Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

Spis treści

1. Podstawowe informacje

Informacje i dane stanowią znaczący potencjał gospodarczy i polityczny. Informacja i jej treść może nie tylko decydować o istnieniu lub nieistnieniu jednostki lub firmy, ale w rzeczywistości ma zdolność wpływania na rozwój sytuacji na świecie. [1]

Ważne jest, aby zdać sobie sprawę, że im bardziej jesteśmy uzależnieni od technologii informacyjno-komunikacyjnych[2] oraz im więcej danych o nas gromadzą i udostępniają, tym bardziej jesteśmy bezbronni.

Wielu konsekwencji spowodowanych cyberatakami, ludzką głupotą lub ignorancją można uniknąć, jeśli przestrzegane będą podstawowe zasady bezpieczeństwa cybernetycznego. [3]

Bezpieczeństwo cybernetyczne jest de facto czymś, co można opisać jako stale ewoluujący i zmieniający się proces, który zależy od wielu zmiennych. Tymi zmiennymi mogą być oczywiście same dane lub elementy TIK podlegające ochronie, faktycznie ustanowione procesy i ich rewizja itp. Najważniejszym elementem jest jednak użytkownik (zarówno końcowy, jak i administrator), który stosuje faktyczne elementy bezpieczeństwa cybernetycznego.

W tym miejscu pojawia się przeszkoda, że otrzymacie informacje, instrukcje i procedury, które poznaliśmy i przetestowaliśmy w dobrej wierze. Przedstawiony zostanie nasz punkt widzenia na kwestię cyberbezpieczeństwa i procesów z nim związanych. Te przewodniki, procedury i zalecenia działają dla nas, ale mogą nie działać dla Ciebie, ponieważ dobrze jest oprzeć własne wdrożenie wszelkich procedur bezpieczeństwa na pewnych sprawdzonych zaleceniach, ale przede wszystkim dobrze jest zindywidualizować, zmodyfikować lub zmienić te procedury w zależności od specyficznych warunków samego użytkownika lub organizacji.

Dyrektywa UE w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) ma na celu utworzenie sieci CSIRT "w celu przyczynienia się do rozwoju zaufania między państwami członkowskimi oraz promowania szybkiej i skutecznej współpracy operacyjnej". [1] Dyrektywa stanowi, że każde państwo członkowskie wyznacza jeden lub więcej CSIRT, które spełniają wymogi określone w pkt 1 załącznika I do dyrektywy (wymogi), obejmujące co najmniej sektory, o których mowa w załączniku II, oraz usługi, o których mowa w załączniku III, odpowiedzialne za obsługę ryzyka i incydentów zgodnie z dobrze zdefiniowanym procesem. Dyrektywa określa ogólne wymagania, których wyznaczone CSIRT muszą przestrzegać, oraz zadania, które muszą wykonywać.[4]

---

[1] Zob. informacje o wpływie wyborów prezydenckich w USA (2016) i we Francji (2017). Zob. na przykład:

Wywiad: kampania mająca na celu wywarcie wpływu na wybory prezydenckie w USA została zlecona przez Putina. [online]. [cyt. 2017 Jun 29]. Dostępny pod adresem: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
Sztab wyborczy Macrona został zaatakowany przez hakerów, twierdzi japońska firma antywirusowa. [online]. [cyt. 2017 Jun 29]. Dostępny pod adresem: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

[3] *WannaCry nie powinien był się w ogóle rozprzestrzeniać. Wystarczyło skorzystać z usługi Windows Update.* [online]. [cyt. 2017 Jun 27]. Dostępny pod adresem: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

[2] Zwane dalej ICT

[4] *Model oceny dojrzałości CSIRT ENISA* [online], 2019 r. WERSJA 2.0. Ateny, Grecja: Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) [cyt. 2021-03-16]. ISBN 978-92-9204-292-9. Dostępny pod adresem: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, s. 6.

1.1. Cyberbezpieczeństwo

"W ciągu ostatniej dekady bezpieczeństwo cybernetyczne zyskało na znaczeniu i stało się jednym z głównych priorytetów wielu polityk krajowych. Dzieje się tak głównie ze względu na przenoszenie się na inne dziedziny bezpieczeństwa, a także z powodu incydentów, które rozsławiły to pojęcie i sprawiły, że opinia publiczna zaczęła zastanawiać się nad potrzebą zapewnienia bezpieczeństwa w cyberprzestrzeni. Wiąże się to z koniecznością ochrony cyberprzestrzeni w taki sposób, aby w jak największym stopniu zachować wszechstronne bezpieczeństwo Republiki Czeskiej, a także prawa jednostek do informacyjnego samostanowienia."[1]

Definicja bezpieczeństwa cybernetycznego może być nieco problematyczna. Dla wielu osób bezpieczeństwo cybernetyczne to obszar, którym de facto zajmują się wyłącznie działy teleinformatyczne.

Założenie to jest błędne od samego początku, ponieważ bezpieczeństwo cybernetyczne dotyczy każdego, kto w życiu codziennym korzysta z jakichkolwiek elementów TIK. Jeśli sami nie zdajemy sobie sprawy z tego, że jesteśmy kluczowym, a w wielu przypadkach wręcz podstawowym elementem bezpieczeństwa cybernetycznego (zarówno w życiu prywatnym, jak i w pracy), to w rzeczywistości zwiększamy prawdopodobieństwo powodzenia cyberataków.

Bezpieczeństwa cybernetycznego nie można dziś ani nie doceniać, ani lekceważyć. Jest to obszar, który ma kluczowe znaczenie dla wielu organizacji, ale także dla samych jednostek, dlatego należy się nim zająć w sposób długofalowy i systematyczny.

*"Kierownictwo organizacji powinno zrozumieć i zaakceptować fakt, że zarządzanie bezpieczeństwem cybernetycznym jest znacznie bardziej zbliżone do innych obszarów bezpieczeństwa i zarządzania kryzysowego. W końcu nawet dzisiejsze wyrafinowane ataki mają często charakter multidyscyplinarny, łącząc obszary ICT, inżynierii społecznej, bezpieczeństwa personelu i obiektów."**[2]*

Wracając do samego terminu "bezpieczeństwo cybernetyczne", warto zacząć od jego analizy. Słowo "**cyber"** oznacza współzależność z elementami technologii informacyjno-komunikacyjnych i cyberprzestrzeni jako takiej.

Bezpieczeństwo

Istnieje wiele definicji serwisu[3] , ale nie ma jednej, ogólnie przyjętej. Większość definicji bezpieczeństwa można znaleźć w literaturze, a nie w samych przepisach. [4]

Mareš definiuje bezpieczeństwo jako "*stan, w którym zagrożenia dla obiektu (zwykle państwa narodowego, a nawet organizacji międzynarodowej) i jego interesów są ograniczone do najniższego możliwego stopnia, a obiekt jest skutecznie wyposażony i gotowy do współpracy w celu wyeliminowania istniejących i potencjalnych zagrożeń".*[5]

Ogień definiuje *"bezpieczeństwo jako cechę przedmiotu lub podmiotu, która określa stopień, stopień jego ochrony przed potencjalnymi szkodami i zagrożeniami".*[6]

Definicja ta została następnie dopracowana w Słowniku interpretacyjnym bezpieczeństwa cybernetycznego:

Bezpieczeństwo (Security)

Właściwość elementu (np. systemu informatycznego), która jest na pewnym poziomie zabezpieczona przed utratą, lub stan zabezpieczenia (na pewnym poziomie) przed utratą. Bezpieczeństwo informatyczne obejmuje ochronę poufności, integralności i dostępności podczas przetwarzania, przechowywania, dystrybucji i prezentacji informacji. [7]

Należy zauważyć, że bezpieczeństwo to nie tylko kwestia państwa, które nadal odgrywa pierwszoplanową rolę w jego zapewnianiu, ale także proces realizowany przez inne podmioty (osoby prawne i fizyczne), które w ostatnim czasie są zmuszone w coraz większym stopniu zajmować się kwestią bezpieczeństwa lub zabezpieczenia swojej działalności przed atakami.

To poszerzenie kręgu bezpieczeństwa powoduje, że konieczne jest zajęcie się m.in. następującymi kwestiami:

- **Czyje bezpieczeństwo jest zagrożone** (organizacji międzynarodowej, państwa, organizacji, jednostki itd.)**?**
- **Jakie wartości są chronione** (organizacje, ludzie, dane itp.)**?**
- **Przed czym są (powinny być) chronione te wartości** (atak fizyczny, cybernetyczny, ataki łączone itp.)**?**
- **Jakie zasoby są potrzebne do ochrony tych wartości**? [8]

Idealnym celem bezpieczeństwa jest stworzenie stanu "absolutnego bezpieczeństwa". Stan ten jest jednak utopią, ponieważ nie da się go realistycznie osiągnąć,[9] , ponieważ zawsze będzie istniało zagrożenie lub ryzyko, które nie zostało uwzględnione w koncepcji projektowania bezpieczeństwa lub zostało celowo pominięte.

Celem bezpieczeństwa nie jest jednak objęcie wszystkich rzeczywistych, mniej rzeczywistych lub całkowicie nieprzewidywalnych i mało prawdopodobnych zagrożeń we wszystkich okolicznościach, ponieważ taka realizacja stworzyłaby całkowicie dysfunkcyjny moloch, który w zasadzie negowałby stosowanie i wdrażanie bezpieczeństwa, a nawet całkowicie je eliminował.

Przykład: *w życiu codziennym zdarza Ci się zatrzasnąć klucze np. w mieszkaniu. Jeśli na to liczyłeś, prawdopodobnie masz zapasowe klucze u rodziny, przyjaciół lub w innym miejscu. Jeśli jednak nie masz zapasowych kluczy, prawdopodobnie wezwiesz ślusarza lub wyważysz drzwi.*

Cyberbezpieczeństwo

Podobnie jak w przypadku pojęcia bezpieczeństwa, bezpieczeństwo cybernetyczne nie ma jednej powszechnie akceptowanej definicji. Bezpieczeństwo cybernetyczne jest podzbiorem samego bezpieczeństwa.

Definiując samo bezpieczeństwo cybernetyczne, warto oprzeć się na ustalonych definicjach. Wymienię kilka takich ustalonych definicji:

1. **Cyberbezpieczeństwo** to **zestaw środków podejmowanych w celu ochrony systemu komputerowego przed nieuprawnionym dostępem lub atakiem**. [10]

2. Słownik oksfordzki podaje, że **cyberbezpieczeństwo** to **stan**, **w którym dane elektroniczne są chronione przed przestępczym lub nieuprawnionym użyciem.** Bezpieczeństwo cybernetyczne obejmuje środki, które należy podjąć, aby osiągnąć ten stan.[11]

3. Według Jiráska i in. **cyberbezpieczeństwo** to *"**zespół środków** prawnych, organizacyjnych, technicznych i edukacyjnych **mających na celu zapewnienie ochrony cyberprzestrzeni"**. "*[12]

4. Narodowa Strategia Cyberbezpieczeństwa Republiki Czeskiej na lata 2015-2020 definiuje cyberbezpieczeństwo w stosunkowo podobny sposób, stwierdzając, że *"Cyberbezpieczeństwo stanowi **zestaw** organizacyjnych, politycznych, prawnych, technicznych i edukacyjnych **środków i narzędzi mających na celu zapewnienie bezpiecznej, chronionej i odpornej cyberprzestrzeni w Republice Czeskiej,** zarówno dla podmiotów sektora publicznego i prywatnego, jak i dla ogółu społeczeństwa czeskiego."* [13]

Mimo że definicje te próbują zdefiniować pojęcie bezpieczeństwa cybernetycznego, są one nieco nieprecyzyjne.

Pierwsza definicja skupia się tylko na komputerze i systemie komputerowym oraz ich ochronie przed dwoma rodzajami cyberataków, podczas gdy spektrum zarówno celów ataków, jak i samych ataków jest znacznie bardziej zróżnicowane.[14]

Druga definicja chroni tylko dane elektroniczne, a nie systemy komputerowe jako takie.

Trzecia definicja skupia się na przyjęciu środków ochrony elementów TIK w cyberprzestrzeni. Definicja ta jest stosunkowo precyzyjna, ale jej ograniczenie wyłącznie do cyberprzestrzeni może być mylące, ponieważ bezpieczeństwo cybernetyczne można również stosować do elementów TIK, które nie są połączone z cyberprzestrzenią lub tworzą własną "cyberprzestrzeń off-line".[15]

Ostatnia definicja jest więc wyraźnie ograniczona tylko do cyberprzestrzeni w Republice Czeskiej, przy jednoczesnym całkowitym pominięciu możliwości ochrony interesów obywateli czeskich lub innych podmiotów, które nie mają siedziby w Republice Czeskiej. Uważamy, że zawężenie cyberbezpieczeństwa tylko do cyberprzestrzeni w Republice Czeskiej jest zrozumiałe z perspektywy wdrażania ustawy o cyberbezpieczeństwie, ale niewłaściwe z perspektywy wdrażania cyberbezpieczeństwa.

Inną definicję bezpieczeństwa cybernetycznego można znaleźć na przykład w dokumencie **Definition of Cybersecurity - Gaps and overlaps in standardisation**[16] Europejskiej Agencji ENISA[17] : *"Bezpieczeństwo cybernetyczne odnosi się do bezpieczeństwa cyberprzestrzeni, gdzie sama cyberprzestrzeń odnosi się do zbioru powiązań i relacji pomiędzy obiektami, które są dostępne za pośrednictwem ogólnej sieci telekomunikacyjnej, oraz do rzeczywistego zbioru obiektów, których interfejsy umożliwiają ich zdalną kontrolę, zdalny dostęp do danych lub zaangażowanie w działania kontrolne w cyberprzestrzeni. Bezpieczeństwo cybernetyczne będzie obejmować paradygmat triady "CIA" w odniesieniu do relacji i obiektów w cyberprzestrzeni, przy jednoczesnym rozszerzeniu tego paradygmatu w celu zapewnienia ochrony prywatności podmiotów (osób i podmiotów) oraz odporności ["odbudowy" po ataku]".*

Biorąc pod uwagę wysiłek włożony w zdefiniowanie pojęcia bezpieczeństwa cybernetycznego, należy oprzeć się na normach prawnych, które dotyczą bezpieczeństwa cybernetycznego.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii[18] stanowi w art. 4 ust. 2, że *"bezpieczeństwo sieci i systemów informatycznych oznacza zdolność tych sieci i systemów informatycznych do wytrzymania z pewnym stopniem niezawodności wszelkich zakłóceń, które zagrażają dostępności, autentyczności, integralności lub poufności przechowywanych, przesyłanych lub przetwarzanych danych lub usług powiązanych oferowanych lub dostępnych za pośrednictwem tych sieci i systemów informatycznych."*.

- **PL - Definicja cyberbezpieczeństwa:** odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. z 2018 r. poz. 1560)

W powyższych definicjach na różne sposoby próbuje się określić zakres relacji, interesów i podmiotów, wobec których stosuje się bezpieczeństwo cybernetyczne. Jednocześnie definiują one cyberprzestrzeń jako środowisko, w którym stosuje się bezpieczeństwo cybernetyczne.

Ze względu na pewną niespójność poglądów na temat tego, co jest, a co nie jest cyberbezpieczeństwem, należy przedstawić naszą własną definicję bezpieczeństwa cybernetycznego, która została opracowana zarówno na podstawie analizy wcześniejszych definicji, jak i

na podstawie naszych własnych doświadczeń.

Bezpieczeństwo cybernetyczne można zdefiniować jako:

- **ogół środków prawnych, organizacyjnych, technicznych i edukacyjnych mających na celu zapewnienie ochrony systemów komputerowych i innych elementów TIK, aplikacji, danych oraz użytkowników,**
- **zdolność systemów i usług komputerowych wykorzystywanych do reagowania na zagrożenia lub ataki cybernetyczne i ich skutki, a także planowanie przywracania funkcjonalności systemów komputerowych i powiązanych usług.**

Bezpieczeństwo cybernetyczne jest realizowane zarówno w cyberprzestrzeni, jak i poza nią. Nie zaleca się ograniczania stosowania powyższych środków i zasad w jakiejkolwiek geolokalizacji (czy to na terytorium danego państwa, Unii czy samej cyberprzestrzeni).

---

[1] *2017 State of Cybersecurity Report* [online]. [cyt. 2018 Jun 29]. Dostępny pod adresem: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[2] *Bezpieczeństwo cybernetyczne: co z tym zrobić?* [online]. [cyt. 2018 Jun 29]. Dostępny pod adresem: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

[3] Jeśli chodzi o interpretację samego terminu, należy wspomnieć o względnej nieprecyzyjności języka czeskiego w porównaniu z językiem angielskim, w którym zazwyczaj używa się dwóch terminów na określenie bezpieczeństwa: **security** i **safety**. Termin **bezpieczeństwo** jest używany w znaczeniu aktywnej ochrony lub aktywnego zabezpieczenia, zabezpieczenia lub ochrony, a termin bezpieczeństwo jest zwykle używany do wyrażenia pasywnego bezpieczeństwa, bezpieczeństwa, cechy stanu lub własności pewnego obiektu.

[4] Zob. np. ustawa konstytucyjna nr 110/1998 Dz.U. o bezpieczeństwie Republiki Czeskiej; ustawa nr 240/2000 Dz.U. o zarządzaniu kryzysowym i o zmianach niektórych ustaw (ustawa kryzysowa); ustawa o cyberbezpieczeństwie itd.

[5] ZEMAN, Petr et al. *Czeska terminologia dotycząca bezpieczeństwa: interpretacja podstawowych terminów* [online]. [cytowany 2018-07-10]. Dostępny na stronie: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

[6] *POŽÁR, Josef. Bezpieczeństwo informacji*. Pilzno: Aleš Čeněk, 2005, s. 37.

[7] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015, s. 23 [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[8] Więcej informacji na ten temat można znaleźć np. w publikacji MAREŠ, Miroslav. *Bezpieczeństwo.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

WAISOVÁ, Šárka. *Bezpieczeństwo: rozwój i zmiany koncepcji.* Pilzno: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

FRANK, Libor. *Studia nad bezpieczeństwem.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

[9] Zob. WAISOVÁ, Šárka. *Bezpieczeństwo: rozwój i transformacja koncepcji*. Pilzno: Aleš Čeněk, 2005. 159 s. ISBN 80-86898-2-10

[10] *Bezpieczeństwo cybernetyczne.* [online]. [cytowany 2018-07-06]. Dostępny na stronie: https://www.merriam-webster.com/dictionary/cybersecurity Tłumaczenie autora.

[11] *Bezpieczeństwo cybernetyczne.* [online]. [cytowany 2018-07-06]. Dostępny na stronie: https://en.oxforddictionaries.com/definition/cybersecurity Tłumaczenie autora.

[12] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015, s. 69 [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[13] *Narodowa Strategia Cyberbezpieczeństwa Republiki Czeskiej na lata 2015-2020* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

[14] Atakowane mogą być również aplikacje, konta użytkowników itp. Jeśli chodzi o faktyczne ataki, to poszczególne ataki zostały opisane m.in. w KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016, s. 181 i nast.

[15] Więcej szczegółów można znaleźć np. w artykule *Nadejście hakerów: historia Stuxnetu.* [online]. [cyt. 1 lipca 2018]. Dostępne na stronie: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/ lub FRUHLINGER, Josh. *Co to jest Stuxnet, kto go stworzył i jak działa?* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

[16] *Definition of Cybersecurity - Gaps and overlaps in standardisation* [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

[17] Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

[18] Zwana dalej "**NIS**" lub "**dyrektywą NIS".** [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

1.2. Zasady bezpieczeństwa cybernetycznego

Następujące zasady, znane również jako triada bezpieczeństwa cybernetycznego, są stosowane w ramach bezpieczeństwa cybernetycznego.[1]

Na potrzeby niniejszej monografii zostaną zdefiniowane trzy triady:

1. **CIA** [C - **Confidentiality (poufność)**; **I** - **Integrity (integralność)**; **A - Availability (dostępność)**].
2. **Elementy bezpieczeństwa cybernetycznego** (ludzie, technologia, procesy).
3. **Cybersecurity Lifecycle** (Prevention, Detection, Response).

1.1.1 Triada CIA

Najbardziej znaną i szeroko stosowaną triadą bezpieczeństwa cybernetycznego jest triada **CIA**, ale samo stosowanie tej podstawowej triady zasad bezpieczeństwa cybernetycznego bez wdrożenia innych zasad jest obecnie niewystarczające do utrzymania odpowiedniego poziomu bezpieczeństwa cybernetycznego.

Na przykład w literaturze przedmiotu wskazuje się na zastosowanie **heksady Parkera**[2] , która jest de facto triadą CIA uzupełnioną o trzy inne elementy: **P/C - Possession/Control (posiadanie/kontrola)**, **A - Authenticity (autentyczność)** i **U - Utility (użyteczność**).

Celem bezpieczeństwa cybernetycznego jest zapewnienie bezpieczeństwa technologii informacyjno-komunikacyjnych jako takich, a także bezpieczeństwa danych i informacji przesyłanych, przetwarzanych i przechowywanych przez te elementy.

Bardzo często triada CIA jest związana przede wszystkim z informacją.

To węższe pojęcie wynika głównie z samej definicji bezpieczeństwa **informacji,** która koncentruje się na ochronie informacji. W kontekście tej ochrony nie ma znaczenia, na jakim nośniku (papier, nośnik elektroniczny itp.) lub w jakim systemie informacje są przetwarzane. Bezpieczeństwo informacji jest następnie stosowane w odniesieniu do informacji w całym cyklu ich życia.

Bezpieczeństwo informacji jest również definiowane przez szereg norm ISO 27000. Do podstawowych standardów bezpieczeństwa informacji należą:

- ISO/IEC 27001:2014 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania
- ISO/IEC 27002:2014 Technika informatyczna - Techniki bezpieczeństwa - Zbiór praktyk dotyczących środków bezpieczeństwa informacji

Powstaje pytanie, czy obecna definicja bezpieczeństwa informacji jest odpowiednia i wystarczająca, czy obejmuje wszystkie kluczowe elementy bezpieczeństwa w cyberprzestrzeni.

Pomimo tego, że w literaturze fachowej i normach prawnych częściej używany jest termin "bezpieczeństwo informacji", uważamy, że w odniesieniu do działań związanych z wykorzystaniem technologii informacyjno-komunikacyjnych lub działań związanych z cyberprzestrzenią bardziej odpowiedni jest termin "bezpieczeństwo cybernetyczne".

Jak stwierdzono powyżej, *"bezpieczeństwo informacji odnosi się do informacji jako takiej"*. Nie uwzględnia to jednak kluczowych elementów związanych z bezpieczeństwem w cyberprzestrzeni.

Za te ważne elementy uważamy **dane, a następnie** same **systemy komputerowe** (lub poszczególne elementy TIK), które umożliwiają faktyczny transfer danych i informacji.

W literaturze i prawodawstwie istnieje wiele definicji danych i informacji. Na potrzeby niniejszej publikacji wybrano definicje związane z problematyką ochrony informacji, ochrony danych lub cyberbezpieczeństwa.

Zgodnie z Konwencją o cyberprzestępczości[3] **dane komputerowe** oznaczają *"**każde wyrażenie faktów, informacji lub pojęć w formie nadającej się do przetwarzania przez system komputerowy,** w tym program mogący spowodować wykonanie funkcji **przez** system komputerowy"*.

Tak więc dane to dowolne elementy posiadające wartość informacyjną, które są przetwarzane przez system komputerowy w celu utworzenia informacji.

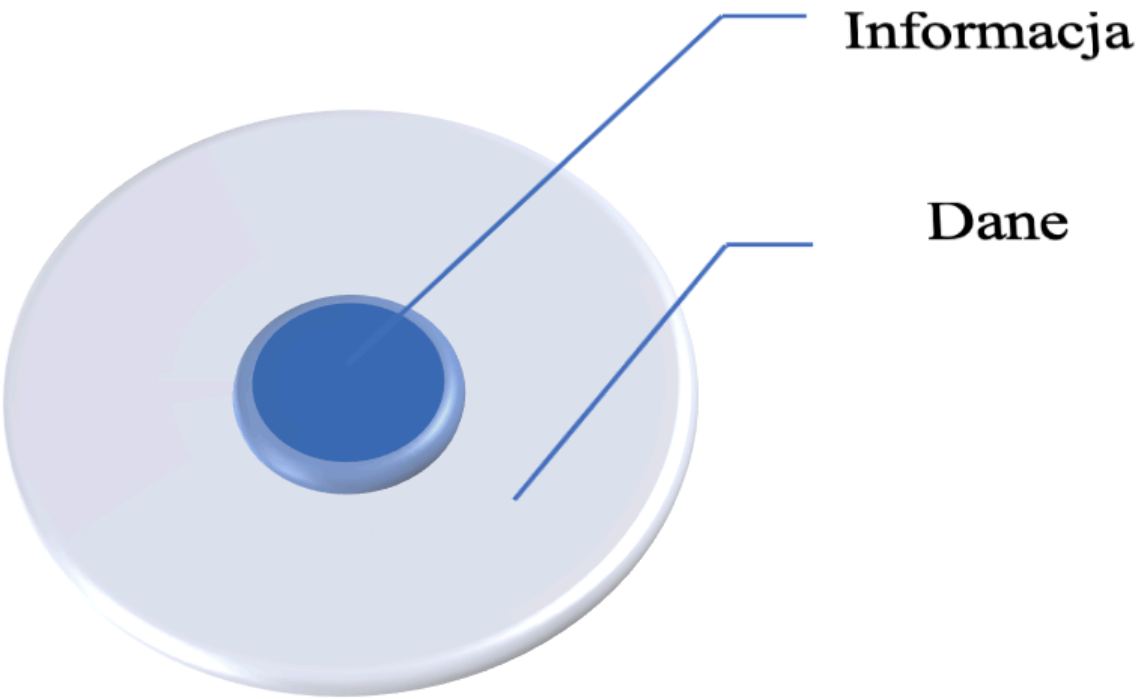
Informacja *"to dane, które zostały przetworzone do postaci użytecznej dla odbiorcy. Tak więc każda informacja to dane, dane, ale wszelkie przechowywane dane niekoniecznie stają się informacją"*.[4]

Wiener twierdzi, że "*informacja to nazwa nadana zawartości tego, co jest wymieniane ze światem zewnętrznym, gdy się do niego dostosowujemy i gdy wpływamy na niego poprzez nasze dostosowanie*". Stwierdza on również, że informacja nie jest ani materią, ani energią, lecz odrębną kategorią fizyczną.[5]

Informacja jest więc postrzegana jako coś bardziej "kwalifikowanego" niż dane. Dane to fakty, które stają się informacjami, gdy są postrzegane lub wyrażane w kontekście i mają znaczenie zrozumiałe dla ludzi.[6]

Z punktu widzenia bezpieczeństwa cybernetycznego kluczowe znaczenie może mieć łączenie "bezsensownych" danych i tworzenie kontekstu, który pozwoli przekształcić dane w "sensowne" informacje. Gdybyśmy bowiem mieli przestrzegać powyższej tezy o bezpieczeństwie informacji, w której chroniona jest tylko sama informacja, mogłoby dojść do poważnych naruszeń bezpieczeństwa.

Poniższy wykres ilustruje związek między danymi a informacjami.[7]



Dane i informacje są przesyłane w cyberprzestrzeni za pomocą systemów komputerowych[8] , które stanowią integralną część bezpieczeństwa cybernetycznego lub bezpieczeństwa informacji.

W związku z powyższym uważamy, że triada CIA[9] powinna być stosowana nie tylko do samych informacji, ale także do innych elementów cyberbezpieczeństwa (danych, systemów komputerowych itp.).

Poufność

Pojęcie poufności określa fakt, że dostęp do informacji, danych lub technologii informacyjno-komunikacyjnych mogą mieć tylko uprawnione do tego podmioty.

Ze względu na dużą ilość przetwarzanych informacji wskazane jest wprowadzenie lub stosowanie jednej z klasyfikacji informacji. Klasyfikacje te można następnie zastosować do innych elementów bezpieczeństwa cybernetycznego i dostępu do nich.

Definiują to normy bezpieczeństwa ISO/IEC 27000:

- *"Informacje powinny być klasyfikowane z uwzględnieniem ich wartości, wymogów prawnych, wrażliwości i krytyczności".*
- *"Należy opracować i wprowadzić w życie procedury oznaczania i przetwarzania informacji, które są zgodne ze schematem klasyfikacji przyjętym przez organizację."*
- *"Aby zapobiec nieupoważnionemu dostępowi do informacji lub ich niewłaściwemu wykorzystaniu, należy ustalić zasady postępowania z nimi i ich przechowywania."*

Przykłady niektórych systemów klasyfikacji:

1. **Klasyfikacja informacji zgodnie z ustawą 412/2005 Coll. o ochronie informacji niejawnych i poświadczeniu bezpieczeństwa**[10] :

- **Ściśle tajne** - nieuprawnione wykorzystanie informacji mogłoby spowodować bardzo poważne szkody dla interesów Republiki Czeskiej.
- **Tajne** - nieuprawnione wykorzystanie informacji mogłoby spowodować poważne szkody dla interesów Republiki Czeskiej.
- **Poufne** - nieuprawnione wykorzystanie informacji mogłoby spowodować zwykłą szkodę dla interesów Republiki Czeskiej.

- **Ograniczone -** nieuprawnione wykorzystanie informacji mogłoby być niekorzystne dla interesów Republiki Czeskiej.

2. Klasyfikacja informacji wykorzystywanych w sferze komercyjnej:

- **Chronione -** nieuprawnione wykorzystanie informacji może spowodować poważne szkody lub zniszczenie organizacji (np. wyciek informacji strategicznych, kodu źródłowego, schematów bezpieczeństwa, haseł itp.)
- **Wewnętrzne -** nieuprawnione posługiwanie się informacjami może spowodować szkody dla organizacji (np. wyciek danych osobowych, umów itp.).
- **Wrażliwe -** nieuprawnione wykorzystanie informacji może mieć negatywny wpływ na firmę (np. niepublikowane informacje o projektach, planowanych wydarzeniach itp.)
- **Publiczne -** nieuprawnione wykorzystanie informacji nie powinno nikomu zaszkodzić i nie powinno mieć żadnego wpływu na społeczeństwo (np. publicznie dostępne kontakty, prezentacje projektów itp.)[11]

Oprócz dwóch powyższych klasyfikacji istnieje szereg innych, przyjętych lub akceptowanych w organizacjach lub przez samych użytkowników, albo na mocy przepisów, albo według uznania użytkownika.

Same klasyfikacje, pod warunkiem ich przestrzegania i stosowania, mogą w znacznym stopniu ograniczyć skutki potencjalnego ataku cybernetycznego.

3. Protokół sygnalizacji świetlnej

W społeczności zajmującej się bezpieczeństwem cybernetycznym od dawna istnieje potrzeba dzielenia się informacjami i danymi (zazwyczaj dotyczącymi ataków cybernetycznych), które mają charakter wrażliwy. Z tego powodu na początku XXI wieku Krajowe Centrum Koordynacji Bezpieczeństwa Infrastruktury[12] stworzyło stronę internetową ***Traffic Light*** **Protocol** (**TLP**)[13] . Protokół ten ma na celu przyspieszenie wymiany informacji między zainteresowanymi stronami, a jednocześnie ustanawia zasady postępowania z przekazywanymi informacjami. Podmiot przekazujący informację (źródło informacji) zawsze oznacza ją kolorem, który określa, w jaki sposób informacja ma być traktowana przez odbiorcę.

Protokół TLP najlepiej definiuje poniższa tabela, zaczerpnięta z witryny US-CERT[14] :

Kolor	**Kiedy należy stosować**	**Jak mogę się podzielić?**
TLP:CZERWONY  **Nie do publikacji,** tylko **dla** uczestników.	Podmioty mogą stosować TLP:RED, gdy informacje nie pozwalają na skuteczną reakcję innych podmiotów i mogłyby prowadzić do wpływu na prywatność, reputację lub działalność tych podmiotów, gdyby zostały niewłaściwie wykorzystane.	Odbiorcy nie mogą udostępniać informacji TLP:RED żadnym podmiotom spoza konkretnej wymiany, spotkania lub rozmowy, w której informacja TLP:RED została pierwotnie zamieszczona. Na przykład w kontekście spotkania (spotkania), informacje TLP:RED są ograniczone do osób bezpośrednio uczestniczących w spotkaniu (spotkaniu). W większości przypadków **informacje oznaczone jako TLP: RED powinny być wymieniane wyłącznie ustnie lub osobiście.**
TLP:AMBER  **Ograniczone ujawnianie informacji.** Publikacja jest możliwa tylko w ramach organizacji uczestników.	Podmioty mogą korzystać z TLP: AMBER w przypadkach, gdy informacja wymaga skutecznej reakcji innych podmiotów i stanowi zagrożenie dla prywatności, reputacji lub działalności, jeśli zostanie udostępniona poza organizacjami uczestniczącymi.	Odbiorcy mogą udostępniać informacje skategoryzowane jako TLP: AMBER członkom własnej organizacji oraz klientom, którzy muszą znać te informacje, aby chronić siebie lub zapobiegać dalszym potencjalnym szkodom. **Jednostki mogą dowolnie ustalać dodatkowe zasady udostępniania, których należy przestrzegać.**
TLP:ZIELONY  Ograniczona publikacja, ograniczona do społeczności.	Podmioty mogą stosować TLP: GREEN, jeśli informacja jest przydatna do podniesienia świadomości wszystkich organizacji uczestniczących. Możliwe jest także udostępnianie tych informacji innym podmiotom w ramach szerszej społeczności lub sektora.	Beneficjenci mogą dzielić się informacjami zawartymi w kategorii TLP: GREEN z partnerami i organizacjami partnerskimi w swoim sektorze lub społeczności. Informacji nie można jednak udostępniać za pośrednictwem publicznie dostępnych kanałów. Informacje z tej kategorii mogą być masowo rozpowszechniane w obrębie danej społeczności. **Informacje zawarte w kategorii TLP: GREEN nie mogą być udostępniane poza społecznością.**
TLP:BIAŁY  Publikacja nie jest w żaden sposób ograniczona.	Jednostki mogą stosować TLP: BIAŁE, jeśli informacje zawierają minimalne lub żadne przewidywalne ryzyko niewłaściwego wykorzystania zgodnie z obowiązującymi zasadami i procedurami ujawniania informacji.	Zgodnie z przepisami i ochroną praw autorskich, **informacje zawarte w kategorii TLP: BIAŁE** mogą być **rozpowszechniane bez ograniczeń.**

"Niepożądane ujawnienie pewnych informacji jest określane w cyberbezpieczeństwie jako naruszenie poufności lub wyciek".[15]

4. Ocena poufności zgodnie z dekretem nr 82/2018 Dz.U. w sprawie środków bezpieczeństwa, incydentów związanych z bezpieczeństwem cybernetycznym, środków reaktywnych, wymogów dotyczących składania wniosków w dziedzinie bezpieczeństwa cybernetycznego i usuwania danych (dekret w sprawie bezpieczeństwa cybernetycznego).[16]

Rozporządzenie w sprawie ochrony cyberprzestrzeni w dużej mierze przyjmuje wprowadzony powyżej Protokół sygnalizacji świetlnej dla skali oceny poufności (zob. załącznik 1 do VoKB).

Poziom	**Opis**	**Przykłady wymogów w zakresie ochrony aktywów**
Niska	Aktywa te są publicznie dostępne lub zostały przeznaczone do publikacji. Naruszenie poufności aktywów nie zagraża uzasadnionym interesom osoby zobowiązanej. W przypadku udostępniania takiego składnika majątku stronom trzecim i stosowania klasyfikacji Traffic Light Protocol (TLP) stosuje się oznaczenie **TLP:WHITE**.	Nie jest wymagana żadna ochrona. Zbycie/usunięcie aktywów na poziomie niskim - zob. załącznik 4.
Średnia	Aktywa te nie są publicznie dostępne i stanowią know-how osoby zobowiązanej, a ochrona tych aktywów nie jest wymagana przez żadne przepisy prawa ani ustalenia umowne. W przypadku udostępniania takiego składnika aktywów stronom trzecim i stosowania klasyfikacji TLP stosuje się głównie oznaczenie TLP**:GREEN** lub TLP:AMBER.	W celu ochrony poufności stosuje się środki kontroli dostępu. Zbycie/usunięcie aktywów na poziomie średnim - patrz Załącznik 4.
High	Aktywa nie są publicznie dostępne, a ich ochrona jest wymagana przez prawo, inne przepisy lub ustalenia umowne (np. tajemnice handlowe, dane osobowe). W przypadku udostępniania takich aktywów stronom trzecim i stosowania klasyfikacji TLP stosuje się w szczególności oznaczenie **TLP:AMBER.**	W celu ochrony poufności stosuje się środki zapewniające kontrolę i rejestrację dostępu. Informacje przekazywane przez sieć łączności są chronione za pomocą środków kryptograficznych. Zbycie/usunięcie aktywów na poziomie wysokim - zob. załącznik 4.
Krytyczne	Aktywa nie są publicznie dostępne i wymagają wyższego poziomu ochrony niż poprzednia kategoria (np. strategiczne tajemnice handlowe, specjalne kategorie danych osobowych). W przypadku udostępniania takiego składnika aktywów stronom trzecim i stosowania klasyfikacji TLP stosuje się w szczególności oznaczenie TLP:RED lub TLP**:AMBER.**	W celu ochrony poufności stosuje się środki zapewniające kontrolę i rejestrację dostępu. Ponadto metody ochrony zapobiegające niewłaściwemu wykorzystaniu zasobów przez administratorów. Transmisja informacji jest chroniona za pomocą środków kryptograficznych. Likwidacja/usunięcie aktywów na poziomie krytycznym - patrz Załącznik 4.

Integralność

Zgodnie ze Słownikiem interpretacyjnym bezpieczeństwa cybernetycznego[17] **integralność jest** definiowana jako "*właściwość dokładności i kompletności*". **Integralność danych** jest definiowana w tym samym słowniku jako *"pewność, że dane nie zostały zmienione". W przenośni odnosi się także do ważności, spójności i dokładności danych, takich jak bazy danych czy systemy plików. Zapewniają to sumy kontrolne, funkcje haszujące, kody samokorygujące, redundancja, rejestrowanie itp. W kryptografii i ogólnie w*

bezpieczeństwie informacji integralność oznacza ważność danych." **Integralność systemu** to *"właściwość polegająca na tym, że system wykonuje swoją zamierzoną funkcję w sposób niezakłócony, bez celowych lub przypadkowych, niezautomatyzowanych manipulacji w systemie".*

Integralność oznacza zatem brak możliwości ingerencji w informacje, dane, systemy komputerowe, ich ustawienia itp. **przez osoby do tego nieuprawnione.**

Jednocześnie integralność stanowi pewnego rodzaju gwarancję integralności systemu, informacji lub danych.

"Niepożądana modyfikacja (zmiana) jest zatem określana w bezpieczeństwie informacji jako naruszenie integralności".[18]

W przypadku naruszenia integralności należy zauważyć, że jeśli dojdzie do niepożądanej zmiany w danych, niepożądana zmiana może w ogóle nie zostać wykryta, a do momentu wykrycia naruszenia integralności może upłynąć znaczna ilość czasu.

Rozporządzenie w sprawie bezpieczeństwa cybernetycznego przedstawia również skalę oceny integralności w załączniku 1.

Poziom	**Opis**	**Przykłady wymogów w zakresie ochrony aktywów**
Niska	Składnik aktywów nie wymaga ochrony integralności. Naruszenie integralności aktywów nie zagraża uzasadnionym interesom dłużnika.	Nie jest wymagana żadna ochrona.
Średnia	Składnik aktywów może wymagać ochrony integralności. Naruszenie integralności składnika aktywów może prowadzić do szkody dla uzasadnionych interesów dłużnika i może mieć mniej poważny wpływ na aktywa podstawowe.	Do ochrony integralności stosuje się standardowe narzędzia (np. ograniczenia dostępu do zapisu).
High	Składnik aktywów wymaga ochrony integralności. Naruszenie integralności aktywów prowadzi do szkody dla uzasadnionych interesów dłużnika i ma znaczący wpływ na aktywa podstawowe.	W celu ochrony integralności stosuje się specjalne środki do śledzenia historii dokonywanych zmian oraz rejestrowania tożsamości osoby dokonującej zmiany. Integralność informacji przesyłanych przez sieci komunikacyjne jest chroniona za pomocą środków kryptograficznych.
Krytyczne	Składnik aktywów wymaga ochrony integralności. Naruszenie integralności prowadzi do bardzo poważnej szkody dla uzasadnionych interesów zobowiązanego, co ma bezpośredni i bardzo poważny wpływ na aktywa podstawowe.	W celu ochrony integralności stosuje się specjalne środki umożliwiające jednoznaczną identyfikację osoby dokonującej zmiany (np. za pomocą technologii podpisu cyfrowego).

Dostępność

Zgodnie z Interpretive Dictionary of Cybersecurity[19] , **dostępność** jest definiowana jako "*właściwość bycia dostępnym i możliwym do wykorzystania na żądanie uprawnionego podmiotu".*

Dostępność można zatem zdefiniować jako gwarancję możliwości dostępu do informacji, danych lub systemu komputerowego w chwili, gdy są one potrzebne. Samodzielny system, który zapewnia integralność i umożliwia dostęp do samego systemu, danych lub informacji, jest bezużyteczny, jeśli nie zapewnia niezawodnego dostępu w razie potrzeby.[20]

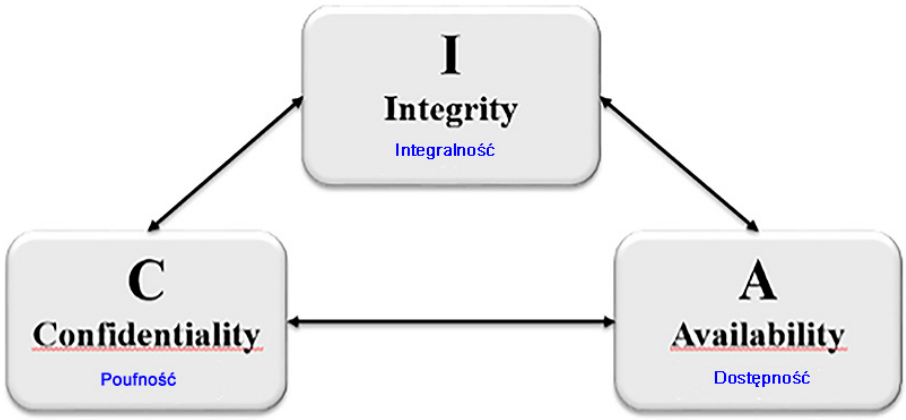
"Zniszczenie pewnych informacji jest określane w bezpieczeństwie informacji jako zakłócenie ich dostępności". [21]

Dekret w sprawie bezpieczeństwa cybernetycznego w załączniku 1 przedstawia również skalę oceny dostępności.

Poziom	**Opis**	**Przykłady wymogów w zakresie ochrony aktywów**
Niski		

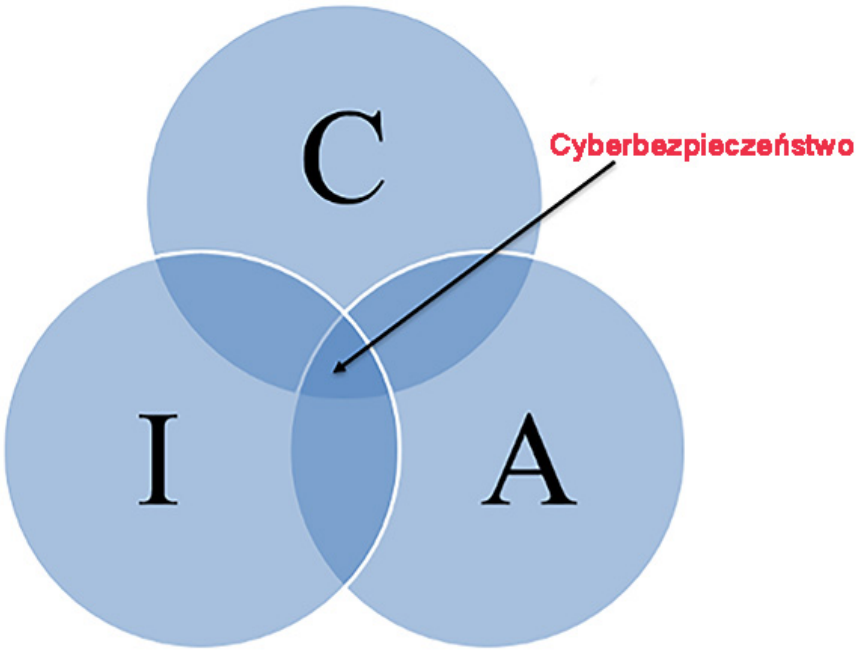
	Zakłócenia w dostępności zasobów nie są istotne, a w przypadku awarii zwykle tolerowany jest dłuższy okres przywracania sprawności (do około 1 tygodnia).	Do ochrony dostępności wystarczą regularne kopie zapasowe.
Średnii	Zakłócenie dostępności zasobu nie powinno trwać dłużej niż jeden dzień roboczy, dłuższa przerwa w dostawie prowadzi do potencjalnego zagrożenia uzasadnionych interesów osoby zobowiązanej.	W celu ochrony dostępności stosuje się powszechnie stosowane metody tworzenia kopii zapasowych i odzyskiwania danych.
Wysoki	Zakłócenia w dostępności zasobu nie powinny przekraczać kilku godzin. Każda awaria musi zostać natychmiast usunięta, ponieważ prowadzi do bezpośredniego zagrożenia uzasadnionych interesów osoby zobowiązanej. Majątek jest uważany za bardzo ważny.	W celu zapewnienia dostępności stosuje się systemy rezerwowe, a przywrócenie usług może wymagać interwencji operatora lub wymiany zasobów technicznych.
Krytyczny	Zakłócenie dostępności środka trwałego jest niedopuszczalne, a nawet krótkotrwała niedostępność (w ciągu kilku minut) prowadzi do poważnego zagrożenia uzasadnionych interesów osoby zobowiązanej. Aktywa są uważane za krytyczne.	Do ochrony dostępności stosuje się systemy zapasowe, a przywracanie usług jest krótkotrwałe i zautomatyzowane.

Triada CIA jest często przedstawiana w formie graficznej, aby lepiej zrozumieć jej poszczególne atrybuty i relacje. Z tego powodu przedstawiono tu typową reprezentację triady CIA. W kolejnej części tego rozdziału triada ta zostanie uzupełniona o elementy (technologia, ludzie, procesy).



Triada CIA

Jeśli spróbujemy zdefiniować przestrzeń bezpieczeństwa cybernetycznego w ramach realizacji triady CIA, to przestrzeń tę można przedstawić jako skrzyżowanie poszczególnych zasad tej triady.



Triada CIA i bezpieczeństwo cybernetyczne

Przeglądanie heksady Parkera [22]

1.1.2 Elementy bezpieczeństwa cybernetycznego

Poniższe trzy elementy lub ich wzajemne oddziaływanie umożliwiają w pewnym stopniu stworzenie lub ustanowienie bezpieczeństwa cybernetycznego. Są to następujące elementy:

- **ludzie**,

- **technologie** i
- **procesy**.

Uważamy, że utopią jest myślenie, że możliwe jest stworzenie absolutnego bezpieczeństwa cybernetycznego lub całkowicie bezpiecznego systemu przy użyciu elementów ICT.

Teoretycznie można by sobie wyobrazić całkowicie odizolowany system komputerowy (wraz ze źródłem zasilania, np. za pomocą agregatu), zamknięty w klatce Faradaya, z jasno określonym kręgiem osób uprawnionych do pracy na tym systemie komputerowym, z zastrzeżeniem, że do tego wyjątkowego środowiska nie można wnosić ani wynosić żadnych nośników (elektronicznych ani innych).

Pojawia się jednak pytanie, czemu miałby służyć taki bezpieczny system i w jaki sposób można by wykorzystać wyniki prac nad tym systemem, czy też jak można by te wyniki wprowadzić w życie, skoro nie jest możliwe wytworzenie wyników prac. Można by wówczas wysunąć kontrargument, że wyniki zostaną opracowane dopiero po zakończeniu projektu, do tego czasu wszystko będzie chronione, a dostęp będzie podlegał wspomnianym wyżej zasadom.

Powstaje jednak pytanie, czy taki sztucznie stworzony i całkowicie odizolowany system jest zabezpieczony przed innymi zagrożeniami, którymi mogą być: brak kopii zapasowych, możliwość fizycznego zniszczenia systemu komputerowego, ujawnienie części informacji przez osoby pracujące z systemem itp.

Każdy system jest tylko tak bezpieczny, jak jego najsłabsze ogniwo (element).

Ludzie

> *"Ludzie często stanowią najsłabsze ogniwo w łańcuchu bezpieczeństwa i są chronicznie odpowiedzialni za awarie systemów bezpieczeństwa"*.
>
> Bruce Schneier[23]

Osoby zajmujące się bezpieczeństwem cybernetycznym mogą być postrzegane jako:

- **twórcy** (**twórców) tego bezpieczeństwa (tj.** zazwyczaj osoby próbującej wyegzekwować i wdrożyć poszczególne elementy bezpieczeństwa cybernetycznego, czy to w odniesieniu do siebie, czy też w odniesieniu do organizacji),
- **beneficjenci przepisów dotyczących bezpieczeństwa cybernetycznego** (tj. ci, którzy zdecydowali się lub są zobowiązani do wdrożenia istniejących przepisów dotyczących bezpieczeństwa cybernetycznego),
- **podmioty, które należy chronić przed atakami cybernetycznymi**,
- **podmioty, które muszą być informowane i szkolone w zakresie przepisów i zasad bezpieczeństwa cybernetycznego**,
- **ryzyko lub zagrożenie w kontekście tworzenia i utrzymywania bezpieczeństwa cybernetycznego**.

Jeśli skupimy się na roli ludzi w budowaniu i utrzymywaniu bezpieczeństwa cybernetycznego, zwłaszcza w kontekście ZoKB, to należy odpowiednio zdefiniować i obsadzić następujące stanowiska:

- komisja ds. bezpieczeństwa cybernetycznego,
- kierownik ds. bezpieczeństwa cybernetycznego,
- architekt ds. bezpieczeństwa cybernetycznego,
- audytor bezpieczeństwa cybernetycznego,
- zespół ds. cyberbezpieczeństwa,
- poręczyciel,
  - aktywa podstawowe,
  - aktywa wspierające,
- powiernik rzeczowy,
- administrator techniczny,
- operator (czasami określany również jako dostawca),
- administrator,
- użytkownik.

Kluczowym elementem każdego systemu bezpieczeństwa są ludzie. W przypadku bezpieczeństwa cybernetycznego ich rola jest jeszcze ważniejsza, a ludzie są zazwyczaj najsłabszym elementem i najczęstszym celem ataków.

Jest kilka powodów, które skłaniają nas do tego stwierdzenia.

Pierwszym z nich jest stosunkowo krótki czas, w którym faktycznie korzystamy z systemów komputerowych. Większość użytkowników zaczęła korzystać z komputerów dopiero po roku 1990, masowo zaczęliśmy łączyć się z Internetem około 1995 roku, a "inteligentne" telefony komórkowe używamy od około 2007 roku. Jednak z wielu portali społecznościowych, które obecnie uważamy za niezbędne i bez których nie wyobrażamy sobie życia, nie korzystamy od ponad 10 lat.

Drugi powód to ogromna dynamika rozwoju sprzętu, a zwłaszcza oprogramowania, która jest nieodłącznie związana z naszą interakcją w świecie cyfrowym. To właśnie dynamizm rozwoju oprogramowania sprawia, że wielu użytkowników nie analizuje szczegółowo kwestii bezpieczeństwa, które są nieuchronnie związane z użytkowaniem oprogramowania.

Trzecim i ostatnim powodem jest fakt, że życie bez technologii informacyjnych i komunikacyjnych jest dla naszego społeczeństwa nie do pomyślenia lub wręcz niemożliwe. Technologie informacyjno-komunikacyjne i związane z nimi aplikacje tworzą cyfrowe awatary nas samych, zawierające jednak znacznie więcej informacji, niż jesteśmy w stanie zapamiętać lub zachować. Wiedzą o tym nie tylko producenci sprzętu i oprogramowania, ale także osoby atakujące, które właśnie z tego powodu obierają sobie za cel ludzi w cyberprzestrzeni.

"Amatorzy hakują systemy, profesjonaliści hakują ludzi".

Bruce Schneier[24]

Naszym zdaniem istotne jest, aby osoby korzystające z technologii informacyjno-komunikacyjnych i decydujące się na interakcje w cyberprzestrzeni mogły:

- **zrozumieć** przynajmniej **podstawowe zasady i reguły mające zastosowanie do bezpieczeństwa** cybernetycznego,
- **rozumieć** przynajmniej **podstawowe funkcje systemów komputerowych** (np. komputera, laptopa, telefonu komórkowego, smart TV itp.), których **używają** do tej interakcji,
- **przeanalizować aplikacje, których używają** do tej interakcji, **a** jeśli nie odpowiadają im te aplikacje lub ich warunki, nie korzystać z nich,
- **wykształcić się w dziedzinie** cyberbezpieczeństwa.

Dlatego, aby ułatwić realizację przynajmniej ostatniego punktu z powyższej listy, postanowiliśmy stworzyć tę publikację i podsumować przynajmniej częściową wiedzę, która może być wykorzystana zarówno przez laików, jak i pracowników IT, którzy postanowili zwrócić większą uwagę na cyberbezpieczeństwo.

Technologia

"Jeśli myślisz, że technologia może rozwiązać Twoje problemy z bezpieczeństwem, to znaczy, że nie rozumiesz problemów i nie rozumiesz technologii".

Bruce Schneier[25]

Technologia jest zazwyczaj środkiem umożliwiającym użytkownikom łączenie się z Internetem, sieciami społecznościowymi i innymi aplikacjami. Jest to narzędzie, które wykorzystuje różne pakiety biurowe do tworzenia dokumentów, wysyłania wiadomości e-mail, oglądania filmów itp. Zwykle zwykły użytkownik postrzega technologie końcowe (komputer, tablet, telefon komórkowy itp.), z których sam korzysta, i wchodzi z nimi w interakcje, natomiast zazwyczaj nie interesują go inne warstwy technologiczne, które są niezbędne do jego aktywności w cyberprzestrzeni.

W przypadku organizacji technologie stanowią pełną gamę urządzeń, począwszy od technologii skierowanych do użytkownika (komputery stacjonarne, urządzenia mobilne itp.), poprzez całą infrastrukturę sieciową (sieć LAN, elementy aktywne, elementy Wi-Fi itp.) i usługi (serwery, aplikacje itp.), aż po elementy służące do zapewnienia bezpieczeństwa zarówno na zewnątrz (zapora sieciowa[26] , systemy IDS/IPS[27] , honeypot[28] itp.), jak i wewnątrz infrastruktury (elementy uwierzytelniania i autoryzacji, monitorowania, analizy itp.)

W ramach budowania i utrzymywania bezpieczeństwa cybernetycznego należy przeanalizować istniejące zasoby i na podstawie tej analizy w razie potrzeby uzupełnić lub zmodyfikować istniejące systemy. Jeśli chodzi o technologię, to w zależności od specyfiki danej organizacji, jej integralną częścią powinny być następujące elementy:

- systemy wykrywania - systemy wykrywania włamań (**IDS**)/systemy zapobiegania włamaniom (**IPS**),
- centralne zarządzanie użytkownikami i rolami,
- scentralizowane zarządzanie klasyfikacją informacji,
- ochrona przed złośliwym kodem (zapora aplikacji, rozwiązania antywirusowe, antyspamowe i inne),
- technologia rejestrowania działań poszczególnych elementów ICT, administratorów i użytkowników (**system dzienników)**,
- systemy kopii zapasowych aktywnych i offline; kopie zapasowe ważnych serwerów, aplikacji i baz danych (**system odzyskiwania danych)**,
- zarządzanie bezpieczeństwem sieci (VLAN, DMZ, firewall itp.).

Technologia jest zazwyczaj tym elementem cyberbezpieczeństwa, na którym jako użytkownicy lub organizacje nie oszczędzamy. Jesteśmy skłonni zapłacić znaczną sumę pieniędzy za technologię, ponieważ "potrzebujemy najnowszego telefonu" lub z prawdziwego i ważnego powodu, jakim jest przestarzałość i brak wsparcia (aktualizacji) danego systemu komputerowego.

Dlatego w celu zapewnienia bezpieczeństwa cyberprzestrzeni konieczne jest utrzymywanie technologii w takim stanie, aby były one w stanie reagować na zmiany związane z rozwojem technologii informacyjno-komunikacyjnych. W szczególności należy dbać o aktualność i bezpieczeństwo technologii (zarówno sprzętu, jak i oprogramowania).

Choć technologia jest z pewnością ważnym elementem procesu tworzenia i utrzymywania bezpieczeństwa cybernetycznego, to naszym zdaniem jest to element najmniej ważny. Znacznie ważniejszymi elementami bezpieczeństwa cybernetycznego są odpowiednio ustalone procesy oraz ludzie, którzy potrafią je stosować lub modyfikować w praktyce i przestrzegać wcześniej ustalonych zasad.

Procesy

> *"Mantra każdego dobrego inżyniera ds.* ***bezpieczeństwa*** *brzmi: '****Bezpieczeństwo to nie produkt, ale proces****'. To coś więcej niż zaprojektowanie silnej kryptografii w systemie; to zaprojektowanie całego systemu w taki sposób, aby wszystkie środki bezpieczeństwa, w tym kryptografia, działały razem".*
>
> Bruce Schneier[29]

Procesy to działania, które należy podjąć, aby ludzie mogli korzystać z technologii i związanych z nią usług.

Z punktu widzenia upływu czasu możliwe jest śledzenie następujących procesów:

- zarządzanie aktywami i ryzykiem
  - definiowanie i kategoryzowanie aktywów,
  - analiza i kategoryzacja ryzyka,
- wdrażanie technologii informacyjno-komunikacyjnych i ich zastosowań,
- zarządzanie użytkownikami i rolami,
- autoryzacja i uwierzytelnianie,
- utrzymanie (aktualizacje) systemów i usług,
- testowanie bezpieczeństwa poszczególnych systemów i usług komputerowych,
- analiza działań naprawczych,
- wdrożenie środków naprawczych,
- audyt bezpieczeństwa cybernetycznego,
- wykrywanie anomalii lub ataków cybernetycznych,
- reagowanie na ataki cybernetyczne i inne incydenty,
- procesy zapewniające ciągłość działania,
- szkolenia i ćwiczenia itp.

Przedstawiona powyżej lista poszczególnych procesów związanych z tworzeniem i utrzymywaniem bezpieczeństwa cybernetycznego nie jest w żadnym wypadku wyczerpująca, a przedstawione procesy można uogólnić. Poszczególne procesy są wdrażane w całym cyklu życia TIK, informacji, danych i użytkownika. [30]

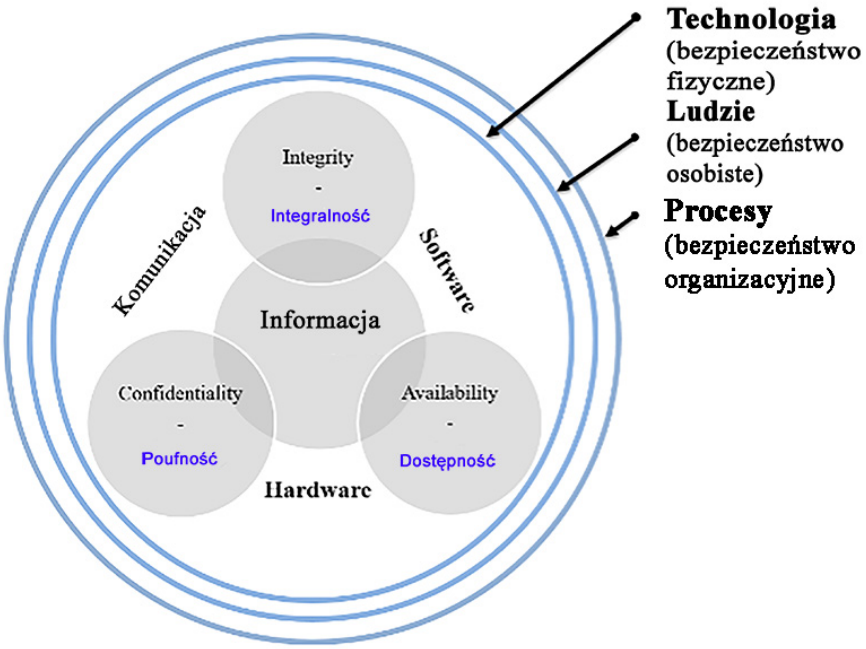
Samo ustanowienie procesów, ich ciągłe utrzymywanie i modyfikowanie jest najtrudniejszą częścią budowania bezpieczeństwa cybernetycznego. Jednocześnie działalność ta stawia najwyższe wymagania administratorowi poszczególnych systemów.

Jeśli organizacja zdecyduje się na wdrożenie zasad bezpieczeństwa cybernetycznego, to oczywiście wskazane jest aktualizowanie zarówno sprzętu, jak i oprogramowania, przestrzeganie ustalonych zasad dostępu do poszczególnych systemów itp.

Jeśli to możliwe, zaleca się również przeprowadzanie w organizacji symulacji typowych cyberataków (np. phishingu, naruszenia służbowej poczty elektronicznej itp.

Testy penetracyjne pozwalają także na znalezienie błędów w już skonfigurowanych procesach.

Jednak tworząc i ustalając zasady bezpieczeństwa cybernetycznego, organizacja powinna przede wszystkim skupić się na zasobach ludzkich i ich edukacji.



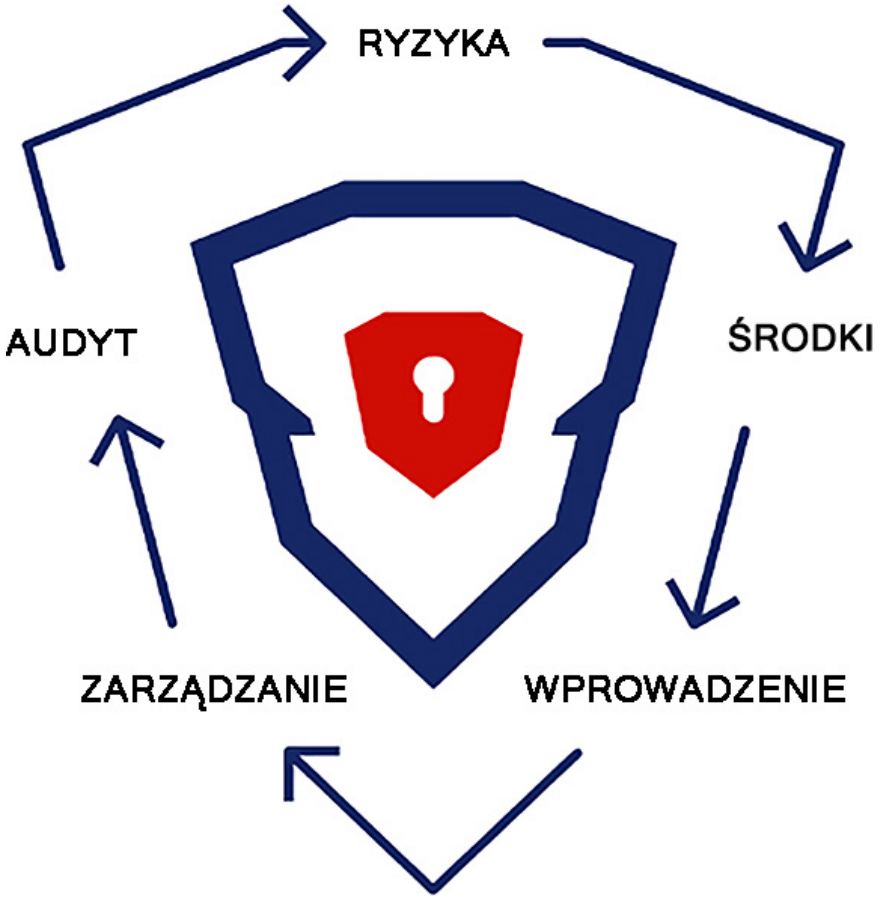
Triada CIA, obejmująca technologię, ludzi i procesy[31]

1.1.3 Cykl życia bezpieczeństwa cybernetycznego

Z perspektywy upływu czasu wdrożenie bezpieczeństwa cybernetycznego wymaga zastosowania lub modyfikacji zarówno triady CIA, jak i podelementów bezpieczeństwa cybernetycznego w całym cyklu ich życia. W szczególności zapobieganie, wykrywanie i reagowanie na ataki. [32]

Bardzo często cykl życia cyberbezpieczeństwa jest przedstawiany za pomocą różnych diagramów. Dla jasności, oto niektóre z nich.

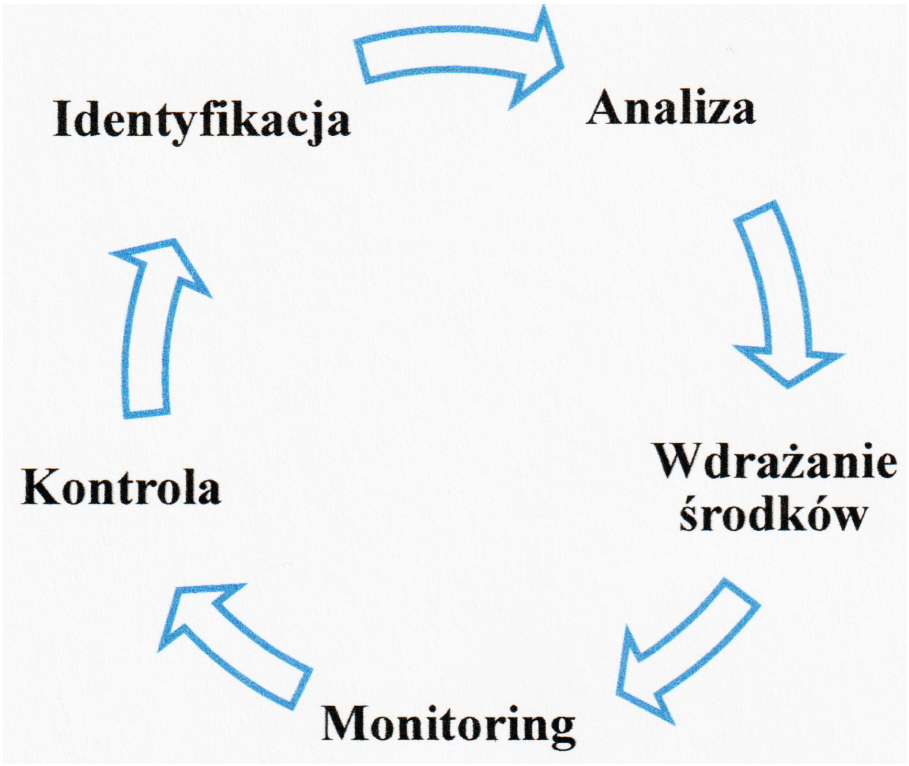
Uproszczony widok cyklu życia bezpieczeństwa cybernetycznego



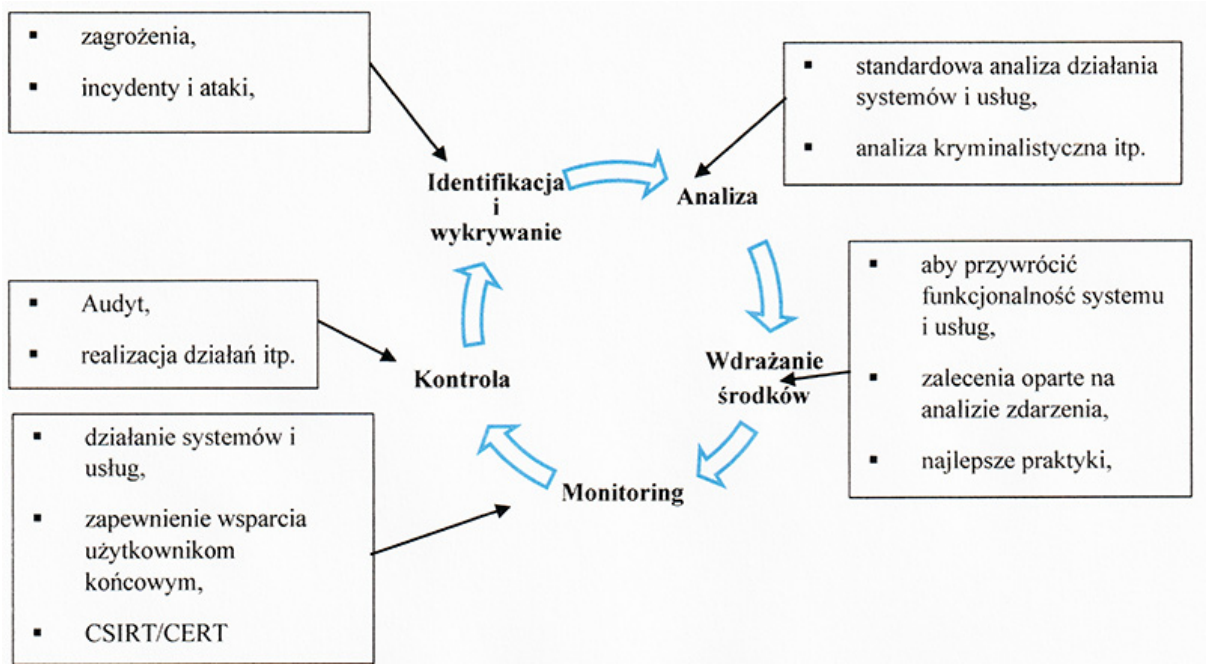
Cykl życia bezpieczeństwa cybernetycznego według kybez.cz[33]

W dziedzinie bezpieczeństwa cybernetycznego nie ma "punktu krytycznego", w którym można by powiedzieć: "Udało się*! Jesteśmy chronieni przed atakami i zagrożeniami cybernetycznymi. Jesteśmy bezpieczni w cyberprzestrzeni".*

Budowanie i utrzymywanie bezpieczeństwa cybernetycznego można porównać do niekończącej się analizy ryzyka, ale z zastrzeżeniem, że ta rutynowa analiza musi być uzupełniona o inne procesy wspierające, które mogą pomóc w zwiększeniu bezpieczeństwa cybernetycznego w organizacji.



Analiza ryzyka



Cykl życia bezpieczeństwa cybernetycznego

Rzeczywiste odwzorowanie cyklu życia cyberbezpieczeństwa może być znacznie bardziej złożone.[34]

Przykład rozwiązania z zakresu bezpieczeństwa cybernetycznego

Ewolucja bezpieczeństwa cybernetycznego

Na zakończenie tego podrozdziału można zadać proste pytanie: *"Dlaczego ja (jako osoba fizyczna) lub organizacja mam w ogóle zawracać sobie głowę bezpieczeństwem cybernetycznym?"*.

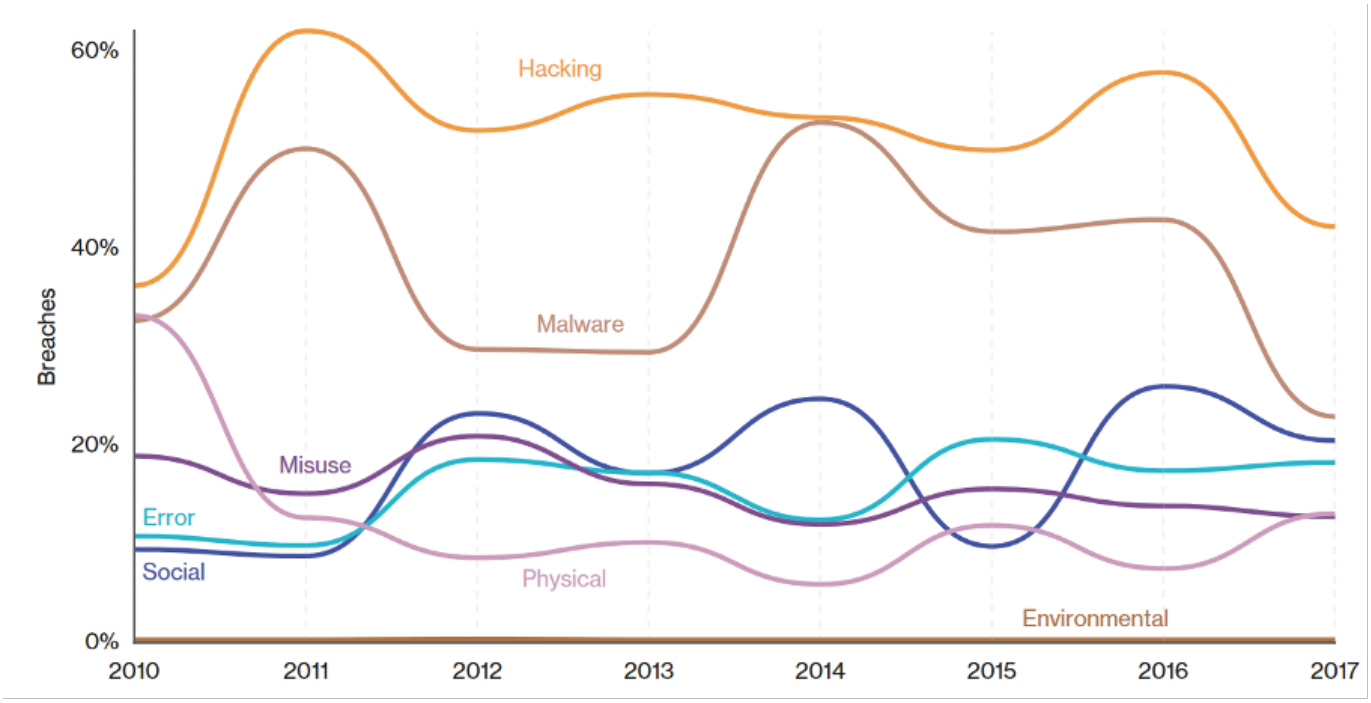
Odpowiedź nie będzie aż tak skomplikowana, choć konieczne będzie przełamanie często zakorzenionego mitu, że ktoś inny - czy to duże organizacje, takie jak Microsoft, Google, Apple, czy dostawcy usług w chmurze, łączności itp. już rozwiązał za mnie problem cyberbezpieczeństwa.

Choć prawdą jest, że organizacje te wdrożyły i stosują częściowe elementy cyberbezpieczeństwa, to jednak cyberbezpieczeństwo, jak każde inne zabezpieczenie, zawsze zaczyna się i kończy na konkretnej osobie lub organizacji, która chce się zabezpieczyć, i zawsze ma na uwadze specyfikę tej osoby lub organizacji.

Raport Data Breach Investigations Report[35] , w którym przeanalizowano przypadki naruszenia bezpieczeństwa prowadzące do utraty danych, za rok 2017 przedstawia następujące fakty:

- napastnik był
  - **osoba spoza organizacji - 73%.**
  - osoba w organizacji - 28%.
  - **zorganizowana grupa przestępcza - 50%**
- został wykorzystany do ataków:
  - **hakerstwo - 48%.**
  - **złośliwe oprogramowanie - 30%**
    - **49% złośliwego oprogramowania** zostało rozesłane, a następnie zainstalowane przez atakującego **za pośrednictwem poczty elektronicznej**
  - **inżynieria społeczna - 43%**
  - napaść fizyczna - 8%[36]
- organizacje będące ofiarami:
  - opieka zdrowotna - 24 %.
  - sektor publiczny (zazwyczaj władze państwowe i lokalne itp.) - 14%.
- motyw ataku:
  - **wzbogacanie - 76%**
  - zdobywanie danych i informacji (szpiegostwo) - 13%.
- **68% ataków zostało wykrytych po kilku miesiącach lub dłużej**

Poniższy wykres przedstawia rozwój poszczególnych ataków od 2010 r. do końca 2017 r.



Rodzaje ataków stosowanych w celu naruszenia bezpieczeństwa[37]

Według raportu National Cyber and Information Security Authority[38] , *"**w 2018** r. **można spodziewać się dalszego wzrostu cyberzagrożeń, zwłaszcza** większej liczby ataków phishingowych nowej generacji, ataków na targowiska, portfele i giełdy kryptowalut, bezplikowych wariantów oprogramowania ransomware, wykorzystania sztucznej inteligencji do cyberataków, ataków na dane w rozwiązaniach Cloud, ataków na IoT, systemy przemysłowe itp. **Oczekuje się, że wzrośnie udział podmiotów państwowych lub sponsorowanych przez państwo w atakach cybernetycznych, a masowe wycieki danych osobowych, haseł i danych dostępowych będą się utrzymywać.** Dlatego tak istotne jest budowanie bezpieczeństwa cybernetycznego systemów teleinformatycznych krytycznych dla funkcjonowania państwa i jego infrastruktury krytycznej."*[39]

Obszar cyberbezpieczeństwa będzie jednym z najważniejszych obszarów w przyszłości, ponieważ można założyć, że wykorzystanie technologii informacyjno-komunikacyjnych i usług związanych z tymi technologiami nie ulegnie zmniejszeniu. Bezpieczeństwo cybernetyczne ma pomóc w identyfikacji słabych punktów w konfiguracji tych systemów i usług.

"Bezpieczeństwo cybernetyczne pomaga również w identyfikacji, ocenie i przeciwdziałaniu zagrożeniom w cyberprzestrzeni, ograniczaniu ryzyka cybernetycznego oraz eliminowaniu skutków cyberataków, przestępstw informacyjnych, cyberterroryzmu i szpiegostwa cybernetycznego w zakresie wzmacniania poufności, integralności i dostępności danych, systemów i innych elementów infrastruktury teleinformatycznej".

Głównym celem bezpieczeństwa cybernetycznego jest ochrona środowiska umożliwiającego realizację praw człowieka do informacji." [40]

---

[1] Zob. np. HSU, D. Frank i D. MARINUCCI (eds.). *Postępy w dziedzinie bezpieczeństwa cybernetycznego: technologia, operacje i doświadczenia*. Nowy Jork: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. s 41.

KADLECOVÁ, Lucie. *Pojęciowe i teoretyczne aspekty bezpieczeństwa cybernetycznego.* [online]. [cytowany 2018-07-21]. Dostępny pod adresem: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

[2] Więcej informacji na ten temat można znaleźć np. w książce *Parkerian Hexad*. [online]. [cyt. 2016 Aug. 20]. Dostępny pod adresem: https://vputhuseeri.wordpress.com/2009/08/16/149/

[3] Artykuł 1 lit. b) Konwencji o cyberprzestępczości. *Konwencja o cyberprzestępczości.* [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

[4] POŽÁR, Josef. *Bezpieczeństwo informacji.* Pilzno: Aleš Čeněk, 2005, s. 25.

[5] Więcej szczegółów w: WIENER, Norbert. *Cybernetyka: czyli sterowanie i komunikacja w organizmach żywych i maszynach.* Praga: Państwowe Wydawnictwo Literatury Technicznej, 1960. 148 s., s. 32 i nast.

[6] ŠÁMAL, Pavel et al. *Kodeks karny II. §§ 140-421. Komentarz.* 2. 2. edycja. Praga: C. H. Beck, 2012, s. 2308.

[7] POŽÁR, Josef. *Bezpieczeństwo informacji.* Pilzno: Aleš Čeněk, 2005, s. 25.

[8] Więcej szczegółów w: KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016, s. 57 i nast.

[9] EVANS, DONALD, PHILIP, BOND i ARDEN BEMET. *Standardy kategoryzacji bezpieczeństwa informacji i systemów informatycznych na szczeblu federalnym (Standards for Security Categorization of Federal Information and Information Systems).* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

ANDRESS, Jason. *Podstawy bezpieczeństwa informacji. Wydanie* drugie. Syngress. 9780128007440

HENDERSON, Anthony. *Triada CIA: poufność, integralność, dostępność.* [online]. [cyt. 2018 Jan 13]. Dostępny pod adresem: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[10] Więcej informacji można znaleźć na stronie https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/.

[11] Por. dalej: ŠULC, Vladimír. *Bezpieczeństwo cybernetyczne.* Pilzno: Aleš Čeněk, 2018. s. 20 i nast.

[12] Obecnie Centrum Ochrony Infrastruktury Kraju - CPNI

[13] Więcej szczegółów można znaleźć np. w dokumencie *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cyt. 2018 Jan 13]. Dostępny pod adresem: https://www.us-cert.gov/tlp

[14] *Definicje i zastosowanie protokołu sygnalizacji świetlnej (TLP).* [online]. [cyt. 2018 Jan 13]. Dostępny pod adresem: https://www.us-cert.gov/tlp

[15] ŠULC, Vladimír. *Cyberbezpieczeństwo.* Pilzno: Aleš Čeněk, 2018. s. 19.

[16] Zwane dalej Rozporządzeniem o bezpieczeństwie cybernetycznym lub **VoKB**.

[17] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015, s. 58 [online]. [cytowany 2018-07-10]. Dostępny pod adresem: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

[18] ŠULC, Vladimír. *Cyberbezpieczeństwo.* Pilzno: Aleš Čeněk, 2018. s. 22.

[19] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015, s. 43 [online]. [cytowany 2018-07-10]. Dostępny pod adresem: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

[20] Zob. np. EVANS, DONALD, PHILIP, BOND i ARDEN BEMET. *Standardy kategoryzacji bezpieczeństwa informacji i systemów informatycznych na szczeblu federalnym (Standards for Security Categorization of Federal Information and Information Systems)*. National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

[21] ŠULC, Vladimír. *Cyberbezpieczeństwo.* Pilzno: Aleš Čeněk, 2018. s. 24.

[22] *Heksada parkerowska*. [online]. [cyt. 2016 Aug 20]. Dostępny pod adresem: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[23] SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570039 ;

[24] SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570035

[25] SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570040

[26] Firewall to system zawierający reguły regulujące przepływ danych w technologiach sieciowych.

[27] **IPS** (Intrusion Prevention System - system zapobiegania włamaniom) - urządzenie monitorujące niepożądaną (złośliwą) aktywność sieciową i/lub aktywność systemu komputerowego. Zwany dalej **IPS.**

IDS (Intrusion Detection System - system wykrywania włamań) to system przeznaczony do wykrywania nietypowych działań, które mogą potencjalnie prowadzić do naruszenia bezpieczeństwa sieci komputerowej, systemów komputerowych, aplikacji itp. Zwany dalej systemem **IDS.**

[28] Honeypot to system, którego zadaniem jest wykrywanie złośliwego oprogramowania lub innych niepożądanych działań, które są następnie analizowane w tym sztucznie stworzonym środowisku.

[29] SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570047

[30] Termin użytkownik jest tu używany w odniesieniu do osoby fizycznej, która jest upoważniona do korzystania z elementów, systemów i aplikacji TIK. Z tego punktu widzenia za użytkownika uważa się zarówno osobę z uprawnieniami administratora, jak i użytkownika końcowego.

[31] Wykres został oparty na wykresie opublikowanym w *metodologii triady CIA*. [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

[32] Więcej informacji na ten temat można znaleźć w artykule SVOBODA, Ivan. *Rozwiązania w zakresie cyberbezpieczeństwa.* Wykład w Akademii CRIF. (23. 9. 2014)

[33] *Podstawowe pojęcia.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://www.kybez.cz/bezpecnost/pojmoslovi

[34] *Pełny zakres usług CGI Cyber Security* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://mss.cgi.com/service-portfolio

[35] *2018 Data Breach Investigation Report. 11th Edition.* [Online]. [cytowany 2018-07-28]. Dostępny pod adresem: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

[36] Poszczególne ataki zwykle wykorzystują kombinację technik i narzędzi.

[37] *2018 Data Breach Investigation Report. 11th Edition.* [Online]. [cytowany 2018-07-28]. Dostępny pod adresem: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf s. 7.

[38] zwana dalej **NUCIB**

[39] *2017 State of Cybersecurity Report* [online]. [cyt. 2018 Jun 29]. Dostępny pod adresem: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[40] *Narodowa Strategia Cyberbezpieczeństwa Republiki Czeskiej na lata 2015-2020* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

1.3. Ryzyko, aktywa, podatność na zagrożenia

1.3.1 Ryzyko

Przed zdefiniowaniem pojęć: zagrożenie, zdarzenie, incydent i atak, uważamy za konieczne zdefiniowanie przynajmniej pojęcia ryzyka, które jest bezpośrednio związane z pojęciami zdefiniowanymi w dalszej części.

Słownik interpretacyjny bezpieczeństwa cybernetycznego definiuje ryzyko jako: *"(1) Niebezpieczeństwo, możliwość wystąpienia szkody, straty, niepowodzenia. (2) Wpływ niepewności na osiąganie celów. (3) Możliwość, że zagrożenie wykorzysta słabość zasobu lub grupy zasobów i wyrządzi szkodę organizacji.*[1]

Ryzyko można również zdefiniować jako **potencjalne zagrożenie, które może się urzeczywistnić i wykorzystać słabe** punkty **danego zasobu.** Zgodnie z art. 4 ust. 9 NIS **ryzyko** definiuje się jako *"**wszelkie możliwe do określenia okoliczności lub zdarzenia, które mogłyby mieć negatywny wpływ na bezpieczeństwo sieci i systemów informatycznych.*** W cyberprzestrzeni na zagrożenia narażeni są użytkownicy, systemy i aplikacje komputerowe, które z nich korzystają, oraz inne elementy TIK.

Termin **ryzyko wyraża prawdopodobieństwo wystąpienia niepożądanego zdarzenia**. Stopień prawdopodobieństwa wystąpienia tego zdarzenia określa się za pomocą analizy ryzyka. Minimalne wartości standardowe dla metod identyfikacji, analizy, oceny i leczenia ryzyka są określone w normie EN 31010.

Valášek i in.[3] stwierdzają, że ocena ryzyka opiera się zwykle na trzech podstawowych pytaniach:

- **Jakie złe (niepożądane) rzeczy mogą się wydarzyć? Co może się nie udać?**
- **Jaka jest możliwość/prawdopodobieństwo, że tak się stanie?**
- **Jak poważne (intensywność, wielkość itp.) mogą być skutki (wpływy, konsekwencje)?**

Jednak, zdaniem Valáška, pytania te stanowią jedynie podstawowe ramy, w których można określić własne ryzyko. Oprócz tych trzech pytań zadawane są następujące pytania uzupełniające, które dotyczą ważnych czynników wpływających na charakterystykę ryzyka:

Czynnik	**Pytanie**
Czas	"Jak długo będziemy zagrożeni?".
Zmienność	"Ponieważ szacunki dotyczące wpływu zdarzenia objętego ryzykiem zbliżają się Rzeczywistość?"
Złożoność	"Czy trudno jest zrozumieć ryzyko?".
Wzajemne relacje	"Jak daleko sięgają różne rodzaje ryzyka lub ryzyka czynniki?"
Wpływy	"Czy można zarządzać ryzykiem?".
Cykl życia	"Jak ryzyko zmienia się w czasie?".
Efektywność kosztowa	"Jak kosztowne są środki ryzyka?".

Dla każdego ryzyka obliczany jest poziom istotności ryzyka, który można wyrazić w następujący sposób:

Znaczenie ryzyka = **Wpływ ryzyka** * **Prawdopodobieństwo** wystąpienia ryzyka

"Wynikiem analizy ryzyka jest określenie znaczenia zdefiniowanego ryzyka. Każde ryzyko, biorąc pod uwagę zakres wymagań, ma różne skutki, które może wywołać. Wpływ lub konsekwencje ryzyka ocenia się w pięciopunktowej skali w następujący sposób:

Ciało	**Prawdopodobieństwo wystąpienia ryzyka**	**Opis zdarzenia**
5	SURE	Ryzyko występuje prawie zawsze lub z prawdopodobieństwem 90-100%.
4	TRUE	Istnieje prawdopodobieństwo wystąpienia ryzyka
3	MOŻLIWE	Ryzyko może czasami wystąpić (np. w określonych warunkach).

2	NIEZWYKŁY	Ryzyko to może czasami wystąpić, ale jest mało prawdopodobne.
1	WYKLUCZONE	Ryzyko to występuje tylko w wyjątkowych przypadkach i w określonych warunkach.

Oprócz wpływu, poszczególne rodzaje ryzyka mogą, ale nie muszą wystąpić. W związku z tym określa się prawdopodobieństwo wystąpienia ryzyka. Również w tym przypadku częstość występowania oceniana jest na pięciopunktowej skali w następujący sposób: [4]

Ciało	**Wpływ ryzyka**	**Opis wpływu**
5	CRISIS	Sytuacja ta poważnie ograniczy lub zakończy działalność firmy (np. bankructwo, utrata życia itp.).
4	ZNACZNE	Sytuacja ta ma bardzo niebezpieczny wpływ na wewnętrzne i zewnętrzne funkcjonowanie firmy (np. znaczne straty finansowe - 100% przekroczenie budżetu, straty czasu, spory sądowe, urazy itp.)
3	CENTRALNA	Sytuacja ta będzie miała niebezpieczny wpływ na wewnętrzne i zewnętrzne funkcjonowanie firmy (np. zostaną poniesione straty, ale firma będzie w stanie kontynuować działalność, wystąpią straty finansowe sięgające 30% budżetu itp.)
2	NIEZNANA	Sytuacja ta ogranicza wewnętrzne funkcjonowanie firmy (np. występują opóźnienia czasowe do maksymalnie 30 dni).
1	WYMAGANE	Chociaż sytuacja ta ogranicza działalność firmy, nie powoduje strat większych niż 5%.

Oprócz powyższego, ocena ryzyka musi uwzględniać także inne okoliczności, takie jak:

§ nieodłączny charakter (rodzaj) ryzyka lub zagrożenia,

§ podatność aktywów na zagrożenia,

§ prawdopodobieństwo przekształcenia się ryzyka w zdarzenie lub incydent związane z bezpieczeństwem.

Analiza ryzyka jest bardzo trudna i wymaga znajomości aktywów, zagrożeń, a przede wszystkim doświadczenia w tej dziedzinie. Na podstawie analizy ryzyka można określić środki minimalizujące lub całkowicie eliminujące ryzyko.

1.3.2 Aktywa

Aktywa to wszystko, co ma wartość dla danej osoby, organizacji lub państwa.

Z punktu widzenia prawa cywilnego majątek może być **rzeczą materialną** (budynek, system komputerowy, sieć, energia, towary itp.) **lub niematerialną** (informacje, wiedza, dane, programy itp.).

Zasobem może być jednak również **właściwość** (np. dostępność i funkcjonalność systemu i danych itp.) lub **reputacja** itp. Z punktu widzenia bezpieczeństwa cybernetycznego zasobem są również **ludzie** (użytkownicy, administratorzy itp.) oraz ich wiedza i doświadczenie.

Zgodnie z sekcją 2(f) i (g) VoKB, **aktywa** dzielą się na **pomocnicze** i **podstawowe.**

Zasoby pomocnicze to zasoby techniczne, pracownicy i wykonawcy zaangażowani w eksploatację, rozwój, zarządzanie lub bezpieczeństwo systemu teleinformatycznego.

Podstawowym składnikiem aktywów jest informacja lub usługa przetwarzana lub dostarczana przez system teleinformatyczny.

1.3.3 Podatność na zagrożenia

Podatność na ataki to słaby punkt zasobu, oprogramowania lub zabezpieczeń, który jest wykorzystywany przez jedno lub więcej zagrożeń.

Podatność, podobnie jak zagrożenie, może być spowodowana różnymi czynnikami, na które składają się działania ludzkie, awarie techniczne i ewentualnie siła wyższa.

W dziedzinie cyberbezpieczeństwa podatności dzieli się na:

- **znane** (opublikowane) **luki w zabezpieczeniach**

    - załatane (**naprawione**) - typowym przypadkiem są luki w oprogramowaniu, dla których producent wydał już aktualizację
    - **niezałatane** (nieleczone) - podmiot, u którego wystąpiła luka (producent, administrator itp.) wie o niej, ale nie zapewnił jej usunięcia

- **nieznane podatności**
    - ukryte
    - nieodkryte

W przypadku nieznanych podatności istotne jest to, czy zostały one odkryte przez atakującego, producenta, analityka bezpieczeństwa, testera penetracyjnego czy użytkownika. Równie ważna jest motywacja osoby, która odkrywa słabe punkty.

Luki w zabezpieczeniach to potencjalne zagrożenia dla bezpieczeństwa. Luki w zabezpieczeniach można do pewnego stopnia wyeliminować poprzez konsekwentne aktualizowanie i wprowadzanie poprawek do całego oprogramowania.[5]

W rozporządzeniu w sprawie bezpieczeństwa cybernetycznego w załączniku 3 wymieniono przykładowo niektóre z tych słabych punktów. **Zgodnie z** tym **dekretem, słabe punkty to:**

1. Niewłaściwa konserwacja systemu informacyjno-komunikacyjnego,

2. przestarzałość systemu informacyjno-komunikacyjnego,

3. Niewystarczająca ochrona obwodu zewnętrznego,

4. Brak świadomości bezpieczeństwa wśród użytkowników i administratorów,

5. nieodpowiednie ustawienia uprawnień dostępu,

6. Nieodpowiednie procedury identyfikacji i wykrywania negatywnych zjawisk bezpieczeństwa, zdarzeń związanych z bezpieczeństwem cybernetycznym i incydentów bezpieczeństwa cybernetycznego,

7. Nieodpowiednie monitorowanie użytkowników i administratorów oraz niewykrycie niewłaściwego lub problematycznego zachowania,

8. niewystarczające określenie zasad bezpieczeństwa, niedokładne lub niejednoznaczne określenie praw i obowiązków użytkowników, administratorów i ról bezpieczeństwa,

9. Niewystarczająca ochrona aktywów,

10. nieodpowiednia architektura zabezpieczeń,

11. Niewystarczająca niezależna kontrola,

12. Niewykrycie we właściwym czasie niewłaściwego postępowania pracowników.

---

[1] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015. s. 99. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[2] MATUROVÁ, Jana i Miroslav VALTA. *Zapobieganie ryzyku - kontrole stanu wyposażenia technicznego.* [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

[3] VALÁŠEK, Jarmil, František KOVÁŘÍK i in. *Zarządzanie kryzysowe w pozamilitarnych sytuacjach kryzysowych*. Praga: Ministerstwo Spraw Wewnętrznych – Dyrekcja Generalna Straży Pożarnej i Ratownictwa Republiki Czeskiej, 2008 [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx

ISBN 978-80-86640-93-8 s. 73

[4] *Analiza ryzyka [*online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

[5] Por. JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny cyberbezpieczeństwa*. [online]. 3rd updated ed. Praga: AFCEA, 2015. s. 29. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

1.4. Zagrożenia, zdarzenia, incydenty i ataki cybernetyczne

Zajmowanie się zagadnieniem "negatywnych zjawisk w cyberprzestrzeni" może być nieco problematyczne, ponieważ w literaturze fachowej oraz w normach prawnych często używa się różnych synonimów na określenie danego negatywnego zjawiska, które mają wyrażać to samo.

Powodem niespójności terminologicznej jest, ponownie, stosunkowo krótki okres, w którym mamy do czynienia z zagrożeniami, atakami i incydentami cybernetycznymi, a także nie zawsze identyczne tłumaczenie z języka angielskiego, który jest używany głównie w informatyce.

1.3.1 Cyberzagrożenie

Zagrożenie można najprościej zdefiniować jako coś, co jest w stanie zakłócić normalny lub uporządkowany stan rzeczy oraz naruszyć prawa innych podmiotów. Jest to działanie negatywne, które może, ale nie musi zostać zakończone. W przypadku rzeczywistej definicji wystarczy, że możliwość wystąpienia negatywnego stanu rzeczy jest bliska i realna.

Zgodnie z definicją Ministerstwa Spraw Wewnętrznych Republiki Czeskiej za zagrożenie uważa się "*każde zjawisko, które ma potencjalną możliwość zaszkodzenia interesom i wartościom chronionym przez państwo". Stopień zagrożenia określa się na podstawie wielkości potencjalnej szkody oraz odległości czasowej (zwykle wyrażonej w kategoriach prawdopodobieństwa lub ryzyka) ewentualnego zastosowania tego zagrożenia."*[1]

W Słowniku interpretacyjnym bezpieczeństwa cybernetycznego zdefiniowano kilka terminów, które są bezpośrednio związane z zagrożeniami cybernetycznymi.

Sam termin **zagrożenie** definiuje się jako "*potencjalną przyczynę niezamierzonego zdarzenia, które może spowodować uszkodzenie systemu lub organizacji*". [2]

Bezpośrednio z tym podstawowym pojęciem związany jest termin **zagrożenie** bezpieczeństwa **informacji**[3] , który definiuje się jako "*potencjalną przyczynę niepożądanego zdarzenia, które może spowodować uszkodzenie systemu i jego zasobów, takie jak zniszczenie, niepożądany dostęp (kompromitacja), modyfikacja danych lub niedostępność usług*". [4]

Oprócz dwóch powyższych terminów autorzy definiują w słowniczku pojęcia: **zagrożenie aktywne, zagrożenie pasywne oraz zaawansowane i trwałe zagrożenie.** [5]

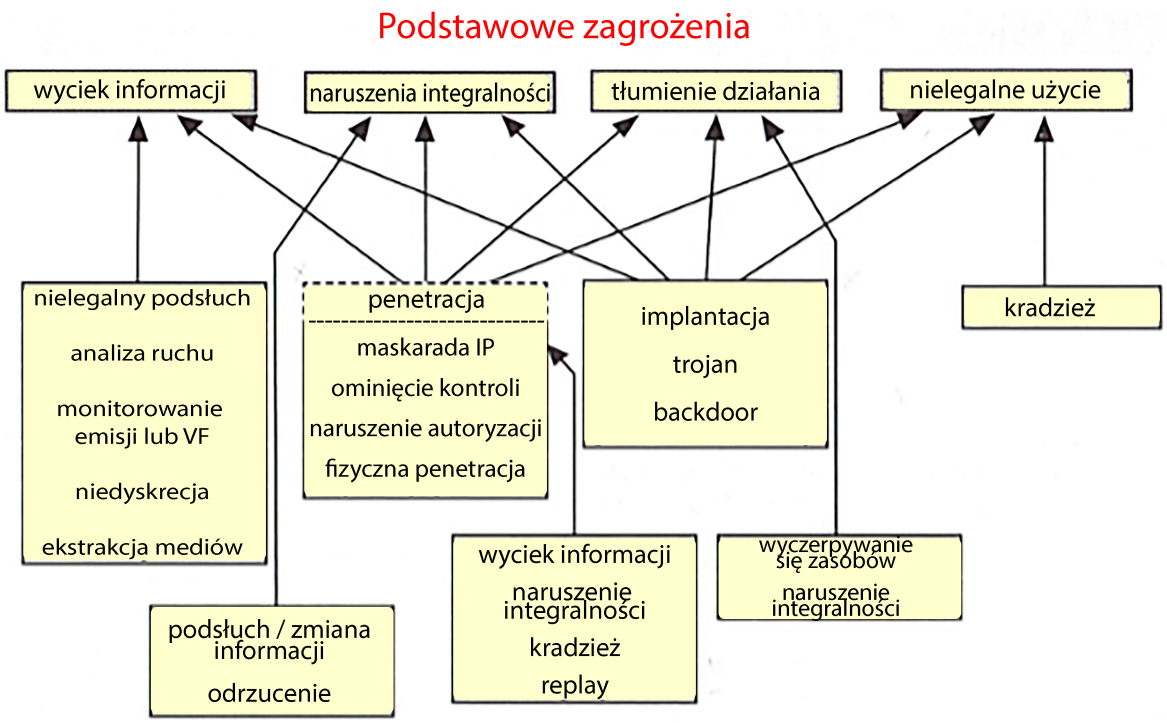
Słownik oksfordzki podaje, że **zagrożenie cybernetyczne to możliwość wystąpienia złośliwej próby uszkodzenia lub zakłócenia pracy sieci lub systemu komputerowego.**[6] System w tym kontekście to system komputerowy.

Zagrożenie cybernetyczne można również zdefiniować jako działanie mające na celu zmianę[7] informacji, aplikacji lub samego systemu.

Jirovský definiuje cztery grupy podstawowych zagrożeń i charakteryzuje ich wzajemne relacje:[8]

1. **Wyciek informacji** to sytuacja, w której chronione informacje zostają ujawnione nieupoważnionemu podmiotowi.
2. **Naruszenie integralności** to uszkodzenie, zmiana lub usunięcie danych.
3. **Blokowanie usługi** oznacza celowe uniemożliwienie dostępu do informacji, aplikacji lub systemu.[9]
4. **Nielegalne wykorzystanie** to wykorzystanie informacji przez nieuprawniony podmiot lub w nieuprawniony sposób.[10]

Zależność tę najlepiej ilustruje poniższy rysunek**.**



Wzajemne powiązania cyberzagrożeń według Jirovsky'ego

Klasyfikacja zagrożeń cybernetycznych

Istnieje wiele klasyfikacji zagrożeń cybernetycznych, z których najbardziej powszechne to:

1. Źródła zagrożeń

a) **Zagrożenia spowodowane przez człowieka.** Jeśli zagrożenie jest spowodowane przez człowieka, należy również skupić się na formie zawinienia, które doprowadziło do jego powstania. Z tej perspektywy można rozróżnić zagrożenia spowodowane przez:

· **celowe działanie,**

Do zagrożeń cybernetycznych spowodowanych umyślnie należą na przykład:

o celowe usuwanie danych, konfiguracji systemu itp,

o fizyczne uszkodzenie systemu komputerowego lub innego elementu ICT,

o kradzież danych i informacji,

o ataki cybernetyczne (złośliwe oprogramowanie, DoS, DDoS, phishing, nieuprawnione podsłuchiwanie itp.)[11]

· **zaniedbania.**

Do zagrożeń cybernetycznych spowodowanych zaniedbaniami należą:

o przypadkowo usunięte dane,

o fizyczne uszkodzenie systemu komputerowego lub innego elementu ICT (np. przez upadek, przewrócenie okablowania strukturalnego itp,)

o uszkodzenie danych, systemów lub innych elementów z powodu braku znajomości aktów wewnętrznych (prawnych lub technicznych),

o inne błędy użytkownika.

b) **Błędy techniczne** (np. błąd oprogramowania lub sprzętu).

c) **Vis maior (siła wyższa)**.

Do zagrożeń cybernetycznych spowodowanych przez siłę wyższą należą na przykład:

· Nieplanowana awaria zasilania (chyba że jest to zagrożenie spowodowane zaniedbaniem ze strony człowieka),

· zdarzenia naturalne (wyładowania atmosferyczne, burze itp.) lub katastrofy (powodzie, trzęsienia ziemi itp.),

· ogień (o ile nie jest to zagrożenie spowodowane przez człowieka).

2. Źródła działań

a) **Zagrożenia wewnętrzne** (źródło zagrożenia znajduje się wewnątrz organizacji)

b) **zagrożenia zewnętrzne** (źródło zagrożenia znajduje się poza organizacją)[12]

3. Cele zagrożenia

a) Atak triady CIA.

· **Poufność** - np. kradzież danych, danych dostępowych i kluczy, sprzętu itp.

· **Integralność** - błędy w bazach danych, ustawieniach uprawnień itp.

· **Dostępność** - np. ataki DoS i DDoS, ataki fizyczne na serwery i okablowanie strukturalne, przerwy w dostawie prądu itp.

b) Atak na element bezpieczeństwa cybernetycznego.

· **Ludzie -** ataki socjotechniczne (w świecie rzeczywistym, ale także w cyberprzestrzeni), phishing, złośliwe oprogramowanie, kradzieże itp.

· **Technologia -** wszystkie zagrożenia wymienione w punkcie 1 niniejszej klasyfikacji**.** Zazwyczaj zagrożenia mogą działać na:

  o Sprzęt (systemy komputerowe punktów końcowych, serwery, kontrolery sieciowe, IoT itp.)

  o bazy danych,

  o sieci i infrastruktury sieciowej,

  o oprogramowanie (system operacyjny lub inne aplikacje),

  o informacje i dane przechowywane w systemach komputerowych.

· **Procesy -** nieuprawnione testowanie bezpieczeństwa lub funkcjonalności procesów ustanowionych w organizacji itp.

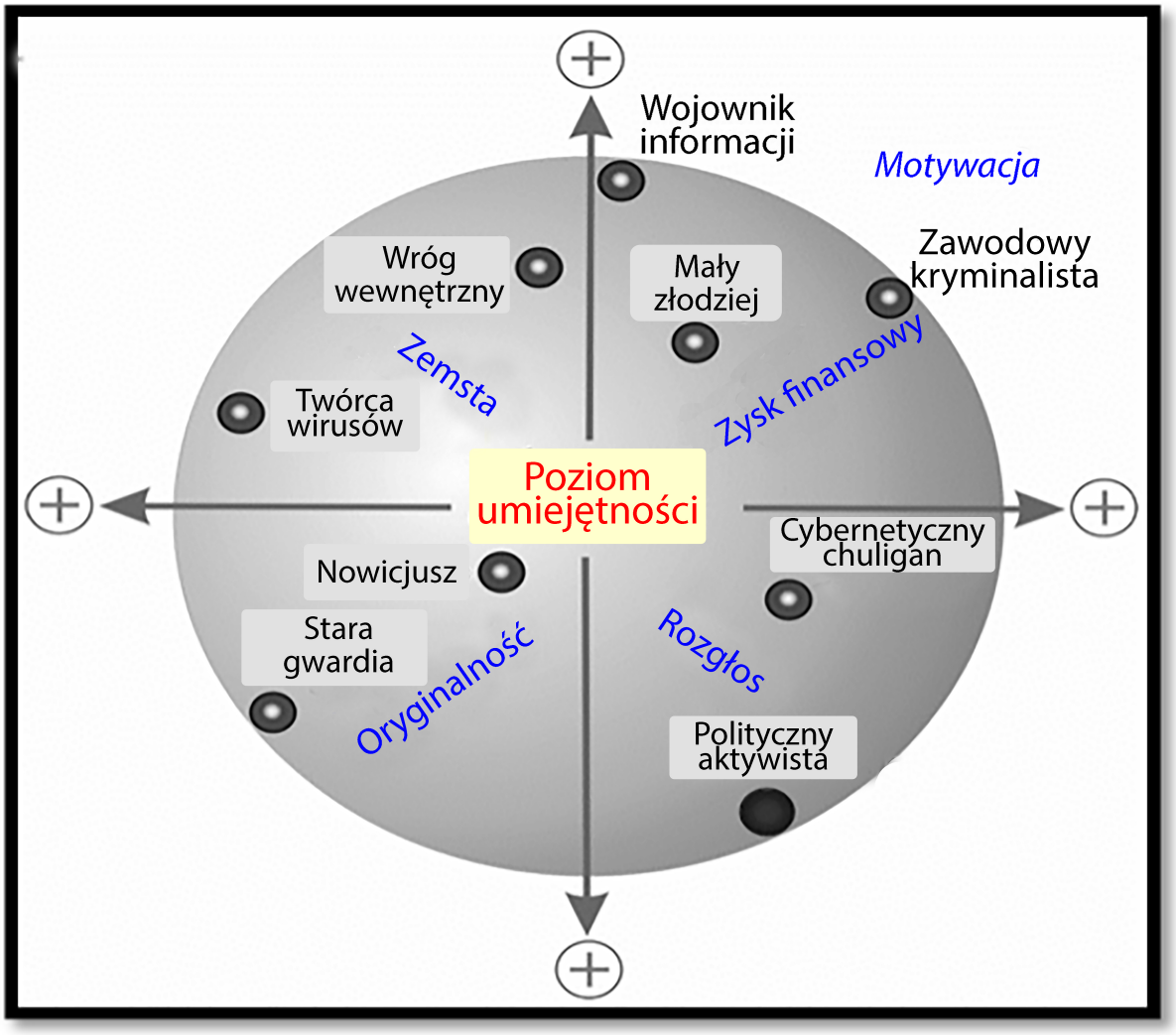
4. Motywacja

Jeśli zagrożenie jest spowodowane celowym działaniem danej osoby, należy zająć się jego motywacją. Analizując motywację do takich działań, można w ramach procesu reagowania na zagrożenie opracować środki naprawcze, które zapobiegną pobudzaniu tej motywacji w przyszłości.

W zależności od motywacji można zaobserwować:

- zagrożenia w celu osiągnięcia korzyści finansowych,
- zagrożenia w celu uzyskania przewagi konkurencyjnej,
- zagrożenia, aby udowodnić swoje umiejętności,
- zagrożenia w odwecie,
- zagrożenia wynikające z nieprzestrzegania przepisów.[13]

Dalszy podział napastników ze względu na motywację przedstawia także strona Rak[14] , na której przedstawiono najbardziej ogólną typizację napastników ze względu na ich motywację, przy czym wiele z wymienionych typów motywacji może się następnie dzielić lub łączyć.



Możliwy podział napastników w cyberprzestrzeni według motywacji

5. Rodzaj zagrożenia

- inżynieria społeczna,
- botnet,
- złośliwe oprogramowanie,
- ransomware,
- spam/oszustwo,
- oszukańcze oferty,
- phishing, pharming, spear phishing, vishing, smishing,
- hakowanie,
- wąchanie,
- ataki DoS, DDoS, DRDoS,
- rozpowszechnianie treści budzących zastrzeżenia,
- kradzież tożsamości,
- APT (Advanced Persistent Threat - zaawansowane trwałe zagrożenie),
- cyberterroryzm,
- wymuszenia w cyberprzestrzeni.

W dekrecie o bezpieczeństwie cybernetycznym w załączniku 3 wymieniono przykładowo niektóre z tych zagrożeń. **Zgodnie z** tym **dekretem, groźbą jest:**

1. naruszenie zasad bezpieczeństwa, nieautoryzowane działania, nadużywanie uprawnień przez użytkowników i administratorów,
2. uszkodzenie lub awaria sprzętu technicznego i/lub oprogramowania,
3. nadużywanie tożsamości,
4. korzystanie z oprogramowania z naruszeniem warunków licencji,
5. złośliwego kodu (na przykład wirusów, oprogramowania szpiegującego, koni trojańskich),

6. naruszenia bezpieczeństwa fizycznego,
7. przerwanie świadczenia usług łączności elektronicznej lub dostaw energii elektrycznej,
8. niewłaściwego wykorzystania lub nieuprawnionej modyfikacji danych,
9. utrata, kradzież lub uszkodzenie składnika majątku,
10. niewywiązanie się przez dostawcę z obowiązku wynikającego z umowy,
11. wykroczenia popełniane przez pracowników,
12. nadużywanie zasobów wewnętrznych, sabotaż,
13. długotrwała przerwa w świadczeniu usług łączności elektronicznej, dostawie energii elektrycznej lub innych podstawowych usług,
14. brak personelu posiadającego niezbędną wiedzę fachową,
15. Ukierunkowany cyberatak z wykorzystaniem socjotechniki, stosowanie technik szpiegowskich,
16. niewłaściwe korzystanie z wymiennych technicznych nośników informacji,
17. włamania do komunikacji elektronicznej (przechwytywanie, modyfikacja).

1.3.2 Wydarzenie związane z bezpieczeństwem cybernetycznym

Prosise i Mandiva charakteryzują **"zdarzenie związane z bezpieczeństwem komputerowym"** (które może być rozumiane jako atak komputerowy lub przestępstwo komputerowe) jako nielegalne, nieuprawnione, niedopuszczalne działanie dotyczące systemu komputerowego lub sieci komputerowej. Działania te mogą mieć na celu np. kradzież danych osobowych, rozsyłanie spamu lub inne formy nękania, sprzeniewierzenie, rozpowszechnianie lub posiadanie pornografii dziecięcej itp.[15]

Jirásek i in. definiują zdarzenie związane z bezpieczeństwem jako *"**zdarzenie, które może spowodować lub doprowadzić do naruszenia** systemów i technologii informatycznych oraz zasad zdefiniowanych w celu ich ochrony (polityki bezpieczeństwa)".*[16]

Definicję zdarzenia bezpieczeństwa można znaleźć również w normie ISO/IEC 27001, punkt 3.5, który mówi, że takie zdarzenie to: *"możliwy do **zidentyfikowania stan** systemu, usługi lub sieci **wskazujący na możliwe naruszenie polityki bezpieczeństwa lub awarię środków bezpieczeństwa**. Może to być również inna sytuacja, która nie miała wcześniej miejsca, a która może być istotna z punktu widzenia bezpieczeństwa informacji".*

Podobną definicję można znaleźć w dokumencie NIST, 800-61 Computer Security Incident Handling Guide, w którym stwierdza się, że *zdarzenie związane z* bezpieczeństwem to "*niekorzystne zdarzenie o negatywnych skutkach, takie jak awaria systemu, zalewanie pakietów, nieuprawnione korzystanie z uprawnień systemowych, nieuprawniony dostęp do danych wrażliwych lub wykonanie złośliwego kodu niszczącego dane*". [17]

Zdarzenie związane z bezpieczeństwem cybernetycznym zostało również zdefiniowane w sekcji 7(1) ustawy o bezpieczeństwie cybernetycznym jako *"**zdarzenie, które może spowodować naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług albo bezpieczeństwa i integralności sieci łączności elektronicznej"**.*

De facto **jest to zdarzenie bez rzeczywistych negatywnych konsekwencji** dla systemu komunikacyjnego lub informatycznego, w istocie jest to tylko zagrożenie, ale musi być ono rzeczywiste.

Jednocześnie autorzy popełniają tautologię, wyjaśniając zdarzenie jako zdarzenie.

Uważamy, że termin "zdarzenie związane z bezpieczeństwem cybernetycznym" byłby właściwszy i prawdopodobnie bardziej zrozumiały, gdyby był określany i interpretowany jako "**zagrożenie cybernetyczne",** ponieważ tak naprawdę istnieje tylko potencjalna przyczyna, która może spowodować zdarzenie niepożądane.

Przykład: *użytkownik otrzymuje wiadomość e-mail zawierającą złośliwy kod (malware) w załączniku w wewnętrznej poczcie firmowej. Złośliwe oprogramowanie jest jednak skompresowane (np. przy użyciu programu WinZip) i nie może zostać zainstalowane bez dalszych działań użytkownika. Takie zdarzenie może samo w sobie nie stanowić naruszenia bezpieczeństwa, ale w pewnych okolicznościach może je naruszyć.*

1.3.3 Incydent cybernetyczny (bezpieczeństwa)

Jirásek et al. definiują Incydent Bezpieczeństwa jako "*naruszenie lub bezpośrednie zagrożenie naruszeniem polityki bezpieczeństwa, zasad bezpieczeństwa lub standardowych reguł bezpieczeństwa dotyczących działania technologii informacyjnych i komunikacyjnych*". ***[18]***

Właściwą definicję **zdarzenia związanego z bezpieczeństwem informacji** zawiera norma ISO/IEC 27001. W artykule 3.6 tej normy zdarzenie związane z bezpieczeństwem informacji jest zdefiniowane jako *"jedno lub więcej niezamierzonych lub nieoczekiwanych zdarzeń związanych z bezpieczeństwem, które z dużym prawdopodobieństwem mogą zagrozić działalności organizacji i naruszyć bezpieczeństwo informacji"*.

Bardzo podobną definicję **incydentu bezpieczeństwa komputerowego** można znaleźć w dokumencie NIST, 800-61 Computer Security Incident Handling Guide, w którym stwierdza się, że jest to *"naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, zasad dopuszczalnego użytkowania (systemu, usługi) lub standardowych praktyk bezpieczeństwa"*.[19]

Incydent bezpieczeństwa cybernetycznego jest również zdefiniowany w sekcji 7(2) ustawy o bezpieczeństwie cybernetycznym jako ***"naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług albo bezpieczeństwa i integralności sieci łączności elektronicznej w wyniku zdarzenia związanego z bezpieczeństwem cybernetycznym".*** "

Ze słownika prawa wynika, że zdarzenie może być spowodowane zarówno umyślnym i niedbałym działaniem człowieka, jak i siłą wyższą. Istotne jest **naruszenie bezpieczeństwa informacji lub usług oraz związanych z nimi systemów informacyjnych i komunikacyjnych.**

Incydent bezpieczeństwa cybernetycznego oznacza zatem rzeczywiste naruszenie bezpieczeństwa informacji w systemach informatycznych lub naruszenie bezpieczeństwa usług albo bezpieczeństwa i integralności sieci łączności elektronicznej, tj. naruszenie systemu informacyjnego lub komunikacyjnego o negatywnych skutkach.

Za pewną część incydentów związanych z cyberbezpieczeństwem odpowiadają również zjawiska losowe, błędy sprzętowe i programowe, błędy popełniane podczas konfiguracji przez administratorów, błędy popełniane przez użytkowników systemu itp.

Przykład: *kontynuując poprzedni przykład, gdy użytkownik wykona na komputerze złośliwy kod, mówimy już o incydencie bezpieczeństwa.*

1.3.4 Cyberatak

Jirásek i in. definiują cyberatak jako *"atak na infrastrukturę informatyczną w celu spowodowania szkód i uzyskania wrażliwych lub strategicznie ważnych informacji". Jest on najczęściej używany w kontekście ataków o podłożu politycznym lub militarnym."*[20]

Taka definicja cyberataku byłaby bardzo restrykcyjna i nie obejmowałaby wszystkich negatywnych działań użytkowników cyberprzestrzeni[21] , zwłaszcza że łączy w sobie warunki uszkodzenia systemu informatycznego i pozyskania informacji. Cyberatak może być również działaniem socjotechnicznym, w którym jedynym celem jest uzyskanie informacji, lub odwrotnie - atakiem DoS lub DDoS, w którym jedynym celem może być zablokowanie (tj. nieuszkodzenie) funkcjonalności jednego lub większej liczby systemów komputerowych lub świadczonych usług.

Różnica między incydentem związanym z bezpieczeństwem cybernetycznym a atakiem cybernetycznym polega przede wszystkim na kwestii winy. Jak wspomniano wcześniej, incydenty związane z bezpieczeństwem cybernetycznym mogą być spowodowane zarówno celowym, jak i niedbałym działaniem człowieka, a także siłą wyższą. W przypadku cyberataku chodzi jednak o celowe działanie człowieka.

Na tej podstawie można zdefiniować **atak cybernetyczny**[22] jako **każde celowe działanie napastnika w cyberprzestrzeni, skierowane przeciwko interesom innej osoby.**

Cyberatak można również zdefiniować jako działanie napastnika lub grupy napastników, którzy wykorzystują technologie informacyjno-komunikacyjne do zaatakowania innej infrastruktury informacyjno-komunikacyjnej w celu zakłócenia dostępności, poufności lub integralności danych.

1.3.5 Cyberprzestępczość

Aby zakończyć omawianie incydentów i ataków cybernetycznych, uważamy, że konieczne jest przynajmniej zarysowanie związku między tymi atakami lub incydentami a cyberprzestępczością.

Definiując treść terminu **cyberprzestępczość, należy** zauważyć, że wraz ze wzrostem możliwości wykorzystania środków informacyjno-komunikacyjnych rośnie również możliwość ich użycia (nadużycia) do popełniania przestępstw. Dlatego też w zasadzie nie istnieje uniwersalna, powszechnie akceptowana definicja, która w pełni oddawałaby zakres i głębię tego pojęcia.

W najbardziej ogólnym ujęciu cyberprzestępstwo można zdefiniować **jako czyn skierowany przeciwko systemowi komputerowemu, sieci komputerowej, danym lub użytkownikom, albo jako czyn, w którym system komputerowy jest wykorzystywany jako narzędzie do popełnienia przestępstwa. Fakt, że** sieć komputerowa lub cyberprzestrzeń jest środowiskiem, w którym odbywa się ta działalność, jest niezbędny do zastosowania definicji cyberprzestępstwa.

Cyberprzestępczość, czyli cyberprzestępczość, stanowi rodzaj najszerszego zbioru wszystkich działań przestępczych, które mają miejsce w środowisku technologii informacyjnych i komunikacyjnych. Bardzo często "tradycyjne przestępstwa" są przenoszone do cyberprzestrzeni, ponieważ można je tam popełniać szybciej i skuteczniej (np. oszustwa, rozpowszechnianie materiałów przedstawiających wykorzystywanie dzieci itp.) Oprócz przenoszenia znanych przestępstw, tworzy się nowe ataki, często jeszcze nieuwzględnione w przepisach.

Należy zauważyć, że nie każdy atak cybernetyczny musi być przestępstwem, ale każde cyberprzestępstwo musi być atakiem cybernetycznym. Wiele ataków cybernetycznych, nawet w przypadku braku norm prawa karnego, można zaliczyć do zachowań, które będą miały charakter przestępstwa cywilnego lub administracyjnego, lub też mogą nie być zachowaniami karalnymi na podstawie jakiejkolwiek normy prawnej (może to być np. tylko zachowanie niemoralne lub niedopuszczalne).

---

[1] *Zagrożenie*. [online]. [cytowany 2018-07-28]. Dostępny pod adresem: http://www.mvcr.cz/clanek/hrozba.aspx

[2] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015. s. 52. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[3] W tym przypadku można zauważyć problem z tłumaczeniem niektórych terminów z języka angielskiego i odwrotnie. Jeśli chcielibyśmy konsekwentnie tłumaczyć termin Information security threat, to poprawnym czeskim odpowiednikiem jest np. threat to information security; zagrożenie dla bezpieczeństwa informacji itp.

[4] Tamże, s. 25.

[5] Ibid. s. 16, 81 i 87

[6] *Cyberzagrożenie*. [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://en.oxforddictionaries.com/definition/cyberthreat

[7] Zmiana oznacza także kradzież informacji, ich zniszczenie lub uniemożliwienie ich wykorzystania.

[8] Por. JIROVSKÝ, Václav. *Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic*. Praga: Grada Publishing, a. s., 2007. s. 21 i nast.

[9] Należą do nich takie ataki, jak **DoS - Denial of Service (odmowa usługi), DDoS - Distributed Denial of Service (rozproszona odmowa usługi)** itp. Więcej szczegółów w: KOLOUCH, Jan. *Cyberprzestępczość*. Praga: CZ.NIC, 2016, s. 295 i nast.

[10] Na przykład włamano się do systemu opartego na opłatach, a jego usługi są wykorzystywane bez uiszczenia opłaty za te usługi.

[11] Na temat poszczególnych ataków cybernetycznych zob. np. *Cyberprzestępczość*. Praga: CZ.NIC, 2016, s. 181 i nast.

[12] Więcej informacji na ten temat można znaleźć np. w: POŽÁR, Josef. *Wybrane zagrożenia dla bezpieczeństwa informacji w organizacjach*. [online]. [cyt. 6 lipca 2018]. Dostępny pod adresem: https://www.cybersecurity.cz/data/pozar2.pdf

[13] Przed czym należy się chronić? - Zagrożenia bezpieczeństwa, zdarzenia, incydenty. [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.kybez.cz/bezpecnost/pred-cim-chranit

[14] Źródło. Homo sapiens kontra bezpieczeństwo. Forum ICT/PERSONALIS 2006 [prezentacja 27 września 2006 r.]. Praga (prezentacja na konferencji).

[15] PROSISE, Chris i Kevin MANDIVA. *Reagowanie na incydenty i informatyka śledcza, wydanie drugie*. Emeryville: McGraw-Hill, 2003, s. 13.

Por. dalej CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition*. Londyn: Academic Press, 2004, s. 9 i nast.

[16] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015. s. 28. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[17] *Przewodnik postępowania w przypadku incydentów związanych z bezpieczeństwem komputerowym* [online]. [cited 2018 Aug 13]**, s. 6. Dostępny w Internecie:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

[18] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015. s. 25. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf.

[19] *Przewodnik postępowania w przypadku incydentów związanych z bezpieczeństwem komputerowym* [online]. [cyt. 2018-02-17], s. 6. Dostępny w: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[20] JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015. s. 71. Dostępny pod adresem: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[21] W szczególności w definicji brakuje określenia jakiejkolwiek innej motywacji atakującego niż ta, która miałaby na celu *...spowodowanie szkód lub zdobycie strategicznie ważnych informacji*. Przykładem nieobjętym tą definicją są ataki o podłożu ekonomicznym, których liczba obecnie gwałtownie wzrasta.

[22] Należy odróżnić pojęcie incydentu bezpieczeństwa od pojęcia cyberataku, który stanowi naruszenie bezpieczeństwa IS/IT i zasad zdefiniowanych w celu jego ochrony (polityka bezpieczeństwa).

1.5. PODSUMOWANIE

ℹ️

· Aby zrozumieć problematykę cyberataków i cyberbezpieczeństwa, należy poznać podstawową terminologię bezpośrednio związaną z wybraną dziedziną. W niniejszym rozdziale przedstawiono wybrane terminy techniczne i prawne.

· Termin "bezpieczeństwo cybernetyczne" nie ma jednej powszechnie akceptowanej definicji. Bezpieczeństwo cybernetyczne jest podzbiorem bezpieczeństwa jako takiego.

  o Definiując samo bezpieczeństwo cybernetyczne, warto oprzeć się na ustalonych definicjach. Wymienię kilka takich ustalonych definicji:

  o Cyberbezpieczeństwo to zestaw środków podejmowanych w celu ochrony systemu komputerowego przed nieuprawnionym dostępem lub atakiem.

  o Słownik oksfordzki podaje, że cyberbezpieczeństwo to stan, w którym dane elektroniczne są chronione przed przestępczym lub nieuprawnionym użyciem. Bezpieczeństwo cybernetyczne obejmuje środki, które należy podjąć, aby osiągnąć ten stan.

  o Według Jiráska i in. cyberbezpieczeństwo to *"zespół środków prawnych, organizacyjnych, technicznych i edukacyjnych mających na celu zapewnienie ochrony cyberprzestrzeni"*.

· Definicję bezpieczeństwa cybernetycznego można znaleźć na przykład w dokumencie Definition of Cybersecurity - Gaps and overlaps in standardisation[1] Europejskiej Agencji ENISA[2] : *"Bezpieczeństwo cybernetyczne odnosi się do bezpieczeństwa cyberprzestrzeni, gdzie sama cyberprzestrzeń odnosi się do zbioru powiązań i relacji pomiędzy obiektami, które są dostępne za pośrednictwem ogólnej sieci telekomunikacyjnej, oraz do rzeczywistego zbioru obiektów, których interfejsy umożliwiają ich zdalną kontrolę, zdalny dostęp do danych lub zaangażowanie w działania kontrolne w cyberprzestrzeni. Bezpieczeństwo cybernetyczne będzie obejmować paradygmat triady "CIA" w odniesieniu do relacji i obiektów w cyberprzestrzeni, przy jednoczesnym rozszerzeniu tego paradygmatu w celu zapewnienia ochrony prywatności podmiotów (osób i podmiotów) oraz odporności ["odbudowy" po ataku]"*.

· Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii[3] stanowi w art. 4 ust. 2, że *"bezpieczeństwo sieci i systemów informatycznych oznacza zdolność tych sieci i systemów informatycznych do wytrzymania z pewnym stopniem niezawodności wszelkich zakłóceń, które zagrażają dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych za pośrednictwem tych sieci i systemów informatycznych."*¨.

· Ryzyko można również zdefiniować jako potencjalne zagrożenie, które może się urzeczywistnić i wykorzystać słabe punkty danego zasobu. Zgodnie z art. 4 ust. 9 NIS ryzyko definiuje się jako *"wszelkie możliwe do określenia okoliczności lub zdarzenia, które mogą mieć negatywny wpływ na bezpieczeństwo sieci i systemów informatycznych"*. W cyberprzestrzeni na zagrożenia narażeni są użytkownicy, systemy i aplikacje komputerowe, które z nich korzystają, a także inne elementy TIK.

· Aktywa to wszystko, co ma wartość dla danej osoby, organizacji lub państwa. Składnik majątku może być rzeczą materialną (budynek, system komputerowy, sieć, energia, towary itp.) lub niematerialną (informacje, wiedza, dane, programy itp.) w rozumieniu prawa cywilnego.

· Zasobem może być jednak również właściwość (np. dostępność i funkcjonalność systemu i danych itp.) lub reputacja itp. Z punktu widzenia bezpieczeństwa cybernetycznego zasobem są również ludzie (użytkownicy, administratorzy itp.) oraz ich wiedza i doświadczenie.

· Podatność na ataki to słaby punkt zasobu, oprogramowania lub zabezpieczeń, który jest wykorzystywany przez jedno lub więcej zagrożeń. Podatność, podobnie jak zagrożenie, może być spowodowana różnymi czynnikami, w tym działaniem człowieka, awarią techniczną i ewentualnie działaniem siły wyższej.

🗝️

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

· bezpieczeństwo cybernetyczne

· CIA

· ryzyko

- aktywa
- podatności nie
- cyberatak
- zagrożenie cybernetyczne

❓

PYTANIA KONTROLNE

- Co to jest triada CIA?
- Jak można zdefiniować bezpieczeństwo cybernetyczne?
- Jakie są elementy bezpieczeństwa cybernetycznego?
- Co należy rozumieć pod pojęciem aktywów?
- Jak można zdefiniować podatność na zagrożenia?

---

[1] *Definition of Cybersecurity - Gaps and overlaps in standardisation* [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

[2] Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

[3] Zwana dalej "**NIS**" lub "**dyrektywą NIS".** [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

2. Zespoły CERT/CSIRT

W XXI wieku nastąpił ogromny rozwój i komercjalizacja Internetu. Gwałtownie wzrosła liczba użytkowników, liczba systemów komputerowych podłączonych do sieci globalnej oraz liczba obsługiwanych usług o znaczeniu krytycznym, zarówno w sferze komercyjnej (np. bankowość elektroniczna, sklepy internetowe, aukcje elektroniczne), jak i rządowej (np. serwisy informacyjne administracji państwowej i samorządowej, rejestry). Incydenty naruszające bezpieczeństwo, ataki cybernetyczne i działania przestępcze popełniane za pośrednictwem technologii informacyjno-komunikacyjnych w świecie rzeczywistym i wirtualnym stają się coraz poważniejsze, a ich wpływ i konsekwencje coraz poważniejsze.

Istotną cechą odróżniającą tę cyberprzestępczość od innych rodzajów przestępstw jest duże opóźnienie, wysoki poziom tolerancji społecznej (w tym obojętność użytkowników), anonimowość sprawcy oraz jego często trudna identyfikacja. Istnieje zatem rosnąca potrzeba doskonalenia środków obrony przed takimi atakami, w szczególności poprawy środowiska i sposobów śledzenia sprawcy, standaryzacji i formalizacji procedur oraz edukacji użytkowników, tak aby byli w stanie rozpoznawać zagrożenia i sytuacje ryzykowne, radzić sobie z nimi, a najlepiej im zapobiegać. W tym celu tworzona jest infrastruktura zespołów CERT i CSIRT.

2.1. Historia

Robak Morris jest uważany za pierwszy przypadek naruszenia bezpieczeństwa, który negatywnie wpłynął na działanie Internetu, powodując wyłączenie około 10% wszystkich podłączonych urządzeń. Robak został umieszczony w Internecie w 1988 roku przez Roberta Morrisa, studenta Uniwersytetu Cornell w USA. Incydent ten zapoczątkował erę tworzenia i rozprzestrzeniania się wirusów komputerowych, robaków, koni trojańskich i innych podobnych "szkodników elektronicznych", określanych wspólnym mianem *złośliwego oprogramowania*. To właśnie to doświadczenie zapoczątkowało pod koniec lat 80. debatę na temat bezpieczeństwa sieci i usług, a następnie doprowadziło do sformułowania podstawowych zasad obrony, zapobiegania i ochrony transmisji danych wrażliwych.

W odpowiedzi na robaka Moriss pierwszy zespół CERT został utworzony na Uniwersytecie Carnegie Meelon (CMU) w USA. Zadaniem tego pierwszego, zebranego ad hoc zespołu CERT było zbadanie robaka Moriss, znalezienie skutecznej obrony i opracowanie rozwiązania problemu. Ostatecznie najcenniejszym wynikiem pracy tego zespołu było uświadomienie sobie, że najważniejsze jest przygotowanie się na możliwość naruszenia bezpieczeństwa z wyprzedzeniem oraz wdrożenie wcześniej zdefiniowanego i przetestowanego planu obrony i odzyskiwania danych w momencie wystąpienia problemu, a nie dopiero rozpoczęcie analizy, co należy zrobić i w jakich krokach. Rezultaty pracy tego pierwszego CERT-u zapoczątkowały erę budowania globalnej infrastruktury tego typu zespołów.

Carnegie Mellon University zarejestrował akronim CERT jako znak towarowy i choć jego użycie przez inne organizacje w tym kontekście nie jest zabronione (organizacja, która chce użyć akronimu w nazwie swojego zespołu, musi poprosić o zgodę na użycie akronimu i zazwyczaj ją otrzymuje), to właśnie to było powodem stworzenia i wprowadzenia drugiego terminu CSIRT.

2.2. Zespoły CERT i CSIRT

CERT (Computer Emergency Response Team - Zespół Reagowania na Incydenty Komputerowe) i CSIRT (Computer Security Incident Response Team - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). Choć każdy z tych skrótów ma nieco inne znaczenie i, co ważniejsze, nieco inną genezę historyczną, to w rzeczywistości dziś oba skróty można rozumieć jako ten sam rodzaj zespołu - zespół, który jest odpowiedzialny za zajmowanie się incydentami bezpieczeństwa i zagrożeniami (cybernetycznymi) w swoim jasno określonym obszarze działania, z perspektywy użytkowników lub innych zespołów, miejsce, do którego mogą się oni zwrócić z wykrytym incydentem bezpieczeństwa, z prośbą o współpracę, wymianę informacji, pomoc itp.

Zespoły CERT/CSIRT tworzone są na poziomie poszczególnych organizacji, zarówno tych, które pośredniczą w funkcjonowaniu Internetu (dostawcy usług internetowych), jak i tych, które wykorzystują Internet do swojej podstawowej działalności (np. firmy informatyczne, dostawcy treści, banki).

Podstawowym obowiązkiem każdego zespołu CSIRT jest reagowanie na zagrożenie ("odpowiedź") oraz współpraca w zakresie reagowania na incydenty. Zespół CSIRT zwykle zajmuje się problemem, który występuje w jego obszarze odpowiedzialności (np. w jego własnej infrastrukturze sieciowej), tzn. tam, gdzie ma realną możliwość interwencji.

CERT/CSIRT danej sieci (organizacji) jest na ogół punktem kontaktowym, do którego użytkownicy mogą się zwracać w przypadku wykrycia problemu bezpieczeństwa (lub nawet podejrzenia takiego problemu) związanego z siecią komputerową lub jedną z udostępnianych usług. Profesjonalny zespół CERT/CSIRT powinien zbadać każdy otrzymany raport o incydencie bezpieczeństwa (lub potencjalnym incydencie bezpieczeństwa) i naprawić go w miarę swoich możliwości.

Nie jest to nic rewolucyjnego i praktycznie nie istnieje; każda większa organizacja, dostawca usług internetowych czy usługodawca ma zespół ds. bezpieczeństwa. **Główna różnica między zwykłym zespołem ds. bezpieczeństwa a zespołem CERT/CSIRT polega na zaangażowaniu w globalną infrastrukturę bezpieczeństwa**, wymianie informacji w ramach tej infrastruktury **oraz przestrzeganiu ustalonych procedur formalnych.**

Istnienie co najmniej jednego oficjalnego zespołu CERT/CSIRT jest pożądane w każdej działającej sieci, zwłaszcza w dużych (tranzytowych, regionalnych, uczelnianych), czyli na poziomie dużych dostawców usług internetowych, ale także w bankach czy u dostawców usług.

Nadrzędne **krajowe** i **rządowe zespoły ds. szczytu mają do odegrania** ważną i **specyficzną rolę w** każdym kraju, dlatego zostanie im poświęcony osobny podrozdział.

W skali globalnej istniejące zespoły CERT/CSIRT można postrzegać jako infrastrukturę służącą rozwiązywaniu problemów związanych z bezpieczeństwem w Internecie. W swojej pracy zespoły CERT/CSIRT opierają się przede wszystkim na własnym doświadczeniu, wcześniej przygotowanych i sprawdzonych w terenie procedurach oraz współpracy i wymianie informacji z innymi zespołami CERT/CSIRT.

Podstawowym wymaganiem społeczności jest **publiczne ogłoszenie przez zespół CERT/CSIRT swoich danych kontaktowych i zasad działania:**

- który jest jego operatorem,
- którzy są jego członkami,
- jak i kiedy można skontaktować się z zespołem,
- jakie usługi oferuje,
- Zakres (numer AS[1] , sieć, domeny, usługi), w którym zespół jest uprawniony do działania i w jaki sposób, tzn. określenie jego uprawnień i odpowiedzialności. Na podstawie tego zakresu zespół jest następnie kontaktowany (np. przez atakowanego) i rozwiązuje swoje problemy (incydenty).

Termin "rozwiązywanie incydentów bezpieczeństwa" może mieć różną specyfikę w zależności od konfiguracji zespołu i jego wewnętrznej polityki - może to być proste wyeliminowanie ataku (wyłączenie źródła problemu, np. poprzez odłączenie zagrożonego systemu komputerowego od sieci), wytropienie napastnika, szybkie przywrócenie działania zaatakowanej usługi/sieci itp.

W zależności od działań zespołu w zakresie postępowania w przypadku wystąpienia zdarzenia naruszającego bezpieczeństwo, zespoły mogą być klasyfikowane jako *wewnętrzne* (instytucjonalne) lub *koordynujące.* Zespół typu wewnętrznego ma zwykle możliwość bezpośredniej interwencji (odłączenie źródła problemu, wprowadzenie filtrowania ruchu sieciowego itp.), zespół typu koordynacyjnego nie ma możliwości bezpośredniej interwencji, jego działalność koncentruje się na komunikacji, współpracy i pośredniczeniu w przekazywaniu informacji (w tej roli występują zwykle tzw. zespoły *narodowe, o których* będzie mowa później).

W przypadku konkretnego incydentu zaangażowane osoby starają się rozwiązać go bezpośrednio u źródła, tj. u tego, kto znajduje się najbliżej źródła lub celu incydentu i może najskuteczniej interweniować (administrator sieci lub usługi końcowej). Idealna sytuacja występuje wtedy, gdy zarówno źródło, jak i cel znajdują się w zasięgu działania zespołu CSIRT, ponieważ bardzo łatwo i szybko można znaleźć konkretnego eksperta w miejscu, w którym występuje problem. Potrafi też wtedy skutecznie rozwiązać problem, a jego reakcje są przewidywalne - ponieważ dobrowolnie opublikował własne reguły gry. Ten proces komunikacji jest bardzo elastyczny, ponieważ komunikacja nie przechodzi przez różne poziomy, jest szybka i dokładna, a odpowiedź może być taka sama. Jeśli jednak atakowany nie może znaleźć odpowiedniego odpowiednika (ponieważ on nie istnieje, nie podaje żadnych użytecznych informacji o sobie, odmawia zajęcia się problemem lub po prostu nie odpowiada), przydałaby się jakaś "dźwignia". Najlepsze zespoły - krajowe i rządowe - zazwyczaj są w stanie zapewnić to w pewnym stopniu.

---

[1] **AS** - Autonomous System (system autonomiczny). System autonomiczny to zbiór sieci IP i routerów pod wspólnym zarządem technicznym, który reprezentuje wspólną politykę routingu w Internecie.

2.3. Jak tworzy się zespół CERT/CSIRT?

Organizacja, która decyduje się na powołanie zespołu CERT/CSIRT, musi na samym początku jasno i zrozumiale określić, co chce osiągnąć poprzez powołanie zespołu, jakiej roli wymaga od zespołu (tj. określić jego zakres, uprawnienia, obowiązki i usługi, które ma świadczyć), a także musi odpowiednio zakotwiczyć zespół w organizacji.

Zakres

Pole kompetencji jest zwykle rozumiane jako obszar cyberprzestrzeni, w którym zespół jest kompetentny do działania i nad którym ma odpowiednie władze i obowiązki określone przez założyciela. Na podstawie zadeklarowanego zakresu działania zespół jest następnie kontaktowany np. przez zaatakowanych i rozwiązuje problemy w swoim zakresie działania. Zakres działania zespołu może być zdefiniowany jako określona sieć (sieci), system (systemy) autonomiczny (autonomiczne), domena (domeny) nominalna, ale są też zespoły, które deklarują jako swój zakres działania umiejętności eksperckie, określoną usługę itp.

Usługi

Aby zespół mógł oficjalnie nazywać się CERT/CSIRT, musi przede wszystkim oferować usługi polegające na rozwiązywaniu lub koordynowaniu rozwiązywania incydentów bezpieczeństwa w określonym zakresie, wypełniając tym samym ideę "reagowania" użytą w akronimach CERT/CSIRT, tzn. musi być w stanie reagować *na* incydenty bezpieczeństwa. Zespół może jednak zaoferować szereg innych usług w wielu dziedzinach, np. szkolenia, ostrzeganie o bieżących atakach, słabościach systemów operacyjnych, audyty bezpieczeństwa, konsultacje w zakresie SW, zalecanie podstawowych zasad bezpieczeństwa, tworzenie i obsługa narzędzi do monitorowania ruchu sieciowego i usług oraz wiele innych.

Członkowie zespołu

Obszarem, który ma decydujący wpływ na jakość zespołu, jest jego obsada. W każdej działającej sieci istnieje zazwyczaj dział lub grupa techników odpowiedzialnych za działanie i rozwój sieci oraz usług, którzy zajmują się także aspektami bezpieczeństwa (zazwyczaj są to "pracownicy IT", "urzędnicy ds. bezpieczeństwa", "administratorzy" itp.) Są to zazwyczaj właściwe osoby, które należy włączyć do zespołu CERT/CSIRT lub zlecić jego utworzenie. Wskazane jest jednak, aby w zespole znaleźli się także innego rodzaju eksperci (np. prawnik, w przypadku zespołów krajowych i rządowych - specjalista ds. komunikacji medialnej, menedżer, socjolog itp.) Zależy to od ukierunkowania, środowiska, oferowanych usług i roli zespołu.

Z perspektywy "zewnętrznej" zespół staje się zespołem CERT/CSIRT, gdy zostanie zaakceptowany jako taki przez inne istniejące zespoły CERT/CSIRT na całym świecie. Droga do zostania zespołem CERT/CSIRT nie jest skomplikowana, na początku drogi wystarczy w jasny sposób zadeklarować, co następuje:

1. **Podstawowe informacje kontaktowe** - nazwa zespołu, nazwa organizacji kierującej zespołem, -adres👍 poczty elektronicznej zespołu, na który można zgłaszać zdarzenia naruszające bezpieczeństwo lub z którym można się skontaktować, numer👍 telefonu👍 zespołu, adres siedziby głównej, nazwiska członków zespołu, godziny, w których można skontaktować się z zespołem itp.

2. **Zakres działania zespołu** - określa, za co zespół jest odpowiedzialny i jaka jest jego rola. To oczywiście zależy od tego, jaki to jest zespół. Możliwe jest utworzenie zespołów o mniej więcej następujących typach:

· ***wewnętrzny*** - obsługuje i odpowiada za konkretną sieć (np. za określony zakres adresów IP, domen), zazwyczaj jest tworzony przez operatora sieci,

· ***koordynacja*** - zespół, którego głównym zadaniem jest koordynowanie rozwiązywania incydentów bezpieczeństwa, a nie ich rozwiązywanie,

· ***sprzedawca*** - zespół zajmujący się incydentami bezpieczeństwa, które dotyczą konkretnego produktu (SW),

· ***krajowe, rządowe*** - specjalne przypadki oparte na zasadach dwóch pierwszych wymienionych zespołów (wewnętrzny i koordynacyjny), ich zakres i rola zależy od założyciela, a często także od ustawodawstwa danego kraju.

3. **Oferowane usługi -** CERT/CSIRT musi świadczyć co najmniej usługę reagowania na incydenty bezpieczeństwa.

Gdy nowo powołany zespół CSIRT/CERT upora się z powyższymi krokami i ustanowi podstawową politykę postępowania z incydentami bezpieczeństwa, obejmującą klasyfikację dotkliwości incydentu, zasady reagowania na incydent, dostępność członków zespołu, zasady komunikacji z autorem zgłoszenia incydentu bezpieczeństwa itp. Oczywistą i zasadniczą częścią tego procesu jest konieczność zapoznania się z podstawowymi zasadami uzgodnionymi przez społeczność CSIRT i przestrzegania ich.

Na samym początku tworzenia zespołu CERT/CSIRT konieczne jest także zbudowanie jego zaplecza technicznego i organizacyjnego, bez którego żaden zespół nie może skutecznie funkcjonować.

Przez zaplecze techniczne rozumiemy np. narzędzie do efektywnego zarządzania zgłoszeniami incydentów bezpieczeństwa, które pozwoli śledzić cały cykl życia incydentu, tj. kiedy zgłoszenie zostało wysłane, przez kogo, kto i na jakim etapie zajmował się incydentem, dlaczego, jak został potraktowany, kto poprosił o współpracę, jak poważny był to incydent i jakie procedury eskalacji zostały do niego zastosowane itp. W tym obszarze zespoły zazwyczaj korzystają z różnych tzw. systemów biletowych, np. RTIR[1] , OTRS[2] . Innymi ważnymi pomocnikami w dziedzinie narzędzi technicznych są różne systemy wykrywania włamań (IDS), systemy audytu bezpieczeństwa sieci i urządzeń, systemy analizy kryminalistycznej, monitorowanie ruchu sieciowego (netflow) itp.

Zaplecze organizacyjne to wspomniana wcześniej "gotowość" do rozwiązania problemu, czyli określenie podstawowych zasad działania zespołu, tak aby każdy członek zespołu znał swoją rolę, obowiązki i odpowiedzialność, politykę postępowania w przypadku wystąpienia incydentów bezpieczeństwa, zasady komunikacji, udostępniania i wymiany informacji, współpracy itp. Podstawą w tej dziedzinie jest na ogół dobrze zarządzane tzw. ***zarządzanie incydentami.***

Gdy powstający zespół opanuje powyższe umiejętności, tzn. będzie w stanie opisać i przedstawić siebie i swoje działania, może podjąć współpracę krajową i międzynarodową.

---

[1] **RTIR** - **Śledzenie** zgłoszeń dotyczących reagowania na incydenty. Więcej informacji na ten temat można znaleźć np. na stronie: http://www.bestpractical.com/rtir/.

[2] **OTRS** - Otwarty źródłowy **system** zgłaszania zgłoszeń. Więcej szczegółów można znaleźć np. na stronie: http://www.otrs.org/.

2.4. Współpraca w zakresie infrastruktury CERT/CSIRT

Zespoły CERT/CSIRT są tworzone na zasadzie dobrowolności, a w ich interesie leży efektywne komunikowanie się ze sobą, wymiana istotnych informacji i wiedzy oraz współpraca. Dlatego zrzeszają się w organizacjach międzynarodowych. Obecnie najbardziej znanymi i najaktywniejszymi organizacjami zajmującymi się tym zagadnieniem i tworzącymi odpowiednie środowisko do realizacji wyżej wymienionych celów są międzynarodowa organizacja **GÉANT**[1] oraz **FIRST** (Forum for Incident Response and Security Teams)[2] .

Obie wyżej wymienione organizacje inicjują i ułatwiają regularne spotkania członków zespołów bezpieczeństwa, wymianę doświadczeń oraz uczestniczą w określaniu podstawowych zasad współpracy i komunikacji pomiędzy światowymi zespołami CERT/CSIRT.

GÉANT, organizacja europejska, prowadzi kilka działań, w których zainteresowane zespoły CERT/CSIRT mogą uczestniczyć:

· **TF-CSIRT** (Task Force for CSIRT) to grupa robocza, która umożliwia zespołom współpracę w ramach regularnych, dwudniowych spotkań odbywających się 3 razy w roku (gospodarzem spotkania jest zwykle zespół CERT/CSIRT). Więcej informacji można znaleźć na stronie: https://tf-csirt.org/.

· **Szkolenie CSIRT** - służy do szkolenia nowych członków zespołu CSIRT/CERT lub tych, którzy zamierzają założyć zespół CERT/CSIRT. Zwykle odbywają się one dwa razy w roku, a trenerami są doświadczeni członkowie renomowanych zespołów CERT/CSIRT oraz inni najlepsi eksperci ds. bezpieczeństwa. Więcej informacji można znaleźć na stronie: https://tf-csirt.org/transits/.

· **Trusted Introducer**[3] - biuro, którego głównym zadaniem jest budowanie zaufania pomiędzy zespołami CERT/CSIRT oraz pomoc w nawiązywaniu nowych. Więcej informacji można znaleźć na stronie: https://www.trusted-introducer.org/.

Oprócz corocznej, dużej konferencji FIRST organizuje szereg szkoleń, opracowuje wytyczne i standardy dla efektywnych zespołów CERT/CSIRT i oczywiście współpracuje z TF-CSIRT.

W ramach globalnej infrastruktury zespołów CERT/CSIRT organizacje GÉANT i FIRST działają jako swego rodzaju "gwarancja", że zespół podający się za zespół CERT/CSIRT rzeczywiście nim jest i że deklarowany przez niego model postępowania jest prawdziwy. Każdy nowy zespół, który chce dołączyć do infrastruktury bezpieczeństwa, przechodzi przez proces indukcji, który sprawdza, czy zespół spełnia standardy społeczności, jest przejrzysty i czy nie ma istotnych powodów, aby go nie przyjąć. W przypadku infrastruktury europejskiej (platforma TF-CSIRT) procesem wpisywania zajmuje się Zaufany Wprowadzający, a nowy zespół faktycznie składa do Zaufanego Wprowadzającego wniosek o wpisanie na listę zespołów i przyznanie statusu zespołu wpisanego na ***listę***.***[4]***

Wśród istniejących drużyn muszą być co najmniej dwie drużyny (zwane sponsorami), które będą wspierać nową drużynę, a żadna z istniejących drużyn nie może sprzeciwić się jej przyjęciu. Jeśli wszystko się powiedzie, informacje o nowej drużynie są zapisywane na liście prowadzonej przez biuro TI (a niektóre z nich są upubliczniane), drużyna uzyskuje status drużyny ***notowanej,*** a społeczność wita nowego członka.

W przypadku FIRST procedura przystąpienia jest bardzo podobna, ale kończy się uzyskaniem ***członkostwa, a*** nie statusu.

Oba procesy mają jedną wspólną cechę - chodzi o to, aby dowiedzieć się i udostępnić jak najwięcej informacji o zespole, opisać jego zachowanie i sposób postrzegania kwestii obsługi incydentu bezpieczeństwa, tak aby odpowiadał on wymaganiom społeczności.

W przypadku Trusted Introducer możliwe jest uzyskanie innych, ważniejszych statusów: ***akredytowanego*** i ***certyfikowanego.*** Różnice są następujące:

· Zespół, który znalazł się na ***liście,*** podał podstawowe informacje o sobie, zadeklarował chęć działania jako zespół CSIRT i został zaakceptowany przez społeczność.

· Zespół posiadający status ***akredytowanego*** deklaruje pożądany przez społeczność poziom praktyki i zobowiązuje się do przestrzegania wspólnych zasad TI.

· Następnie ***certyfikowany*** zespół wykazał swój "poziom dojrzałości" w procesie certyfikacji.

Bycie ***akredytowanym*** lub ***certyfikowanym*** zespołem wymaga ciągłych starań o utrzymanie statusu zespołu. Częścią tego wysiłku jest obowiązek aktualizowania informacji o drużynie w spisie TI. Nieprzestrzeganie tych zasad w dłuższej perspektywie może doprowadzić do utraty statusu drużyny, a w najgorszym wypadku do jej wydalenia ze społeczności. Obowiązek ten dotyczy także zespołów ***wpisanych na listę,*** które - jeśli nie przejdą procesu akredytacji w ciągu trzech lat od wpisania na listę - muszą odnowić swój status na liście, wykazując się wsparciem ze strony innych zespołów (tj. proces ponownego wpisania na listę). Mechanizm ten gwarantuje, że informacje zawarte w wykazie TI są w wysokim stopniu aktualne, a przez to wiarygodne.

Inną organizacją działającą w dziedzinie bezpieczeństwa jest **ENISA** (Europejska Agencja Bezpieczeństwa Sieci i Informacji), http://www.enisa.europa.eu/). Współpracuje ona ściśle z państwami członkowskimi UE i sektorem prywatnym, a jej zakres obejmuje szereg działań, w tym ogólnoeuropejskie ćwiczenia w zakresie bezpieczeństwa cybernetycznego, opracowywanie krajowych strategii

bezpieczeństwa cybernetycznego, współpracę i budowanie potencjału zespołów CERT/CSIRT, zajmowanie się kwestiami ochrony danych osobowych oraz prace nad opracowywaniem i wdrażaniem przepisów dotyczących bezpieczeństwa sieci i informacji.

Wszystkie trzy organizacje mają jeszcze jedną wspólną funkcję - gromadzą know-how od całej społeczności i umożliwiają dzielenie się nim (poprzez formułowanie dokumentów dotyczących najlepszych praktyk, wytycznych, zaleceń).

---

[1]Stowarzyszenie powstało w wyniku połączenia TERENY (Trans-European Research and Education Networking Association) i DANTE.

[2] Więcej informacji na temat FIRST można znaleźć na stronie: https://www.first.org.

[3] Dłuższy również **TI**.

[4] ***Listed -*** umieszczenie lub dosłowne "wpisanie" drużyny do bazy danych wszystkich zarejestrowanych drużyn.

2.5. Hierarchia zespołów CERT/CSIRT?

Zespoły CERT/CSIRT nie mają oficjalnej hierarchii, która czyniłaby jeden zespół lepszym od drugiego. Wszystkie zespoły są równe pod względem funkcjonowania, komunikacji, współpracy i wymiany informacji i nie są w tych obszarach ograniczone. Istnienie tzw. najlepszych zespołów *narodowych* i *rządowych sprawia* wrażenie, że istnieje wyższość między zespołami, ale tak nie jest. Jedyną "wyższość", choć właściwsze byłoby określenie "większe możliwości działania", daje najwyższemu zespołowi ustawodawstwo danego kraju, które reguluje jego uprawnienia (np. w zakresie wymaganej reakcji na zagrożenia bezpieczeństwa ze strony operatorów sieci i służb itp.)

W świecie zespołów CERT/CSIRT kluczowa jest gotowość do dzielenia się ważnymi informacjami o incydentach i zagrożeniach. Wymaga to, aby zespoły ufały sobie nawzajem, a użytkownicy ufali swoim zespołom. Zdobycie zaufania użytkowników i społeczności jest zadaniem długoterminowym, a zespoły muszą wykazać się odpowiednimi cechami we wszystkich aspektach swojej działalności i stopniowo budować zaufanie - nie tylko do swoich możliwości pomocy, ale także do zdolności zapewnienia poufności i uczciwego traktowania udostępnianych danych, przejrzystości postępowania itp.

2.6. Krajowe i rządowe zespoły CERT/CSIRT

Szczególną formą zespołów CERT/CSIRT są zespoły krajowe i rządowe. Współpracują z innymi zespołami CERT/CSIRT jak równy z równym, ale ich rola w całym systemie jest inna.

Krajowy CERT/CSIRT działa jako ostatnia deska ratunku - ostatnia instancja, do której można zwrócić się o interwencję, pomoc i interwencję. Jej celem jest (w kraju lub regionie, w którym działa) pośredniczenie w kontakcie między zaatakowanym a sprawcą problemu oraz ułatwianie pomyślnego rozwiązania problemu. Zespoły narodowe nie kontrolują (zazwyczaj) infrastruktury fizycznej, więc nie mają (w przeciwieństwie do zespołów wewnętrznych/instytucjonalnych) możliwości bezpośredniej interwencji. Ich rolą jest pośredniczenie w kontaktach lub koordynowanie (stąd nazwa zespół koordynacyjny) działań różnych podmiotów, gdy problem jest większy i wymaga współpracy kilku podmiotów.

Zgodnie z zasadą działania całej struktury, incydenty, które przechodzą przez krajowy system CSIRT, stanowią zwykle tylko ułamek ogólnej liczby. Większość incydentów jest rozwiązywana w drodze bezpośredniej komunikacji, bez konieczności eskalacji i mediacji. Oznacza to, że do zespołu krajowego trafiają głównie incydenty, których nie da się rozwiązać w inny sposób (osoby odpowiedzialne odmawiają ich rozwiązania, niełatwo jest ustalić, kto jest odpowiedzialny za ich rozwiązanie), bardzo poważne lub powtarzające się problemy, problemy, które mogą mieć szeroki zasięg itp.

Krajowy zespół CERT/CSIRT zazwyczaj ma w swoim zakresie obowiązków edukację i współpracę. Obejmuje to zarówno edukację publiczną, jak i pracę w ramach infrastruktury internetowej. Celem jest wspieranie tworzenia innych zespołów CERT/CSIRT w kraju, inicjowanie ich działalności na arenie międzynarodowej oraz wspieranie wdrażania standardowych praktyk i procedur. Wszystko to znacznie zwiększa przejrzystość środowiska i daje osobom atakowanym szansę na skuteczne dochodzenie roszczeń.

Rządowe **zespoły CERT/CSIRT** zazwyczaj koncentrują się na administracji państwowej i samorządowej oraz na reagowaniu na incydenty zagrażające bezpieczeństwu państwa i jego służb. Rządowy CERT/CSIRT może mieć formę wewnętrznego zespołu zdolnego do bezpośredniej interwencji w przypadku wystąpienia problemu. Jego istnienie jest zwykle poparte przepisami prawa.

Nie jest to jednak dogmat; sytuacja różni się w zależności od kraju. Istnieją kraje, w których istnieje tylko drużyna narodowa (i działa ona także jako drużyna rządowa), istnieją kraje, w których istnieje drużyna rządowa (i działa ona jako drużyna narodowa), istnieją kraje, w których istnieją obie te drużyny, istnieją kraje, w których nie ma żadnej z nich, a rolę drużyny najwyższej zastępuje jedna z istniejących drużyn itd.

2.7. Sytuacja w Republice Czeskiej i na świecie

Obecnie na całym świecie oficjalnie działa około 380 zespołów bezpieczeństwa CERT/CSIRT, które są członkami FIRST lub europejskiej platformy TFCSIRT -(lub obu).

W Republice Czeskiej oficjalnie utworzono 39 zespołów bezpieczeństwa CERT/CSIRT, które zostały uznane przez urząd Trusted Intoducer, co sprawia, że Czechy są niemal światowym "supermocarstwem", a pod względem liczebności konkurują tylko z Francją, Niemcami i Wielką Brytanią. Nie chodzi tu oczywiście o ilość, ale przede wszystkim o jakość.

Pierwszym zespołem ds. bezpieczeństwa typu CERT/CSIRT, który powstał w Republice Czeskiej, jest zespół ds. bezpieczeństwa **CESNET-CERTS** (https://csirt.cesnet.cz/). Została ona oficjalnie założona w 2003 roku, a w styczniu 2004 roku została oficjalnie uznana przez międzynarodową infrastrukturę i urząd Trusted Introducer. Jest on obsługiwany przez stowarzyszenie CESNET[1] i odpowiada za obsługę i koordynację rozwiązywania problemów związanych z bezpieczeństwem w -e-infrastrukturze CESNET. Opracowuje m.in. narzędzia bezpieczeństwa i świadczy usługi uświadamiające dla użytkowników w swojej strefie wpływów.

Inne zespoły zostały utworzone w stowarzyszeniu CZ.NIC (CZ.NIC-CSIRT) w 2008 r., na Uniwersytecie Masaryka w Brnie (CSIRT-MU) w 2009 r., w Active24 (zespół Active24-CSIRT) w 2012 r. oraz w ramach projektu wspieranego przez Ministerstwo Spraw Wewnętrznych Republiki Czeskiej zespół CSIRT.CZ (od 2011 r. Narodowy CSIRT Republiki Czeskiej).

Duży rozkwit w dziedzinie budowania zespołów CERT/CSIRT ds. bezpieczeństwa można zaobserwować w Czechach szczególnie od 2013 r., kiedy to Republika Czeska stanęła w obliczu serii ataków DDoS na publiczne serwisy www. Wydarzenie to zapoczątkowało następnie powstanie projektu Fenix (https://fe.nix.cz/) w czeskim centrum peeringowym NIX.CZ.

Celem tego projektu jest zapewnienie dostępności usług internetowych w podmiotach zaangażowanych w to działanie w przypadku ataku DoS. W projekcie Fenix określono szereg zasad technicznych i organizacyjnych, które muszą być spełnione przez podmioty zainteresowane przystąpieniem do projektu, a jedną z nich jest oficjalnie ukonstytuowany CERT/CSIRT. Dla wielu organizacji stało się to bodźcem do sformalizowania swoich zespołów ds. bezpieczeństwa jako zespołów CERT/CSIRT i włączenia ich do międzynarodowej infrastruktury.

Innym bodźcem motywacyjnym, który doprowadził do powstania nowych zespołów, było przyjęcie i późniejsze wprowadzenie w życie ustawy o bezpieczeństwie cybernetycznym. Wiele organizacji uświadomiło sobie, że bezpieczeństwo jest wartościowym zagadnieniem i że istnieją korzyści z utworzenia zespołu typu CERT/CSIRT.

Obecna infrastruktura zespołów CERT/CSIRT w Republice Czeskiej, licząca 39 zespołów, składa się z zespołów krajowych i rządowych, zespołów na poziomie dużych dostawców usług internetowych, kilku zespołów w sektorze akademickim, zespołów w sektorze bankowym, w firmach informatycznych, u rejestratorów domen i wreszcie w czeskim centrum peeringowym NIX.CZ, w stowarzyszeniu CZ.NIC. Podsumowując, jest to bardzo zróżnicowana i ostatecznie solidna i sprawna infrastruktura, w której nie brakuje doświadczeń z różnych sektorów.

Aktualną listę czeskich zespołów CERT/CSIRT można znaleźć pod adresem: https://tiw.trusted-introducer.org/directory/country_LICSA.html.

---

[1]Stowarzyszenie CESNET, z. s. p. o., jest stowarzyszeniem osób prawnych, założonym w 1996 r. przez uniwersytety i Akademię Nauk Republiki Czeskiej. Jest operatorem krajowej szybkiej sieci komputerowej na potrzeby nauki, badań, rozwoju i edukacji CESNET2. Więcej informacji można znaleźć na stronie http://www.cesnet.cz/.

2.8. Krajowy CSIRT Republiki Czeskiej

W grudniu 2010 roku w Republice Czeskiej oficjalnie utworzono Krajowy CSIRT Republiki Czeskiej. Stowarzyszenie CZ.NIC i Ministerstwo Spraw Wewnętrznych podpisały (16 grudnia 2010 r.) Memorandum, na mocy którego administrator czeskiej domeny narodowej stowarzyszenia CZ.NIC przejął agendę zespołu CSIRT.CZ i od stycznia 2011 r. prowadzi go jako Krajowy CSIRT Republiki Czeskiej w imieniu Ministerstwa Spraw Wewnętrznych.

CSIRT.CZ (http://www.csirt.cz/) został założony w ramach grantu Ministerstwa Spraw Wewnętrznych *Republiki* Czeskiej *"Cyberzagrożenia z punktu widzenia interesów bezpieczeństwa Republiki Czeskiej"* (kod identyfikacyjny projektu VD20072010B013) i zbudowany przez stowarzyszenie CESNET. To miejsce pracy zostało określone jako modelowe miejsce pracy i zostało zbudowane w celu sprawdzenia stanu infrastruktury bezpieczeństwa w Republice Czeskiej oraz sprawdzenia możliwości zbudowania rozproszonej hierarchii systematycznego rozwiązywania problemów bezpieczeństwa w sieciach komputerowych w Republice Czeskiej przez zespoły CSIRT. Działalność tego zespołu została oficjalnie zainaugurowana 3 kwietnia 2008 r., a w maju tego samego roku został on przedstawiony innym europejskim zespołom CERT/CSIRT na spotkaniu społeczności TF-CSIRT (które odbyło się w Oslo w Norwegii) jako obiekt typu CSIRT pełniący rolę *"ostatniej szansy"* dla Republiki Czeskiej i został zaakceptowany przez społeczność.

CSIRT.CZ stworzył podstawy do dalszego rozwoju infrastruktury CERT/CSIRT najwyższego szczebla w Republice Czeskiej, zwłaszcza w zakresie współpracy. Zweryfikowało to również i potwierdziło założenie, że istnienie zespołów CERT/CSIRT najwyższego szczebla w Czechach ma sens.

Krajowy CSIRT Republiki Czeskiej wykonuje również inne zadania KB.

2.9. Rządowy CERT Republiki Czeskiej

W dniu 19 października 2011 r. rząd Republiki Czeskiej przyjął uchwałę nr 781 ustanawiającą Biuro Bezpieczeństwa Narodowego (NSA) jako agencję wiodącą w zakresie bezpieczeństwa cybernetycznego w Republice Czeskiej oraz organ krajowy w tej dziedzinie. Od początku swojego powołania KBN koncentruje się na trzech zadaniach - napisaniu ustawy o cyberbezpieczeństwie, budowie NCKB (Narodowego Centrum Cyberbezpieczeństwa) oraz budowie rządowego CERT-u Republiki Czeskiej.

Rządowy zespół CERT Republiki Czeskiej, GovCERT.CZ, został włączony do społeczności międzynarodowej w 2012 r., w związku z czym Republika Czeska należy do krajów, które posiadają zarówno krajowy, jak i rządowy zespół CERT/CSIRT.

GovCERT.CZ jest odpowiedzialny za sieci administracji państwowej, samorządowej i infrastruktury krytycznej Republiki Czeskiej. Zespół zajmuje się również rozwojem i funkcjonowaniem służb bezpieczeństwa, edukacją oraz jest zaangażowany we współpracę krajową i międzynarodową.

Rządowy CERT Republiki Czeskiej wykonuje także inne zadania.

2.10. Z którym zespołem CERT/CSIRT należy się skontaktować?

Tytuł tego podrozdziału to także częsta skarga internauty, który znalazł się w kłopotach (np. został zaatakowany, skradziono mu tożsamość, zhakowano jego profil na Facebooku lub konto poczty elektronicznej, był świadkiem rozpowszechniania pornografii dziecięcej). Co powinien zrobić taki użytkownik? Skontaktować się z policją czeską? Czy też do dostawcy połączenia, np. do jego działu pomocy technicznej? Czy też do Krajowego Biura ds. Cyberbezpieczeństwa i Informacji, ponieważ jest to organ odpowiedzialny za bezpieczeństwo cybernetyczne? Na infolinię Národního centra bezpečnějšího internetu? A może do jakiegoś zespołu CSIRT, skoro ciągle o nich mówią? Ale który z nich?

Proces zgłaszania i rozwiązywania incydentów bezpieczeństwa (a właściwie "z kim mam się skontaktować, aby zgłosić lub rozwiązać incydent bezpieczeństwa") **można rozpatrywać z dwóch perspektyw.** Z perspektywy techników (administratorów sieci i usług, członków zespołów ds. bezpieczeństwa) oraz z perspektywy użytkowników.

Dla techników (administratorów sieci i usług, członków zespołów ds. bezpieczeństwa) odpowiedź na pytanie "do kogo właściwie powinienem się zgłosić z prośbą o podjęcie działań" jest dość oczywista, ale wynika to z zapału, doświadczenia, a przede wszystkim bardzo dobrej znajomości środowiska internetowego i jego podstawowych zasad, a także wiedzy, gdzie można znaleźć informacje kontaktowe dotyczące poszczególnych istniejących sieci, usług, domen itp.

Dla członków zespołów CERT/CSIRT podstawowym źródłem informacji kontaktowych są bazy danych RIR, bazy danych TLD oraz katalogi zespołów CERT/CSIRT.

Rejestry **RIR** (Regional Internet Registries) przechowują i udostępniają informacje o tym, komu przydzielono dany blok adresów IP. Świat jest podzielony na regiony i każdy RIR (obecnie RIPE, ARIN, APNIC, LACNIC, AFRINIC) przydziela adresy IP dla swojego regionu. Region Europy, Bliskiego Wschodu i części Azji jest zarządzany przez RIPE NCC (https://www.ripe.net/). Biura RIR prowadzą publicznie dostępne bazy danych, które zawierają dane o przydzielonych sieciach internetowych i ich administratorach. Te bazy danych umożliwiają sprawdzenie, która organizacja i którzy administratorzy są odpowiedzialni za konkretne adresy IP.

Innym źródłem przydatnych informacji są dane o domenach obsługiwanych i udostępnianych przez administratorów domen najwyższego poziomu, w przypadku TLD .cz jest to stowarzyszenie CZ.NIC.

Do tego dochodzą zespoły CERT/CSIRT, które zwykle określają swój obszar działania za pomocą identyfikatorów internetowych, domen nazw lub po prostu słownie. Ze względu na ich liczbę, sposób definiowania zakresu działania, a zwłaszcza różnice w ich poziomie, nie zawsze łatwo jest znaleźć zespół, który byłby w stanie pomóc. Aby ułatwić nawigację między zespołami, stworzono swego rodzaju "katalogi", które są prowadzone przez FIRST i Biuro Zaufanego Przedstawiciela. Katalogi te zawierają podstawowe informacje o zespołach CERT/CSIRTech, ich kontaktach, zakresie działania itp.

Proces zgłaszania i rozwiązywania incydentów bezpieczeństwa (technicznie rzecz biorąc - ***obsługa incydentów***) nie jest procesem ścisłym, wręcz przeciwnie, i wiele zależy od doświadczenia, a czasem nawet kreatywności osoby, która ten proces realizuje. Wymiana informacji między zespołami jest zazwyczaj szybka i sprawna, choć i to często nie gwarantuje szybkiego rozwiązania problemu, gdyż cała infrastruktura jest jeszcze dość "uboga" w tym zakresie, a niestety trzeba powiedzieć, że poziom zespołów jest również różny.

Optymalnym stanem infrastruktury byłoby, gdyby każdy adres IP znajdował się w zasięgu działania oficjalnego zespołu CSIRT. W tej sytuacji jednak infrastruktura zespołów CERT/CSIRT jest daleka od istnienia.

Z perspektywy zwykłego użytkownika sytuacja jest bardzo niejasna i wręcz myląca. Co zatem powinien zrobić użytkownik w przypadku incydentu bezpieczeństwa i z kim powinien się skontaktować? Trudno wymagać od użytkownika, aby wiedział o zespołach CERT/CSIRT, znalazł właściwy, zapoznał się z jego polityką zgłaszania incydentów bezpieczeństwa i podjął odpowiednie działania. W pierwszej kolejności użytkownik powinien skontaktować się ze swoim administratorem sieci lub serwisu (jeśli go posiada) albo skontaktować się z dostawcą połączenia, tj. z działem pomocy technicznej dostawcy usług internetowych lub jego działem obsługi użytkownika. Po stronie dostawcy usług internetowych powinien istnieć jasno opisany punkt dostępu (kontakt) dla użytkowników, do którego użytkownicy mogą i powinni się zwracać w przypadku, gdy są celem ataku, odkryją incydent bezpieczeństwa lub mają poczucie, że coś jest nie tak. Dlatego środowisko dostawców usług internetowych jest jednym z najważniejszych obszarów, w którym powinien zostać powołany oficjalny zespół CERT/CSIRT, świadczący usługi bezpieczeństwa dla użytkowników ich sieci.

Oczywiście mogą zdarzyć się sytuacje, w których zarówno technik, jak i użytkownik robią wszystko jak należy, a rozwiązania nie widać. Osoba lub zespół nie reaguje na zgłoszony problem lub wręcz odmawia zajęcia się nim (twierdząc, że to nie ich problem lub że nie jest on aż tak poważny) itp. W tym momencie do akcji wkracza policja czeska (użytkownik może się z nią skontaktować, aby złożyć skargę karną), albo najwyższa instancja (krajowa lub rządowa), do której użytkownik może się zwrócić w ostateczności i od której może oczekiwać pomocy i reakcji.

Pomiędzy zespołem krajowym a rządowym istnieje bardzo ścisła współpraca i wymiana informacji oraz istotnych danych, a zatem przekazywanie zgłoszonego problemu do rozwiązania przez jeden zespół drugiemu lub bezpośrednia współpraca nad rozwiązaniem.

Zespoły krajowe i rządowe powinny być miejscem, do którego operatorzy sieci, służby (a w razie potrzeby także użytkownicy) mogą zwracać się o pomoc i konsultacje w przypadku problemów, niejasności itp., np. znalezienie odpowiedniego partnera do komunikacji (zagraniczny zespół CERT/CSIRT), pośredniczenie w komunikacji (tak, czasem przydaje się "dźwignia" ze strony najwyższego zespołu, partner jest wtedy bardziej chętny) oraz źródło know-how i informacji.

Ogólnie rzecz biorąc, byłoby jednak pożądane, aby administratorzy sieci i usług oraz członkowie zespołów ds. bezpieczeństwa opanowali i stosowali zasady procesu *obsługi incydentów* oraz zmaksymalizowali komunikację bezpośrednio (nie za pośrednictwem zespołów wyższego szczebla). Dzięki temu proces obsługi incydentów przebiega szybko i sprawnie; dodatkowe etapy pośrednie mogą powodować nieprzyjemne opóźnienia i, niestety, zniekształcenia. Jak jednak wspomniano, zależy to od powagi sytuacji i problemu, który ma być rozwiązany.

Centra **CERT/CSIRT i ich infrastruktura na ogół nie są wszechstronne i nie reprezentują bezpieczeństwa "w pigułce".**

Ich istnienie to tylko jeden z kamieni milowych w obszarze budowania bezpieczeństwa Internetu, w którym ważną rolę odgrywają wszystkie zainteresowane strony, a więc administratorzy sieci i usług, menedżerowie decydujący o podstawach skutecznego zabezpieczenia sieci i usług, dostawcy usług internetowych, operatorzy usług krytycznych, służby bezpieczeństwa, państwo i wreszcie my - użytkownicy.

Aktualną listę zespołów CSIRT/CERT można znaleźć na stronie:

https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map .

2.11. PODSUMOWANIE

· Różnica między zwykłym zespołem ds. bezpieczeństwa a zespołem CERT/CSIRT polega głównie na zaangażowaniu w globalną infrastrukturę bezpieczeństwa, wymianie informacji w ramach tej infrastruktury oraz przestrzeganiu ustalonych procedur formalnych.

· Podstawowym wymogiem społeczności jest publiczne ogłoszenie przez zespół CERT/CSIRT swoich danych kontaktowych i zasad działania:

  - o który jest jego operatorem,
  - o którzy są jego członkami,
  - o jak i kiedy można skontaktować się z zespołem,
  - o jakie usługi oferuje,
  - o Zakres (numer AS[1] , sieć, domeny, usługi), w którym zespół jest uprawniony do działania i w jaki sposób, tzn. określenie jego uprawnień i odpowiedzialności. Na podstawie zakresu działania zespół jest następnie kontaktowany (np. przez atakowanego) i rozwiązuje odpowiednie problemy (incydenty).

· Zakres działania zespołu - określa, za co zespół jest odpowiedzialny i jaka jest jego rola. To oczywiście zależy od tego, jaki to jest zespół. Możliwe jest utworzenie zespołów o mniej więcej następujących typach:

  - o wewnętrzny - obsługuje i odpowiada za konkretną sieć (np. za określony zakres adresów IP, domen), zwykle jest tworzony przez operatora sieci,
  - o koordynacja - zespół, którego głównym zadaniem jest koordynowanie rozwiązywania incydentów bezpieczeństwa, a nie ich rozwiązywanie,
  - o sprzedawca - zespół zajmujący się incydentami bezpieczeństwa, które dotyczą konkretnego produktu (SW),
  - o krajowe, rządowe - specjalne przypadki oparte na zasadach dwóch pierwszych wymienionych zespołów (wewnętrzny i koordynacyjny), ich zakres i rola zależy od założyciela, a często także od ustawodawstwa danego kraju.

· Zespoły CERT/CSIRT nie mają oficjalnej hierarchii, która czyniłaby jeden zespół lepszym od drugiego. Wszystkie zespoły są równe pod względem funkcjonowania, komunikacji, współpracy i wymiany informacji i nie są w tych obszarach ograniczone.

· Krajowy CERT/CSIRT działa jako ostatnia deska ratunku - ostatnia instancja, do której można zwrócić się o interwencję, pomoc i interwencję.

· Rządowe zespoły CERT/CSIRT zazwyczaj koncentrują się na administracji państwowej i samorządowej oraz na reagowaniu na incydenty zagrażające bezpieczeństwu państwa i jego służb. Rządowy CERT/CSIRT może mieć formę wewnętrznego zespołu zdolnego do bezpośredniej interwencji w przypadku wystąpienia problemu. Jego istnienie jest zwykle poparte przepisami prawa.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

· Zespół CSIRT

· Zespół CERT

· Obsługa incydentów

· Hierarchia zespołów

· Zakres

PYTANIA KONTROLNE

- Co to jest zespół CSIRT/CERT?
- W jaki sposób tworzy się i powołuje zespół CSIRT/CERT?
- Na czym skupia się krajowy zespół CSIRT?
- Na czym skupia się rządowy zespół CSIRT?
- Jakie są podstawowe wymagania społeczności lokalnej wobec zespołu CERT/CSIRT?

---

[1] **AS** - Autonomous System (system autonomiczny). System autonomiczny to zbiór sieci IP i routerów pod wspólnym zarządem technicznym, który reprezentuje wspólną politykę routingu w Internecie.

3. Ramy prawne CSIRT/CERT

W dniu 6 lipca 2016 r. została przyjęta przez Parlament Europejski Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii (Dyrektywa NIS).

W dyrektywie w sprawie bezpieczeństwa sieci i informacji przewidziano środki prawne mające na celu podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego w UE poprzez zapewnienie:

· gotowości państw członkowskich poprzez wymaganie od nich odpowiedniego wyposażenia. Na przykład zespołu reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT) i właściwym krajowym organem ds. bezpieczeństwa sieci i informacji,

· współpracy między wszystkimi państwami członkowskimi poprzez utworzenie Grupy Współpracy, która będzie wspierać i ułatwiać współpracę strategiczną i wymianę informacji między państwami członkowskimi.

· kultury bezpieczeństwa w sektorach, które mają kluczowe znaczenie dla naszej gospodarki i społeczeństwa, a ponadto w znacznym stopniu opierają się na TIK, takich jak energetyka, transport, gospodarka wodna, bankowość, infrastruktura rynków finansowych, opieka zdrowotna i infrastruktura cyfrowa.

Przedsiębiorstwa określone przez państwa członkowskie jako podmioty świadczące usługi podstawowe w wyżej wymienionych sektorach będą musiały podjąć odpowiednie środki bezpieczeństwa i powiadamiać właściwe organy krajowe o poważnych incydentach. Kluczowi dostawcy usług cyfrowych, tacy jak wyszukiwarki, usługi przetwarzania w chmurze i rynki internetowe, będą musieli spełnić wymogi dotyczące bezpieczeństwa i powiadamiania określone w nowej dyrektywie.

W oparciu o znaczące postępy poczynione w ramach europejskiego forum państw członkowskich w zakresie wspierania dyskusji i wymiany dobrych praktyk politycznych, w tym opracowania zasad europejskiej współpracy w sytuacjach kryzysów cybernetycznych, należy powołać grupę współpracy, w skład której wejdą przedstawiciele państw członkowskich, Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ("ENISA"), w celu wspierania i ułatwiania strategicznej współpracy między państwami członkowskimi w zakresie bezpieczeństwa sieci i systemów informatycznych. Aby grupa ta była skuteczna i obejmowała wszystkich, konieczne jest, by wszystkie państwa członkowskie dysponowały minimalnymi zdolnościami i strategią zapewniającą wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium. Ponadto wymogi dotyczące bezpieczeństwa i powiadamiania powinny mieć zastosowanie do operatorów usług podstawowych i dostawców usług cyfrowych, aby promować kulturę zarządzania ryzykiem i zapewnić zgłaszanie najpoważniejszych incydentów.

Istniejące możliwości nie są wystarczające, aby zapewnić wysoki poziom bezpieczeństwa sieci i systemów informacyjnych w Unii. Państwa członkowskie mają bardzo zróżnicowane poziomy gotowości, co doprowadziło do fragmentarycznego podejścia w całej Unii. Powoduje to nierówny poziom ochrony konsumentów i przedsiębiorstw oraz osłabia ogólny poziom bezpieczeństwa sieci i systemów informacyjnych w Unii. Brak wspólnych wymogów dla operatorów usług podstawowych i dostawców usług cyfrowych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii. Uniwersytety i ośrodki badawcze mają do odegrania decydującą rolę w stymulowaniu badań, rozwoju i innowacji w tych dziedzinach.

Dyrektywa UE w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) ma na celu utworzenie sieci CSIRT "w celu przyczynienia się do rozwoju zaufania między państwami członkowskimi oraz promowania szybkiej i skutecznej współpracy operacyjnej". Dyrektywa stanowi, że każde państwo członkowskie wyznacza jeden lub więcej CSIRT spełniających wymogi określone w pkt 1 załącznika I do dyrektywy (wymogi), obejmujących co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III, odpowiedzialnych za obsługę ryzyka i incydentów zgodnie z dobrze zdefiniowanym procesem.

Dyrektywa NIS ma na celu utworzenie sieci CSIRT "w celu przyczynienia się do rozwoju pewności i zaufania między państwami członkowskimi oraz promowania szybkiej i skutecznej współpracy operacyjnej". Dyrektywa stanowi, że każde państwo członkowskie wyznacza jeden lub więcej CSIRT, które muszą spełniać zestaw określonych wymogów wysokiego szczebla. [1]

Zgodnie z art. 9 NIS stanowi:

"Każde państwo członkowskie wyznacza co najmniej jeden CSIRT spełniający wymogi określone w załączniku I pkt 1, obejmujący co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III, odpowiedzialny za obsługę ryzyka i incydentów zgodnie z dobrze zdefiniowanym procesem. CSIRT może zostać utworzony w ramach właściwego organu.

I NISD nadal tak twierdzi:

· *CSIRTS posiadają odpowiednie zasoby, aby skutecznie realizować swoje zadania*

· *Państwa członkowskie zapewniają skuteczną, wydajną i bezpieczną współpracę swoich CSIRT.*

· *Państwa członkowskie zapewniają swoim CSIRT dostęp do odpowiedniej, bezpiecznej i odpornej infrastruktury komunikacyjnej i informacyjnej na szczeblu krajowym.*

· *Państwa członkowskie informują Komisję o kompetencjach i głównych elementach procesu obsługi incydentów w swoich CSIRT.*

· *Państwa członkowskie mogą zwrócić się do ENISA o pomoc w tworzeniu krajowych CSIRT**[2]** .*

Załącznik I do NISD nosi tytuł *WYMAGANIA I ZADANIA ZESPOŁÓW REAGOWANIA NA INCYDENTY BEZPIECZEŃSTWA KOMPUTEROWEGO (CSIRT)* i został tu przytoczony w całości ze względu na jego duże znaczenie dla krajowej/rządowej społeczności CSIRT w UE:

(1) Wymagania dotyczące CSIRT:

(a) CSIRT zapewniają wysoki poziom dostępności swoich usług łączności, unikając pojedynczych punktów awarii, oraz dysponują kilkoma sposobami kontaktowania się z innymi i kontaktowania się z nimi przez cały czas. Ponadto kanały komunikacji powinny być jasno określone i dobrze znane okręgowi wyborczemu i partnerom współpracy.

(b) Pomieszczenia CSIRT i wspierające je systemy informacyjne są zlokalizowane w bezpiecznych miejscach.

(c) Ciągłość działania:

(i) CSIRT są wyposażone w odpowiedni system zarządzania zgłoszeniami i ich przekierowywania, aby ułatwić przekazywanie zadań.

(ii) CSIRT dysponują odpowiednią liczbą pracowników, aby zapewnić ich stałą dostępność.

(iii) CSIRT opierają się na infrastrukturze, której ciągłość jest zapewniona. W tym celu należy udostępnić redundantne systemy i zapasową przestrzeń roboczą.

(d) CSIRT mają możliwość uczestniczenia, jeżeli wyrażą taką wolę, w międzynarodowych sieciach współpracy.

(2) Zadania CSIRT:

(a) Zadania CSIRT obejmują co najmniej następujące elementy:

(i) monitorowanie incydentów na poziomie krajowym;

(ii) zapewnianie wczesnego ostrzegania, alarmowania, ogłaszania i rozpowszechniania informacji o zagrożeniach i incydentach wśród odpowiednich zainteresowanych stron;

(iii) reagowanie na incydenty;

(iv) zapewnienie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej;

(v) uczestnictwo w sieci CSIRTs.

(b) CSIRT nawiązują współpracę z sektorem prywatnym.

(c) Aby ułatwić współpracę, CSIRT promują przyjęcie i stosowanie wspólnych lub znormalizowanych praktyk w zakresie:

(i) procedury postępowania w przypadku incydentów i ryzyka;

(ii) systemy klasyfikacji incydentów, ryzyka i informacji.

---

[1] *Model oceny dojrzałości CSIRT ENISA* [online], 2019 r. WERSJA 2.0. Ateny, Grecja: Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) [cyt. 2021-03-16]. ISBN 978-92-9204-292-9. Dostępny pod adresem: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, s. 5-6.

[2] *Model oceny dojrzałości CSIRT ENISA* [online], 2019 r. WERSJA 2.0. Ateny, Grecja: Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) [cyt. 2021-03-16]. ISBN 978-92-9204-292-9. Dostępny pod adresem: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, s. 11.

3.1. Republika Czeska

Ramy prawne dla zespołów CSIRT/CERT w Republice Czeskiej są częściowo określone w ustawie o cyberbezpieczeństwie. Ustawa określa warunki istnienia krajowych i rządowych zespołów CSIRT/CERT, ale z drugiej strony nie ogranicza możliwości tworzenia i istnienia innych zespołów CSIRT/CERT.

Na podstawie ustawy o cyberbezpieczeństwie **w Republice Czeskiej obowiązkowo powoływane są dwa zespoły** CERT/CSIRT**: krajowy i rządowy**. Każdy z tych zespołów ma ściśle określone prawa i obowiązki (§ 17 i nast. ustawy o zespołach CERT).

Zespoły, których kompetencje są określone w ustawie o bezpieczeństwie cybernetycznym, są zobowiązane do przestrzegania ograniczeń określonych w tej ustawie.

3.1.1 Krajowy CERT

Krajowy zespół CERT jest określony w rozdziale 17 CCC. Równocześnie stwierdza się, że:

(1) **Krajowy zespół CERT, w zakresie określonym w niniejszej ustawie, zapewnia wymianę informacji na poziomie krajowym i międzynarodowym w dziedzinie cyberbezpieczeństwa.**

(2) **Operator krajowego zespołu CERT**

a) otrzymuje powiadomienia o danych kontaktowych od organów i osób, o których mowa w § 3 lit. a), b) i h), oraz rejestruje i przechowuje te dane,

b) przyjmuje zgłoszenia incydentów związanych z bezpieczeństwem cybernetycznym od organów i osób, o których mowa w § 3 lit. b) i h), oraz rejestruje, przechowuje i chroni te dane,

c) ocenia incydenty związane z bezpieczeństwem cybernetycznym, w które zaangażowane są organy i osoby, o których mowa w § 3 lit. b) i h),

d) zapewnia wsparcie metodologiczne, pomoc i współpracę organom i osobom, o których mowa w § 3 lit. a), b) i h), w przypadku incydentu związanego z bezpieczeństwem cybernetycznym,

e) pełnieni funkcję punktu kontaktowego dla organów i osób, o których mowa w § 3 lit. a), b) i h),

f) przeprowadza oceny podatności na zagrożenia bezpieczeństwa cybernetycznego,

g) przekazuje do Urzędu dane dotyczące incydentów naruszenia bezpieczeństwa cybernetycznego zgłoszonych zgodnie z sekcją 8 ust. 3, bez określania podmiotu zgłaszającego,

h) przekazuje EBA, na jego wniosek, dane, o których mowa w art. 16 ust. 5 i 6,

i) pełni rolę CSIRT zgodnie z odpowiednim rozporządzeniem Unii Europejskiej[1] **,**

j) informuje właściwy organ innego państwa członkowskiego, bez wskazywania zgłaszającego, o incydencie zagrażającym bezpieczeństwu cybernetycznemu, który ma znaczący wpływ na ciągłość świadczenia usługi podstawowej lub cyfrowej w tym państwie członkowskim, i jednoczesne poinformowanie o tym Urzędu, przy jednoczesnym zachowaniu bezpieczeństwa i interesów handlowych zgłaszającego,

k) współpracuje z CSIRT innych państw członkowskich; oraz

l) otrzymuje zgłoszenia incydentów w zakresie bezpieczeństwa cybernetycznego od organów i osób niewymienionych w sekcji 3 oraz, jeśli pozwalają na to jego możliwości, przetwarza je i zapewnia wsparcie metodologiczne, pomoc i współpracę organom lub osobom, których dotyczy incydent w zakresie bezpieczeństwa cybernetycznego.

(3) **Operator krajowego zespołu CERT może również prowadzić we własnym imieniu i na własną odpowiedzialność inną działalność gospodarczą w zakresie cyberbezpieczeństwa nieuregulowaną w niniejszej ustawie, pod warunkiem że działalność ta nie zakłóca wypełniania obowiązków, o których mowa w ust. 2.**

(4) **Operator krajowego zespołu CERT koordynuje swoje działania z Urzędem w zakresie wykonywania obowiązków, o których mowa w ust. 2.**

(5) **Operator krajowego CERT działa bezstronnie, wykonując swoje obowiązki na mocy podsekcji 2.**

Przepis ten definiuje instytucję krajowego centrum nadzoru, dla którego w przepisach stosuje się skrót krajowy CERT, oraz określa jego działalność. Ustawa przewiduje, że krajowy CERT będzie obsługiwany, co do zasady, przez podmiot prawa prywatnego, który zawrze umowę publicznoprawną z NSA i będzie służył głównie jako wspólny punkt kontaktowy i koordynacyjny dla osób zobowiązanych prawa prywatnego. Dostawcy usług łączności elektronicznej, podmioty udostępniające sieci łączności elektronicznej oraz podmioty udostępniające istotne sieci będą realizować ustawowy obowiązek powiadamiania krajowego centrum monitorowania.

Standardowy model prawa prywatnego dotyczący wykonywania funkcji przez krajowy CERT ułatwia komunikację między krajowym CERT a zobowiązanymi podmiotami, wykorzystując go jako obowiązkowy punkt kontaktowy. W istocie osoby te będą miały zazwyczaj charakter prywatnoprawny. Krajowy CERT będzie mógł także uczestniczyć w międzynarodowych sieciach podobnych krajowych punktów monitorowania prawa prywatnego i korzystać z wiedzy, która jest w nich nieformalnie przekazywana.

Domniemany prywatnoprawny charakter krajowego CERT jest właściwy ze względu na znaczenie i cel ustawy, także dlatego, że operator krajowego CERT może, jeżeli jest osobą prawa prywatnego, podejmować inicjatywę zmierzającą do osiągnięcia celu ustawy także za milczącym przyzwoleniem, tj. poprzez każde działanie ze swej prywatnej woli, które nie narusza obowiązku prawnego. W ten sposób operator krajowego CERT będzie mógł np. udzielać pomocy metodycznej i informacyjnej podmiotom spoza zakresu podmiotowego ustawy, tj. osobom spoza definicji poszczególnych kategorii osób zobowiązanych, które wyrażą zainteresowanie taką pomocą. Krajowy CERT będzie mógł również rozwijać własną działalność edukacyjną, wydawniczą, badawczą, rozwojową itp. Warunkiem ograniczającym działalność inicjatywną krajowego zespołu CERT dla osiągnięcia celu ustawy jest nieograniczone wypełnianie przez nie obowiązków enumeratywnie wymienionych w ustawie.

W § 17 ust. 2 lit. a), b), d) i e)

Dostawcy usług cyfrowych są dodawani do podmiotów, z którymi komunikuje się i współpracuje narodowy operator CERT.

W sprawie § 17 ust. 2 lit. c)

Dostawców usług cyfrowych dodaje się do podmiotów, z którymi współpracuje operator krajowego zespołu CERT, w tym przypadku przy ocenie incydentów związanych z bezpieczeństwem cybernetycznym. Przepis ten jest odwrotny do przepisu, który nakłada na dostawców usług cyfrowych obowiązek zgłaszania incydentów związanych z bezpieczeństwem cybernetycznym do krajowego operatora CERT.

W sprawie § 17 ust. 2 lit. g)

Jest to zmiana brzmienia przepisu i wyraźne zastosowanie obowiązku informacyjnego do incydentów zgłaszanych przez podmioty zobowiązane.

W sprawie § 17 ust. 2 lit. h)

Doprecyzowano brzmienie przepisu i usunięto ograniczenie dotyczące sytuacji, w których krajowy CERT przekazuje Urzędowi dane kontaktowe osób zobowiązanych.

W § 17 ust. 2 lit. i)-l)

Krajowy Zespół Reagowania na Incydenty Komputerowe (CERT) zyskuje nowe kompetencje i związane z nimi obowiązki w oparciu o dyrektywę zawartą w tym przepisie. Przepis ten jest ściśle związany z sekcją 8, która m.in. reguluje kwestię zgłaszania incydentów związanych z bezpieczeństwem cybernetycznym, które mają wpływ na system informatyczny dostawcy usług cyfrowych. W tym zakresie CERT krajowy jest m.in. wyznaczony jako jeden z CSIRT-ów (Computer Security Incident Response Team) w Republice Czeskiej; CERT rządowy (Narodowe Centrum Cyberbezpieczeństwa, które jest częścią BBN) jest drugim CSIRT-em w rozumieniu dyrektywy dla incydentów przeciwko bezpieczeństwu sieci i systemów informatycznych wyznaczonych operatorów usług podstawowych.

CSIRT-y muszą spełniać wymagania Załącznika I Dyrektywy, co w przypadku krajowego CERT prowadzonego przez CZ.NIC jest spełnione zarówno przez wymagania dla operatora krajowego CERT określone w art. 18 Ustawy, jak i przez treść zamówienia publicznego zawartego z NSA na podstawie art. 19. Zgodnie z ust. 1 tego przepisu umowa ta ma zapewnić realizację działań określonych w sekcji 17, tj. także nowych wymagań wynikających z dyrektywy.

Zgodnie z dyrektywą, zadania CSIRT są następujące:

Krajowy CERT: przyjmuje zgłoszenia incydentów naruszenia bezpieczeństwa cybernetycznego, ocenia je, zapewnia wsparcie metodologiczne, pomoc i współpracę zainteresowanym podmiotom, pełni rolę punktu kontaktowego, przeprowadza oceny podatności na zagrożenia bezpieczeństwa cybernetycznego, przekazuje dane o incydentach do KWB, pełni rolę CSIRT zgodnie z dyrektywą, współpracuje z innymi CSIRT, komunikuje się z właściwymi organami innych państw członkowskich i wreszcie przyjmuje dobrowolne zgłoszenia incydentów naruszenia bezpieczeństwa cybernetycznego. Spełnia zatem wymagania określone w Załączniku I do Dyrektywy:

- *Monitorowanie incydentów na poziomie krajowym - § 17 ust. 2 lit. b), c), l)*
- *Wydawanie wczesnych ostrzeżeń i alarmów, powiadamianie i rozpowszechnianie informacji o zagrożeniach i incydentach wśród odpowiednich zainteresowanych stron - § 17 ust. 2 lit. d), e), g), j)*
- *Reagowanie na incydenty - § 17(2)(c), (d)*

· *Zapewnienie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej - § 17 ust. 2 lit. f)*

· *Udział w sieci CSIRT - według uznania operatora krajowego CERT, patrz dalej komentarz do § 20.*

Obowiązek powołania co najmniej jednego zespołu bezpieczeństwa typu CSIRT odpowiedzialnego za zarządzanie ryzykiem i obsługę incydentów według ściśle określonych procedur i spełniającego wymagania dla zespołów bezpieczeństwa typu CSIRT wynika z art. 9 ust. 1 NIS.

Dyrektywa NIS stanowi, że ten obowiązkowy zespół musi obejmować co najmniej sektory wymienione w załączniku II (rodzaje podmiotów) oraz usługi wymienione w załączniku III (rodzaje usług cyfrowych).

W załączniku I do dyrektywy NIS określono zadania i wymogi dla CSIRT. Do zadań i obowiązków tych osób, zgodnie z załącznikiem I do NIS, należy:

1. Wymagania dla zespołów CSIRT

· CSIRT-y będą dbać o to, aby w ich usługach komunikacyjnych nie było punktów krytycznych (pojedynczych punktów awarii), aby usługi te były szeroko dostępne i aby istniało wiele sposobów kontaktowania się z innymi oraz aby w każdej chwili można było się z nimi skontaktować. Ponadto kanały komunikacji muszą być jasno określone i dobrze znane współpracującym partnerom oraz podmiotom wchodzącym w skład zespołów.

· CSIRT-y i wspierające je systemy informacyjne znajdują się w bezpiecznym miejscu.

· Ciągłość działania:

o CSIRT-y są wyposażone w odpowiednie systemy zarządzania wnioskami i routingu, aby ułatwić przekazywanie informacji,

o Zespoły CSIRT są odpowiednio obsadzone, aby były dostępne przez cały czas,

o CSIRT-y muszą pracować z infrastrukturą, której ciągłość działania jest zagwarantowana. W tym celu muszą być dostępne systemy i lokalizacje zapasowe.

· CSIRT-y muszą mieć możliwość uczestniczenia w międzynarodowych sieciach współpracy, jeśli chcą być ich częścią.

2. Zadania CSIRT-ów

· Do zadań CSIRT-ów należy co najmniej:

  o monitorowanie incydentów na poziomie krajowym,

  o wydawanie wczesnych ostrzeżeń i alarmów, powiadamianie i rozpowszechnianie informacji o zagrożeniach i incydentach wśród odpowiednich interesariuszy,

  o reagowanie na incydenty,

  o Zapewnienie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej,

  o uczestnictwo w sieci CSIRT.

· CSIRT-y nawiązują współpracę z sektorem prywatnym.

· Aby ułatwić współpracę, CSIRT-y promują przyjęcie i stosowanie wspólnych lub standardowych procedur w terenie:

  o zarządzanie incydentami i ryzykiem,

  o klasyfikację incydentów, zagrożeń i informacji.

Stowarzyszenie CZ.NIC prowadzi **narodowy zespół CSIRT Republiki Czeskiej - CSIRT.CZ** (więcej szczegółów na stronie https://csirt.cz/).

W sprawie ustępów 1), 2) i 4)

Zgodnie z ustawą o bezpieczeństwie cybernetycznym, operator krajowego zespołu CERT:

· **otrzymuje powiadomienia o danych kontaktowych** od organów i osób, o których mowa w § 3 lit. a), b) i h) ZoKB, oraz rejestruje i przechowuje te dane,

· odbiera od organów i osób, o których mowa w § 3 (b) i ❤️ KK, **zgłoszenia dotyczące incydentów bezpieczeństwa cybernetycznego** oraz rejestruje, przechowuje i chroni te dane,

· **ocenia incydenty związane z bezpieczeństwem cybernetycznym** w organach i u osób, o których mowa w § 3 lit. b) i h) KSH,

· **zapewnia wsparcie metodyczne, pomoc i współpracę organom i osobom, o których mowa w** § 3 (a), (b) i ❤️ KK, **w przypadku incydentu związanego z cyberbezpieczeństwem**,

o Zasięg działania zespołu CSIRT.CZ obejmuje cały zakres adresowy Republiki Czeskiej. Z CSIRT.CZ mogą kontaktować się wszyscy administratorzy sieci, którzy potrzebują pomocy w radzeniu sobie z incydentem wymagającym skoordynowanej reakcji lub którzy podejrzewają, że incydent może mieć wpływ na cały kraj. Dalsze informacje i wskazówki dotyczące zgłaszania incydentów można znaleźć na stronie[2] . **Zespół CSIRT.CZ nie ma uprawnień wykonawczych** i pełni rolę koordynatora, który może również zapewnić pomoc metodyczną w rozwiązywaniu incydentów.[3]

· **działa jako punkt kontaktowy** dla organów i osób, o których mowa w § 3 lit. a), b) i h) ZOKB,

· **przeprowadza oceny podatności na zagrożenia** bezpieczeństwa cybernetycznego,

· **przekazuje dane dotyczące incydentów naruszenia bezpieczeństwa cybernetycznego** zgłaszanych zgodnie z art. 8 ust. 3 u.o.k.k., bez podawania podmiotu zgłaszającego,

· **przekazuje NUCIB na żądanie dane kontaktowe, o których mowa** w pkt 16(5) i (6) ZoKB,

· **pełni rolę CSIRT zgodnie z dyrektywą NIS**,

· **informuje właściwy organ innego państwa członkowskiego**, bez wskazywania zgłaszającego, o **incydencie zagrażającym bezpieczeństwu cybernetycznemu, który ma znaczący wpływ** na ciągłość świadczenia usługi podstawowej lub cyfrowej w tym państwie członkowskim, mając na uwadze bezpieczeństwo i interesy handlowe zgłaszającego,

· **współpracuje z CSIRT-ami innych państw członkowskich**,

· **otrzymuje zgłoszenia incydentów w zakresie bezpieczeństwa cybernetycznego od innych osób** niewymienionych w sekcji 3 CCC i, jeśli pozwalają na to jego możliwości, przetwarza je oraz zapewnia wsparcie metodologiczne, pomoc i współpracę organom lub osobom, których dotyczy incydent w zakresie bezpieczeństwa cybernetycznego.

CZ.NIC jest zobowiązana do koordynowania działań krajowego zespołu CSIRT z działaniami NUCIB, zgodnie z § 17 ust. 4 ZOKB.

Oprócz obowiązków wyraźnie określonych w ustawie o bezpieczeństwie cybernetycznym, CSIRT Narodowy wyznaczył sobie inne zadania[4] , w tym:

· **Powiadomienie o zakażeniu w domenie .CZ**

CSIRT.CZ opracował tracker open source do celów centralnego monitorowania i rozwiązywania zagrożeń w domenie drugiego poziomu: Malicious Domain Manager.

Aplikacja służy jako centralny punkt gromadzenia i analizowania informacji o złośliwych adresach URL w domenie .CZ.

Aplikacja obsługuje historię zagrożeń w danej domenie oraz bezpośredni kontakt z posiadaczem zagrożenia. Kontakt z właścicielami domen odbywa się za pośrednictwem dedykowanego adresu malware@nic.cz.

· **Skaner internetowy**

W przypadku organizacji non-profit i sektora publicznego podstawową usługą są bezpłatne testy penetracyjne witryn internetowych. Testowanie składa się z testów automatycznych i ręcznych, których celem jest znalezienie słabych punktów w zabezpieczeniach aplikacji. Każda nieprawidłowość w zakresie bezpieczeństwa jest oznaczona szacunkowym poziomem potencjalnego ryzyka i zawiera opis zaleceń dotyczących potencjalnych poprawek.

Więcej informacji można znaleźć na stronie https://www.skenerwebu.cz.

· **Edukacja i wykłady**

We współpracy z Akademią CZ.NIC regularnie prowadzone są szkolenia Bezpieczeństwo komputerowe w praktyce oraz Podstawy funkcjonowania zespołu CSIRT. CSIRT.CZ prowadzi również specjalistyczne kursy dla sił bezpieczeństwa, instytucji państwowych i edukacyjnych oraz wykłady ad hoc.

· **Pomoc w utworzeniu zespołu CERT/CSIRT**

· **Grupy robocze**

Zespół CSIRT.CZ organizuje regularne spotkania zespołów ds. bezpieczeństwa i członków społeczności bezpieczeństwa w Republice Czeskiej.

· **Testy warunków skrajnych**

Po atakach DDoS w 2013 roku, których celem były ważne usługi w Republice Czeskiej, Laboratoria CZ.NIC przygotowały **testy warunków skrajnych** o takiej samej i większej intensywności jak wspomniane wyżej ataki DDoS. We współpracy z CSIRT.CZ usługa ta jest świadczona bezpłatnie wszystkim zainteresowanym osobom, które spełniają wymagania wstępne.

· **System wykrywania włamań**

We współpracy z CESNET CSIRT.CZ prowadzi system, który wykrywa podejrzane zachowania systemów podłączonych do Internetu.

W przypadku podejrzanych prób połączeń z określonych adresów IP, odpowiedzialni administratorzy są natychmiast informowani o takich zdarzeniach (poprzez adres e-mail ids@csirt.cz).

· **Działanie honeypotów**

W ramach badań nad bezpieczeństwem CSIRT.CZ prowadzi szereg honeypotów we współpracy z Laboratoriami CZ.NIC. W ramach projektu Honeynet na stronie https://honeymap.cz można znaleźć wizualizacje ataków w czasie rzeczywistym. Analizowane są nowo przechwycone próbki złośliwego oprogramowania.

· **PROKI**

Wysyłanie informacji o incydentach bezpieczeństwa pochodzących z zakresu czeskich adresów IP.

W sprawie ustępów 3) i 5)

Postanowienia art. 17 ust. 2 ZOKB umożliwiają CZ.NIC prowadzenie we własnym imieniu i na własną odpowiedzialność innej działalności gospodarczej w zakresie cyberbezpieczeństwa, która nie jest bezpośrednio uregulowana w ustawie o cyberbezpieczeństwie. Warunkiem jest jednak, aby ta inna działalność gospodarcza nie przeszkadzała w wykonywaniu zadań krajowego CSIRT.

Stowarzyszenie CZ.NIC jest zobowiązane do bezstronnego działania podczas pełnienia obowiązków krajowego zespołu CSIRT.

Zgodnie z postanowieniami § 18 ZOKB operatorem krajowego CERT może zostać wyłącznie osoba prawna,

a) która spełnia warunki określone w ust. 2 oraz

b) z którą Organizacja zawarła umowę o charakterze publicznoprawnym zgodnie z sekcją 19.

***(2)* Operatorem krajowego CERT może być wyłącznie osoba prawna, która**

a) nie prowadzi ani nie prowadziła działalności sprzecznej z interesem Republiki Czeskiej w rozumieniu przepisów o ochronie informacji niejawnych,

b) obsługuje systemy informatyczne lub usługi i sieci łączności elektronicznej lub zarządza nimi[5] lub uczestniczy w ich obsłudze i zarządzaniu przez co najmniej 5 lat,

c) ma wykształcenie techniczne w zakresie bezpieczeństwa cybernetycznego,

d) jest członkiem międzynarodowej organizacji działającej w dziedzinie cyberbezpieczeństwa,

e) nie ma żadnych zaległości podatkowych zarejestrowanych w ewidencji podatkowej Administracji Finansowej Republiki Czeskiej lub Administracji Celnej Republiki Czeskiej ani w ewidencji podatków, składek na ubezpieczenie społeczne i składek na powszechne ubezpieczenie zdrowotne,

f) nie została prawomocnie skazany za przestępstwo, o którym mowa w art. 7 ustawy o odpowiedzialności karnej osób prawnych i postępowaniu wobec nich,

g) nie jest osobą zagraniczną w rozumieniu jakiegokolwiek innego prawa; oraz

h) nie została ustanowiona lub powołana wyłącznie dla zysku; pozostaje to bez uszczerbku dla możliwości postępowania operatora krajowego CERT zgodnie z art. 17 ust. 3.

***(3)* Wnioskodawca wykazuje zgodność z warunkami, przedkładając**

a) oświadczenie pisemne w przypadku ust. 2 lit. a)-d), g) i h); oraz

b) potwierdzenie przez Administrację Finansową Republiki Czeskiej i Administrację Celną Republiki Czeskiej w przypadku ustępu 2 lit. e).

***(4) Z* treści oświadczenia, o którym mowa w ust. 3 lit. a), musi jasno wynikać, że oferent spełnia odpowiednie wymagania. Potwierdzenie, o którym mowa w ust. 3 lit. b), że wnioskodawca nie ma zaległości podatkowych zarejestrowanych w organach Administracji Finansowej Republiki Czeskiej lub organach Administracji Celnej Republiki Czeskiej, lub w rejestrach podatków, składek na ubezpieczenie społeczne i składek na publiczne ubezpieczenie zdrowotne, nie może być starsze niż 30 dni. W celu udowodnienia warunku, o którym mowa w ust. 2 lit. f), Urząd występuje o wyciąg z rejestru karnego na podstawie innego przepisu prawnego**[6] **.**

***(5)* Operator krajowego CERT wykonuje czynności, o których mowa w art. 17 ust. 2 lit. a)-c), e) oraz g)-l), nieodpłatnie. Operator krajowego CERT ponosi koszty niezbędne do prawidłowego i efektywnego wykonywania czynności, o których mowa w art. 17 ust. 2.**

***(6)* Urząd publikuje na swojej stronie internetowej szczegółowe informacje dotyczące operatora krajowego CERT, a mianowicie jego nazwę lub nazwę handlową, adres siedziby, osobisty numer identyfikacyjny, identyfikator skrzynki danych oraz adres strony internetowej.**

Przepis ten określa ogólne warunki wyboru operatora krajowego zespołu CERT. Jednocześnie reguluje sposób ustanowienia obowiązku prowadzenia krajowego CERT w formie zamówienia publicznego zawieranego z NSA. Zastosowanie instytucji umowy prawa publicznego odpowiada założeniu, że operatorem krajowego CERT będzie osoba prawa prywatnego. Chociaż obowiązki operatora krajowego CERT w zakresie wykonywania działań, o których mowa w niniejszej ustawie, mają w przeważającej mierze charakter prywatnoprawny, to w odniesieniu do dostawców usług łączności elektronicznej, podmiotów udostępniających sieci łączności elektronicznej oraz podmiotów udostępniających istotne sieci operator krajowego CERT będzie pełnił rolę podmiotu, poprzez którego działania osoby zobowiązane wypełniają niektóre ze swoich obowiązków prawnych, zazwyczaj obowiązek zgłaszania danych teleadresowych, a w przypadku podmiotów udostępniających istotne sieci również obowiązek zgłaszania wystąpienia incydentów naruszenia bezpieczeństwa cybernetycznego.

Ponieważ krajowy CERT jest miejscem pracy o dużym znaczeniu dla systemu bezpieczeństwa cybernetycznego Republiki Czeskiej, jego operator musi mieć siedzibę w Republice Czeskiej. W związku z tym, biorąc pod uwagę stopień narażenia krajowego zespołu CERT na zagrożenia bezpieczeństwa, wymóg ten nie może być postrzegany jako dyskryminujący osoby mające siedzibę w innych państwach członkowskich UE. Uczciwość, przejrzysta struktura własności oraz brak zaległych zobowiązań finansowych wobec państwa to standardowe warunki formalne wymagane w przypadku współpracy między państwem a podmiotem prawa prywatnego. Ustawa formułuje również materialne warunki pełnienia funkcji operatora krajowego CERT, wymagając od operatora krajowego CERT wykazania się umiejętnościami merytorycznymi, doświadczeniem i zdolnością techniczną do wykonywania czynności nałożonych na niego tą ustawą, a także zdolnością do współpracy z podmiotami zagranicznymi działającymi w obszarze cyberbezpieczeństwa. Ustawa wymaga ponadto, aby operator krajowego CERT wykonywał czynności powierzone mu tą ustawą w sposób bezstronny, bez względu na jakiekolwiek stosunki umowne lub inne, jakie mogą go łączyć z podmiotami zobowiązanymi.

W § 18 ust. 5

Przepis ten jest odpowiedzią na rozszerzenie kompetencji krajowego operatora CERT w § 17 i odpowiednio rozszerza zakres działań, które krajowy operator CERT wykonuje nieodpłatnie.

W § 18 ust. 5

Zmiana legislacyjna i techniczna związana z rozszerzeniem kompetencji krajowego operatora CERT. W celu zapewnienia spójnego wypełniania obowiązków wynikających z dyrektywy, a następnie z ustawy o cyberbezpieczeństwie, zapisano obowiązek wydatkowania przez krajowy CERT odpowiednich środków finansowych w celu zapewnienia realizacji swoich kompetencji.

W sprawie ustępów 1) i 2)

Operatorem narodowego zespołu CERT jest stowarzyszenie CZ.NIC.

W § 18 ZoKB określono warunki, na jakich podmiot może zostać operatorem krajowego CERT.

Operatorem krajowego CERT może być wyłącznie **osoba prawna**[7] **, z którą NUCIB** (lub wcześniej NSA) **zawarł umowę o zamówienie publiczne**[8] (zgodnie z § 19 ZoKB), i **która spełnia następujące warunki:**

a) nie prowadzi ani nie prowadziła działalności sprzecznej z interesem Republiki Czeskiej w rozumieniu przepisów o ochronie informacji niejawnych,

Zgodnie z art. 2 lit. b) ZOUI *"interesami Republiki Czeskiej* są: *zachowanie jej konstytucyjności, suwerenności i integralności terytorialnej, utrzymanie porządku i bezpieczeństwa wewnętrznego, zobowiązań międzynarodowych i obronności, ochrona gospodarki oraz ochrona życia lub zdrowia osób fizycznych".*

b) obsługuje systemy informatyczne lub usługi i sieci łączności elektronicznej, **zarządza nimi lub** uczestniczy w ich obsłudze i zarządzaniu przez co **najmniej 5 lat,**

c) ma wykształcenie techniczne w zakresie bezpieczeństwa cybernetycznego,

d) jest członkiem międzynarodowej organizacji działającej w dziedzinie cyberbezpieczeństwa,

Wymóg obsługi jednego z systemów wymienionych w lit. c), posiadania kwalifikacji technicznych w dziedzinie bezpieczeństwa cybernetycznego oraz członkostwa w międzynarodowej organizacji działającej w dziedzinie bezpieczeństwa cybernetycznego daje państwu gwarancję, że dana osoba zajmowała się bezpieczeństwem cybernetycznym, reagowaniem na incydenty itp. przez wystarczająco długi okres czasu i na wysokim poziomie. De facto jest to wykazanie faktycznych umiejętności, doświadczenia i zdolności technicznych do wykonywania czynności nałożonych na niego przez CCB.

e) nie ma żadnych zaległości podatkowych zarejestrowanych w ewidencji podatkowej Administracji Finansowej Republiki Czeskiej lub Administracji Celnej Republiki Czeskiej ani **w ewidencji podatków, składek na ubezpieczenie społeczne i składek na powszechne ubezpieczenie zdrowotne,**

f) nie została prawomocnie skazany za przestępstwo, o którym mowa w art. 7 ustawy o odpowiedzialności karnej osób prawnych i postępowaniu wobec nich,

Brak zaległych zobowiązań finansowych wobec państwa, a także dowód uczciwości, to standardowy wymóg formalny przy zawieraniu umowy w przypadku współpracy między państwem a podmiotem prawa prywatnego.

Artykuł 18 ust. 2 lit. f) ustawy o bezpieczeństwie cybernetycznym jest niezgodny ze stanem faktycznym ze względu na zmianę ustawy nr 418/2011 Coll. w sprawie odpowiedzialności karnej osób prawnych i postępowania przeciwko nim. W rozdziale 7 ustawy określono przestępstwa, które mogą być popełniane przez osoby prawne. W obecnie obowiązującym ustawodawstwie rozdział 7 zawiera negatywną definicję przestępstw.

Paragraf 7 TOPO (z mocą obowiązującą od 1 grudnia 2016 r.) stanowi, że osoba prawna może zostać pociągnięta do odpowiedzialności karnej za popełnienie wszystkich przestępstw, z wyjątkiem tych wymienionych wyczerpująco w tym przepisie.

Poza określeniem zakresu przestępstw, w przypadku odpowiedzialności karnej osób prawnych należy również zająć się kwestią przypisywalności. Mimo że osoba prawna jest konstrukcją fikcyjną, prawo generalnie uznaje w odniesieniu do osób prawnych ich zdolność do działania zgodnie z prawem (tj. także niezgodnie z prawem), w tym do przypisywania winy. Wina jako warunek odpowiedzialności karnej jest przypisywana osobie prawnej, jeśli wystąpiły okoliczności określone w art. 8 ust. 2 Ustawy o odpowiedzialności karnej osób prawnych.

Zgodnie z art. 8 ust. 1 ustawy o TOPO, przestępstwem popełnionym przez osobę prawną jest czyn bezprawny popełniony w jej interesie lub w ramach jej działalności, jeśli osoba ta działała w taki sposób, że

a) organu statutowego lub członka organu statutowego, lub innej osoby zajmującej kierownicze stanowisko w ramach podmiotu prawnego, która jest upoważniona do działania w imieniu lub na rzecz podmiotu prawnego,

b) osoba pełniąca funkcję kierowniczą w danej osobie prawnej, która wykonuje czynności zarządcze lub kontrolne na rzecz tej osoby prawnej, nawet jeśli nie jest ona osobą, o której mowa w punkcie (a),

c) osoba, która ma decydujący wpływ na zarządzanie osobą prawną, jeśli jej zachowanie było przynajmniej jednym z warunków wystąpienia skutku powodującego odpowiedzialność karną osoby prawnej, lub

d) pracownik lub osoba na podobnym stanowisku (dalej zwana "pracownikiem") w ramach wykonywania swoich obowiązków, nawet jeśli nie jest to osoba, o której mowa w lit. a)-c),

jeśli osobę prawną można przypisać postępowaniu wyżej wymienionej osoby zgodnie z sekcją 8(2) TOPO.

g) nie jest osobą zagraniczną na podstawie innych przepisów prawnych,

Zgodnie z § 3024 Kodeksu cywilnego osobą zagraniczną jest osoba fizyczna zamieszkująca lub osoba prawna mająca siedzibę poza Republiką Czeską.

Ze względu na znaczenie krajowego zespołu CERT w dziedzinie cyberbezpieczeństwa Republiki Czeskiej wymagane jest, aby operator tego zespołu znajdował się w Republice Czeskiej. Wymóg ten nie może być postrzegany jako dyskryminacja wobec innych osób mających siedzibę w innym państwie członkowskim Unii.

h) nie została ustanowiona lub powołana wyłącznie w celu osiągnięcia zysku; nie narusza to możliwości postępowania operatora krajowego CERT zgodnie z art. 17 ust. 3 ZOKB.

W sprawie ustępów 3) i 4)

Osoba prawna, która chce zostać operatorem krajowego CERT, musi udowodnić spełnienie warunków, przedkładając oświadczenie (w przypadku § 18 ust. 2 lit. a)-d), g), h) RWKC) oraz zaświadczenie z Administracji Finansowej Republiki Czeskiej i Administracji Celnej Republiki Czeskiej (w przypadku § 18 ust. 2 lit. e) RWKC).

Z treści oświadczenia musi jasno wynikać, że oferent spełnia odpowiednie wymagania. Potwierdzenie, że oferent nie zalega z podatkami w swoich rejestrach prowadzonych przez Czeski Urząd Finansowy lub Urząd Celny Republiki Czeskiej lub w rejestrach dotyczących podatków, składek na ubezpieczenie społeczne i składek na publiczne ubezpieczenie zdrowotne nie **może być starsze niż 30 dni.**

W celu **udowodnienia, że osoba prawna nie została skazana za** przestępstwo, **KIK zwraca się o wyciąg z rejestru karnego.**

W ustępie 5)

Operator krajowego CERT **wykonuje czynności, o których mowa w art. 17 ust. 2 u.o.k.k., nieodpłatnie**. Jedynymi wyjątkami od zasady nieodpłatności są następujące działania:

- **zapewnia wsparcie metodyczne, pomoc i współpracę organom i osobom, o których mowa w** § 3 (a), (b) i ❤️ KK, **w przypadku incydentu związanego z cyberbezpieczeństwem,**
- **przeprowadza oceny podatności na zagrożenia** bezpieczeństwa cybernetycznego.

Operator krajowego CERT jest zobowiązany do ponoszenia kosztów niezbędnych do prawidłowego i efektywnego wykonywania czynności, o których mowa w art. 17 ust. 2 u.o.k.k.

W ustępie 6)

Aby umożliwić kontakt z operatorem krajowego zespołu CERT, jego dane są publikowane na stronie internetowej NACIB. Publikowane są następujące informacje: nazwa firmy, adres siedziby, osobisty numer identyfikacyjny, identyfikator skrzynki danych oraz adres strony internetowej.

1.1.2 CERT rządowy

Rządowy CERT jako część Urzędu

a) otrzymuje powiadomienie o danych kontaktowych od organów i osób, o których mowa w punktach c)-g) sekcji 3,

b) przyjmuje zgłoszenia o incydentach w zakresie bezpieczeństwa cybernetycznego od organów i osób, o których mowa w § 3 lit. c)-g),

c) ocenia dane dotyczące zdarzeń i incydentów związanych z bezpieczeństwem cybernetycznym w krytycznej infrastrukturze informatycznej, systemie informatycznym usług podstawowych, głównych systemach informatycznych oraz innych systemach informatycznych administracji publicznej,

d) zapewnia wsparcie metodyczne i pomoc organom i osobom, o których mowa w § 3 lit. c)-g),

e) zapewnia pomoc organom i osobom, o których mowa w § 3 lit. c)-g), w przypadku wystąpienia incydentu bezpieczeństwa cybernetycznego oraz zdarzenia związanego z bezpieczeństwem cybernetycznym,

f) otrzymuje sugestie i dane od organów i osób, o których mowa w § 3, oraz od innych organów i osób, a także ocenia te sugestie i dane,

g) otrzymuje dane od krajowego operatora CERT i ocenia te dane,

h) otrzymuje i ocenia dane od organów odpowiedzialnych za bezpieczeństwo cybernetyczne za granicą,

i) udostępnia, zgodnie z sekcją 9 ust. 4, operatorowi krajowego zespołu CERT, organom pełniącym za granicą obowiązki w zakresie bezpieczeństwa cybernetycznego oraz innym osobom działającym w dziedzinie bezpieczeństwa cybernetycznego dane z rejestru incydentów,

j) przeprowadza oceny podatności na zagrożenia bezpieczeństwa cybernetycznego,

k) informuje właściwy organ innego państwa członkowskiego, bez wskazywania zgłaszającego, o incydencie zagrażającym bezpieczeństwu cybernetycznemu, który ma znaczący wpływ na ciągłość podstawowych usług w tym państwie członkowskim lub wpływa na świadczenie usług cyfrowych w tym państwie członkowskim, przy jednoczesnym zachowaniu bezpieczeństwa i interesów handlowych zgłaszającego,

l) otrzymuje zgłoszenia incydentów bezpieczeństwa cybernetycznego od organów i osób niewymienionych w sekcji 3; rządowy CERT przetwarza te zgłoszenia i - jeżeli pozwalają na to jego możliwości, a incydent bezpieczeństwa cybernetycznego ma istotne skutki - zapewnia wsparcie metodologiczne, pomoc i współpracę organom lub osobom, których dotyczy incydent bezpieczeństwa cybernetycznego,

m) pełni rolę CSIRT zgodnie z odpowiednim rozporządzeniem Unii Europejskiej[9] **; oraz**

n) współpracuje z CSIRT-ami innych państw członkowskich.

Rządowy CERT wchodzi w skład NSA, czyli Narodowego Centrum Cyberbezpieczeństwa, które jest jednostką organizacyjną NSA zapewniającą jego działalność. Rządowy CERT jest pomyślany jako centralne publiczne miejsce pracy i publiczny "pojedynczy punkt kontaktowy" w zakresie bezpieczeństwa cybernetycznego. Jego działania obejmują otrzymywanie danych kontaktowych od wybranych osób zobowiązanych, otrzymywanie informacji o stanie cyberbezpieczeństwa, w szczególności otrzymywanie obowiązkowych i inicjowanych zgłoszeń incydentów cyberbezpieczeństwa oraz innych danych o stanie cyberbezpieczeństwa od krajowych i zagranicznych organów publicznych i podmiotów współpracujących, a także ich ocenę. Ponadto rządowy CERT zapewnia pomoc wybranym rodzajom osób zobowiązanych w przypadku incydentu związanego z bezpieczeństwem cybernetycznym, zapewnia współdziałanie z innymi organami i podmiotami zapewniającymi bezpieczeństwo cybernetyczne w Republice Czeskiej oraz w państwach współpracujących lub sojuszniczych, a także przeprowadza oceny podatności na zagrożenia bezpieczeństwa cybernetycznego.

W § 20 lit. a), b), d) i e)

Wśród podmiotów, z którymi komunikuje się i współpracuje rządowy CERT, dodaje się nowe podmioty obowiązkowe - operatorów usług podstawowych oraz administratorów i operatorów systemów informatycznych usług podstawowych.

W sprawie § 20 lit. c)

Systemy informatyczne, na podstawie których rządowy zespół CERT ocenia dane dotyczące zdarzeń i incydentów związanych z bezpieczeństwem cybernetycznym, obejmują systemy informatyczne, od których zależy świadczenie podstawowych usług.

W sprawie § 20(i)

Techniczna zmiana legislacyjna wynikająca z konieczności dodania nowych liter do tego przepisu.

W § 20 lit. j) i k)-n)

Dyrektywa nadaje rządowemu zespołowi CERT nowe kompetencje i związane z nimi obowiązki. Przepis ten jest ściśle powiązany z sekcją 8, która reguluje kwestię zgłaszania incydentów związanych z bezpieczeństwem cybernetycznym.

Zgodnie z ustawą zmienioną niniejszym wnioskiem, rządowy CERT: otrzymuje zgłoszenia incydentów w zakresie bezpieczeństwa cybernetycznego, ocenia je, zapewnia wsparcie metodologiczne, pomoc i współpracę zainteresowanym podmiotom, działa jako punkt kontaktowy, przeprowadza oceny podatności w dziedzinie bezpieczeństwa cybernetycznego, przekazuje dane o incydentach do KWB, pełni rolę CSIRT zgodnie z dyrektywą, współpracuje z innymi CSIRT, komunikuje się z właściwymi organami innych państw członkowskich oraz, co nie mniej ważne, przyjmuje dobrowolne zgłoszenia incydentów w zakresie bezpieczeństwa cybernetycznego.

Spełnia to wymagania określone w Załączniku I do Dyrektywy:

- *Monitorowanie incydentów na poziomie krajowym - § 20 (b), (c), (f), (g), (l).*
- *Wydawanie wczesnych ostrzeżeń i alarmów, powiadamianie i rozpowszechnianie informacji o zagrożeniach i incydentach wśród właściwych interesariuszy - § 20 (d), (e), (i),* 👇 .
- *Reagowanie na incydenty - § 20 (d), (e).*
- *Zapewnienie dynamicznej analizy ryzyka i incydentów oraz świadomości sytuacyjnej - § 20 lit. j).*
- *Uczestnictwo w sieci CSIRT - § 20(m).*

Pełniąc rolę CSIRT, rządowy CERT, będący częścią NSA, będzie również spełniał wymogi dyrektywy dotyczące udziału CSIRT w sieci CSIRT zgodnie z art. 12 dyrektywy. Udział przedstawicieli krajowych zespołów CERT pozostawia się do ich decyzji.

Artykuł 9 dyrektywy stanowi, że każde państwo członkowskie tworzy jeden lub więcej CSIRT, ale nie nakłada na przedstawicieli wszystkich CSIRT danego państwa członkowskiego obowiązku uczestniczenia w pracach sieci CSIRT. Dlatego wystarczy pełne uczestnictwo co najmniej jednego CSIRT-u, który będzie realizowany przez przedstawicieli rządowego CERT-u. Przepis ten reguluje procedurę postępowania rządowego zespołu CERT w przypadku, gdy zgłoszony incydent bezpieczeństwa cybernetycznego ma istotny wpływ na ciągłość świadczenia podstawowych usług lub na świadczenie usług cyfrowych w innym państwie członkowskim Unii Europejskiej. W takim przypadku, zgodnie z art. 14 ust. 5, a w konsekwencji z art. 16 ust. 6 dyrektywy, rządowy CERT jest uprawniony do informowania o incydencie właściwych organów innych państw członkowskich.

W art. 20 dyrektywy przewidziano sytuację, w której podmiot, który nie został wyznaczony jako operator usług podstawowych i nie jest dostawcą usług cyfrowych, zgłasza naruszenie bezpieczeństwa swoich systemów informatycznych i stara się zaradzić tej sytuacji. W takim przypadku może dobrowolnie zgłosić incydent bezpieczeństwa cybernetycznego do rządowego zespołu CERT i współpracować z nim w celu rozwiązania sytuacji. W takim przypadku rządowy CERT przetwarza zgłoszenie i, jeżeli pozwalają na to jego możliwości, udziela uzasadnionej odpowiedzi na zgłoszenie, tak jakby był to incydent bezpieczeństwa cybernetycznego o znaczących skutkach, tak jakby był to incydent bezpieczeństwa cybernetycznego zgłoszony mu przez operatora usług podstawowych.

Na mocy ustawy o cyberbezpieczeństwie **w Republice Czeskiej obowiązkowo powoływane są dwa zespoły** typu CERT/CSIRT**: krajowy i rządowy.**

Operatorem krajowego CERT jest osoba prawna, z którą NÚKIB (dawniej NSA) zawarł umowę publicznoprawną (zob. § 19 ZoKB).

Rządowy CERT (**GovCERT.CZ** - więcej szczegółów na stronie https://www.govcert.cz/) został powołany na mocy prawa jako część Krajowego Biura ds. Cyberbezpieczeństwa i Informacji (wcześniej podlegał NSA).

Zgodnie z ustawą o bezpieczeństwie cybernetycznym, rządowy zespół CERT:

· **otrzymuje powiadomienia o danych kontaktowych** od organów i osób, o których mowa w sekcji 3 lit. c)-g) ZOKB,

· **otrzymuje zgłoszenia dotyczące incydentów związanych z bezpieczeństwem cybernetycznym** od organów i osób, o których mowa w § 3 lit. c)-g) KSH,

· **ocenia dane** dotyczące **zdarzeń** i **incydentów** związanych z bezpieczeństwem cybernetycznym w krytycznej infrastrukturze informatycznej, systemie informatycznym usług podstawowych, głównych systemach informatycznych oraz innych systemach informatycznych administracji publicznej,

· **zapewnia wsparcie metodyczne i pomoc organom i osobom,** o których mowa w § 3 lit. c)-g) ZOKB,

· **zapewnia pomoc** organom i osobom, o których mowa w § 3 lit. c)-g) KK, **w przypadku wystąpienia incydentu bezpieczeństwa cybernetycznego oraz zdarzenia związanego z bezpieczeństwem cybernetycznym,**

  o Reagowanie na incydenty związane z bezpieczeństwem jest jednym z podstawowych działań zespołu rządowego. W przypadku zgłoszenia incydentu związanego z cyberbezpieczeństwem zespół GovCERT.CZ jest gotowy do udzielenia specjalistom IT pomocy technicznej, w tym doradztwa w zakresie dalszych środków zapobiegawczych. W przypadku stwierdzenia, że incydent jest wymierzony w wiele podmiotów, zespół GovCERT.CZ jest gotowy do koordynowania wspólnej reakcji. [10]

· **otrzymuje sugestie i dane** od organów i osób, o których mowa w punkcie 3 ZOKB, oraz od innych organów i osób, **a także ocenia te** sugestie i dane,

· **otrzymuje dane od krajowego operatora CERT** i ocenia te dane,

· **otrzymuje** i ocenia **dane od organów odpowiedzialnych za bezpieczeństwo cybernetyczne za granicą,**

· **udostępnia dane z rejestru incydentów** (zob. art. 9 ust. 4 u.o.k.k.) operatorowi krajowego zespołu CERT, organom prowadzącym działania związane z bezpieczeństwem cybernetycznym za granicą oraz innym osobom działającym w obszarze bezpieczeństwa cybernetycznego,

· **przeprowadza oceny podatności na zagrożenia** bezpieczeństwa cybernetycznego,

· **informuje właściwy organ innego państwa członkowskiego, bez wskazywania zgłaszającego, o incydencie zagrażającym bezpieczeństwu cybernetycznemu, który ma znaczący wpływ** na ciągłość podstawowych usług w tym państwie członkowskim lub wpływa na świadczenie usług cyfrowych w tym państwie członkowskim, przy jednoczesnym zachowaniu bezpieczeństwa i interesów handlowych zgłaszającego,

· **otrzymuje zgłoszenia incydentów bezpieczeństwa cybernetycznego od organów i osób niewymienionych w sekcji 3 CST**; rządowy CERT przetwarza te zgłoszenia i - jeżeli pozwalają na to jego możliwości, a incydent bezpieczeństwa cybernetycznego ma istotny wpływ - zapewnia wsparcie metodologiczne, pomoc i współpracę organom lub osobom, których dotyczy incydent bezpieczeństwa cybernetycznego,

· **działa jako CSIRT zgodnie z** art. 9 NIS,

· **współpracuje z CSIRT-ami innych państw członkowskich**.

Oprócz obowiązków wyraźnie określonych w ustawie o bezpieczeństwie cybernetycznym, rządowy CERT wyznaczył sobie inne zadania[11] , w tym:

· **Udostępnianie danych**

  o GovCERT.CZ uzyskuje szereg raportów i danych dotyczących potencjalnie zainfekowanych systemów informatycznych w Republice Czeskiej we współpracy z różnymi międzynarodowymi organizacjami zajmującymi się bezpieczeństwem cybernetycznym. Przekazuje te informacje innym podmiotom w ramach swojej działalności proaktywnej. Udostępniane dane są podzielone na następujące projekty:

- **BotnetFeed** - narzędzie to służy do przetwarzania danych z pobranych serwerów C&C o stacjach końcowych podłączonych do botnetów. Aby zidentyfikować potencjalnie zainfekowany system komputerowy, adres IP oraz informacje o botnecie, do którego jest on włączony, są przekazywane do menedżera zakresu IP.

- **IHAP** (Incident Handling Automation Project)**, MDM** (Malicious Domain Manager) - w ramach tych projektów zbierane są fragmenty wskaźników kompromitacji (IoC) z różnych serwerów. Do najczęstszych wskaźników należą: phishing, ataki typu brute force, alerty o identyfikatorach, spam, próby skanowania, wykorzystywanie luk w zabezpieczeniach, występowanie złośliwego oprogramowania i wiele innych. Na podstawie tych danych przygotowywane są krótkie raporty, które zawsze zawierają adres IP zaatakowanego komputera oraz krótkie podsumowanie rodzaju incydentu.

· **Shadowserver** - projekt koncentruje się na ciągłym poszukiwaniu istotnych informacji o podatnościach w cyberprzestrzeni oraz występowaniu tych podatności na konkretnych adresach IP.

· **Wdrażanie Honeypotów**

· **Testy penetracyjne**

Jest to legalna próba przeniknięcia do testowanych systemów. W efekcie powstaje raport o podatnościach w testowanej jednostce, który jest kierowany wyłącznie do jej właściciela, który na jego podstawie podejmuje odpowiednie działania zabezpieczające.

Inną możliwością jest wykonanie skanowania podatności na ataki w ramach projektu OWASP (Open Web Application Security Project).

· **HUB informacyjny**

Strona govcert.cz zawiera informacje, badania, analizy i artykuły na temat aktualnych zagrożeń i podatności systemów w Republice Czeskiej. Dokumenty te są uzupełniane regularnymi miesięcznymi biuletynami podsumowującymi istotne incydenty związane z bezpieczeństwem w Republice Czeskiej i za granicą.

· **Działalność edukacyjna i badawcza**

· **Laboratorium kryminalistyczne i laboratorium SCADA**

---

[1] Artykuł 9 WNIS

[2] *Kiedy należy się z nami skontaktować.* [online]. [cytowany 2018-07-07]. Dostępny pod adresem: https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/

[3] *Usługi CSIRT.CZ.* [online]. [cytowany 2018-07-07]. Dostępny pod adresem: https://csirt.cz/page/2764/sluzby/

[4] Wszystkie zadania zostały zaczerpnięte z: *Services CSIRT.CZ.* [online]. [cytowany 2018-07-07]. Dostępny pod adresem: https://csirt.cz/page/2764/sluzby/

[5] Ustawa nr 127/2005 Dz.U. o komunikacji elektronicznej i o zmianach w niektórych powiązanych ustawach (Ustawa o komunikacji elektronicznej), z późniejszymi zmianami.

[6] Ustawa nr 269/1994 Zb. o Rejestrze Karnym, z późniejszymi zmianami.

[7] Zgodnie z artykułem 20(1) Kodeksu Cywilnego, osoba prawna to *"**zorganizowana jednostka, która zgodnie z prawem posiada osobowość prawną lub której osobowość prawna jest uznawana przez prawo".** Osoba prawna może, niezależnie od przedmiotu swojej działalności, mieć prawa i obowiązki zgodne z jej charakterem prawnym."* Państwo jest uznawane za osobę prawną w dziedzinie prawa prywatnego. (ART. 21 CC).

Osoba prawna może być osobą prawa prywatnego lub publicznego, w zależności od interesu osoby prawnej (art. 144 kpk). Z punktu widzenia prawa cywilnego korporacje (zob. § 210 i nast. KC), fundacje (zob. § 303 i nast. KC) oraz konstytucje (zob. § 402 i nast. KC) są osobami prawnymi.

[8] Zastosowanie instytucji zamówienia publicznego na podstawie art. 160 i nast. kodeksu postępowania cywilnego odpowiada założeniu, że operatorem narodowego CERT będzie osoba prawa prywatnego.

[9] Zob. art. 9 Konwencji NIS

[10] *Świadczone usługi.* [online]. [cited 2018 Aug 1]. Dostępny pod adresem: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

[11] Wszystkie zadania pochodzą z: *Świadczone usługi.* [online]. [cytowany 2018-07-07]. Dostępny pod adresem: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

3.2. Polska

Ramy prawne dla zespołów CSIRT/CERT w Polsce

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wyróżnia 3 krajowe CSIRT-y:

- CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Szefa Agencji Bezpieczeństwa Wewnętrznego

- CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Ministra Obrony Narodowej

- CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy

Ponadto w ustawie wymieniono następujące podmioty wchodzące w skład krajowego systemu bezpieczeństwa cybernetycznego:

- operatorzy podstawowych usług;

- dostawców usług cyfrowych;

- sektorowe zespoły ds. bezpieczeństwa cybernetycznego;

- jednostki sektora finansów publicznych, o których mowa w art. 1. 9 pkt 1-6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia

- 2009 r. o finansach publicznych (Dz.U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62, 1000 i 1366);

- instytuty badawcze;

- Narodowy Bank Polski;

- Bank Gospodarstwa Krajowego;

- Urząd Dozoru Technicznego;

- Polska Agencja Żeglugi Powietrznej;

- Polskie Centrum Akredytacji;

- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;

- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827 oraz z 2018 r. poz. 1496);

- podmioty świadczące usługi w zakresie bezpieczeństwa cybernetycznego;

- właściwe organy ds. bezpieczeństwa cybernetycznego;

- Pojedynczy punkt kontaktowy ds. bezpieczeństwa cybernetycznego;

- pełnomocnik rządu ds. bezpieczeństwa cybernetycznego;

- Kolegium Bezpieczeństwa Cybernetycznego.

Role, sposoby działania i inne regulacje dotyczące podmiotów polskiego systemu cyberbezpieczeństwa określa ustawa.

3.3. PODSUMOWANIE

o Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii (Dyrektywa NIS) została przyjęta przez Parlament Europejski.

o W dyrektywie w sprawie bezpieczeństwa sieci i informacji przewidziano środki prawne mające na celu podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego w UE poprzez zapewnienie:

- gotowości państw członkowskich poprzez wymaganie od nich odpowiedniego wyposażenia. Na przykład powołania zespołem reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT) i właściwego krajowym organu ds. bezpieczeństwa sieci i informacji,
- współpracy między wszystkimi państwami członkowskimi poprzez utworzenie Grupy Współpracy, która będzie wspierać i ułatwiać współpracę strategiczną i wymianę informacji między państwami członkowskimi.
- kultury bezpieczeństwa w sektorach, które mają kluczowe znaczenie dla naszej gospodarki i społeczeństwa, a ponadto w znacznym stopniu opierają się na TIK, takich jak energetyka, transport, gospodarka wodna, bankowość, infrastruktura rynków finansowych, opieka zdrowotna i infrastruktura cyfrowa.

o Państwa członkowskie przyjęły różne podejścia do wdrażania NIS.

o Ramy prawne dla zespołów CSIRT/CERT w Republice Czeskiej są częściowo określone w ustawie o cyberbezpieczeństwie. Ustawa określa warunki istnienia krajowych i rządowych zespołów CSIRT/CERT, ale z drugiej strony nie ogranicza możliwości tworzenia i istnienia innych zespołów CSIRT/CERT.

> Na podstawie ustawy o cyberbezpieczeństwie **w Republice Czeskiej obowiązkowo powoływane są dwa zespoły** CERT/CSIRT**: krajowy i rządowy**. Każdy z tych zespołów ma ściśle określone prawa i obowiązki (§ 17 i nast. ustawy o zespołach CERT).

o Ramy prawne dla zespołów CSIRT/CERT w Polsce

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wyróżnia 3 krajowe CSIRT-y:

- CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Szefa Agencji Bezpieczeństwa Wewnętrznego

- CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Ministra Obrony Narodowej

- CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, kierowany przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy

Ponadto w ustawie wymieniono następujące podmioty wchodzące w skład krajowego systemu bezpieczeństwa cybernetycznego:

- operatorzy podstawowych usług;

- dostawców usług cyfrowych;

- sektorowe zespoły ds. bezpieczeństwa cybernetycznego;

- jednostki sektora finansów publicznych, o których mowa w art. 1. 9 pkt 1-6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia

- 2009 r. o finansach publicznych (Dz.U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62, 1000 i 1366);

- instytuty badawcze;

- Narodowy Bank Polski;

- Bank Gospodarstwa Krajowego;

- Urząd Dozoru Technicznego;

- Polska Agencja Żeglugi Powietrznej;

- Polskie Centrum Akredytacji;

- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;

- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827 oraz z 2018 r. poz. 1496);

- podmioty świadczące usługi w zakresie bezpieczeństwa cybernetycznego;

- właściwe organy ds. bezpieczeństwa cybernetycznego;

- Pojedynczy punkt kontaktowy ds. bezpieczeństwa cybernetycznego;

- pełnomocnik rządu ds. bezpieczeństwa cybernetycznego;

- Kolegium Bezpieczeństwa Cybernetycznego.

Role, sposoby działania i inne regulacje dotyczące podmiotów polskiego systemu cyberbezpieczeństwa określa ustawa.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- bezpieczeństwo cybernetyczne
- CSIRT/CERT
- dyrektywa NIS
- ENISA
- okręg wyborczy
- krajowe i rządowe CSIRT/CERT
- współpraca zespołów

PYTANIA KONTROLNE

- Czy istnieje hierarchia pomiędzy zespołami CSIRT/CERT?
- Jak definiowany jest zakres działania zespołu CSIRT/CERT?
- Co jest rządowym zespołem CSIRT/CERT?
- Co jest krajowym zespołem CSIRT/CERT?
- Jakie są role i zadania innych zespołów CSIRT/CERT?
- Jak wygląda struktura zespołów CSIRT/CERT w Twoim kraju?

4. Wnioski

Żyjemy w czasach, w których technologie informacyjne i komunikacyjne są nieodłącznie związane z każdym aspektem naszej egzystencji. Pewnym paradoksem jest to, że de facto nie mamy możliwości uniknięcia tego przenikania się i interakcji z ICT, co jednocześnie czyni nas bardziej podatnymi na zagrożenia.

W miarę jak rośnie ilość danych i informacji przechowywanych u poszczególnych dostawców usług internetowych, coraz częściej poruszane są kwestie ich skutecznego zabezpieczenia, przekazywania lub usuwania, nie tylko na podstawie umowy zawartej między dostawcą usług a użytkownikiem końcowym, ale także na podstawie nowo powstających przepisów.

Państwa, organizacje i osoby fizyczne są coraz bardziej świadome, że informacje i dane stanowią znaczący potencjał, który jest coraz częściej atakowany w ramach ataków cybernetycznych, mających na celu kradzież, uszkodzenie, uniemożliwienie dostępu lub usunięcie danych.

Jeśli chcemy żyć we współczesnym społeczeństwie i korzystać z jego dobrodziejstw, nie można zrezygnować z technologii informacyjno-komunikacyjnych, a już na pewno nie ma sensu zaprzestać ich stosowania. Musimy zacząć uczyć się, jak korzystać z tych technologii i usług, jak unikać lub przynajmniej eliminować skutki cyberataków.

Wielu negatywnych zdarzeń można uniknąć, jeśli osoby prywatne i organizacje będą przestrzegać przynajmniej podstawowych zasad bezpieczeństwa cybernetycznego.

W cyberprzestrzeni, podobnie jak w świecie rzeczywistym, nie ma jednego systemu bezpieczeństwa i ochrony, który można by powszechnie stosować wobec wszystkich. Jeśli chcemy zająć się bezpieczeństwem, należy podejść do niego w sposób holistyczny i zindywidualizowany.

Technologie informacyjne i komunikacyjne to dziedzina, która rozwija się najbardziej dynamicznie i masowo. Obszary, na które powinniśmy zwrócić szczególną uwagę w tym kontekście, to bezpieczeństwo i edukacja użytkowników.

5. Wykaz literatury

1. *2018 Data Breach Investigation Report. 11th Edition.* [Online]. [cytowany 2018-07-28]. Dostępny pod adresem: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

2. *Analiza ryzyka [*online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

3. ANDRESS, Jason. *Podstawy bezpieczeństwa informacji. Wydanie* drugie. Syngress. 9780128007440

4. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* Londyn: Academic Press, 2004, s. 9 i nast.

5. *Metodologia triady CIA.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

6. *Przewodnik postępowania w przypadku incydentów związanych z bezpieczeństwem komputerowym* [online]. [cited 2018 Aug 13], s. 6. Dostępny w Internecie: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

7. *Bezpieczeństwo cybernetyczne.* [online]. [cytowany 2018-07-06]. Dostępny na stronie: https://en.oxforddictionaries.com/definition/cybersecurity Tłumaczenie autora.

8. *Bezpieczeństwo cybernetyczne.* [online]. [cytowany 2018-07-06]. Dostępny na stronie: https://www.merriam-webster.com/dictionary/cybersecurity Tłumaczenie autora.

9. *Cyberzagrożenie.* [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://en.oxforddictionaries.com/definition/cyberthreat

10. *Definition of Cybersecurity - Gaps and overlaps in standardisation* [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

11. *Model oceny dojrzałości CSIRT ENISA* [online], 2019 r. WERSJA 2.0. Ateny, Grecja: Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) [cyt. 2021-03-16]. ISBN 978-92-9204-292-9. Dostępny pod adresem: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, s. 6.

12. EVANS, DONALD, PHILIP, BOND i ARDEN BEMET. *Standardy kategoryzacji bezpieczeństwa informacji i systemów informatycznych na szczeblu federalnym (Standards for Security Categorization of Federal Information and Information Systems).* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cytowany 2017 Dec 10]. Dostępny pod adresem: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

13. FRANK, Libor. *Studia nad bezpieczeństwem.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

14. FRUHLINGER, Josh. *Co to jest Stuxnet, kto go stworzył i jak działa?* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

15. HENDERSON, Anthony. *Triada CIA: poufność, integralność, dostępność.* [online]. [cyt. 2018 Jan 13]. Dostępny pod adresem: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

16. *Zagrożenie.* [online]. [cytowany 2018-07-28]. Dostępny pod adresem: http://www.mvcr.cz/clanek/hrozba.aspx

17. HSU, D. Frank i D. MARINUCCI (eds.). *Postępy w dziedzinie bezpieczeństwa cybernetycznego: technologia, operacje i doświadczenia*. Nowy Jork: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. s 41.

18. JIRÁSEK, Petr, Luděk NOVÁK i Josef POŽÁR. *Słownik interpretacyjny bezpieczeństwa cybernetycznego*. [online]. Wydanie 3 zaktualizowane. Praga: AFCEA, 2015, s. 23 [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

19. JIROVSKÝ, Václav. *Cyberprzestępczość to nie tylko hakerstwo, cracking, wirusy i trojany bez tajemnic.* Praga: Grada Publishing, a. s., 2007. s. 21 i nast.

20. KADLECOVÁ, Lucie. *Pojęciowe i teoretyczne aspekty bezpieczeństwa cybernetycznego.* [online]. [cytowany 2018-07-21]. Dostępny pod adresem: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

21. KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016.

22. *Bezpieczeństwo cybernetyczne: co z tym zrobić?* [online]. [cyt. 2018 Jun 29]. Dostępny pod adresem: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

23. *Sztab wyborczy Macrona został zaatakowany przez hakerów, twierdzi japońska firma antywirusowa.* [online]. [cyt. 2017 Jun 29]. Dostępny pod adresem: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

24. MAREŠ, Miroslav. *Bezpieczeństwo.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

25. MATUROVÁ, Jana i Miroslav VALTA. *Zapobieganie ryzyku - kontrole stanu wyposażenia technicznego.* [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

26. *Narodowa Strategia Cyberbezpieczeństwa Republiki Czeskiej na lata 2015-2020* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

27. *Parkerian Hexad*. [online]. [cyt. 2016 Aug. 20]. Dostępny pod adresem: https://vputhuseeri.wordpress.com/2009/08/16/149/

28. *POŽÁR, Josef. Bezpieczeństwo informacji*. Pilzno: Aleš Čeněk, 2005, s. 37.

29. POŽÁR, Josef. *Wybrane zagrożenia dla bezpieczeństwa informacji w organizacji.* [online]. [cyt. 2018 lipiec 6]. Dostępny pod adresem: https://www.cybersecurity.cz/data/pozar2.pdf

30. PROSISE, Chris i Kevin MANDIVA. *Reagowanie na incydenty i informatyka śledcza, wydanie drugie.* Emeryville: McGraw-Hill, 2003, s. 13.

31. Przed czym należy się chronić? - Zagrożenia bezpieczeństwa, zdarzenia, incydenty. *[online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.kybez.cz/bezpecnost/pred-cim-chranit*

32. *Nadejście hakerów: historia Stuxnetu.* [online]. [cytowany 2018-07-01]. Dostępny pod adresem: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

33. RAK, Roman. Homo sapiens kontra bezpieczeństwo. Forum ICT/PERSONALIS 2006 [prezentacja 27 września 2006 r.]. Praga (prezentacja na konferencji).

34. SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570039 ;

35. SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570035

36. SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570047

37. SCHNEIER, Bruce. [online]. [cytowany 2018-07-18]. Dostępny pod adresem: https://www.azquotes.com/quote/570040

38. *Wytyczne NIS.* [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

39. SVOBODA, Ivan. *Rozwiązania w zakresie bezpieczeństwa cybernetycznego.* Wykład w Akademii CRIF. (23. 9. 2014)

40. ŠÁMAL, Pavel et al. *Kodeks karny II. §§ 140-421. Komentarz.* 2. 2. edycja. Praga: C. H. Beck, 2012, s. 2308.

41. ŠULC, Vladimír. *Cyberbezpieczeństwo.* Pilzno: Aleš Čeněk, 2018. s. 20 i nast.

42. *Wywiad: kampania mająca na celu wywarcie wpływu na wybory prezydenckie w USA została zlecona przez Putina.* [online]. [cyt. 2017 Jun 29]. Dostępny pod adresem: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin

43. *Pełny zakres usług CGI Cyber Security* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://mss.cgi.com/service-portfolio

44. *Definicje i zastosowanie protokołu sygnalizacji świetlnej (TLP).* [online]. [cyt. 2018 Jan 13]. Dostępny pod adresem: https://www.us-cert.gov/tlp

45. VALÁŠEK, Jarmil, František KOVÁŘÍK i in. *Zarządzanie kryzysowe w pozamilitarnych sytuacjach kryzysowych*. Praga: Ministerstwo Spraw Wewnętrznych - Dyrekcja Generalna Korpusu Pożarnictwa i Ratownictwa Republiki Czeskiej, 2008 [online]. [cyt. 1 lipca 2018]. Dostępny pod adresem: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx

46. WAISOVÁ, Šárka. *Bezpieczeństwo: rozwój i zmiany koncepcji.* Pilzno: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

47. *WannaCry nie powinien był się w ogóle rozprzestrzeniać. Wystarczyło skorzystać z usługi Windows Update.* [online]. [cyt. 2017 Jun 27]. Dostępny pod adresem: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

48. WIENER, Norbert. *Cybernetyka: czyli sterowanie i komunikacja w organizmach żywych i maszynach.* Praga: Państwowe Wydawnictwo Literatury Technicznej, 1960. 148 s.

49. *Podstawowe pojęcia.* [online]. [cytowany 2018-07-10]. Dostępny pod adresem: https://www.kybez.cz/bezpecnost/pojmoslovi

50. ZEMAN, Petr et al. *Czeska terminologia dotycząca bezpieczeństwa: interpretacja podstawowych terminów* [online]. [cytowany 2018-07-10]. Dostępny na stronie: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

51. *2017 State of Cybersecurity Report* [online]. [cyt. 2018 Jun 29]. Dostępny pod adresem: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf