycznych[24]. Często okazuje się jednak, że popełniony czyn znacznie wychodzi poza ramy zdefiniowanego przez kodeks karny czynu przestępczego. W skrajnych przypadkach może nawet doprowadzić do konieczności wprowadzenia stanu wyjątkowego[25].

Dopiero w Strategii Bezpieczeństwa RP z 2014 roku cyberbezpieczeństwo jest jednym z celów strategicznych w zakresie bezpieczeństwa. Szczególną wagę przywiązywano tutaj do funkcjonowania systemu teleinformatycznego RP z uwzględnieniem jego dostępności, a także integralności i zachowania poufności wszystkich danych[26].

Odrębnym narzędziem jest stosowanie Polityki Ochrony Cyberprzestrzeni RP. Jej najważniejszym celem strategicznym jest osiągnięcie akceptowanego poziomu bezpieczeństwa cyberprzestrzeni państwa, które będzie realizowane poprzez budowanie odpowiednich ram organizacyjno – prawnych, a także systemu efektywnej koordynacji i wymiany informacji między poszczególnymi użytkownikami działającymi w ramach określonej cyberprzestrzeni RP[27]. Cel ten został wyznaczony również w Rządowym programie ochrony cyberprzestrzeni RP na lata 2011–2016, a także w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020.

W Strategii podkreślono, że wszelkie działania mające na celu poprawę poziomu bezpieczeństwa, powinny rozpocząć się od wprowadzenia odpowiednich zmian prawnych. Dlatego też niezbędne jest dokonanie szczegółowego przeglądu wszystkich przepisów prawnych, które obecnie obowiązują. W dalszej kolejności należy doprowadzić do ich harmonizacji oraz zwiększenia skuteczności działania czy też poprawy przepływu informacji między każdym, kto jest zaangażowany w aktywne tworzenie krajowego systemu cyberbezpieczeństwa[28].

Kluczowe wydaje się tutaj wprowadzenie założeń uwzględnionych w Dyrektywie NIS. Uwzględnia ona, bowiem wszystkie wymagania bezpieczeństwa dotyczące podmiotów zarówno państwowych jak i prywatnych z sektorów: energetycznego, transportowego, a także bankowości czy infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę oraz całej infrastruktury cyfrowej. Zagwarantowanie właściwego poziomu skuteczności stworzonego systemu cyberbezpieczeństwa wiąże się, bowiem z koniecznością dołączenia do niego całego sektora publicznego, a także telekomunika-

[24] M.Grzelak, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe, 22/2012, s. 132-135.
[25] Ibidem., s. 132-135.
[26] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2014, s. 12.
[27] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013, s. 8
[28] Strategia cyberbezpieczeństwa RP na lata 2016-2020, s. 9-14.

cyjnego. Ważne jest również uwzględnienie tych kwestii, które odnoszą się do usług zaufania oraz usług publicznych, które są świadczone przez szeroko rozumiany sektor prywatny. Jednocześnie Dyrektywa NIS wdraża minimalne wymagania przeznaczone dla dostawców wszystkich usług cyfrowych, czyli poszczególnych internetowych platform handlowych jak również wyszukiwarek internetowych oraz wszelkich usług przetwarzania w chmurze[29].

Jednocześnie, mając świadomość tego, że nieustannie rozwija się społeczeństwo informacyjne, zwiększa zakres elektronicznej administracji oraz gospodarki cyfrowej oraz w świetle zagrożeń w cyberprzestrzeni konieczne jest wzmocnienie wszystkich struktur krajowych obowiązujących w ramach krajowego systemu ochrony cyberprzestrzeni.

Kluczowym zadaniem poszczególnych organów państwowych jest zdefiniowanie konkretnego zakresu odpowiedzialności całego podmiotu koordynującego ten system, a także wyszczególnienia obowiązków oraz uprawnień przypisanych poszczególnym uczestnikom systemu jak metodom oddziaływania uprawnionego koordynatora na każdy innych podmiot. Konieczne jest także ustalenie kompetencji organów właściwych, które są odpowiedzialne za pełnienie nadzoru nad systemami teleinformatycznymi w sektorach, gdzie świadczy się usługi zarówno kluczowe jak i cyfrowe[30].

Rozbudowa całego tego systemu odnosi się również do systematycznego poszerzania struktur, które odpowiadają za cyberbezpieczeństwo na poziomie operacyjnym. Zalicza się do nich[31]:

- Narodowe Centrum Cyberbezpieczeństwa (NCC);
- CSIRT Narodowy;
- sektorowe zespoły reagowania na zdarzenia (CSIRT sektorowe);
- centra wymiany oraz analizy informacji.

Dodatkowo, ważne jest wprowadzenie jeszcze na poziomie prawodawstwa właściwych struktur tych jednostek. Konieczne jest w tym przypadku usprawnienie procesu przepływu informacji oraz doprecyzowanie wszelkich powiązań, które występują pomiędzy każdym interesariuszem. Ważne jest, by doprowadzić do zniwelowania pewnej niechęci, która cechuje każdy podmiot, a która odnosi się do dzielenia się informacjami. Poszczególne podmioty stosunkowo niechętnie dzielą się informacjami dotyczącymi zauważonych zagrożeń, a także incydentów czy też szacowania strat. Dlatego też ważne jest opracowanie czy też rozbudowanie krajowej sieci CSIRT[32]:

- narodowy;
- sektorowy;
- komercyjny;
- przedsiębiorców.

[29] Ibidem.
[30] Ibidem.
[31] Ibidem.
[32] Ibidem.

W ten sposób można doprowadzić do sytuacji, w której wymieniałyby się one wszystkimi informacjami na temat zagrożeń bezpieczeństwa oraz wszelkich incydentach, które pojawiają się w konkretnym sektorze lub w dziale administracji.

Należy tutaj podkreślić, że wszystkie działania, które są prowadzone w cyberprzestrzeni zostały włączone w planowanie operacyjne. Są one częścią operacji, które są podejmowane przez SZ RP samodzielnie oraz w zespole sojuszniczym czy też koalicyjnym. W ten sposób dąży się do tego, by udoskonalić wszystkie struktury wojskowe, które gwarantują efektywne planowanie, a także dowodzenie czy zarządzanie zasobami, jak i umiejętnościami oraz zdolnościami. Planowane jest także zwiększenie poziomu kwalifikacji, poprzez prowadzone szkolenia wewnętrzne i wysoko wyspecjalizowane szkolenia zewnętrzne, które przygotowane są w odpowiedzi na generowane przez resort obrony narodowej potrzeby i oczekiwania[33].

Istotnym aktem prawnym jest również Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 dotyczącej identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznych: „celem przytoczonego rozporządzenia jest m.in. zapewnienie wzajemnego uznawania akceptacji elektronicznej identyfikacji przez państwa członkowskie, ujednolicenie ram prawnych świadczenia usług zaufania oraz prowadzenie nadzoru nad dostawcami usług w UE czy zapewnienie uznawania usług zaufania związanych z transakcjami elektronicznymi oraz uwierzytelnianiem witryn internetowych”[34].

Warto tutaj podkreślić, że w rozporządzeniu wskazano kilka poziomów bezpieczeństwa obowiązującego w ramach systemów identyfikacji elektronicznej. Zalicza się do nich poziom[35]:

- niski – środek identyfikacji elektronicznej gwarantujący ograniczony pozom zaufania względem podawanej czy też zgłaszanej tożsamości wybranej osoby oraz może odnosić się do technicznych specyfikacji i standardów lub procedur, których celem jest ograniczenie ryzyka podszywania się czy też modyfikacji tożsamości,
- średni – odnosi się do środka identyfikacji elektronicznej, gwarantuje średni poziom zaufania względem podawanej czy zgłaszanej tożsamości wybranej osoby, charakteryzuje się w kontekście do technicznych specyfikacji jak i standardów i procedur, które są z nim powiązane i które odnoszą się do stosowanych zabezpieczeń mających na celu obniżenie ryzyka podszycia się albo modyfikacji tożsamości,
- wysoki – gwarantuje wysoki poziom zaufania.

[33] Ibidem.
[34] A. Turbalska, Bezpieczeństwa państwa w cyberprzestrzeni, Wyd. WSEiI, Lublin, 2017, s. 26-30.
[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 dotyczącej identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznych.

W sytuacji naruszenia bezpieczeństwa lub w przypadku chociażby częściowej kompromitacji całego systemu identyfikacji elektronicznej, co może wpływać na wiarygodność całego systemu trans granicznego uwierzytelnienia systemu, państwo notyfikujące musi natychmiast zawiesić lub unieważnić to uwierzytelnienie i powiadomić o tym wszystkie kraje.

Podsumowanie

Można, więc powiedzieć, że system prawny oraz pozostałe elementy składające się na system bezpieczeństwa informacyjnego, który ma za zadanie chronić obywateli i wszystkie podmioty działające w ramach systemu, jest dopiero rozwijany. Nie uwzględnia on jednak jeszcze wszystkich zagrożeń, a tym samym nie stanowi efektywnego narzędzia pozwalającego na przeciwdziałanie pojawiającym się niebezpieczeństwo. Dlatego też pozostałe rozwiązania, przygotowywane zwykle przez niezależne organizacje czy też działania podejmowane w ramach poszczególnych jednostek rządowych, są o wiele bardziej dopasowane do rozwijających się zagrożeń. Są one na tyle elastyczne, by móc dostosowywać się do zmieniających się uwarunkowań.

Bibliografia:

1. Aleksandrowicz T., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska praw międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego, 15/2016.
2. Grzelak M., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* Bezpieczeństwo Narodowe, 22/2012.
3. *Krajobraz bezpieczeństwa polskiego internetu*. Raport Roczny z działalności CERT Polska, 2018.
4. Midor K*., Technologia informacyjna w obszarze cyberbezpieczeństwa państwa i społeczeństwa,* Systemy Wspomagania w Inżynierii Produkcji, 6/2017.
5. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.
6. *Raport Roczny z działalności CERT Polska*, 2017.
7. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2014.
8. *Strategia cyberbezpieczeństwa RP na lata 2016-2020*, Warszawa, 2015.
9. *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015.
10. Turbalska A., *Bezpieczeństwa państwa w cyberprzestrzeni,* Wyd. WSEiI, Lublin 2017.

Netografia:

11. https://odo24.pl/blog-post.bezpieczenstwo-w-cyberprzestrzeni-zarys-problemu-wyzwania-i-zagrozenia
12. https://www.motorolasolutions.com/content/dam/msi/docs/pl_pl/services/cybersecurity_services_comprehensive_brochure_polish.pdf