CSIRT A CERT

Co-funded by the Erasmus+ Programme of the European Union

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

Obsah

1. Úvod

Informace a data představují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj.[1]

Je třeba si uvědomit, že čím více budeme závislí na informačních a komunikačních technologiích[2] a čím více dat o nás tyto technologie budou sbírat a sdílet, tím se staneme zranitelnějšími.

Řadě následků, které jsou způsobeny kybernetickými útoky, lidskou hloupostí či neznalostí, je přitom možné se vyhnout, pokud budou respektovány základní principy kybernetické bezpečnosti.[3]

Kybernetická bezpečnost je de facto něco, co je možné popsat jako neustále se vyvíjející a měnící se proces, který je závislý na řadě proměnných. Těmito proměnnými samozřejmě mohou být data či samotné prvky ICT, jež jsou předmětem ochrany, vlastní nastavené procesy a jejich revize aj. Tím nejvýznamnějším prvkem je však uživatel (ať již koncový uživatel či administrátor), který vlastní prvky kybernetické bezpečnosti aplikuje.

Právě zde se nachází onen pomyslný kámen úrazu spočívající v tom, že vám budou v dobré víře předány informace, návody a postupy, které jsme si osvojili a otestovali. To, co bude prezentováno, je náš náhled na problematiku kybernetické bezpečnosti a procesů s ní spojených. Tyto návody, postupy a doporučení fungují u nás, ale nemusí fungovat u vás, neboť při vlastní implementaci jakýchkoliv bezpečnostních postupů je dobré vycházet z určitých ověřených doporučení, ale především je vhodné individualizovat, modifikovat či měnit tyto postupy v závislosti na specifických podmínkách ať už uživatele samotného, či organizace.

Směrnice EU o bezpečnosti sítí a informací (směrnice NIS) má za cíl vytvořit síť CSIRT "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". [1] Směrnice stanoví, že každý členský stát určí jeden nebo více CSIRT, které budou splňovat požadavky stanovené v bodě 1 přílohy I směrnice (požadavky), které pokrývají alespoň odvětví uvedená v příloze II a služby uvedené v příloze I. v příloze III, odpovědné za řešení rizik a incidentů v souladu s dobře definovaným postupem. Směrnice stanoví vysoké požadavky, které musí jmenované jednotky CSIRT dodržovat, a úkoly, které musí plnit.[4]

[1] Viz informace o ovlivnění prezidentských voleb v USA (2016) a Francii (2017). Blíže viz např.:

Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin. [online]. [cit. 29. 6. 2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin
Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma. [online]. [cit. 29. 6. 2017]. Dostupné z:http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san
[3] *WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

[2] Dále jen ICT

[4] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Dostupné z: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 6

1.1. Kybernetická bezpečnost

„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.“[1]

Vymezení pojmu kybernetická bezpečnost může být do určité míry problematické. Pro řadu lidí představuje kybernetická bezpečnost oblast, kterou se zabývají de facto výhradně oddělení informačních a komunikačních technologií.

Tato premisa je od počátku chybná, neboť kybernetická bezpečnost se týká každého z nás, kdo využívá jakékoliv prvky ICT ve svém každodenním životě. Pokud si sami neuvědomíme, že jsme klíčovým, a v mnoha případech stěžejním prvkem kybernetické bezpečnosti (ať už ve svém soukromí či v práci), tak vlastně zvyšujeme pravděpodobnost úspěchu kybernetických útoků.

Kybernetickou bezpečnost nelze v současné době ani podceňovat ani bagatelizovat. Je to oblast, která je pro řadu organizací, ale i jedinců samotných klíčová, a proto by měla být řešena dlouhodobě a systematicky.

„Management organizací by měl pochopit a akceptovat, že řízení kybernetické bezpečnosti spadá mnohem více k dalším oblastem bezpečnosti a krizového managementu. Vždyť i dnešní sofistikované útoky jsou často multidisciplinární a kombinují v sobě oblasti ICT, sociálního inženýrství, personální a objektové bezpečnosti.“ ***[2]***

Vrátíme-li se k vlastnímu pojmu kybernetická bezpečnost, je vhodné vyjít z rozboru tohoto sousloví. Slovo **kyber** reprezentuje provázanost s prvky informačních a komunikačních technologií a kyberprostorem jako takovým.

Bezpečnost

Definic pojmu **bezpečnost (security)**[3] existuje celá řada, avšak neexistuje žádná jednotná, obecně akceptovaná definice. Většina definic pojmu bezpečnost je uváděna spíše v odborné literatuře, než v legislativě samotné.[4]

Mareš definuje bezpečnost jako *„stav, kdy jsou na nejnižší možnou míru limitovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizace) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat.“*[5]

Požár definuje *„bezpečnost jako vlastnost nějakého objektu nebo subjektu, která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.“*[6]

Tato definice pak byla dále upřesněna ve Výkladovém slovníku kybernetické bezpečnosti:

Bezpečnost (Security)

Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací. [7]

Je třeba si uvědomit, že bezpečnost není v současné době jen otázkou státu, který však v oblasti zajištění bezpečnosti stále hraje primární roli, ale že jde o proces realizovaný i jinými subjekty (právnické a fyzické osoby), které byly v poslední době nuceny se stále více zabývat právě otázkou bezpečnosti, respektive zabezpečení svých aktivit před útoky.

Díky tomuto rozšiřování okruhu bezpečnosti, je nezbytné se zabývat mimo jiné následujícími otázkami:

- **O čí bezpečnost se jedná** (mezinárodní organizace, stát, organizace, jednotlivec aj.)**?**
- **Jaké hodnoty jsou chráněny** (organizace, osoby, data aj.)**?**
- **Před čím jsou (mají být) tyto hodnoty chráněny** (fyzické, kybernetické, kombinované útoky aj.)**?**
- **Jaké prostředky je třeba vynaložit k ochraně těchto hodnot?** [8]

Ideálním cílem bezpečnosti je vytvoření stavu „absolutního bezpečí“. Tento stav je ale utopií, protože jej není možné reálně dosáhnout,[9] neboť vždy bude existovat hrozba či riziko, které nebylo do konceptu tvorby bezpečnosti zahrnuto, nebo bylo záměrně opomenuto.

Smyslem bezpečnosti však není za všech okolností postihnout všechna reálná, méně reálná či zcela nepředpokládatelná a nepravděpodobná rizika, neboť by takovouto implementací vznikl zcela nefunkční moloch, který by ve své podstatě aplikaci a implementaci bezpečnosti popíral, nebo i zcela eliminoval.

Příklad: *Také se vám v běžném životě stane, že si například zabouchnete klíče uvnitř bytu. Pokud jste s touto variantou počítali, máte nejspíš náhradní klíče u rodiny, známých, či jinde. Pokud však nemáte náhradní klíče, zavoláte zřejmě zámečníka, nebo vyrazíte dveře.*

Kybernetická bezpečnost

Stejně jako u pojmu bezpečnost, ani kybernetická bezpečnost nemá jednotnou obecně uznávanou definici. Kybernetická bezpečnost představuje podmnožinu bezpečnosti jako takové.

Při vlastním definování kybernetické bezpečnosti je vhodné vycházet z již ustálených definic. Uvedu několik takto ustálených definic:

1. **Kybernetická bezpečnost** představuje **soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem**.[10]

2. Oxford dictionary uvádí, že **kybernetická bezpečnost** představuje **stav, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat**. Do kybernetické bezpečnosti je pak třeba zahrnout i opatření, která je třeba přijmout k dosažení tohoto stavu.[11]

3. Dle Jiráska a kol. představuje **kybernetická bezpečnost (Cyber Security)** *„**souhrn** právních, organizačních, technických a vzdělávacích **prostředků směřujících k zajištění ochrany kybernetického prostoru.**“*[12]

4. Relativně obdobně je kybernetická bezpečnost definována i v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. V této strategii je uvedeno, že: *„Kybernetická bezpečnost představuje **souhrn** organizačních, politických, právních, technických a vzdělávacích **opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice**, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.“* [13]

Tyto definice se sice snaží vymezit pojem kybernetické bezpečnosti, ale dopouští se určitých nepřesností.

První definice se zaměřuje jen na počítač a počítačový systém a jejich ochranu před dvěma typy kybernetických útoků, přičemž spektrum jak cílů útoků, tak především útoků samotných je značně rozmanitější.[14]

Druhá definice pak chrání pouze elektronická data, a ne počítačové systémy jako takové.

Třetí definice se zaměřuje na přijetí prostředků, které mají sloužit k ochraně prvků ICT v rámci kyberprostoru. Tato definice je relativně přesná, avšak její omezení pouze na kyberprostor může být zavádějící, neboť kybernetickou bezpečnost lze aplikovat i na prvky ICT, které nejsou zapojeny do kyberprostoru, či si vytváří svůj vlastní „off-line kyberprostor“.[15]

Poslední z definic se pak explicitně omezuje pouze na kyberprostor v České republice, přičemž zcela pomíjí možnost ochrany zájmů občanů ČR či dalších subjektů, kteří nejsou usídleni v ČR. Domníváme se, že zúžení kybernetické bezpečnosti pouze na kyberprostor ČR je sice z pohledu implementace zákona o kybernetické bezpečnosti pochopitelné, avšak z pohledu implementace kybernetické bezpečnosti nevhodné.

Další definici kybernetické bezpečnosti je možné nalézt například v dokumentu **Definition of Cybersecurity - Gaps and overlaps in standardisation**[16] Evropské agentury ENISA[17]: *„Kyberbezpečnost se vztahuje na bezpečnost kyberprostoru, kde samotný kybernetický prostor odkazuje na soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a na samotnou sadu objektů, jejichž rozhraní umožňující jejich dálkové ovládání, vzdálený přístup k datům, anebo jejich zapojení do řídících akcí v rámci kyberprostoru. Kyberbezpečnost bude zahrnovat paradigma ‚CIA‘ triády pro vztahy a objekty v rámci kyberprostoru a zároveň bude toto paradigma rozšiřováno z důvodu zajištění ochrany soukromí subjektů (fyzických a právnických osob) a odolnosti [‚zotavení se‘ (recovery) z útoku].“*

Vzhledem ke snaze o definování pojmu kybernetické bezpečnosti je vhodné vycházet i z právních norem, které se kybernetické bezpečnosti věnují.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[18] v čl. 4 odst. 2 uvádí, že *„bezpečnost sítí a informačních systémů představuje schopnost těchto sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.“*

Výše uvedené definice se různými způsoby snaží vymezit okruh vztahů, zájmů a subjektů, vůči kterým dochází k uplatňování kybernetické bezpečnosti. Současně je v nich vymezován i kyberprostor, jakožto prostředí, ve kterém je kybernetická bezpečnost aplikována.

Díky určité nejednotnosti v názorech na to, co vše je a co není kybernetická bezpečnost, je vhodné představit vlastní definici kybernetické bezpečnosti, která vznikla jak na základě analýzy definic předchozích, tak na základě vlastních zkušeností.

Kybernetickou bezpečnost je možné vymezit jako:

§ **souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů,**

§ **schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.**

Kybernetická bezpečnost je realizována jak v rámci kyberprostoru, tak mimo něj. Není vhodné aplikaci výše uvedených prostředků a principů, jakkoliv geolokačně (ať již na území daného státu, Unie či kyberprostoru samotného) omezovat.

---

[1] *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[2] *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29. 6. 2018]. Dostupné z: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

[3] Z pohledu výkladu vlastního pojmu je nutné zmínit relativní nepřesnost češtiny oproti angličtině, která pro pojem bezpečnost využívá typicky dva pojmy: **security** a **safety**. Pojem **security** je využíván ve smyslu aktivní ochrany či aktivního zabezpečení, zajištění či ochrany a pojem **safety** je využíván zpravidla k vyjádření pasivní bezpečnosti, bezpečí, charakteristice stavu či vlastnosti určitého objektu.

[4] Viz např. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky; zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon); zákon o kybernetické bezpečnosti aj.

[5] ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10. 7. 2018]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

[6] *POŽÁR, Josef. Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 37.

[7] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 23. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[8] Blíže viz např. MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

FRANK, Libor. *Bezpečnostní studia.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

[9] Viz WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. 159 s. ISBN 80-86898-2-10

[10] *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.

[11] *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.

[12] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 69. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

[13] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

[14] Napadány mohou být i aplikace, účty uživatelů aj. Pokud se jedná o vlastní útoky, pak jednotlivé útoky jsou popsány např v: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 181 a násl.

[15] Blíže viz např. *Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/ či FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cit. 1. 7. 2018]. Dostupné z: 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]. [cit. 10. 12. 2017]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

[17] The European Union Agency for Network and Information Security

[18] Dále jen **směrnice NIS** či **NIS**. [online]. [cit. 1. 7. 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

1.2. Principy kybernetické bezpečnosti

Při uplatňování kybernetické bezpečnosti dochází k implementaci následujících principů, které jsou také nazývány triády kybernetické bezpečnosti.[1]

Pro účely této monografie budou vymezeny následující tři triády:

1. **CIA** [**C** – **Confidentiality** (důvěrnost); **I** – **Integrity** (celistvost); **A – Availability** (dostupnost)].
2. **Prvky kybernetické bezpečnosti** (**L**idé, **T**echnologie, **P**rocesy).
3. **Životní cyklus kybernetické bezpečnosti** (**P**revence, **D**etekce, **R**eakce).

1.1.1 Triáda CIA

Nejznámější a nejpoužívanější triádou kybernetické bezpečnosti je triáda **CIA**, avšak prosté využívání této základní triády principů kybernetické bezpečnosti bez implementace principů dalších je v současné době k udržení adekvátní úrovně kybernetické bezpečnosti nedostačující.

V odborné literatuře se například poukazuje na uplatňování **Parkerian hexad**[2], což je de facto triáda CIA, která je doplněna o další tři prvky: **P/C - Possession/Control** (držení či kontrola), **A – Authenticity** (autentičnost) a **U – Utility** (užitečnost).

Smyslem kybernetické bezpečnosti je zajistit jak bezpečnost ICT jako takových, tak i zejména dat a informací, které jsou těmito prvky přenášeny, zpracovávány a uchovávány.

Velmi často je triáda CIA vztahována primárně právě k informacím.

Toto užší pojetí vyplývá zejména z vlastní definice **informační bezpečnost**i, která se zaměřuje na ochranu informací. V rámci této ochrany pak není podstatné, na jakém typu nosiče (papír, elektronická média aj.) či v rámci jakého systému jsou informace zpracovávány. Informační bezpečnost je pak aplikována na informace po celý jejich životní cyklus.

Informační bezpečnost je definována i řadou norem ISO 27000. Mezi základní normy informační bezpečnosti patří:

- ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
- ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací

Otázkou je, zda je v současné době vymezení pojmu informační bezpečnost adekvátní a dostačující, respektive zda se vztahuje na všechny klíčové prvky bezpečnosti v rámci kyberprostoru.

I přes skutečnost, že v odborné literatuře i právních normách je běžněji využíván pojem informační bezpečnost, jsme přesvědčeni, že ve vztahu k aktivitám spojeným s využíváním ICT, respektive k aktivitám souvisejícím s kyberprostorem, je vhodnějším pojmem pojem kybernetická bezpečnost.

Jak již bylo uvedeno výše: *„informační bezpečnost se vztahuje na informace jako takové“*. Tímto však dochází k opomenutí klíčových prvků, které se k bezpečnosti v kyberprostoru vztahují.

Za tyto významné prvky považujeme **data a** pak samotné **počítačové systémy** (resp. jednotlivé prvky ICT), které umožnují vlastní přenos dat a informací.

V odborné literatuře i v právních předpisech existuje celá řada definic pojmů data a informace. Pro účely této publikace jsou vybrány definice, které se vztahují k problematice ochrany informací, dat či ke kybernetické bezpečnosti.

Dle Úmluvy o kyberkriminalitě[3] se **počítačovými daty** rozumí *„**jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému**, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.“*

Data jsou tedy jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačovým systémem, přičemž jsou zpracovávány tak, aby následně utvořila informaci.

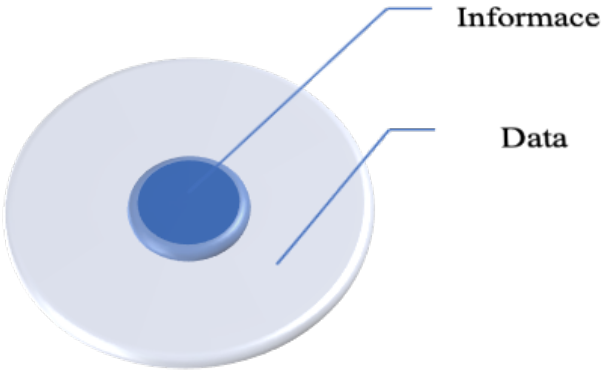
Informace *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“*[4]

Wiener tvrdí, že *„informace je název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.“* Dále také uvádí, že informace není ani hmotou ani energií, ale samostatnou fyzikální kategorií.[5]

Informace jsou tedy vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.[6]

Právě ono propojení „bezvýznamných“ dat a vytvoření určitého kontextu, který z dat teprve složí „významnou“ informaci, může být klíčové z pohledu kybernetické bezpečnosti. Pokud bychom totiž respektovali výše uvedenou tezi informační bezpečnosti, v rámci které jsou chráněny pouze informace jako takové, pak by mohlo dojít k výraznému narušení bezpečnosti.

Vztah dat a informací demonstruje následující graf.[7]



Data a informace jsou v rámci kyberprostoru přenášeny pomocí počítačových systémů[8], jež jsou nedílnou součástí kybernetické či informační bezpečnosti.

Na základě výše uvedeného jsme přesvědčeni, že je třeba triádu CIA[9] uplatňovat nejen na informace samotné, ale i na další prvky kybernetické bezpečnosti (data, počítačové systémy atp.)

Důvěrnost (Confidentiality)

Pojem důvěrnost definuje tu skutečnost, že k informacím, datům, či ICT mají přístup pouze subjekty, které jsou k tomu autorizované (oprávněné).

Vzhledem k velkému rozsahu zpracovávaných informací je vhodné zavést či aplikovat některou z klasifikací informací. Tyto klasifikace je pak možné aplikovat i na ostatní prvky kybernetické bezpečnosti a přístup k nim.

Bezpečnostní standardy ISO/IEC 27000 definují že:

- *„Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.“*
- *„Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“*
- *„Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.“*

Příklady některých klasifikačních schémat:

1. **Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti**[10]:

- **Přísně tajné (Top secret)** - neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážnou újmu zájmům České republiky.
- **Tajné (Secret)** - neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu zájmům České republiky.
- **Důvěrné (Confidential)** - neoprávněné nakládání s informacemi by mohlo způsobit prostou újmu zájmům České republiky.
- **Vyhrazené (Restricted) -** neoprávněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republikyněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republiky.

2. **Klasifikace informací využívaná v komerční sféře**:

- **Chráněné -** neoprávněné nakládání s informacemi by mohlo způsobit závažné poškození či zničení organizace (např. únik strategických informací, zdrojových kódů, schémat zabezpečení, hesel aj.).
- **Interní -** neoprávněné nakládání s informacemi by mohlo způsobit poškození organizace (např. únik osobních údajů, smluv aj.).
- **Citlivé -** neoprávněné nakládání s informacemi by mohlo mít negativní dopad na společnost (např. dosud nezveřejněné informace o projektech, plánovaných akcích aj.).
- **Veřejné -** neoprávněné nakládání s informacemi by nemělo nikoho poškodit a nemělo by mít jakýkoliv dopad na společnost (např.

veřejně dostupné kontakty, prezentace projektů aj.).[11]

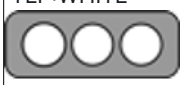
Vedle dvou výše uvedených klasifikací existuje celá řada dalších klasifikací, které jsou v rámci organizací či jednotlivci samotnými přijímány či akceptovány ať již na základě právního předpisu, či uvážení uživatele samotného.

Klasifikace samotné, za předpokladu, že jsou respektovány a dodržovány, mohou výrazně zmírnit dopad případného kybernetického útoku.

3. Traffic Light Protocol

V rámci komunity kybernetické bezpečnosti vznikla v minulosti potřeba sdílet informace a data (typicky o kybernetických útocích), která mají citlivou povahu. Z tohoto důvodu byl v National Infrastructure Security Coordination Centre[12] vytvořen na počátku roku 2000 **protokol TLP** (***Traffic Light Protocol***)[13]. Tento protokol si klade za cíl zrychlit výměnu informací mezi zainteresovanými subjekty a zároveň stanovuje pravidla pro nakládání s předávanými informacemi. Subjekt, který předává informace (zdroj informace), vždy označí informaci určitou barvou, která stanovuje, jak má daný příjemce s informací nakládat.

Protokol TLP je nejvhodněji vymezen v následující tabulce, která byla převzata z US-CERT[14]:

Barva	**Kdy má být použita**	**Jak lze sdílet?**
TLP:RED  **Neurčeno k zveřejnění,** pouze pro účastníky.	Subjekty mohou používat TLP: RED v případech, kdy informace neumožňuje účinnou reakci dalších subjektů a mohly by vést k dopadům na soukromí, pověst nebo operace těchto subjektů, pokud by byly zneužity.	Příjemci nesmějí sdílet informace zařazené v kategorii TLP: RED s žádnými subjekty mimo konkrétní výměnu, schůzku nebo konverzaci, v rámci které byly informace TLP:RED původně zveřejněny. V rámci schůzky (setkání) se například informace TLP: RED omezuje na ty osoby, které se schůzky (setkání) přímo účastní. Ve většině případů **by informace označené TLP: RED měly být vyměňovány pouze verbálně nebo osobně.**
TLP:AMBER  **Omezené zveřejnění.** Zveřejnění je možné jen v organizaci účastníků.	Subjekty mohou používat TLP: AMBER, v případech, kdy informace vyžadují účinnou reakci dalších subjektů a přináší riziko pro soukromí, pověst nebo operace, v případě, že jsou sdíleny mimo zúčastněné organizace.	Příjemci mohou sdílet informace zařazené v kategorii TLP: AMBER s členy své vlastní organizace a s klienty nebo zákazníky, kteří potřebují tyto informace znát, aby se mohli chránit nebo zabránili dalšímu případnému poškození. **Subjekty mohou volně stanovovat další pravidla sdílení, at tato musí být dodržována.**
TLP:GREEN  Omezené zveřejnění, omezené na komunitu.	Subjekty mohou používat TLP: GREEN, pokud jsou informace užitečné pro zvýšení informovanosti všech zúčastněných organizací. Také je možné tyto informace sdílet s dalšímy subjekty v rámci širší komunity nebo sektoru.	Příjemci mohou sdílet informace zařazené v kategorii TLP: GREEN s partnery a partnerskými organizacemi v rámci svého sektoru nebo komunity. Informace však není možné sdílet prostřednictvím veřejně přístupných kanálů. Informace v této kategorii mohou být v rámci dané komunity komunity masivně rozšiřovány. **Informace zařazené v kategorii TLP: GREEN nesmí být uvolněna mimo komunitu.**
TLP:WHITE  Zveřejnění není nijak omezeno.	Subjekty mohou používat TLP: WHITE, pokud informace obsahují minimální nebo žádné předvídatelné riziko zneužití v souladu s platnými pravidly a postupy pro zveřejnění.	V souladu s pravidly a ochranou práv autorských mohou být **informace zařazené v kategorii TLP: WHITE distribuovány bez omezení.**

„O nežádoucím zpřístupnění (disclosure) určitých informací se v kybernetické bezpečnosti hovoří jako o narušení jejich důvěrnosti, či úniku (leakage).“[15]

4. Hodnocení důvěrnosti dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)[16]

Vyhláška o kybernetické bezpečnosti do značné míry přebírá výše představený Traffic Light Protocol pro stupnici hodnocení důvěrnosti (viz příloha č. 1 VoKB).

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká		

	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení **TLP:WHITE**.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP:GREEN** nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP:AMBER**.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo **TLP:AMBER**.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4.

Integrita (Integrity)

Dle Výkladového slovníku kybernetické bezpečnosti[17] je **integrita** definována jako *„vlastnost přesnosti a úplnosti.“* **Integrita dat** je pak ve stejném slovníku definována jako *„jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.“* **Integrita systému** pak je *„vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.“*

Integrita tedy představuje nemožnost zásahu do informací, dat, počítačových systémů, jejich nastavení atp. **jinou osobou, než tou, která je k takovému úkonu oprávněna.**

Zároveň integrita představuje jakousi záruku neporušenosti systému, informací či dat.

„O nežádoucí modifikaci (alteration) se proto v informační bezpečnosti hovoří jako o narušení integrity (integrity).“[18]

V případě, že dojde k porušení integrity, je třeba si uvědomit, že pokud dojde k nežádoucí změně dat, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout značná doba, než je porušení integrity zjištěno.

Vyhláška o kybernetické bezpečnosti v příloze č. 1 představuje také stupnici pro hodnocení integrity.

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká		Není vyžadována žádná ochrana.

	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Dostupnost (Availability)

Dle Výkladového slovníku kybernetické bezpečnosti[19] je **dostupnost** definována jako *„vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.“*

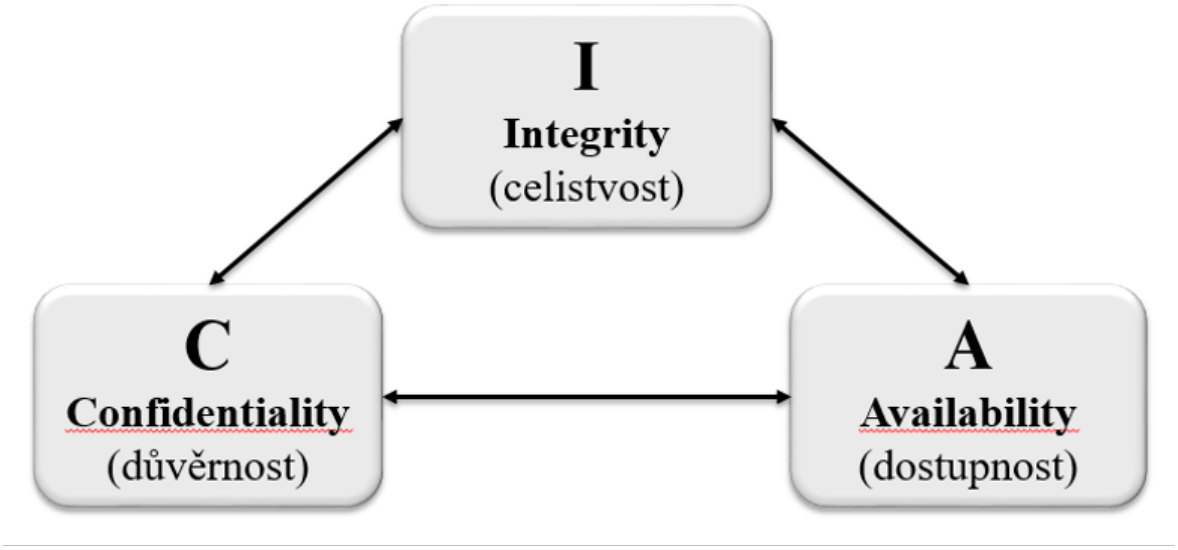
Dostupnost je tedy možné definovat jako garanci možnosti přístupu k informaci, datům, nebo počítačovému systému v okamžiku potřeby. Sebedokonalejší systém zajišťující integritu a umožňující přístup k systému samotnému, datům či informacím je nevyužitelný, pokud nebude zajišťovat spolehlivý přístup dle potřeby.[20]

„O zničení (destruction) určitých informací se v informační bezpečnosti hovoří jako o narušení jejich dostupnosti (availability).“ [21]

Vyhláška o kybernetické bezpečnosti v příloze č. 1 představuje i stupnici pro hodnocení dostupnosti.

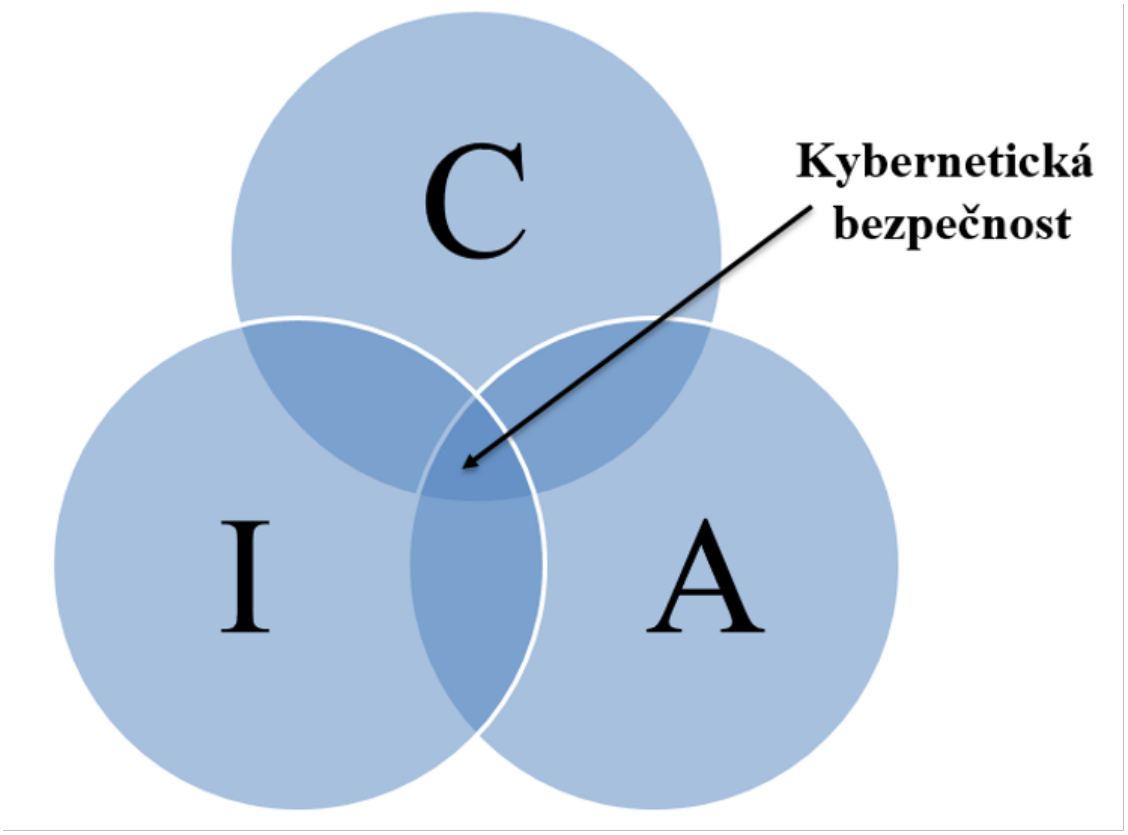
Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Triáda CIA bývá mnohdy pro lepší pochopení jejích jednotlivých atributů a vztahů znázorňována graficky. I z tohoto důvodu je na tomto místě prezentováno typické znázornění triády CIA. V další části této kapitoly je pak tato triáda doplněna o prvky (technologie, lidé, procesy).



Obrázek 1: Triáda CIA

Pokud bychom se snažili vymezit prostor kybernetické bezpečnosti v rámci implementace triády CIA, pak by tento prostor bylo možné zobrazit jako průnik jednotlivých principů této triády.



Obrázek 2: Triáda CIA a kybernetická bezpečnost

Obrázek 3: Zobrazení Parkenian hexad[22]

1.1.2 Prvky kybernetické bezpečnosti

Následující tři prvky, respektive jejich vzájemná interakce, umožňují do určité míry vytvořit či nastolit kybernetickou bezpečnost. Těmito prvky jsou:

- **lidé**,
- **technologie** a
- **procesy**.

Domníváme se, že je utopické si myslet, že je možné vytvořit absolutní kybernetickou bezpečnost či absolutně zabezpečený systém, v rámci něhož jsou využívány prvky ICT.

Teoreticky by sice bylo možné si představit zcela izolovaný počítačový systém (včetně zdroje napájení např. pomocí agregátu), uzavřený ve Faradayově kleci, se zcela jasně definovaným okruhem osob, které jsou oprávněny na tomto počítačovém systému pracovat, s tím, že není možné vnášet ani vynášet žádná média (elektronická či jiná) z tohoto unikátního prostředí.

Otázkou však je, k čemu by takto zabezpečený systém sloužil a jakým způsobem by byly využity výsledky práce na tomto systému, respektive jak by bylo možné tyto výsledky uvést v život, když není možné vynášet výsledky činnosti. Protiargumentem by pak mohlo být tvrzení, že vyneseny budou výsledky až v okamžiku ukončení projektu, do té doby bude vše chráněno a přístup bude podléhat již výše uvedenému režimu.

Nicméně je otázkou, zda takto uměle vytvořený a zcela izolovaný systém je chráněn i proti dalším hrozbám, kterými může být neexistence záloh, možnost fyzického zničení počítačového systému, vyzrazení dílčích informací lidmi, kteří s daným systémem pracují atd.

Jakýkoliv systém je tak bezpečný, jak bezpečný je jeho nejslabší článek (prvek).

Lidé

> *„People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.“*
>
> Bruce Schneier[23]

Na lidi v interakci s kybernetickou bezpečností je možné nahlížet jako na:

- **strůjce (tvůrce) této bezpečnosti** (tj. typicky osoby, které se snaží prosadit a implementovat jednotlivé prvky kybernetické bezpečnosti, ať již ve vztahu k sobě samotnému, či ve vztahu k organizaci),
- **příjemce pravidel kybernetické bezpečnosti** (tj. osoby, které se rozhodly či jsou nuceny implementovat již existující pravidla kybernetické bezpečnosti),
- **subjekty, které je třeba chránit před kybernetickými útoky**,
- **subjekty, které je třeba informovat a proškolit o pravidlech a principech kybernetické bezpečnosti**,
- **riziko či hrozbu v rámci vytváření a udržování kybernetické bezpečnosti**.

Pokud se zaměříme na roli lidí v rámci budování a udržování kybernetické bezpečnosti, zejména v souvislosti se ZoKB, pak je třeba definovat a vhodným způsobem personálně zajistit následující pozice:

- výbor kybernetické bezpečnosti,
- manager kybernetické bezpečnosti,
- architekt kybernetické bezpečnosti,
- auditor kybernetické bezpečnosti,
- tým kybernetické bezpečnosti,
- garant,
  - primárních aktiv,
  - podpůrných aktiv,
- věcný správce,
- technický správce,
- provozovatel (někdy také označován jako dodavatel),
- administrátor,
- uživatel.

Lidé představují klíčový prvek jakékoliv bezpečnosti. V případě kybernetické bezpečnosti se jejich role ještě umocňuje a typicky jsou právě lidé oním nejslabším prvkem a současně nejčastějším cílem útočníků.

Důvodů, které nás vedou k tomuto tvrzení, je několik.

Tím prvním je relativně krátká doba, po kterou skutečně využíváme počítačové systémy. Většina uživatelů začala využívat některý z počítačových systémů teprve po roce 1990, k Internetu jsme se masověji začali připojovat okolo roku 1995 a „chytré" mobilní telefony využíváme přibližně od roku 2007. Řadu sociálních sítí, které v současné době považujeme za nezbytnou součást, bez které si nedovedeme svůj život představit, však nevyužíváme více než 10 let.

Druhý důvod spočívá v obrovské dynamice vývoje jak hardwaru, tak zejména softwaru, který se s naší interakcí v digitálním světě neodmyslitelně pojí. Právě dynamika vývoje softwaru neumožňuje řadě uživatelů, aby se podrobněji zabývali otázkami bezpečnosti, které se nevyhnutelně právě k používání softwaru pojí.

Třetím a posledním důvodem je ta skutečnost, že život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný. ICT a aplikace s těmito technologiemi spojené vytváří digitální avatary nás samotných, avšak s mnohem větším množstvím informací, než jsme si jako fyzické osoby schopné zapamatovat či uchovat. Tuto skutečnost si kromě výrobců hardwaru i softwaru uvědomují i útočníci a právě z tohoto důvodu cíleně útočí na lidi v kyberprostoru.

„Amateurs hack systems, professionals hack people."

Bruce Schneier[24]

Dle našeho názoru je nezbytné, aby lidé, kteří užívají ICT a rozhodli se pro interakci v kyberprostoru:

- **pochopili** alespoň **základní principy a pravidla**, která se vztahují ke kybernetické **bezpečnosti**,
- **porozuměli** alespoň **základním funkcím počítačových systémů** (např. PC, notebook, mobil, smart TV aj.), **které** k této interakci **používají**,
- **zanalyzovali si aplikace, které** k této interakci **používají**, a případně, pokud jim činnost těchto aplikací či jejich smluvní podmínky nevyhovují, aplikace nevyužívali,
- **vzdělávali se** v oblasti kybernetické bezpečnosti.

Proto, abychom usnadnili alespoň poslední položku z výše uvedeného seznamu, jsme se rozhodli vytvořit tuto publikaci a shrnout v ní alespoň dílčí poznatky, které mohou využít jak laičtí uživatelé, tak IT pracovníci, kteří se rozhodli věnovat zvýšenou pozornost právě oblasti kybernetické bezpečnosti.

Technologie

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier[25]

Technologie pro uživatele zpravidla představují prostředek, který mu umožní připojit se k Internetu, sociálním sítím a dalším aplikacím. Je to nástroj, který využívá různé kancelářské balíčky při tvorbě dokumentů, zasílá e-maily, sleduje video aj. Běžný uživatel zpravidla vnímá a interaguje s koncovými technologiemi (PC, tablet, mobilní telefon aj.), které sám osobně využívá, přičemž o další technologické vrstvy, které jsou nezbytné pro jeho činnost v kyberprostoru, se zpravidla nezajímá.

Pro organizace pak technologie představují celou škálu zařízení od technologií určených pro uživatele (desktop, mobilní zařízení aj.), přes kompletní infrastrukturu sítě (LAN, aktivní prvky, Wi-Fi prvky aj.) a služeb (servery, aplikace aj.), po prvky, které slouží k zajištění zabezpečení ať již na perimetru (firewall[26], IDS/IPS[27], honeypot[28] aj.), tak v rámci infrastruktury (prvky určené k autentizaci a autorizaci, monitoringu, analýze aj.).

V rámci budování a udržování kybernetické bezpečnosti je třeba analyzovat stávající aktiva a na základě této analýzy případně doplnit či modifikovat stávající systémy. V rámci technologií by měly být nedílnou součástí ICT organizace, s ohledem na specifika té které organizace, následující prvky:

- detekční systémy - Intrusion Detection System (**IDS**)/Intrusion Prevention System (**IPS**),
- centrální správa uživatelů a rolí,
- centralizovaná správa klasifikace informací,
- ochrana před škodlivým kódem (aplikační firewall, antivirové, antispamové a jiné řešení),
- technologie pro zaznamenávání činností jednotlivých prvků ICT, administrátorů a uživatelů (**log system)**,
- aktivní a offline zálohovací systémy; zálohy vitálních serverů, aplikací a databází (**recovery system)**,
- správa síťové bezpečnosti (VLAN, DMZ, firewall aj.).

Technologie jsou zpravidla tou součástí kybernetické bezpečnosti, na které, ať již jako sami uživatelé či organizace, nešetříme. Za technologie jsme ochotni zaplatit nemalou část finančních prostředků, buď z důvodu, že „potřebujeme nejnovější telefon“, či z reálného a opodstatněného důvodu spočívajícího v zastaralosti a dalším nepodporování (aktualizaci) daného počítačového systému.

Proto, aby bylo možné zajistit kybernetickou bezpečnost, je třeba udržovat technologie v takovém stavu, aby byly schopny reagovat na změny, které se k vývoji ICT pojí. Zejména by měly být technologie (jak hardware, tak software) udržovány aktualizované a zabezpečené.

Byť jsou technologie jistě významnou součástí procesu tvorby a udržování kybernetické bezpečnosti, jsou dle našeho názoru součástí nejméně významnou. Mnohem významnějšími prvky kybernetické bezpečnosti jsou vhodně nastavené procesy a lidé, kteří umějí dané procesy v praxi aplikovat či modifikovat a předem dohodnutá pravidla dodržovat.

Procesy

*„The mantra of any good security engineer is: ‚**Security is a not a product, but a process.**‘ It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.“*

Bruce Schneier[29]

Procesy představují činnost, kterou je třeba vynaložit, aby bylo možné technologie a s nimi spojené služby používat lidmi.

Z hlediska plynutí času je možné sledovat procesy:

- řízení aktiv a rizik,
  - definování a kategorizace aktiv,
  - analýza a kategorizace rizik,
- implementace ICT a aplikací,
- správa uživatelů a rolí,
- autorizace a autentizace,
- údržby (aktualizace) systémů a služeb,
- testování zabezpečení jednotlivých počítačových systémů a služeb,
- analýza nápravných opatření,
- realizace nápravných opatření,
- audit kybernetické bezpečnosti,
- detekce anomálií či kybernetických útoků,
- reakce na kybernetické útoky či jiné incidenty,
- procesy k zajištění kontinuity,
- školení a cvičení atd.

Výše uvedený výčet jednotlivých procesů, které se pojí k vytváření a udržování kybernetické bezpečnosti, rozhodně není úplný, přičemž nastíněné procesy mohou být granularizovány. Jednotlivé procesy jsou realizovány v rámci celého životního cyklu ICT, informací, dat a ve vztahu k uživatelům.[30]

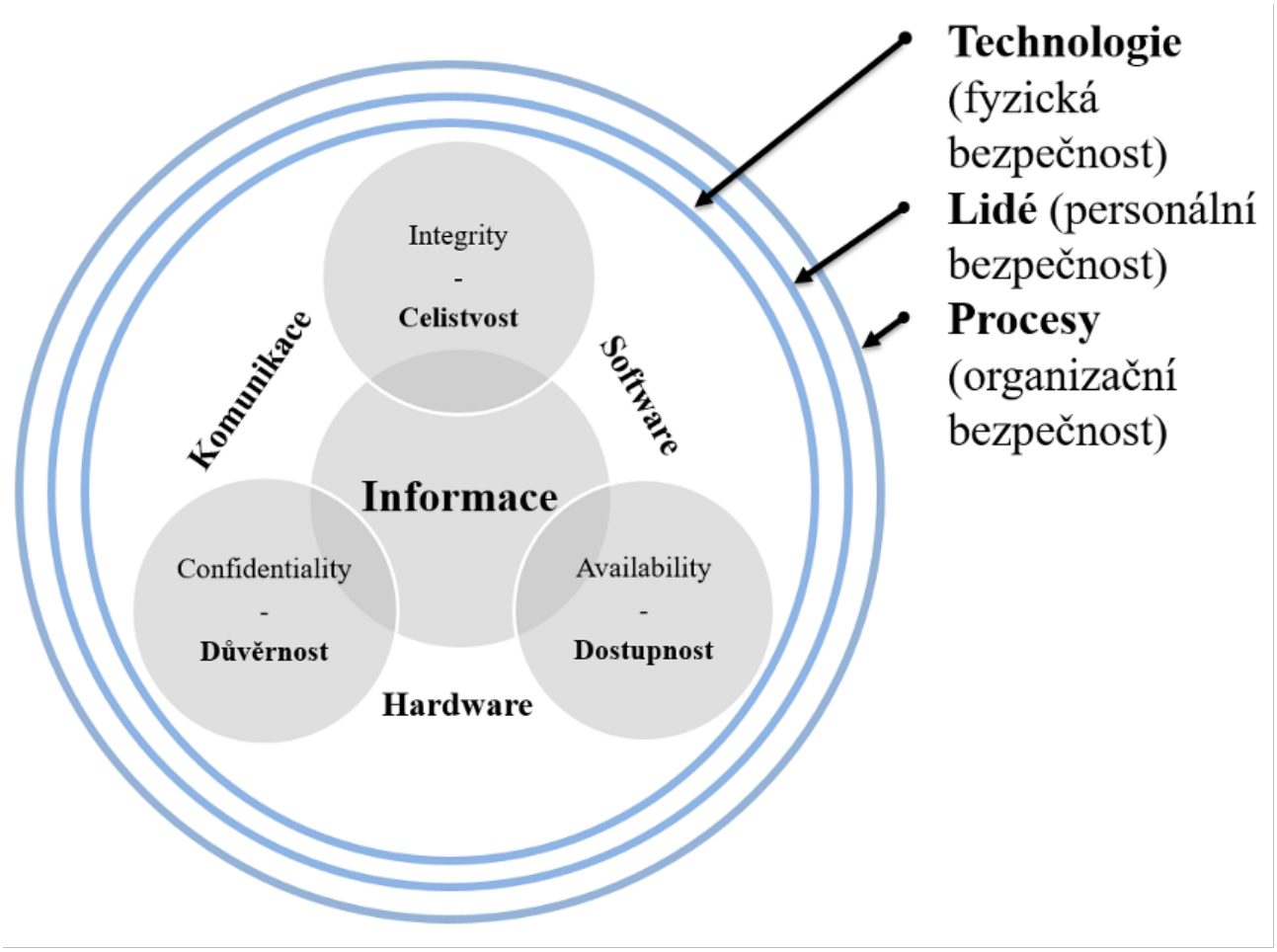
Vlastní nastavení procesů, jejich neustálá údržba či modifikace představuje nejnáročnější část budování kybernetické bezpečnosti. Zároveň tato činnost klade nejvyšší nároky na správce jednotlivých systémů.

Pokud se organizace rozhodne implementovat pravidla kybernetické bezpečnosti, pak je samozřejmě vhodné udržovat hardware i software aktualizovaný, dodržovat pravidla, která jsou nastavena pro přístup k jednotlivým systémům aj.

Pokud je to možné, je vhodné v organizaci provádět i simulace typických kybernetických útoků (např. phishing, business e-mail compromise aj.) z důvodu reálné demonstrace těchto útoků a možných dopadů, pokud se osoba stane obětí takovýchto útoků.

Penetrační testování zároveň umožňuje nalézt chyby v již nastavených procesech.

Organizace by se však již při tvorbě a nastavování pravidel kybernetické bezpečnosti měla primárně zaměřit zejména na oblast lidských zdrojů a jejich edukaci.

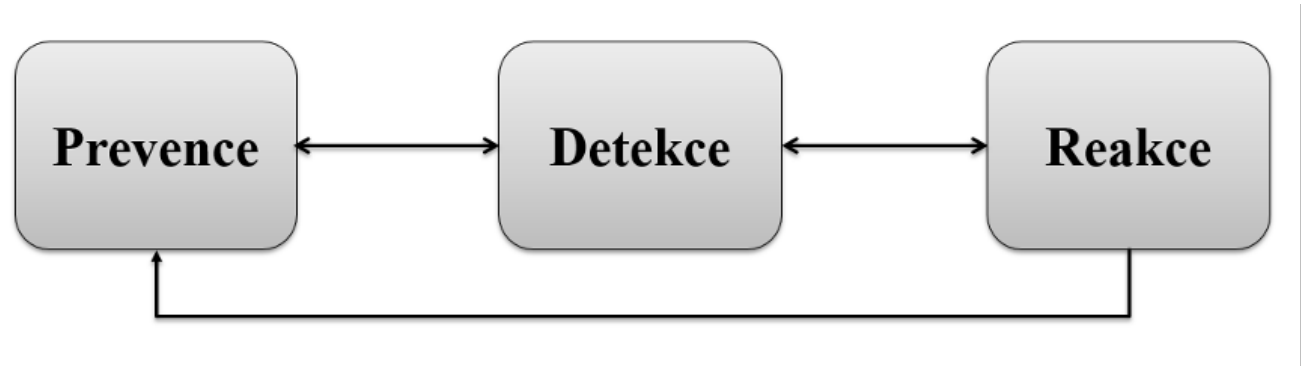


Obrázek 4: Triáda CIA doplněná o technologie, lidi a procesy[31]

1.1.3 Životní cyklus kybernetické bezpečnosti

Z pohledu plynutí času je při realizaci kybernetické bezpečnosti třeba uplatňovat, případně modifikovat jak triádu CIA, tak dílčí prvky kybernetické bezpečnosti v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.[32]

Velmi často je životní cyklus kybernetické bezpečnosti zobrazován pomocí různých diagramů. Pro přehlednost uvádím některé z nich.

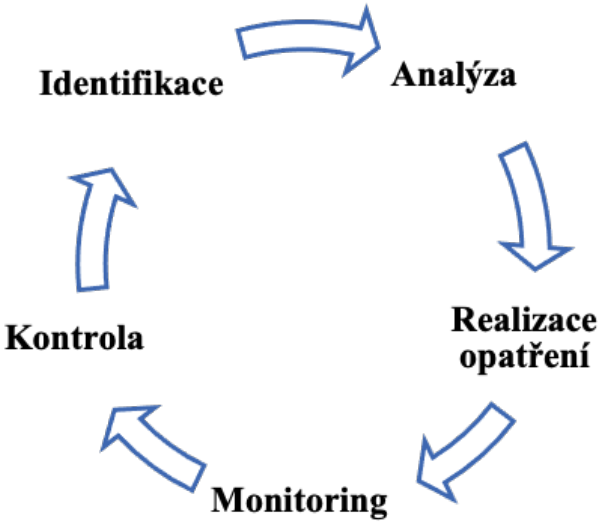


Obrázek 5: Zjednodušené zobrazení životní cyklu kybernetické bezpečnosti

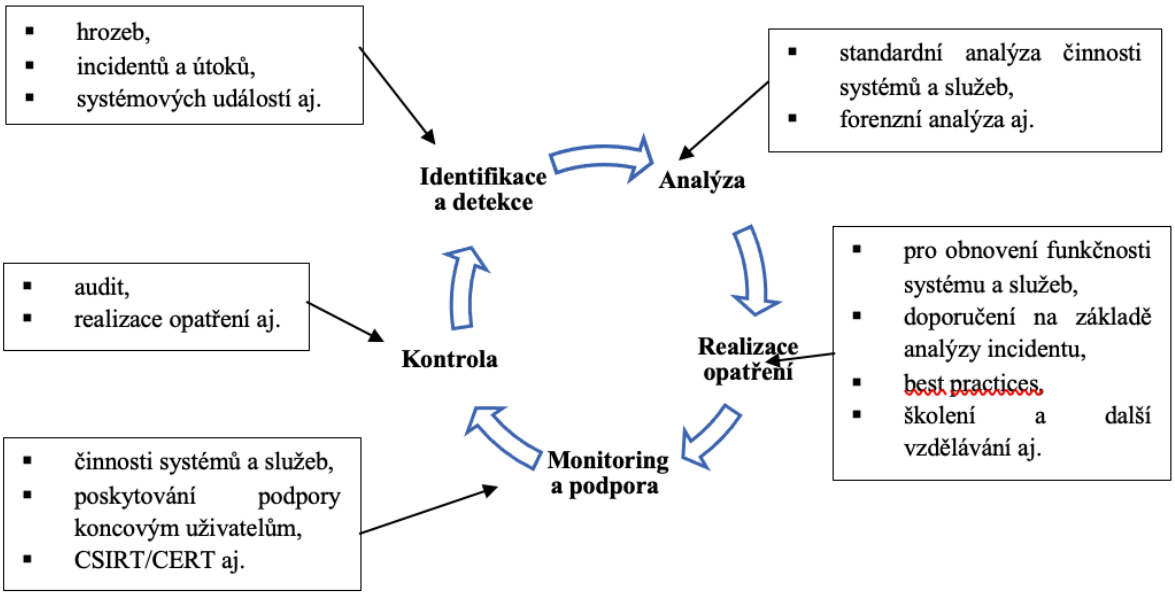
Obrázek 6: Životní cyklus kybernetické bezpečnosti dle kybez.cz[33]

Při řešení kybernetické bezpečnosti neexistuje žádný „záchytný bod", v rámci kterého by bylo možné říci: *„Zvládli jsme to! Jsme chráněni proti kybernetickým útokům či hrozbám. Jsme kyberneticky bezpeční."*

Budování a udržování kybernetické bezpečnosti je možné přirovnat k nikdy nekončící analýze rizik, avšak s tím, že tuto běžnou analýzu je třeba doplnit o další podpůrné procesy, které mohou pomoci se zvýšením kybernetické bezpečnosti v organizaci.



Obrázek 7: Analýza rizik



Obrázek 8: Životní cyklus kybernetické bezpečnosti

Vlastní znázornění životního cyklu kybernetické bezpečnosti může být značně komplexnější.[34]

Obrázek 9: Příklad řešení kybernetické bezpečnosti

Evoluce kybernetické bezpečnosti

Na závěr této subkapitoly by bylo možné si položit jednoduchou otázku: *„Proč bych se měl já (jako jedinec), nebo organizace vůbec zabývat kybernetickou bezpečností?“*

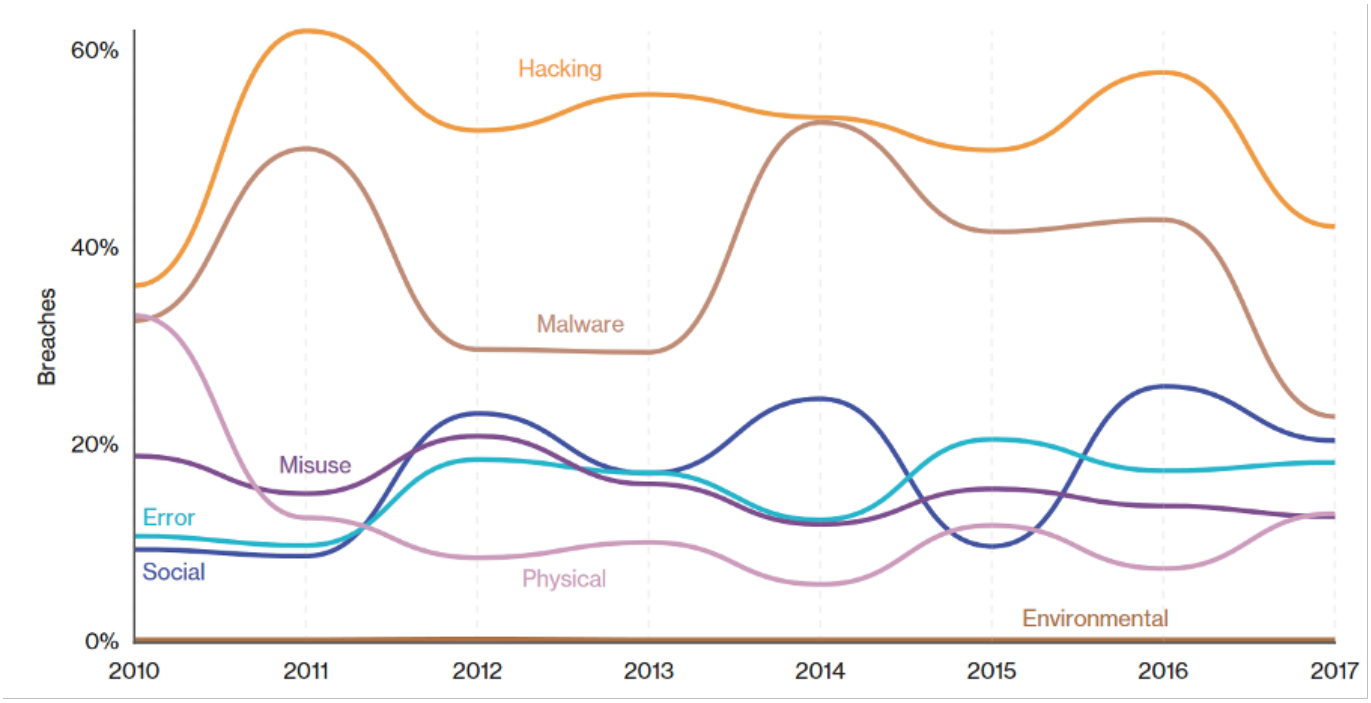
Odpověď nebude až tak komplikovaná, byť bude nutné rozbít mnohdy zakořeněný mýtus, že někdo jiný, ať již velké organizace typu Microsoft, Google, Apple či poskytovatelé cloudových služeb, konektivity atd., za mě problematiku kybernetické bezpečnosti již řeší.

Pravdou je, že tyto organizace zavedly a aplikují dílčí prvky kybernetické bezpečnosti, avšak kybernetická bezpečnost, stejně jako bezpečnost jakákoliv jiná, vždy začíná a končí u konkrétní osoby či organizace, která se chce zabezpečit, a to vždy s ohledem na specifika dané osoby či organizace.

Z Data Breach Investigations Report[35], která se zabývá narušení bezpečnosti vedoucím ke kompromitaci dat, za rok 2017 vyplývají následující fakta:

- útočníkem byla
  - **osoba mimo organizaci - 73 %**
  - osoba v rámci organizace - 28 %
  - **organizovaná zločinecká skupina – 50 %**
- k útokům bylo využito:
  - **hackingu - 48 %**
  - **malware - 30 %**
- **49 % malware** bylo útočníkem distribuováno a následně nainstalováno **skrze e-mail**
  - **sociálního inženýrství - 43 %**
  - fyzického útoku - 8 %[36]
- oběťmi jsou organizace působící ve:
  - zdravotnictví – 24 %
  - veřejném sektoru (typicky státní správa a samospráva aj.) – 14 %
- motiv útoku:
  - **obohacení se – 76%**
  - zisk dat a informací (špionáž) – 13 %
- **68 % útoků bylo odhaleno až po několika měsících, či po delší době**

Následujících graf prezentuje vývoj jednotlivých útoků od roku 2010 do konce roku 2017.



Obrázek 10: Typy útoků použitých k narušení bezpečnosti[37]

Dle zprávy Národního úřadu pro kybernetickou a informační bezpečnost[38] *„**lze v roce 2018 očekávat další nárůst kybernetických hrozeb,** zejména další phishingové útoky nové generace, útoky na tržiště, peněženky a směnárny kryptoměn, bezsouborové varianty ransomware, využívání umělé inteligence ke kybernetickým útokům, útoky na data v Cloudových řešeních, útoky na internet věcí, průmyslové systémy atd. **Očekává se, že se zvýší podíl státních nebo státem podporovaných aktérů kybernetických útoků, že bude i nadále docházet k masivním únikům osobních dat, hesel a přístupových údajů.** Proto je nezbytné budovat kybernetickou bezpečnost informačních a komunikačních systémů důležitých pro chod státu a jeho kritické infrastruktury.“*[39]

Oblast kybernetické bezpečnosti bude do budoucna jednou z nejvýznamnějších oblastí, neboť lze předpokládat, že k redukci využívání ICT a služeb s těmito technologiemi spojených nedojde. Kybernetická bezpečnost má pomáhat při identifikaci nedostatků v nastavení těchto systémů a služeb.

„Kybernetická bezpečnost také pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.

Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka“ [40]

---

[1] Viz např. HSU, D. Frank a D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. s 41.

KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21. 7. 2018]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

[2] Blíže viz např. *Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/

[3] Čl. 1 písm. b) Úmluvy o kyberkriminalitě. *Úmluva o kyberkriminalitě.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

[4] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

[5] Blíže viz WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s s. 32 a násl.

[6] ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vyd. Praha: C. H. Beck, 2012, s. 2308

[7] POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

[8] Blíže viz: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 57 a násl.

[9] Blíže viz např. EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440

HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, availability.* [online]. [cit. 13. 1. 2018]. Dostupné z: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[10] Blíže viz https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/

[11] Srov. dále: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 20 a násl.

[12] V současnosti Centre for Protection of National Infrastructure - CPNI

[13] Blíže viz např. *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

[14] *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

[15] ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 19

[16] Dále jen vyhláška o kybernetické bezpečnosti či **VoKB**.

[17] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 58. [online]. [cit. 10. 7. 2018]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

[18] ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 22

[19] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 43. [online]. [cit. 10. 7. 2018]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

[20] Viz např. EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

[21] ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 24

[22] *The Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[23] SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570039

[24] SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570035

[25] SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570040

[26] Firewall je systém obsahující pravidla, dle kterých se řídí datové toky v rámci síťových technologií.

[27] **IPS** (**I**ntrusion **P**revention **S**ystem), zařízení monitorující nežádoucí (škodlivé) aktivity v síti a/nebo aktivity počítačových sytémů. Dále jen **IPS.**

IDS (**I**ntrusion **D**etection **S**ystem) představuje systém má za úkol detekovat neobvyklé aktivity, které mohou potencionálně vést k narušení bezpěčnosti počítačové sítě, počítačových systémů, aplikací aj. Dále jen **IDS.**

[28] Honeypot je systém jehož smyslem je detekovat malware či další nežádoucí aktivity, které jsou následně v tomto uměle vytvořeném prostředí analyzovány.

[29] SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570047

[30] Pojem uživatele je tady používán pro vyjádření fyzické osoby, která je oprávněna využívat prvky ICT, jednotlivé systémy a aplikace. Z tohoto hlediska se tedy uživatelem rozumí jak osoba s oprávněními správce, tak koncový uživatel.

[31] Předlohou grafu byl graf zveřejněný v: *CIA triad methodology.* [online]. [cit. 10. 7. 2018]. Dostupné z: *https*://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

[32] Blíže viz SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23. 9. 2014)

[33] *Základní pojmy.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

[34] *The complete breadth of CGI Cyber Security services.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://mss.cgi.com/service-portfolio

[35] *2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

[36] V rámci jednotlivých útoků zpravidla dochází ke kombinování technik a nástrojů.

[37] *2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf s. 7

[38] Dále jen **NÚKIB**

[39] *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

[40] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

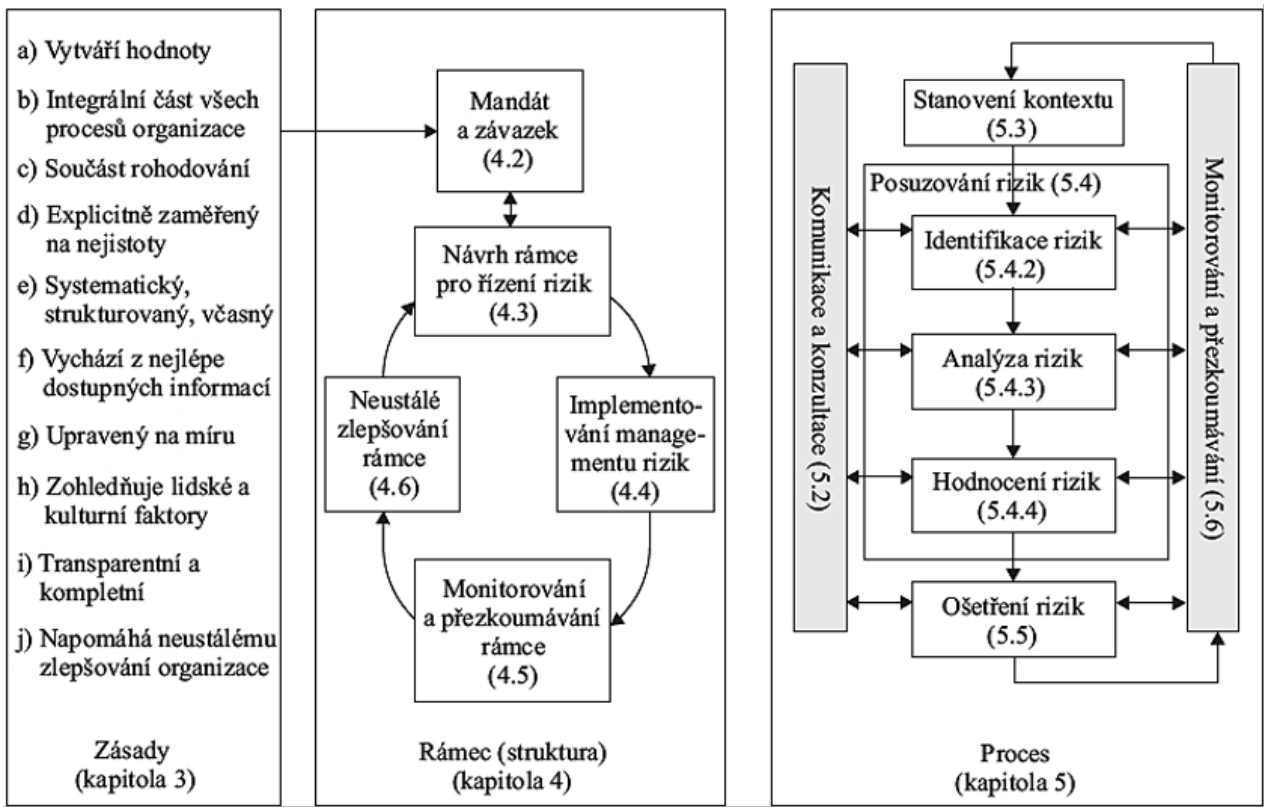
1.3. Riziko, aktivum, zranitelnost

Před vymezením pojmů hrozba, událost, incident a útok považujeme za nezbytné alespoň rámcově definovat pojem riziko, které s následně definovanými pojmy bezprostředně souvisí.

Výkladový slovník kybernetické bezpečnosti definuje riziko jako: *„(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.“*[1]

Riziko je také možné definovat jako **potenciál, že se hrozba stane reálnou a využije zranitelnosti aktiva**. Dle čl. 4 odst. 9 NIS se **rizikem** rozumí ***„jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.“*** V kyberprostoru jsou rizikům vystaveni jak uživatelé, tak počítačové systémy a aplikace, které je využívají, tak další prvky ICT.

Pojem **riziko vyjadřuje pravděpodobnost, s jakou může nastat nechtěná událost**. Míra pravděpodobnosti, s jakou tato událost nastane, se vyjadřuje pomocí analýzy rizik. Minimální normové hodnoty pro metody identifikace, analýzy, hodnocení a ošetření rizik jsou definovány v ČSN EN 31010.



Obrázek 11: Vazby mezi principy, rámcem a procesem managementu rizik[2]

Valášek a kol.[3] uvádějí, že se při stanovení rizik obvykle vychází ze tří základních otázek:

§ **Co špatného (nežádoucího) se může stát? Co může selhat?**

§ **Jaká je možnost / pravděpodobnost, že se to stane?**

§ **Jak závažné (intenzita, velikost apod.) mohou být účinky (dopady, následky)?**

Dle Valáška však tyto otázky představují pouze základní rámec, který je schopen definovat vlastní riziko. Vedle těchto tří otázek jsou pokládány následující doplňující otázky, které se vztahují k významným faktorům ovlivňujícím charakteristiku rizika:

Faktor	Otázka
Čas	„Jak dlouho budeme riziku vystaveni (ohroženi)?“
Nestálost	„Jak se blíží odhady dopadů rizikové události skutečnosti?“
Složitost	„Je obtížné riziku porozumět?“

Vzájemné vztahy	„Jak dalece spolu souvisí různá rizika nebo rizikové faktory?“
Ovlivnění	„Je možné riziko zvládat?“
Životní cyklus	„Jak se riziko mění v čase?“
Nákladová efektivnost	„Jak nákladná jsou opatření vůči riziku?“

U každého rizika se počítá stupeň významnosti rizika, který je možné vyjádřit následovně:

Významnost rizika = **Dopady** rizika * **Pravděpodobnost** výskytu rizika

„Výsledkem analýzy rizik je stanovení významnosti definovaných rizik. Každé riziko, s ohledem na zadání, má různé dopady, které může způsobit. Dopady rizika neboli následky hodnotíme v pětibodové stupnici např. takto:“

Body	**Pravděpodobnost výskytu rizika**	**Popis výskytu**
5	JISTÉ	Riziko se téměř vždy vyskytne nebo s pravděpodobností 90 – 100 %.
4	PRAVDĚPODOBNÉ	Riziko se pravděpodobně vyskytne
3	MOŽNÉ	Riziko se někdy může vyskytnout (např. za specifických podmínek).
2	NEPRAVDĚPODOBNÉ	Riziko se někdy může vyskytnout, ale je to nepravděpodobné.
1	VYLOUČENÉ	Riziko se vyskytne pouze ve výjimečných případech a za specifických podmínek.

Kromě dopadu jednotlivá rizika mohou nastat anebo také nemusí. Proto se stanovuje pravděpodobnost vzniku rizika. Výskyt opět hodnotíme na pětibodové stupnici takto:[4]

Body	**Dopad rizika**	**Popis dopadu**
5	KRIZOVÉ	Situace zásadně omezí nebo ukončí provoz firmy (např. bankrot, ztráty na životech apod.).
4	VÝZNAMNÉ	Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod firmy (např. vznik významných ztrát finančních - 100% nad rozpočet, časových, vznik soudních sporů, vzniknou zranění apod.).
3	STŘEDNÍ	Situace nebezpečně ovlivní vnitřní i vnější chod firmy (např. ztráty vzniknou, ale firma je schopna dále fungovat, vzniknou finanční ztráty do výše 30 % rozpočtu apod.).
2	NEVÝZNAMNÉ	Situace omezuje vnitřní chod firmy (např. dojde k časovým zpožděním do max. výše 30 dní).
1	ZANEDBATELNÉ	Situace sice negativně omezuje chod firmy, ale nezpůsobuje ztráty větší než 5 %.

Při hodnocení rizika je krom výše uvedeného třeba přihlédnout i k dalším okolnostem, kterými jsou:

§ vlastní povaha (druh) rizika či hrozby,

§ zranitelnost aktiva,

§ pravděpodobnosti, že se riziko promění v bezpečnostní událost či incident.

Analýza rizik je značně obtížná a vyžaduje znalost aktiv, hrozeb a zejména je třeba mít v této oblasti již nějaké zkušenosti. Na základě analýzy rizik je možné stanovit opatření za účelem minimalizace nebo úplného odstranění rizik.

1.3.1 Aktivum

Aktivem se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát.

Aktivum může být **věcí hmotnou** (budova, počítačový systém, sítě, energie, zboží aj.) **či nehmotnou** (informace, znalosti, data, programy aj.) z pohledu občanského práva.

Aktivem však může být i **vlastnost** (např. dostupnost a funkčnost systému a dat aj.) či **dobré jméno**, reputace atd. **Lidé** (uživatelé, administrátoři aj.) a jejich znalosti a zkušenosti jsou také z pohledu kybernetické bezpečnosti aktivem.

Dle § 2 písm. f) a g) VoKB se **aktiva** dělí na **podpůrná** a **primární.**

Podpůrným aktivem je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

1.3.2 Zranitelnost

Zranitelnost (vulnerability) označuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami.

Zranitelnost, stejně jako hrozba, může být způsobena celou řadou faktorů spočívajících jak v jednání člověka, technické závadě, tak případně zásahu vyšší moci.

V oblasti kybernetické bezpečnosti se zranitelnosti dělí na:

- **zranitelnosti známé** (publikované)
    - **opravené** (ošetřené) – typickým případem jsou zranitelnosti softwaru, na který již výrobce vydal aktualizaci
    - **neopravené** (neošetřené) – dotčený subjekt (výrobce, správce aj.) o zranitelnosti ví, ale nezajistil její opravu
- **zranitelnosti neznámé**
    - skryté
    - neobjevené

V případě neznámých zranitelností je významné, zda jsou objeveny útočníkem, výrobcem, bezpečnostním analytikem, osobou zabývající se penetračním testováním či uživatelem. Stejně tak je významná motivace osoby, která danou zranitelnost objeví.

Bezpečnostní zranitelnosti jsou potenciálními bezpečnostními hrozbami. Bezpečnostní zranitelnosti lze do určité míry eliminovat důsledným aktualizováním a záplatováním veškerého softwaru.[5]

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí příkladmo některé ze zranitelností. **Dle** této **vyhlášky je zranitelností:**

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nevhodné nastavení přístupových oprávnění,
6. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
7. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
8. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
9. nedostatečná ochrana aktiv,
10. nevhodná bezpečnostní architektura,
11. nedostatečná míra nezávislé kontroly,
12. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

---

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 99. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[2] MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - provádění kontrol technického stavu technických zařízení.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

[3] VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení při nevojenských krizových situacích*. Praha: Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 1. 7. 2018]. Dostupné z: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx

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

[4] *Analýza rizik.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

[5] Srov. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 29. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

1.4. Kybernetické hrozby, události, incidenty a útoky

Vypořádat se s problematikou „negativních kybernetických jevů“ může být poněkud problematické, neboť různá odborná literatura, jakož i právní normy mnohdy používají pro definování určitého negativního jevu různá synonyma, která mají vyjádřit totéž.

Důvodem pro neustálenost terminologie je jednak opět relativně krátká doba, po kterou se vypořádáváme s kybernetickými hrozbami, útoky a incidenty, a jednak i ne vždy shodný překlad z angličtiny, která je v oblasti IT využívána primárně.

1.4.1 Kybernetická hrozba

Hrozbu můžeme nejjednodušeji definovat jako něco, co je schopno narušit běžný či řádný stav věcí a zasáhnout do práv jiných subjektů. Jde o negativní působení, které může, ale nemusí být dokončeno. Pro vlastní definici je dostačující, že možnost negativního stavu hrozí a je reálná.

Dle dikce Ministerstva vnitra ČR se za hrozbu považuje *„jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.“*[1]

Výkladový slovník kybernetické bezpečnosti definuje několik pojmů, které se bezprostředně vztahují ke kybernetickým hrozbám.

Vlastní pojem **hrozba** (threat) je definován jako *„potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“*[2]

S tímto základním pojmem pak bezprostředně souvisí i pojem **bezpečnostní hrozba** (Information security threat)[3], který je definován jako *„potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.“*[4]

Vedle dvou výše uvedených pojmů definují autoři ve výkladovém slovníku i pojmy **aktivní hrozba, pasivní hrozba a pokročilá a trvalá hrozba.**[5]

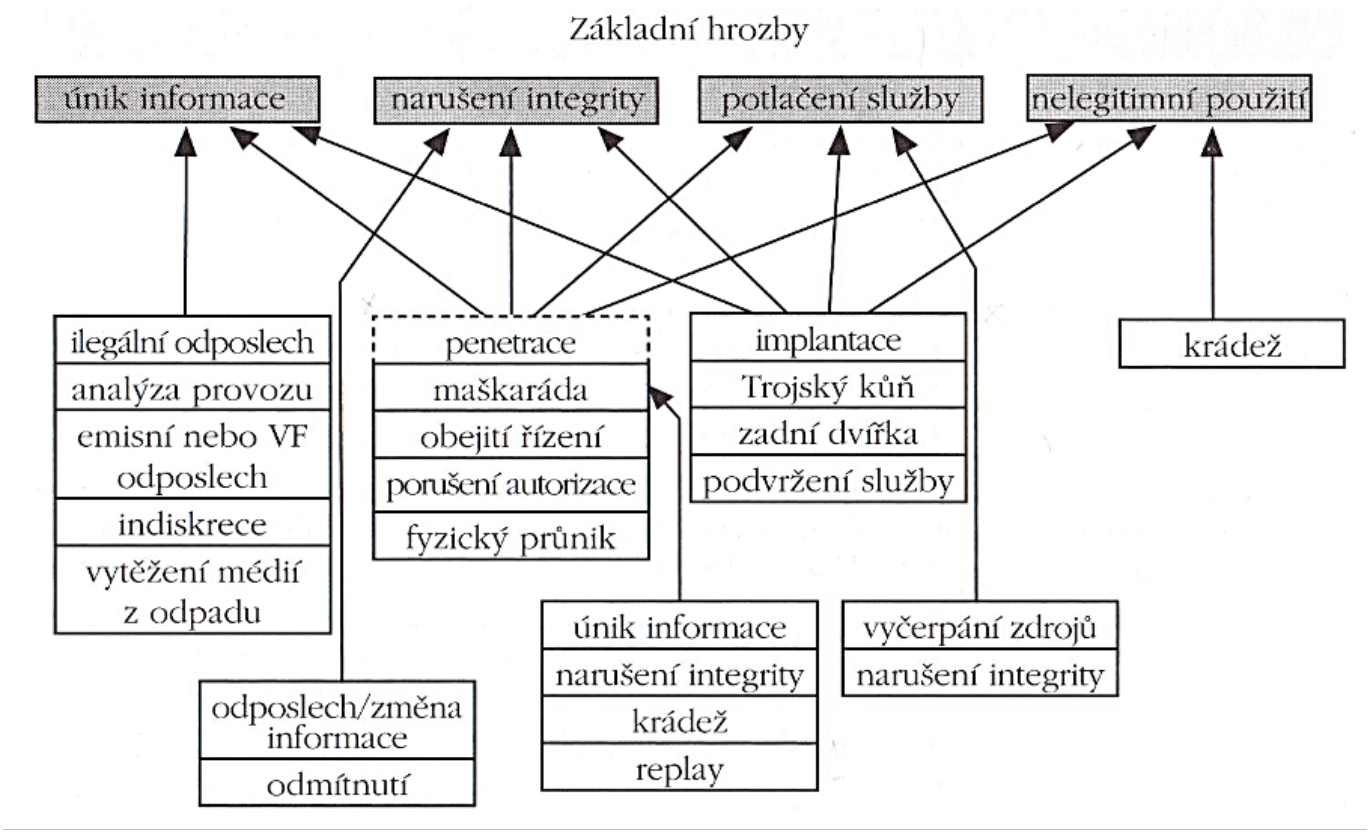
Oxford dictionary uvádí, že **kybernetickou hrozbou je možnost škodlivého pokusu o poškození nebo narušení počítačové sítě nebo systému.**[6] Přičemž za systém je v tomto kontextu považován počítačový systém.

Kybernetickou hrozbu lze také definovat jako akt směřující ke změně[7] informace, aplikací či systému samotného.

Jirovský vymezuje čtyři skupiny základních hrozeb a zároveň charakterizuje jejich vztah:[8]

1. **Únik informace** je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
2. **Narušení integrity** představuje poškození, změnu, či vymazání dat.
3. **Potlačení služby** znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému.[9]
4. **Nelegitimní použití** je užití informací neautorizovaným subjektem či neoprávněným způsobem.[10]

Uvedený vztah je nejlépe znázorněn na následujícím obrázku.



Obrázek 12: Vzájemný vztah jednotlivých kybernetických hrozeb dle Jirovského

Klasifikace kybernetických hrozeb

Vlastních klasifikací kybernetických hrozeb existuje celá řada, přičemž nejčastěji jsou tyto hrozby členěny dle:

1. Zdroje hrozby

a) **Hrozby způsobené člověkem.** V případě, že je hrozba způsobena člověkem, je vhodné se zaměřit i na formu zavinění, jež vedlo k iniciaci dané hrozby. Z tohoto pohledu je možné rozlišovat hrozby způsobené:

- **úmyslně,**

Mezi úmyslně způsobené kybernetické hrozby je možné zařadit například:

- úmyslné smazání dat, konfigurace systému aj.,
- fyzické poškození počítačového systému či jiného prvku ICT,
- zcizení dat a informací,
- kybernetické útoky (malware, DoS, DDoS, phishing, neoprávněný odposlech aj.).[11]

- **z nedbalosti.**

Mezi kybernetické hrozby způsobené z nedbalosti je možné zařadit například:

- omylem smazaná data,
- fyzické poškození počítačového systému či jiného prvku ICT (např. pádem, překopnutím strukturované kabeláže aj.),
- poškození dat, systémů či jiných prvků na základě neseznámení se s interními akty (právními či technickými),
- jiná chyba uživatele.

b) **Technické chyby** (např. chyba softwaru či hardwaru).

c) **Vis maior (vyšší moc)**.

Mezi kybernetické hrozby způsobené vyšší mocí je možné zařadit například:

- neplánovaný výpadek napájení (pokud se nejedná o hrozbu způsobenou člověkem z nedbalosti),

- přírodní události (zásah blesku, vichřice aj.) či katastrofy (povodně, zemětřesení aj.),
- požár (pokud se nejedná o hrozbu způsobenou člověkem).

2. Zdroje působení

a) **hrozby vnitřní** (zdroj hrozby se nachází uvnitř organizace)

b) **hrozby vnější** (zdroj hrozby se nachází mimo organizaci)[12]

3. Cíle hrozby

a) Útok na triádu CIA.

- **Confidentiality** (důvěrnost) – např. krádeže dat, přístupových údajů a klíčů, hardware aj.
- **Integrity** (celistvost) – chyby v databázích, v nastavení oprávnění aj.
- **Availability** (dostupnost) – např. DoS a DDoS útoky; fyzické útoky na servery a strukturovanou kabeláž; výpadky proudu aj.

b) Útok na některý z prvků kybernetické bezpečnosti.

- **Lidé –** útoky sociálním inženýrstvím (ve světě reálném, ale i kyberprostoru), phishing, malware, krádeže aj.
- **Technologie –** veškeré hrozby uvedené v bodě 1 této klasifikace**.** Typicky mohou hrozby působit na:
  - hardware (koncové počítačové systémy, servery, řídící prvky sítě, IoT aj.),
  - databáze,
  - síť a síťovou infrastrukturu,
  - software (operační systém či jiné aplikace),
  - informace a data uložená v počítačových systémech.

- **Procesy –** neoprávněné testování zabezpečení či funkčnosti procesů nastavených v organizaci aj.

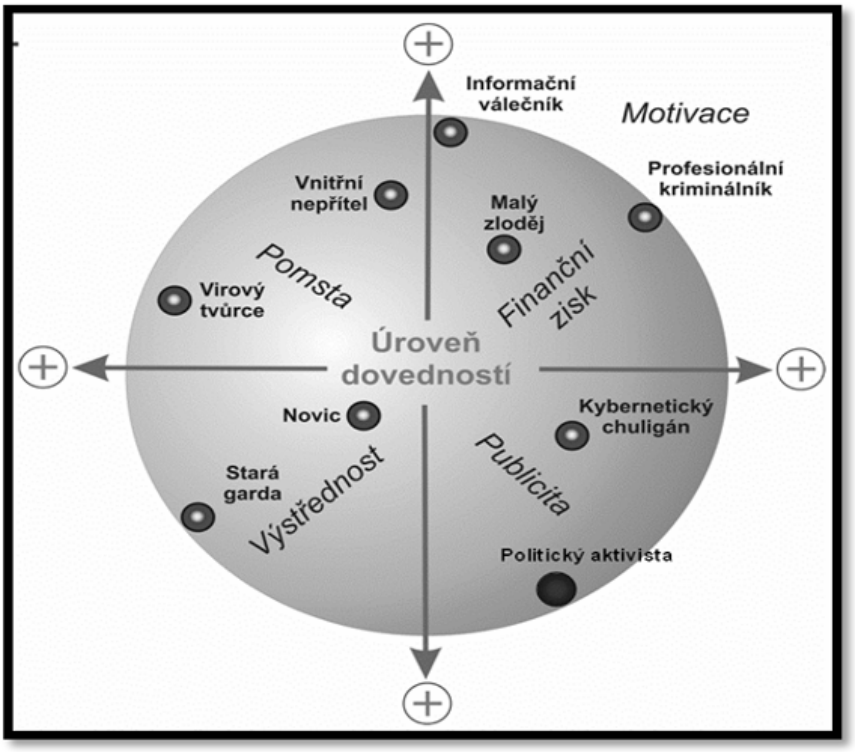
4. Motivace

Pokud je hrozba způsobena úmyslným jednáním člověka, je vhodné se při řešení hrozby zabývat i její motivací. Na základě analýzy motivace takovéhoto jednání je v rámci procesu reakce na hrozbu možné vytvořit nápravná opatření, aby nedocházelo ke stimulu této motivace i v budoucnu.

Dle motivace lze sledovat:

- hrozby za účelem získání finančního prospěchu,
- hrozby za účelem získání konkurenční převahy,
- hrozby za účelem dokázání svých schopností,
- hrozby za účelem odplaty,
- hrozby z důvodu neplnění povinností.[13]

Další členění útočníků dle motivace představuje i Rak[14], který znázorňuje nejobecnější typizaci útočníků dle jejich motivace, přičemž mnohé z uvedených typů motivací se mohou následně dělit či vzájemně splývat.



Obrázek 13: Možné členění útočníků v kyberprostoru dle motivace

5. Typ hrozby

- sociální inženýrství,
- botnet,
- malware,
- ransomware,
- spam/scam,
- podvodné nabídky,
- phishing, pharming, spear phishing, vishing, smishing,
- hacking,
- sniffing,
- DoS, DDoS, DRDoS útoky,
- šíření závadového obsahu,
- identity theft,
- APT (Advanced Persistent Threat),
- kyberterorismus,
- kybernetické výpalné či vydírání (cyber extortion).

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí příkladmo některé z hrozeb. **Dle** této **vyhlášky je hrozbou:**

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,

11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace).

1.4.2 Kybernetická bezpečnostní událost

Prosise a Mandiva charakterizují tzv. **„počítačovou bezpečnostní událost"** (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.[15]

Jirásek a kol. definují bezpečnostní událost (Security event), jako: *„**událost, která může způsobit nebo vést k narušení** informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika).*"[16]

Definici pojmu bezpečnostní událost je možné nalézt i v čl. 3.5 ISO/IEC 27001, kde je uvedeno, že takovouto událostí je: *„**identifikovatelný stav** systému, služby, nebo sítě**, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření**. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací.*"

Obdobnou definici je možné nalézt i v příručce NIST, 800-61 Computer Security Incident Handling Guide, kde je uvedeno, že bezpečnostní událostí je: *„nepříznivá událost s negativním důsledkem, jako jsou havárie (pády) systému, packet flooding, neautorizované použití systémových oprávnění, neautorizovaný přístup k citlivým datům nebo spuštění škodlivého kódu, který ničí data."*[17]

Kybernetickou bezpečnostní událost definuje i zákon o kybernetické bezpečnosti v § 7 odst. 1 jako *„**událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací**."*

De facto **jde o událost bez zatím reálného negativního následku** pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná.

Autoři se zároveň dopouštějí tautologie, neboť vysvětlují událost, jako událost.

Domníváme se, že pojem kybernetická bezpečnostní událost by bylo vhodnější a zřejmě i srozumitelnější označovat a vykládat jako **kybernetickou hrozbu**, neboť zde skutečně pouze existuje potencionální příčina, která může způsobit nežádoucí událost.

Příklad: *Uživateli je do interní firemní pošty doručena e-mailová zpráva obsahující v příloze škodlivý kód (malware). Tento malware je však zkomprimován (např. pomocí WinZip) a bez další činnosti uživatele nemůže být nainstalován. Takováto událost ještě sama o sobě nemusí znamenat narušení bezpečnosti, ale je za jistých okolností způsobilá ji narušit.*

1.4.3 Kybernetický (bezpečnostní) incident

Jirásek a kol. definují bezpečnostní incident (Security Incident), jako *„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie."* ***[18]***

Vlastní definici **informačního bezpečnostního incidentu**, pak přináší norma ISO/IEC 27001. V čl. 3.6 této normy je informační bezpečnostní incident definován jako: *„jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací."*

Velmi podobnou definici **počítačového bezpečnostního incidentu** je také možné nalézt i v příručce NIST, 800-61 Computer Security Incident Handling Guide, která uvádí, že jde o *„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, politiky akceptovatelného použití (systému, služby) nebo standardní bezpečnostní praxe."*[19]

Kybernetický bezpečnostní incident definuje i zákon o kybernetické bezpečnosti v § 7 odst. 2 jako *„**narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.**"*

Z dikce zákona tedy vyplývá, že incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, ale i vyšší mocí. Podstatné je, že **dojde k narušení bezpečnosti informací, nebo služeb a informačních a komunikačních systémů s nimi spojených.**

Kybernetický bezpečnostní incident tak představuje skutečné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

Za určitou část kybernetických bezpečnostních incidentů jsou zodpovědné i náhodné jevy, chyby hardwaru, softwaru, chyby učiněné při konfiguraci administrátory, chyby uživatelů systémů aj.

Příklad: *Navážeme-li na předchozí příklad, pak v okamžiku, kdy uživatel spustí na počítači škodlivý kód, mluvíme již o vzniku bezpečnostního incidentu.*

1.3.4 Kybernetický útok (Cyber Attack)

Jirásek a kol. definují kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků."*[20]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru[21], zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství, kde je jediným cílem získat informace, či naopak útok DoS, či DDoS, kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem primárně spočívá v otázce zavinění. Jak již bylo uvedeno dříve, kybernetický bezpečnostní incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, případně vyšší mocí. U kybernetického útoku však jde o úmyslné jednání člověka.

Na základě výše uvedeného je tedy možné **kybernetický útok**[22] definovat jako **jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.

Kybernetický útok lze také definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.

1.3.5 Kyberkriminalita (Cybercrime)

Na závěr pojednání o kybernetických incidentech a útocích považujeme za nutné alespoň rámcově vymezit vztah mezi těmito útoky či incidenty a kyberkriminalitou.

Při vymezení obsahu pojmu **kyberkriminalita** je třeba si uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.

Nejobecněji je možné kyberkriminalitu definovat **jako jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.** Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

Kyberkriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Velmi často je přenášena „klasická trestná činnost" do kyberprostoru, neboť je zde tuto trestnou činnost možné páchat rychleji a efektivněji (např. podvody, šíření materiálů zobrazujících zneužívání dětí aj.). Vedle této transpozice známé kriminality pak dochází ke vzniku nových, mnohdy dosud právem neřešených útoků.

Je třeba si uvědomit, že ne každý kybernetický útok musí být trestným činem, ale každý kybernetický trestný čin musí být zároveň kybernetickým útokem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či netolerované jednání).

---

[1] *Hrozba.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 52. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[3] V tomto případě je vidět problém s překladem některých pojmů z angličtiny a naopak. Pokud bychom chtěli důsledně přeložit pojem Information security threat, pak správným českým ekvivalentem je např. hrozba pro bezpečnost informací; hrozba zabezpečení informací aj.

[4] Tamtéž s. 25

[5] Tamtéž s. 16, 81 a 87

[6] *Cyberthreat.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat

[7] Změnou je míněna i krádež informace, její zničení, či zmaření jejího užití.

[8] Srov. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. s. 21 a násl.

[9] Jde například o útoky typu **DoS - Denial of Service**, **DDoS** – **Distributed Denial of Service** aj. Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 295 a násl.

[10] Například dojde k napadení zpoplatněného systému a využívání jeho služeb bez platby za služby.

[11] Jednotlivé kybernetické útoky viz např.: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 181 a násl.

[12] Blíže viz např. POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

[13] Před čím chránit? – Bezpečnostní hrozby, události, incidenty. [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

[14] Zdroj: RAK, Roman. Homo sapiens versus security. ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

[15] PROSISE, Chris a Kevin MANDIVA. *Incident response & komputer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 13

Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.

[16] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 28. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[17] *Computer Security Incident Handling Guide* [online]. [cit. 13. 8. 2018]**, s. 6. Dostupné z:** https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[18] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 25. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[19] *Computer Security Incident Handling Guide* [online]. [cit. 17. 2. 2018], s. 6. Dostupné z: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[20] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 71. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[21] V uvedené definici chybí zejména vymezení jakékoliv jiné motivace útočníka, než té, která spočívá ve *...způsobení poškození či zisku strategicky důležitých informací.* Jako příklad, který tato definice nepostihuje, lze uvést ekonomicky motivované útoky, jejichž počet v současnosti dramaticky roste.

[22] Od pojmu kybernetický útok je třeba odlišit pojem bezpečnostní incident, který představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika).

1.5. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

ℹ️

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Pro pochopení problematiky kybernetických útoků a kybernetické bezpečnosti je třeba znát základní terminologii, která se zvolenou oblastí bezprostředně souvisí. Tato kapitola prezentuje vybrané technické, ale i legální pojmy.
- Pojem kybernetická bezpečnost nemá jednotnou obecně uznávanou definici. Kybernetická bezpečnost představuje podmnožinu bezpečnosti jako takové.
  - Při vlastním definování kybernetické bezpečnosti je vhodné vycházet z již ustálených definic. Uvedu několik takto ustálených definic:
  - Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem.
  - Oxford dictionary uvádí, že kybernetická bezpečnost představuje stav, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat. Do kybernetické bezpečnosti je pak třeba zahrnout i opatření, která je třeba přijmout k dosažení tohoto stavu.
  - Dle Jiráska a kol. představuje kybernetická bezpečnost (Cyber Security) *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“*
- Definici kybernetické bezpečnosti je možné nalézt například v dokumentu Definition of Cybersecurity - Gaps and overlaps in standardisation[1] Evropské agentury ENISA[2]: *„Kyberbezpečnost se vztahuje na bezpečnost kyberprostoru, kde samotný kybernetický prostor odkazuje na soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a na samotnou sadu objektů, jejichž rozhraní umožňující jejich dálkové ovládání, vzdálený přístup k datům, anebo jejich zapojení do řídících akcí v rámci kyberprostoru. Kyberbezpečnost bude zahrnovat paradigma ‚CIA' triády pro vztahy a objekty v rámci kyberprostoru a zároveň bude toto paradigma rozšiřováno z důvodu zajištění ochrany soukromí subjektů (fyzických a právnických osob) a odolnosti [‚zotavení se' (recovery) z útoku].“*
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[3] v čl. 4 odst. 2 uvádí, že *„bezpečnost sítí a informačních systémů představuje schopnost těchto sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.“*¨
- Riziko je také možné definovat jako potenciál, že se hrozba stane reálnou a využije zranitelnosti aktiva. Dle čl. 4 odst. 9 NIS se rizikem rozumí *„jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.“* V kyberprostoru jsou rizikům vystaveni jak uživatelé, tak počítačové systémy a aplikace, které je využívají, tak další prvky ICT.
- Aktivem se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát. Aktivum může být věcí hmotnou (budova, počítačový systém, sítě, energie, zboží aj.) či nehmotnou (informace, znalosti, data, programy aj.) z pohledu občanského práva.
- Aktivem však může být i vlastnost (např. dostupnost a funkčnost systému a dat aj.) či dobré jméno, reputace atd. Lidé (uživatelé, administrátoři aj.) a jejich znalosti a zkušenosti jsou také z pohledu kybernetické bezpečnosti aktivem.
- Zranitelnost (vulnerability) označuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami. Zranitelnost, stejně jako hrozba, může být způsobena celou řadou faktorů spočívajících jak v jednání člověka, technické závadě, tak případně zásahu vyšší moci.

🗝️

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- kybernetická bezpečnost
- CIA
- riziko
- aktivum
- zranitelsnot
- kybernetický útok
- kybernetická hrozba

❓

KONTROLNÍ OTÁZKY

- Co je to triáda CIA?
- Jak je možné definovat kybernetickou bezpečnost?
- Z jakých prvků se kybernetická bezpečnost skládá?
- Co vše se rozumí aktivem?

- Jak je možné definovat zranitelnost?

---

[1] *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10. 12. 2017]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

[2] The European Union Agency for Network and Information Security

[3] Dále jen směrnice NIS či NIS. [online]. [cit. 1. 7. 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

2. CERT/CSIRT týmy

Internet zaznamenal v 21. století masivní rozvoj a komercionalizaci. Dramaticky se zvýšil počet uživatelů, počet počítačových systémů připojených do globální sítě a také počet provozovaných kritických služeb, ať už ze sféry komerční (např. elektronické bankovnictví, e-shopy, elektronické aukce), tak také ze sféry státní (např. informační servis státní správy a samosprávy, registry). Bezpečnostní incidenty, kybernetické útoky a trestná činnost páchaná prostřednictvím informačních a komunikačních technologií v reálném i virtuálním světě jsou čím dál více závažnější a zhoršují se také jejich dopady a následky.

Výraznou odlišností této kyberkriminality od ostatních druhů kriminality je její vysoká latentnost, vysoká míra tolerance společností (včetně lhostejnosti uživatelů), anonymita pachatele a jeho často obtížná identifikace. Vzrůstá tak potřeba zefektivnit obranu proti těmto útokům, především zlepšit prostředí a prostředky umožňující dohledání pachatele, sjednotit a zformalizovat postupy a také vzdělávat uživatele, aby byli schopni rozpoznat hrozby a rizikové situace, vypořádat se s nimi a v ideálním případě jim předcházet. Za tímto účelem je budována infrastruktura bezpečnostních týmů CERT a CSIRT.

2.1. Historie

Za první bezpečnostní incident, který negativně ovlivnit provoz tehdejšího Internetu tím, že vyřadil z chodu přibližně 10 % všech připojených zařízení, je označován tzv. Morissův červ *(Morris worm)*. Červ byl do Internetu vypuštěn v roce 1988 Robertem Morrisem, studentem Cornellovy univerzity v USA. Tento incident odstartoval éru vytváření a šíření počítačových virů, červů, trojských koní a další podobné „elektronické havěti", souhrnně označovaných jako *malware*. A právě tato zkušenost nastartovala na konci 80. let minulého století diskuzi o bezpečnosti sítí a služeb, aby následně došlo ke zformulování základních principů obrany, prevence a ochrany přenosu citlivých dat.

V reakci na Morissův červ byl na Carnegie Meelon University (CMU) v USA zformován první CERT tým. Tento první ad-hoc sestavený CERT měl za úkol prozkoumání Morissova červu, nalezení účinné obrany a návrhu řešení problémové situace. Nejcennějším výsledkem práce tohoto týmu nakonec bylo zjištění, že nejdůležitější je být na možnost narušení bezpečnosti předem připraven a v okamžiku problému spustit předem definovaný a vyzkoušený záchranný plán obrany a obnovy, a ne teprve začít zkoumat, co je nutné udělat a v jakých krocích. Výsledek práce tohoto prvního CERTu tak odstartoval éru budování světové infrastruktury týmů tohoto typu.

Carnegie Mellon University si zkratku CERT zaregistrovala jako ochrannou známku, a ač se jejímu užití ostatními organizacemi v tomto kontextu nebrání (organizace, která chce ve jménu svého týmu tuto zkratku použít, musí požádat o svolení zkratku používat a obvykle jej dostane), právě toto bylo příčinou vzniku a zavedení druhého pojmu CSIRT.

2.2. CERT a CSIRT týmy

CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team). Každá z těchto zkratek má sice trochu jiný význam a hlavně trochu jinou historickou genezi, ve skutečnosti je dnes za oběma zkratkami možno chápat stejný typ týmu - tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů a (kyber) hrozeb, z pohledu uživatelů nebo jiných týmů tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem, se žádostí o spolupráci, výměnu informací, pomoc apod.

CERT/CSIRT týmy vznikají na úrovni jednotlivých organizací, přičemž jde jak o organizace, které zprostředkovávají chod Internetu (ISP - poskytovatelé připojení a služeb), tak také o organizace, které prostředí Internetu používají ke své hlavní činnosti (např. IT firmy, poskytovatelé obsahu, banky).

Základní povinností každého CSIRT týmu je reakce na hrozbu („response“) a spolupráce při řešení incidentů. CSIRT tým obvykle řeší problém, který se vyskytne v jeho poli působnosti (např. vlastní síťové infrastruktuře), tedy tam, kde má reálné možnosti k zásahu.

CERT/CSIRT dané sítě (organizace) obecně představuje záchytný bod, na který se uživatelé mohou obrátit se zjištěným bezpečnostním problémem (nebo jen podezřením na problém), který se týká počítačové sítě nebo některé z provozovaných služeb. Profesionální CERT/CSIRT tým by každé přijaté hlášení (i potenciálního) bezpečnostního incidentu měl prozkoumat a podle svých možností zjednat nápravu.

Nejde o nic převratného a v praxi neexistujícího, každá větší organizace, poskytovatel připojení nebo poskytovatel služeb provozuje bezpečnostní tým. **Rozdíl mezi běžným bezpečnostním týmem a týmem typu CERT/CSIRT je zejména v zapojení do** světové bezpečnostní infrastruktury, sdílení informací v rámci této infrastruktury **a dodržování** stanovených formálních postupů.

Existence alespoň jednoho oficiálního CERT/CSIRT týmu je žádoucí v každé provozované síti, obzvláště pak v těch velkých (tranzitní, regionální, univerzitní), tzn. na úrovni velkých ISP, ale také v bankách nebo u poskytovatelů služeb.

Významnou a **specifickou roli mají** v rámci jednotlivých států zastřešující **vrcholové týmy** - tzv. **národní** a **vládní**, kterým bude věnována samostatná subkapitola.

Globálně lze pak na existující CERT/CSIRT týmy nahlížet jako na infrastrukturu, která řeší bezpečnostní problémy Internetu. Při práci čerpá CERT/CSIRT tým především ze svých zkušeností, předem připravených a v praxi ověřených postupů a ze spolupráce a výměny informací s ostatními CERT/CSIRT týmy.

Základním požadavkem komunity **je, aby CERT/CSIRT tým veřejně deklaroval své** kontaktní informace **a** pravidla činnosti:

- kdo je jeho provozovatel,
- kdo jsou jeho členové,
- způsob jak a kdy je možné tým zastihnout,
- jaké služby nabízí,
- pole působnosti (číslo AS[1], síť, domény, služby), ve kterém je tým způsobilý konat a jakým způsobem, tzn. definování jeho pravomocí a odpovědnosti. Na základě pole působnosti je potom tým kontaktován (např. napadenými) a řeší jemu příslušející problémy (incidenty).

Termín řešit bezpečnostní incident přitom může mít různá specifika v závislosti na nastavení týmu a jeho interní politice - může to být prostá eliminace útoku (zneškodnění zdroje problému např. odpojením kompromitovaného počítačového systému od sítě), dohledání útočníka, rychlé obnovení provozu napadené služby/sítě apod.

Právě v závislosti na činnosti týmu při řešení bezpečnostního incidentu je možné týmy označit jako *interní* (institucionální) nebo *koordinační*. Tým interního typu má obvykle možnost přímého zásahu (odpojit zdroj problému, zavést filtraci síťové provozu apod.), tým koordinačního typu možnost přímého zásahu nemá, jeho činnost se soustřeďuje na komunikaci, spolupráci a zprostředkování informací (v této roli jsou obvykle tzv. *národní* týmy, o kterých bude řeč dále).

V případě řešení konkrétního incidentu se jej zúčastnění snaží řešit přímo u zdroje, tzn. s tím, kdo má ke zdroji nebo cíli incidentu nejblíže a může co nejefektivněji zasáhnout (správce koncové sítě nebo služby). Ideální situace nastává, je-li zdroj i cíl v poli působnosti nějakého CSIRT týmu, protože je velmi jednoduché a rychlé najít konkrétního odborníka v místě problému. Ten potom také dokáže problém efektivně řešit a jeho reakce jsou předvídatelné -protože svá pravidla hry sám dobrovolně zveřejnil. Tento postup při komunikaci je velmi pružný díky tomu, že komunikace neprochází přes různé úrovně, je rychlá a přesná a stejná potom může být i reakce. Pokud však napadený nemůže nalézt odpovídající protějšek (ať už proto, že neexistuje, nedává o sobě žádné použitelné informace, odmítá problém řešit nebo prostě nereaguje), hodila by se nějaká „páka“. Tu jsou obvykle do jisté míry schopny poskytnout vrcholové týmy - národní a vládní.

[1] **AS** – **A**utonomous **S**ystem (autonomní systém). Autonomní systém je množina IP sítí a routerů pod společnou technickou správou, která reprezentuje vůči Internetu společnou routovací politiku.

2.3. Jak vzniká CERT/CSIRT tým

Organizace, která se rozhodne zřídit tým typu CERT/CSIRT, si musí na začátku jasně a srozumitelně definovat, čeho chce vytvořením týmu dosáhnout, jakou roli od týmu požaduje (tzn. specifikuje jeho pole působnosti, jeho pravomoci, zodpovědnost a provozované služby) a musí jej také vhodným způsobem ukotvit v organizaci.

Pole působnosti

Polem působnosti je obvykle myšlena oblast kyberprostoru, ve které je tým způsobilý konat a nad kterou má příslušné pravomoci a odpovědnosti definované zřizovatelem. Na základě deklarovaného pole působnosti je potom tým kontaktován např. napadenými a řeší problémy ve sféře svého vlivu. Pole působnosti týmu může být definováno jako konkrétní síť/sítě, autonomní systém(y), jmenná doména/domény, objevují se ale také týmy, které jako pole působnosti uvádějí své expertní dovednosti, konkrétní službu apod.

Služby

Aby se tým mohl oficiálně nazývat týmem typu CERT/CSIRT, je potřeba, aby nabízel především službu řešení nebo koordinace řešení bezpečnostních incidentů v rámci svého definovaného pole působnosti, a tím naplnil myšlenku „response" použité ve zkratkách CERT/CSIRT, tzn. je třeba, aby tento tým uměl *reagovat* na bezpečnostní incident. Tým ale může nabízet řadu dalších služeb z mnoha oblastí, např. školení, varování před aktuálními útoky, slabinami OS, bezpečnostní audity, SW konzultace, doporučení základních bezpečnostních pravidel, vývoj a provoz nástrojů pro sledování provozu sítě a služeb a mnoho dalších.

Členové týmu

Oblastí, která má rozhodující vliv na kvalitu týmu, je jeho personální obsazení. V každé provozované síti obvykle existuje oddělení, nebo skupina techniků, kteří mají na starosti provoz a rozvoj sítě a služeb a zabývají se také bezpečnostními aspekty (obecně „IT staff", „bezpečáci", „správci" aj.). To jsou obvykle ty správné osoby pro začlenění do CERT/CSIRT týmu, nebo pro pověření jej vybudovat. V týmu je ovšem vhodné mít i další typy odborníků (např. právníka, v případě národních a vládních týmů najde uplatnění odborník přes komunikaci s médii, manažer, sociolog aj.). Záleží na zaměření, prostředí, nabízených službách a roli týmu.

Z „vnějšího" pohledu se tým stane CERT/CSIRT týmem tehdy, až jej jako takový akceptují ostatní již existující světové CERT/CSIRT týmy. Cesta k získání statutu CERT/CSIRT tým není složitá, na jejím začátku stačí jasným způsobem deklarovat následující:

1. **Základní kontaktní informace** – jméno týmu, jméno organizace provozující tým, e-mailová adresa(y) týmu, na kterou je možné hlásit bezpečnostní incidenty nebo tým kontaktovat, telefonní číslo(a) týmu, adresu sídla, jména členů týmu, pracovní dobu po kterou je tým k zastižení apod.

2. **Pole působnosti týmu** – definuje, za co tým zodpovídá a jaká je jeho role. To se samozřejmě odvíjí od toho, o jaký tým jde. Je možné zřídit týmy zhruba těchto typů:

   - ***interní*** – slouží a zodpovídá za konkrétní síť (např. za konkrétní rozsah IP adres, domény), obvykle je zřízen provozovatelem sítě,
   - ***koordinační*** – tým, jehož hlavním úkolem je koordinovat řešení bezpečnostních incidentů, nemusí je cíleně řešit,
   - ***vendor*** – tým zabývající se řešením bezpečnostních incidentů, které se dotýkají konkrétního produktu (SW),
   - ***národní, vládní*** – speciální případy založené na principech prvních dvou zmíněných týmů (interní a koordinační), jejich pole působnosti a role závisí na zřizovateli a často také na legislativě konkrétní země.

3. **Nabízené služby –** tým typu CERT/CSIRT musí provozovat alespoň službu řešení bezpečnostních incidentů.

V okamžiku, kdy se nově zřízený CSIRT/CERT tým vypořádá s výše uvedenými kroky a stanoví si základní týmovou politiku řešení bezpečnostních incidentů, která obnáší klasifikaci vážnosti incidentů, pravidla reakce na incidenty, dosažitelnost členů týmu, pravidla pro komunikaci s autorem hlášení bezpečnostního incidentu apod., je na dobré cestě, aby jej okolní týmy akceptovaly. Samozřejmou a nezbytnou součástí je nutnost seznámit se se základními pravidly, na kterých se CSIRT komunita dohodla, a dodržovat je.

Na úplném počátku vytváření týmu typu CERT/CSIRT stojí také vybudování jeho technického a organizačního zázemí, bez kterého nemůže efektivně fungovat žádný tým.

Technickým zázemím se myslí například nástroj pro efektivní správu hlášení bezpečnostních incidentů, který umožní sledovat celý jeho životní cyklus, tj. kdy bylo hlášení zasláno, kým, kdo se v kterých fázích incidentem zabýval, proč, jak postupoval, kdo koho požádal o spolupráci, o jak závažný incident se jednalo a jaké se na něj uplatnily eskalační procedury apod. Pro tuto oblast týmy obvykle používají různé tzv. ticketovací systémy, např. RTIR[1], OTRS[2]. Dalšími důležitými pomocníky na poli technických nástrojů jsou různé systémy IDS (Intrusion Detection System), systémy pro bezpečnostní audity sítě a zařízení, systémy pro forenzní analýzu, sledování provozu sítě (netflow) apod.

Organizační zázemí představuje právě onu zmiňovanou „připravenost" na problém, tzn. definování základních pravidel pro chod týmu tak, aby každý člen týmu znal svou roli, povinnosti a zodpovědnost, politiku postupu řešení bezpečnostních incidentů, pravidla pro komunikaci, sdílení a výměnu informací, spolupráci apod. Základem v této oblasti je obecně dobře zvládnutý tzv. ***incident management*.**

V okamžiku, kdy nově vznikající tým zvládne výše uvedené, tzn. dokáže sebe a svou činnost popsat a vykonávat, může se zapojit do spolupráce na národní a mezinárodní úrovni.

---

[1] **RTIR** - **R**equest **Tracker** for **I**ncident **R**esponse. Blíže viz např.: http://www.bestpractical.com/rtir/.

[2] **OTRS** - **O**pen **S**ource **T**icket **R**equest **Systém**. Blíže viz např.: http://www.otrs.org/.

2.4. Spolupráce CERT/CSIRT infrastruktury

CERT/CSIRT týmy vznikají na dobrovolné bázi a v jejich zájmu je navzájem efektivně komunikovat, vyměňovat si důležité informace a poznatky a spolupracovat. Sdružují se proto v mezinárodních organizacích. V současnosti nejznámější a nejaktivnější organizace, které se touto problematikou zabývají a vytvářejí vhodné prostředí pro výše uvedené záměry, jsou mezinárodní organizace **GÉANT**[1] a organizace **FIRST** (Forum for Incident Response and Security Teams)[2].

Obě výše zmíněné organizace iniciují a umožňují pravidelná setkávání členů bezpečnostních týmů, výměnu zkušeností a podílí se na definování základních pravidel spolupráce a komunikace mezi světovými CERT/CSIRT týmy.

Evropsky působící organizace GÉANT provozuje hned několik aktivit, do kterých se v případě zájmů světové CERT/CSIRT týmy mohou zapojit:

- **TF-CSIRT** (Task Force for CSIRT) je pracovní skupina, která umožňuje spolupráci týmů formou pravidelných dvou-třídenních setkání, která se konají 3x ročně (toto setkání obvykle hostuje některý CERT/CSIRT tým). Více informací je možné nalézt na: https://tf-csirt.org/.
- **CSIRT Training** – slouží pro vyškolení nových členů CSIRT/CERT týmů, nebo pro ty, kdo se chystají CERT/CSIRT tým založit. Koná se obvykle 2x ročně a školiteli jsou zkušení členové renomovaných CERT/CSIRT týmů a další špičkoví odborníci z oblasti bezpečnosti. Více informací je možné nalézt na: https://tf-csirt.org/transits/.
- **Trusted Introducer**[3] – úřad, jehož primárním úkolem je budování důvěry mezi jednotlivými CERT/CSIRT týmy a pomoci při vzniku nových. Více informací je možné nalézt na: https://www.trusted-introducer.org/.

Organizace FIRST kromě každý rok pořádané velké výroční konference pořádá řadu školení, vytváří návody a standardy pro efektivní práci CERT/CSIRT týmů a samozřejmě spolupracuje s aktivitou TF-CSIRT.

Organizace GÉANT a FIRST v rámci světové infrastruktury CERT/CSIRT týmů plní roli jakési „záruky" toho, že tým, který o sobě tvrdí, že je CERT/CSIRT týmem, jím opravdu je, a že jím deklarovaný model chování je pravdivý. Každý nový tým, který se chce zapojit do bezpečnostní infrastruktury, prochází vstupním procesem, který ověří, zda tým odpovídá standardům komunity, je transparentní a neexistují závažné důvody proti jeho přijetí. V případě evropské infrastruktury (platformy TF-CSIRT) tento vstupní proces zajišťuje úřad Trusted Introducer a nový tým jej vlastně žádá o registraci v seznamu týmů a udělení statusu ***listed***.***[4]***

Mezi existujícími týmy se také musí najít alespoň dva týmy (tzv. sponzoři), které nový tým podpoří a žádný již etablovaný tým nesmí vznést námitku proti jeho přijetí. Pokud se vše podaří, jsou informace o novém týmu uloženy do seznamu, který udržuje úřad TI (a část z nich je zveřejněna), tým získává status ***listed*** a komunita přivítá nového člena.

V případě organizace FIRST je vstupní procedura velmi podobná, jen končí ne udělením statusu, ale získáním ***členství***.

Oba procesy mají jedno společné - jde o zjištění a zpřístupnění maximálního množství informací o daném týmu, popisu jeho chování a vnímání problematiky řešení bezpečnostních incidentů tak, aby to korespondovalo s požadavky komunity.

V případě úřadu Trusted Introducer je možné dosáhnout na další, významnější, statusy, a to statusy ***accredited*** a ***certified***. Rozdíly jsou následující:

- Tým s dosaženým statusem ***listed*** o sobě poskytl základní informace, deklaroval snahu chovat se jako CSIRT tým a komunita jej přijala.
- Tým se statusem ***accredited*** deklaruje komunitou požadovanou úroveň svých postupů a zavázal se dodržovat společné TI politiky.
- Tým se statusem ***certified*** pak prokázal svou „úroveň zralosti" (maturity) v rámci certifikačního procesu.

Být ***accredited*** nebo ***certified*** týmem vyžaduje kontinuální úsilí o udržení stavu týmu. Součástí tohoto úsilí je také povinnost udržovat v seznamu TI o týmu aktuální informace. Pokud by tak tým dlouhodobě nečinil, může o své statusy přijít a v nejhorším případě být komunitou vyloučen. Tato povinnost se týká také ***listed*** týmů, které v případě, že do tří let od získání statusu listed neprojdou procesem akreditace, musí svůj status listed obnovit prokázáním podpory ze strany ostatních týmů (tzn. re-listed proces). Tento mechanismus zajišťuje vysokou míru aktuálnosti informací v seznamu TI a tím jejich důvěryhodnost.

Další organizací, která působí v oblasti bezpečnosti, je organizace **ENISA** (European Network and Information Security Agency, http://www.enisa.europa.eu/). Ta úzce spolupracuje s členskými státy EU a soukromým sektorem a zastřešuje řadu aktivit zahrnujících celoevropské kybernetické bezpečnostní cvičení, rozvoj národních strategií v oblasti kybernetické bezpečnosti, spolupráci mezi CERT/CSIRT týmy a budování jejich kapacit, zabývá se problematikou ochrany osobních údajů a spolupracuje na vytváření a implementaci práva v záležitostech týkajících se síťové informační bezpečnosti (NIS - Network Information Security).

Všechny tři zmíněné organizace mají společnou ještě jednu funkci – shromažďují know-how z celé komunity a umožňují jeho sdílení (formulováním tzv. best-practices dokumentů, návodů, doporučení).

[1]Sdružení vzniklo sloučením sdružení TERENA (Trans-European Research and Education Networking Association) a společnosti DANTE.

[2] Více informací o organizaci FIRST je možné nalézt na: https://www.first.org

[3] Déle také **TI**.

[4] ***Listed –*** uvedení nebo doslova „zalistování" týmu v databázi všech registrovaných týmů.

2.5. Hierarchie CERT/CSIRT týmů?

CERT/CSIRT týmy žádnou oficiální hierarchii, která by jeden tým činila nadřazeným jinému týmu, **nemají**. Všechny týmy jsou si z hlediska fungování, komunikace, spolupráce a výměny informací rovnocenné a nejsou v těchto oblastech nijak limitovány. Existence tzv. vrcholových *národních* a *vládních* týmů sice trochu evokuje, že nadřazenost mezi týmy existuje, ale není tomu tak. Jedinou „nadřazenost", ale spíše by bylo na místě říci „větší akceschopnost", dává vrcholovému týmu legislativa dané země, která upravuje jeho pravomoci (např. v oblasti požadované reakce na bezpečnostní hrozby ze strany provozovatelů sítí a služeb apod.).

Ve světě CERT/CSIRT týmů je klíčová ochota sdílet důležité informace o incidentu a hrozbách. K tomu je nezbytné, aby si týmy navzájem důvěřovaly a také aby svým týmům věřili uživatelé. Získat důvěru uživatelů a komunity je dlouhodobý úkol, týmy musí své kvality ukazovat při všech aspektech svého fungování a důvěryhodnost si budovat postupně - nejen schopností pomoci, ale také schopností zajistit důvěrnost sdílených dat a korektní zacházení s nimi, transparentností chování apod.

2.6. Národní a vládní CERT/CSIRT týmy

Národní a vládní týmy jsou speciální formou CERT/CSIRT týmů. Jednají s ostatními CERT/CSIRT týmy jako rovný s rovnými, ale jejich role v celém systému je odlišná.

Národní CERT/CSIRT plní funkci jakéhosi last resort – poslední instance, u které je možné žádat o zásah, pomoc a intervenci. Jeho cílem je (v rámci státu, nebo oblasti kde působí) zprostředkovat kontakt mezi napadeným a původcem problému a napomoci úspěšnému řešení problému. Národní týmy (obvykle) nevládnou nad fyzickou infrastrukturou, takže nemají (na rozdíl od týmů interního/institucionálního typu) možnost přímého zásahu. Jejich role spočívá ve zprostředkování kontaktu, případně v koordinaci (odtud typ týmu koordinační) postupu jednotlivých řešitelů v případě, že problém je rozsáhlejší a jeho řešení vyžaduje spolupráci více složek.

Z principu fungování celé struktury jsou incidenty, které projdou přes systém národního CSIRTu, zpravidla jen zlomkem celkového počtu. Většina incidentů se vyřeší v rámci přímé komunikace, bez nutnosti eskalací a zprostředkování. K národnímu týmu se tak dostávají převážně incidenty, které nelze vyřešit jinak (zodpovědné osoby je řešit odmítají, není jednoduché identifikovat, kdo je za jejich řešení zodpovědný), velmi závažné nebo opakující se problémy, nebo problémy, které mohou mít plošný dopad apod.

Národní CERT/CSIRT má obvykle ve svém popisu práce také vzdělávání a spolupráci. Jedná se jak o osvětu směrem k veřejnosti, tak o působení v rámci internetové infrastruktury. Cílem je podpora vytváření dalších CERT/CSIRT týmů v zemi, jejich uvádění na mezinárodní scénu a podpora při zavádění standardních postupů a procedur. To vše výrazně zvyšuje transparentnost prostředí a dává napadeným šanci efektivně se dobrat nápravy.

Vládní **CERT/CSIRT** se obvykle zaměřuje na oblast státní správy a samosprávy a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb. Vládní CERT/CSIRT může mít podobu týmu interního s možností přímého zásahu v případě problému. Jeho existence je obvykle podpořena legislativně.

Výše uvedené ale není dogma, situace v jednotlivých zemích se liší. Jsou země, kde funguje pouze národní tým (a plní také funkci vládního), jsou země, kde funguje vládní (a plní roli národního), jsou země, kde existují oba, jsou země, kde není ani jeden a roli vrcholového týmu supluje jeden z existujících týmů a pod.

2.7. Situace v ČR a ve světě

V současné době je ve světě oficiálně konstituováno okolo 380 bezpečnostních týmů typu CERT/CSIRT, které jsou buď členy organizace FIRST, nebo evropské platformy TF-CSIRT (případně obou).

V České republice je aktuálně oficiálně zřízeno a úřadem Trusted Intoducer uznáno 39 bezpečnostních týmů typu CERT/CSIRT, což z České republiky činí takřka světovou „velmoc", kdy co do počtu konkuruje pouze Francie, Německo a Velká Británie. Nejde samozřejmě o kvantitu, ale především o kvalitu.

Prvním bezpečnostním týmem typu CERT/CSIRT, který v České republice vznikl, je bezpečnostní tým **CESNET-CERTS** (https://csirt.cesnet.cz/). Byl oficiálně konstituován v roce 2003, v lednu 2004 jej pak oficiálně uznala mezinárodní infrastruktura a úřad Trusted Introducer. Je provozován sdružením CESNET[1] a je zodpovědný za řešení a koordinaci řešení bezpečnostních incidentů v e-infrastruktuře CESNET. Mimo jiné se zabývá vývojem bezpečnostních nástrojů a pro uživatele ve sféře svého vlivu poskytuje také služby osvětového charakteru.

Další týmy pak byly založeny ve sdružení CZ.NIC (CZ.NIC-CSIRT) v roce 2008,na Masarykově univerzitě v Brně (CSIRT-MU) v roce 2009, ve společnosti Active24 (tým Active24-CSIRT) v roce 2012 a v rámci projektu podporovaného Ministerstvem vnitra ČR tým CSIRT.CZ (od roku 2011 Národní CSIRT ČR).

Velký boom v oblasti budování bezpečnostních CERT/CSIRT týmů můžeme v České republice pozorovat především od roku 2013, kdy Česká republika čelila sérii DDoS útoků na veřejné www služby. Tato událost následně iniciovala vznik projektu Fenix (https://fe.nix.cz/) na půdě českého peeringového centra NIX.CZ.

Smyslem tohoto projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity. Projekt Fenix definoval řadu technických a organizačních pravidel, které musí zájemci o vstup do projektu splnit a jedním z nich je také oficiálně konstituovaný tým typu CERT/CSIRT. To bylo pro řadu organizací impulsem, aby své bezpečnostní týmy formalizovaly do podoby CERT/CSIRT týmu a začlenily je do mezinárodní infrastruktury.

Za další motivační impuls, který vedl ke konstituování nových týmů, lze také označit přijetí a následnou účinnost zákona o kybernetické bezpečnosti. Řada organizací pochopila, že bezpečností se vyplatí zabývat, a že zřízení týmu typu CERT/CSIRT přináší výhody.

Současná infrastruktura CERT/CSIRT týmů v ČR čítající 39 týmů sestává z národního a vládního týmu, jsou zde týmy na úrovni velkých ISP, několik týmů v akademickém sektoru, týmy v bankovním odvětví, v IT firmách, u doménových registrátorů a v neposlední řadě také na půdě českého peeringového centra NIX.CZ, na půdě sdružení CZ.NIC. Dohromady se tak jedná o velice různorodou a ve výsledku robustní a životaschopnou infrastrukturu, které nechybí zkušenosti z různých odvětví.

Aktuální seznam českých CERT/CSIRT týmů je možné nalézt na: https://tiw.trusted-introducer.org/directory/country_LICSA.html

---

[1]Sdružení CESNET, z. s. p. o., je zájmové sdružení právnických osob, založené v roce 1996 vysokými školami a Akademií věd České republiky. Provozuje národní vysokorychlostní počítačovou síť určenou pro vědu, výzkum, vývoj a vzdělávání CESNET2. Více viz http://www.cesnet.cz/.

2.8. Národní CSIRT České republiky

V prosinci roku 2010 se oficiálního zřízení Národního CSIRTu České republiky dočkala i Česká republika. Sdružení CZ.NIC a Ministerstvo vnitra podepsaly (16. prosince 2010) Memorandum, podle kterého správce české národní domény sdružení CZ.NIC převzal agendu týmu CSIRT.CZ a od ledna 2011 jej z pověření MV ČR provozuje jako Národní CSIRT ČR.

Pracoviště CSIRT.CZ (http://www.csirt.cz/) vzniklo v rámci plnění grantu Ministerstva vnitra České republiky *„Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky“* (identifikační kód projektu je VD20072010B013) a bylo vybudováno sdružením CESNET. Toto pracoviště bylo označováno jako modelové a bylo vybudováno za účelem ověření stavu bezpečnostní infrastruktury v ČR a ověření realizovatelnosti vybudování distribuované hierarchie pro systematické plošné řešení bezpečnostní problematiky v počítačových sítích ČR prostřednictvím CSIRT týmů. Provoz tohoto týmu byl oficiálně spuštěn 3. dubna 2008, v květnu téhož roku byl na zasedání TF-CSIRT komunity (které proběhlo v Oslu, Norsko) představen ostatním evropským CERT/CSIRT týmům jako pracoviště typu CSIRT s rolí *„last resort“* pro Českou republiku a jako takový byl komunitou přijat.

Pracoviště CSIRT.CZ položilo základy pro další rozvoj vrcholové úrovně CERT/CSIRT infrastruktury v ČR, a to především v oblasti spolupráce. Zároveň ověřil a potvrdil předpoklad, že vrcholové CERT/CSIRT týmy v České republice mají smysl.

Národní CSIRT České republiky plní i další úkoly KB.

2.9. Vládní CERT České republiky

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu (NBÚ) gestorem problematiky kybernetické bezpečnosti v České republice a zároveň národní autoritou pro tuto oblast. NBÚ se od počátku svého jmenování soustředilo na tři úkoly – napsání zákona o kybernetické bezpečnosti, vybudování NCKB (Národního centra kybernetické bezpečnosti) a vybudování Vládní CERT ČR.

Vládní CERT ČR, tým GovCERT.CZ, byl do mezinárodní komunity začleněn v roce 2012, a tím se Česká republika zařadila mezi země, které mají Národní i Vládní CERT/CSIRT tým.

Do kompetence GovCERT.CZ spadají sítě státní správy, samosprávy a kritické infrastruktury ČR. Tým se dále soustřeďuje na vývoj a provoz bezpečnostních služeb, osvětu a zapojuje se také do národní a mezinárodní spolupráce.

Vládní CERT České republiky plní i další úkoly.

2.10. Na který CERT/CSIRT tým se obrátit?

Název této subkapitoly je zároveň častým postesknutím uživatele Internetu, který se dostal do problému (např. na něj někdo útočí, zcizil mu identitu, naboural facebookový profil nebo e-mailový účet, nebo se stal svědkem šíření dětské pornografie). Co má takový uživatel dělat? Obrátit se na Policii ČR? Nebo na poskytovatele připojení, např. jeho helpdesk? Nebo na Národní úřad pro kybernetickou a informační bezpečnost, když je gestorem pro oblast kyberbezpečnosti? Na horkou linku Národního centra bezpečnějšího internetu? Nebo na nějaký CSIRT tým, když se o nich pořád mluví? Ale na který?

Na proces hlášení a řešení bezpečnostních incidentů (neboli opravdu „na koho se mám obrátit, když chci ohlásit nebo řešit zjištěný bezpečnostní incident“) **je možné nahlížet ze dvou úhlů pohledu.** Z pohledu techniků (správců sítí a služeb, členů bezpečnostních týmů) a z pohledu uživatelů.

Pro techniky (správce sítí a služeb, členy bezpečnostních týmů) je odpověď na otázku „na koho se mám se žádostí o akci vlastně obrátit“ celkem jasná, ale to je dáno drilem, zkušenostmi a především velmi dobrou znalostí prostředí Internetu a jeho základních principů, jakož i znalostí toho, kde jsou k mání kontaktní informace k jednotlivým existujícím sítím, službám, doménám apod.

Pro členy CERT/CSIRT týmů jsou základními zdroji kontaktních informací databáze RIRů, databáze provozovatelů domén nejvyšší úrovně a katalogy CERT/CSIRT týmů.

RIR (Regionální Internetový Registr) drží a zpřístupňují informace o tom, komu byl přidělen který blok IP adres. Svět je rozdělen na oblasti a každý RIR (aktuálně RIPE, ARIN, APNIC, LACNIC, AFRINIC) přiděluje IP adresy pro svoji oblast. Oblast Evropy, Blízkého východu a části Asie je pod správou organizace RIPE NCC (https://www.ripe.net/). RIR provozují veřejně přístupné databáze, které obsahují údaje o přidělených internetových sítích a jejich správcích. Tyto databáze tak umožňují vyhledat údaje o tom, která organizace a kteří správci jsou zodpovědní za konkrétní IP adresy.

Dalším zdrojem užitečných informací jsou údaje o doménách, které provozují a zpřístupňují správci domén nejvyšší úrovně, pro TLD doménu .cz je to sdružení CZ.NIC.

A pak je zde oblast CERT/CSIRT týmů, které své pole působnosti obvykle definují pomocí internetových identifikátorů, jmenných domén, nebo klidně jen slovně. Vzhledem k jejich počtu, způsobu definování jejich pole působnosti a zejména rozdílům v jejich úrovni není vždy snadné najít tým, který je schopný pomoci. Pro usnadnění orientace mezi týmy vznikly jakési „katalogy“, o které se starají organizace FIRST a úřad Trusted Introducer. Tyto katalogy obsahují základní informace o CERT/CSIRTech, kontaktech, jejich poli působnosti apod.

Proces hlášení a řešení bezpečnostních incidentů (odborně ***incident handling***) není exaktní proces, právě naopak, a hodně záleží na zkušenostech a občas i kreativitě člověka, který tento proces provádí. Výměna informací mezi týmy obvykle probíhá rychle a efektivně, i když ani to často nezaručuje rychlé vyřešení problému, protože na to je celá infrastruktura ještě stále poměrně „řídká“, a bohužel je nutné konstatovat, že i úroveň týmů je různá.

Optimální stav infrastruktury by byl ten, kdyby se každá IP adresa vyskytovala v poli působnosti oficiálního CSIRT týmu. V této situaci ale infrastruktura CERT/CSIRT týmů zdaleka není.

Z pohledu normálního uživatele je situace značně nejasná a popravdě i matoucí. Co by tedy uživatel měl v případě zjištění bezpečnostního incidentu vlastně dělat a na koho by se měl obrátit? Těžko po uživateli chtít, aby se orientoval v problematice CERT/CSIRT týmů, dokázal si najít ten správný, nastudoval jeho politiku hlášení bezpečnostních incidentů a šel konat. Uživatel by se v první řadě měl obrátit na administrátora své sítě či služeb (pokud někoho takového má), případně by měl spolupracovat s poskytovatelem připojení, tzn. helpdeskem svého ISP nebo jeho uživatelskou podporou. Na straně poskytovatele připojení či služeb by měl pro jeho uživatele existovat jasně popsaný vstupní bod (kontakt), na který by se uživatelé mohli a měli obracet v případě, kdy se stanou cílem útoku, zjistí bezpečnostní incident, nebo mají pocit, že něco není v pořádku. To je důvod, proč je prostředí poskytovatelů připojení jednou z nejdůležitějších oblastí, kde by měl být konstituován oficiální CERT/CSIRT tým a poskytovat služby z oblasti bezpečnosti uživatelům své sítě.

Samozřejmě může nastat situace, kdy jak technik, tak uživatel udělá všechno správně, a řešení problému stejně není v dohledu. Osoba či tým na hlášený problém nereaguje, nebo jej dokonce odmítá řešit (s tím, že to není jeho problém, nebo to není tak vážné) apod. To je právě moment, kdy ke slovu přichází buď Policie ČR (uživatel se na ni může obrátit s podáním trestního oznámení), nebo vrcholový tým (národní nebo vládní), na nějž se uživatel může obrátit jako na poslední instanci, od které lze očekávat pomoc a reakci.

Mezi národním a vládním týmem existuje velmi úzká spolupráce a výměna informací a relevantních dat, a tedy i předání nahlášeného problému k řešení od jednoho týmu k druhému nebo přímo spolupráce na řešení.

Národní i vládní tým by obecně pro provozovatele sítí, služeb (a v případě nutnosti i pro uživatele) měly být místem, kde je v případě problémů, nejasností apod. možné žádat o pomoc a konzultaci, např. dohledání vhodného protějšku ke komunikaci (zahraničního CERT/CSIRT týmu), zprostředkování komunikace (ano, někdy se „páka“ vrcholového týmu hodí, protějšek je pak ochotnější), a zdrojem know-how a informací.

Obecně by ale bylo žádoucí, aby správci sítí a služeb a členové bezpečnostních týmů zvládali a aplikovali principy procesu *incident handling* a maximum komunikace probíhalo přímo (ne přes vrcholové týmy). To činí proces incident handlingu rychlým a efektivním, další mezistupně do něj mohou vnášet nepříjemná zdržení a bohužel i zkreslení. Ale jak už bylo řečeno, záleží na závažnosti situace a řešeného problému.

Týmy typu CERT/CSIRT a jejich infrastruktura obecně nejsou všespasitelné a neznamenají zajištění bezpečnosti „v kostce".

Jejich existence je jen jeden z kamínků v oblasti budování bezpečnosti Internetu, ve kterém hrají svou důležitou roli všichni zainteresovaní, tj. správci sítí, služeb, manažeři, kteří rozhodují o zázemí pro efektivní zabezpečení sítí a služeb, ISP, provozovatelé kritických služeb, bezpečnostní složky, stát, a v neposlední řadě také my uživatelé.

Aktuální seznam týmů CSIRT/CERT je možné nalézt na:

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

2.11. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

ℹ️

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Rozdíl mezi běžným bezpečnostním týmem a týmem typu CERT/CSIRT je zejména v zapojení do světové bezpečnostní infrastruktury, sdílení informací v rámci této infrastruktury a dodržování stanovených formálních postupů.
- Základním požadavkem komunity je, aby CERT/CSIRT tým veřejně deklaroval své kontaktní informace a pravidla činnosti:
  - kdo je jeho provozovatel,
  - kdo jsou jeho členové,
  - způsob jak a kdy je možné tým zastihnout,
  - jaké služby nabízí,
  - pole působnosti (číslo AS[1], síť, domény, služby), ve kterém je tým způsobilý konat a jakým způsobem, tzn. definování jeho pravomocí a odpovědnosti. Na základě pole působnosti je potom tým kontaktován (např. napadenými) a řeší jemu příslušející problémy (incidenty).
- Pole působnosti týmu – definuje, za co tým zodpovídá a jaká je jeho role. To se samozřejmě odvíjí od toho, o jaký tým jde. Je možné zřídit týmy zhruba těchto typů:
  - interní – slouží a zodpovídá za konkrétní síť (např. za konkrétní rozsah IP adres, domény), obvykle je zřízen provozovatelem sítě,
  - koordinační – tým, jehož hlavním úkolem je koordinovat řešení bezpečnostních incidentů, nemusí je cíleně řešit,
  - vendor – tým zabývající se řešením bezpečnostních incidentů, které se dotýkají konkrétního produktu (SW),
  - národní, vládní – speciální případy založené na principech prvních dvou zmíněných týmů (interní a koordinační), jejich pole působnosti a role závisí na zřizovateli a často také na legislativě konkrétní země.
- CERT/CSIRT týmy žádnou oficiální hierarchii, která by jeden tým činila nadřazeným jinému týmu, nemají. Všechny týmy jsou si z hlediska fungování, komunikace, spolupráce a výměny informací rovnocenné a nejsou v těchto oblastech nijak limitovány.
- Národní CERT/CSIRT plní funkci jakéhosi last resort – poslední instance, u které je možné žádat o zásah, pomoc a intervenci.
- Vládní CERT/CSIRT se obvykle zaměřuje na oblast státní správy a samosprávy a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb. Vládní CERT/CSIRT může mít podobu týmu interního s možností přímého zásahu v případě problému. Jeho existence je obvykle podpořena legislativně.

🗝️

- CSIRT tým
- CERT tým
- Incident handling
- Hierarchie týmů
- Pole působnosti

❓

- Co to je CSIRT/CERT tým?
- Jak vzniká a jak se etabluje CSIRT/CERT tým?
- Na co se zaměřuje národní CSIRT tým?
- Na co se zaměřuje vládní CSIRT tým?
- Jaké jsou základní požadavky komunity na CERT/CSIRT tým?

---

[1] **AS** – **A**utonomous **S**ystem (autonomní systém). Autonomní systém je množina IP sítí a routerů pod společnou technickou správou, která reprezentuje vůči Internetu společnou routovací politiku.

3. Legislativní rámec CSIRT/CERT

On 6 July 2016, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) was adopted by the European Parliament.

The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
- a culture of security across sectors that are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and to notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the new Directive.

Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

The existing capabilities are not sufficient to ensure a high level of security of network and information systems within the Union. Member States have very different levels of preparedness, which has led to fragmented approaches across the Union. This results in an unequal level of protection of consumers and businesses, and undermines the overall level of security of network and information systems within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role to play in spurring research, development and innovation in those areas.

The EU Network and Information Security Directive (NIS Directive) aims to create a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in the Directive's point (1) of Annex I (requirements), covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well–defined process.

The NIS Directive aims at creating a CSIRT Network "to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". The Directive states that each Member State shall designate one or more CSIRTs that shall comply with a set of defined high-level requirements.[1]

According to Article 9 of NIS states:

„Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority."

And NISD continues to state that:

· *The CSIRTS have adequate resources to effectively carry out their tasks*

· *Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs*

· *Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level*

· *Member States shall inform the Commission about the remit, as well as the main elements of the incident- handling process, of their CSIRTs*

· *Member States may request the assistance of ENISA in developing national CSIRTs**[2]***

Annex I of NISD is labelled *REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)* and is quoted here in full because of its great relevance for the national/governmental CSIRT community inside the EU:

(1) Requirements for CSIRTs:

(a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(b) CSIRTs' premises and the supporting information systems shall be located in secure sites.

(c) Business continuity:

(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.

(ii) CSIRTs shall be adequately staffed to ensure availability at all times.

(iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.

(d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.

(2) CSIRTs' tasks:

(a) CSIRTs' tasks shall include at least the following:

(i) monitoring incidents at a national level;

(ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

(iii) responding to incidents;

(iv) providing dynamic risk and incident analysis and situational awareness;

(v) participating in the CSIRTs network.

(b) CSIRTs shall establish cooperation relationships with the private sector.

(c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:

(i) incident and risk-handling procedures;

(ii) incident, risk and information classification schemes.

---

[1] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Dostupné z: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 5-6

[2] *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Dostupné z: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 11

3.1. Česká republika

Legislativní rámec CSIRT/CERT týmů v ČR je částečně stanoven zákonem o kybernetické bezpečnosti. Tento zákon stanoví podmínky pro existenci národního a vládního CSIRT/CERT týmu, avšak na druhou stranu nijak neomezuje vznik a existenci jiných CSIRT/CERT týmů.

Na základě zákona o kybernetické bezpečnosti **jsou v ČR povinně zřízeny dva týmy** typu CERT/CSIRT, **a to národní a vládní**. Každý z těchto týmů má zákonem (§ 17 a násl. ZoKB) přesně stanovená práva a povinnosti.

Týmy, jejichž působnost je vymezena zákonem o kybernetické bezpečnosti, jsou povinny respektovat limity tímto zákonem stanovené.

3.1.1 Národní CERT

Národní CERT tým je definován v § 17 ZoKB. Současně je uvedeno, že:

***(1)* Národní CERT zajišťuje v rozsahu stanoveném tímto zákonem sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti.**

***(2)* Provozovatel národního CERT**

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a), b) a h) a tyto údaje eviduje a uchovává,

b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a h) a tyto údaje eviduje, uchovává a chrání,

c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) a h),

d) poskytuje orgánům a osobám uvedeným v § 3 písm. a), b) a h) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,

e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h),

f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

g) předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele,

h) předává Úřadu na vyžádání údaje podle § 16 odst. 5 a 6,

i) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[1]**,**

j) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

k) spolupracuje s týmy CSIRT jiných členských států a

l) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob neuvedených v § 3, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.

***(3)* Provozovatel národního CERT může vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností uvedených v odstavci 2.**

***(4)* Provozovatel národního CERT při plnění povinností uvedených v odstavci 2 koordinuje svou činnost s Úřadem.**

***(5)* Provozovatel národního CERT musí při plnění povinností podle odstavce 2 postupovat nestranně.**

Toto ustanovení definuje instituci národního dohledového pracoviště, pro které je použito legislativní zkratky národní CERT a vymezuje jeho činnost. Zákon předpokládá, že národní CERT bude provozován zpravidla osobou soukromého práva, která uzavře s NBÚ veřejnoprávní smlouvu, a bude sloužit zejména jako společné kontaktní a koordinační místo pro povinné osoby soukromého práva. Vůči národnímu dohledovému pracovišti budou poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě realizovat svou zákonnou notifikační povinnost.

Model standardně soukromoprávního výkonu funkcí národního CERT usnadňuje komunikaci mezi národním CERT a povinnými osobami využívajícími jej povinně jako kontaktní místo. Tyto osoby budou mít totiž rovněž zpravidla soukromoprávní povahu. Národní CERT se bude také moci zapojit do mezinárodních sítí obdobných soukromoprávních národních dohledových pracovišť a těžit z poznatků, které se v rámci těchto sítí neformálně předávají.

Předpokládaný soukromoprávní charakter národního CERT je vzhledem ke smyslu a účelu zákona vhodný i z toho důvodu, že provozovatel národního CERT může, jedná-li se o osobu soukromého práva, vyvíjet iniciativně k dosažení účelu zákona též aktivity na základě tacitního dovolení, tj. libovolné aktivity podle své soukromé vůle neporušující zákonné povinnosti. Provozovatel národního CERT tak bude moci například poskytovat metodickou a informační pomoc i subjektům stojícím mimo osobní působnost zákona, tj. osobám mimo definice jednotlivých kategorií povinných osob, které o to projeví zájem. Národní CERT bude moci dále vyvíjet vlastní vzdělávací, publikační, výzkumnou nebo vývojovou činnost apod. Podmínkou omezující iniciativně vykonávané činnosti národního CERT k dosažení účelu tohoto zákona je jejich bezrospornost s plněním povinností vyčtených v zákoně taxativně.

K § 17 odst. 2 písm. a), b), d) a e)

Mezi subjekty, se kterými komunikuje a spolupracuje provozovatel národního CERT, se doplňují poskytovatelé digitálních služeb.

K § 17 odst. 2 písm. c)

Mezi subjekty, se kterými spolupracuje provozovatel národního CERT, v tomto případě, u nichž vyhodnocuje kybernetické bezpečnostní incidenty, se doplňují poskytovatelé digitálních služeb. Toto ustanovení je v obráceném gardu k ustanovení, které stanoví povinnost poskytovatelů digitálních služeb hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT.

K § 17 odst. 2 písm. g)

Jedná se o jazykovou úpravu ustanovení a výslovného vztažení povinnosti předávání informací na incidenty nahlášené povinnými subjekty.

K § 17 odst. 2 písm. h)

Zpřesňuje se znění ustanovení a ruší se omezení situací, za kterých národní CERT předává Úřadu kontaktní údaje povinných osob.

K § 17 odst. 2 písm. i) až l)

Národní CERT (Computer Emergency Response Team) na základě směrnice v tomto ustanovení získává nová kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který mimo jiné upravuje hlášení kybernetických bezpečnostních incidentů, které postihly informační systém poskytovatele digitálních služeb. Národní CERT se v tomto ohledu mimo jiné určuje jako jeden z týmů CSIRT (Computer Security Incident Response Team) v České republice; vládní CERT (Národní centrum kybernetické bezpečnosti, jež je součástí NBÚ) je druhým týmem CSIRT ve smyslu směrnice pro incidenty proti bezpečností sítí a informačních systémů určených provozovatelů základních služeb.

Týmy CSIRT musí naplňovat požadavky přílohy I směrnice, to je v případě národního CERT provozovaným sdružením CZ.NIC naplněno jednak požadavky na provozovatele národního CERT stanovené § 18 zákona a obsahem veřejnoprávní smlouvy, kterou s ním dle § 19 NBÚ uzavřel. Tato smlouva dle odstavce 1 tohoto ustanovení má zajistit plnění činností podle § 17, tedy i nových požadavků vyplývajících ze směrnice.

Konkrétně úkolům týmu CSIRT podle směrnice odpovídá zákon takto:

Národní CERT: přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je, poskytuje dotčeným subjektů metodickou podporu, pomoc a součinnost, působí jako kontaktní místo, provádí hodnocení zranitelnosti v oblasti kybernetické bezpečnosti, předává NBÚ údaje o incidentech, plní roli týmu CSIRT podle směrnice, spolupracuje s jinými týmy CSIRT, komunikuje s příslušnými orgány jiných členských států a v neposlední řadě přijímá dobrovolná hlášení o kybernetických bezpečnostních incidentech. Tím naplňuje požadavky přílohy I směrnice:

- *Monitorování incidentů na vnitrostátní úrovni - § 17 odst. 2 písm. b), c), l)*
- *Vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám – § 17 odst. 2 písm. d), e), g), j)*
- *Reakce na incidenty - § 17 odst. 2 písm. c), d)*
- *Poskytování dynamické analýzy rizik a incidentů a přehledu o situaci - § 17 odst. 2 písm. f)*
- *Účast v síti CSIRT – na uvážení provozovatele národního CERT, viz dále komentář k § 20.*

Povinnost zřídit alespoň jeden bezpečnostní tým typu CSIRT, který by byl odpovědný za zvládání rizik a řešení incidentů podle řádně vymezených postupů a splňují požadavky na bezpečnostní týmy typu CSIRT vyplývá z čl. 9 odst. 1 NIS.

Směrnice NIS stanoví, že tento povinně zřízený tým musí pokrýt svojí činností alespoň odvětví uvedená v příloze č. II (druhy subjektů) a služby uvedené v příloze III (druhy digitálních služeb).

V příloze č. I směrnice NIS jsou definovány úkoly a požadavky na bezpečnostní týmy typu CSIRT. Mezi tyto úkoly a povinnosti dle přílohy č. I NIS patří:

1. **Požadavky na týmy CSIRT**

- Týmy CSIRT zajistí, aby v jejich komunikačních službách nebyla žádná kritická místa (tzv. single points of failure), a tyto služby tak byly široce dostupné, a disponují několika způsoby, jimiž budou kontaktovat ostatní a jimiž bude možné kontaktovat je, a to kdykoli. Komunikační kanály musí být navíc jasně specifikované a spolupracujícím partnerům a subjektům spadajícím do působnosti týmů dobře známé.
- Pracoviště týmů CSIRT a jejich podpůrné informační systémy se nacházejí na bezpečném místě.
- Kontinuita činnosti:
  - týmy CSIRT jsou vybaveny vhodnými systémy řízení a směrování požadavků, které usnadní předávání,
  - týmy CSIRT jsou náležitě personálně obsazeny tak, aby byly kdykoli k dispozici,
  - týmy CSIRT musí pracovat s infrastrukturou, jejíž kontinuita je zaručena. Za tímto účelem musí být k dispozici záložní systémy a pracoviště.
- Týmy CSIRT musí mít možnost účastnit se mezinárodních sítí pro spolupráci, pokud chtějí být jejich součástí.

2. **Úkoly týmů CSIRT**

- Úkoly týmů CSIRT zahrnují alespoň:
  - monitorování incidentů na vnitrostátní úrovni,
  - vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám,
  - reakce na incidenty,
  - poskytování dynamické analýzy rizik a incidentů a přehledu o situaci,
  - účast v síti CSIRT.
- Týmy CSIRT naváží spolupráci se soukromým sektorem.
- V zájmu usnadnění spolupráce týmy CSIRT prosazují přijetí a používání společných či standardních postupů v oblasti:
  - řešení incidentů a rizik,
  - klasifikace incidentů, rizik a informací.

Sdružení CZ.NIC provozuje **národní tým CSIRT České republiky – CSIRT.CZ** (blíže viz https://csirt.cz/).

K odst. 1), 2) a 4)

Dle zákona o kybernetické bezpečnosti provozovatel národního CERT:

- **přijímá oznámení kontaktních údajů** od orgánů a osob uvedených v § 3 písm. a), b) a h) ZoKB a tyto údaje eviduje a uchovává,
- **přijímá hlášení o kybernetických bezpečnostních incidentech** od orgánů a osob uvedených v § 3 písm. b) a h) ZoKB a tyto údaje eviduje, uchovává a chrání,
- **vyhodnocuje kybernetické bezpečnostní incidenty** u orgánů a osob uvedených v § 3 písm. b) a h) ZoKB,
- **poskytuje orgánům a osobám** uvedeným v § 3 písm. a), b) a h) ZoKB **metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu**,

Polem působnosti týmu CSIRT.CZ je celý adresní rozsah České republiky. O pomoc s řešením incidentů se na CSIRT.CZ mohou obrátit všichni správci sítí, kteří potřebují pomoci s řešením incidentu vyžadujícím koordinaci řešení nebo mají podezření, že by incident mohl mít celoplošný dopad. Bližší informace a pokyny k hlášení incidentů je možné nalézt zde[2]. **Tým CSIRT.CZ nemá výkonné pravomoci** a při řešení incidentů působí v roli koordinátora, který může poskytnout také metodickou pomoc při jejich řešení.[3]

působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h) ZoKB,

provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

předává NÚKIB údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3 ZoKB, bez uvedení ohlašovatele,

- **předává NÚKIB na vyžádání kontaktní údaje** podle § 16 odst. 5 a 6 ZoKB,
- **plní roli týmu CSIRT podle směrnice NIS**,
- **informuje** bez uvedení identifikačních údajů ohlašovatele **příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem** na kontinuitu poskytování základní nebo digitální služby v tomto členském

státě a zároveň o tom informuje NÚKIB, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,
- **spolupracuje s týmy CSIRT jiných členských států**,
- **přijímá hlášení o kybernetických bezpečnostních incidentech od dalších osob,** neuvedených v § 3 ZoKB, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.

Sdružení CZ.NIC je dle § 17 odst. 4 ZoKB **povinno koordinovat činnost národního CSIRT týmu s činností NÚKIB**.

Vedle povinností explicitně stanovených zákonem o kybernetické bezpečnosti si národní CSIRT stanovil i další úkoly[4], mezi které patří:

Informování o nákaze v doméně .CZ

Pro účely centrálního monitoringu a řešení hrozeb v doméně druhého řádu vyvinul CSIRT.CZ open source tracker: Malicious Domain Manager.

Aplikace slouží jako centrální bod pro sběr a analýzu informací o škodlivých URL v doméně .CZ.

Aplikace podporuje historii hrozeb v doméně a přímé kontaktování jejich držitele. Držitelé domén jsou kontaktováni z dedikované adresy malware@nic.cz.

- **Skener webu**

Pro neziskový a veřejný sektor primárně je poskytována služba bezplatného penetračního testování webových stránek. Testování spočívá v automatických a ručních testech zaměřených na hledání bezpečnostních slabin v aplikaci. Každý bezpečnostní nález je označený odhadnutou mírou potencionálního rizika a obsahuje popis doporučení pro jeho případnou opravu.

Blíže viz https://www.skenerwebu.cz.

- **Vzdělávaní a přednášky**

Ve spolupráci s Akademií CZ.NIC jsou pravidelně realizovány školení Počítačová bezpečnost prakticky a Základy fungování CSIRT týmu. CSIRT.CZ také realizuje specializované kurzy pro bezpečnostní složky, státní i vzdělávací instituce či přednášky ad hoc.

- **Pomoc při zřizovaní CERT/CSIRT týmu**
- **Pracovní skupiny**

Tým CSIRT.CZ pořádá pravidelné setkání bezpečnostních týmů a členů bezpečnostní komunity v České republice.

- **Zátěžové testy**

Po DDoS útocích z roku 2013, které byly zaměřené na významné služby v České republice, připravily Laboratoře CZ.NIC **zátěžové testy** dosahující stejné a vyšší intenzity, jako zmiňované DDoS útoky. Ve spolupráci s CSIRT.CZ se tato služba poskytuje bezplatně pro všechny zájemce, kteří splní vstupní podmínky.

- **Intrusion Detection System**

Ve spolupráci se sdružením CESNET provozuje CSIRT.CZ systém detekující podezřelé chování systémů připojených do sítě Internet.

V případě zaznamenání podezřelých pokusů o připojení z konkrétních IP adres, jsou o takové události ihned informování zodpovědní administrátoři (prostřednictvím e-mailové adresy ids@csirt.cz).

- **Provozování honeypotů**

V rámci bezpečnostního výzkumu provozuje CSIRT.CZ ve spolupráci s Laboratořemi CZ.NIC řadu honeypotů. V rámci projektu Honeynet je možné nalézt vizualizaci útoků v reálném čase na https://honeymap.cz. Nově zachycené vzorky malwaru jsou analyzovány.

- **PROKI**

Rozesílání informací o bezpečnostních incidentech, jež mají původ v rozsahu českých IP adres.

K odst. 3) a 5)

Ustanovení § 17 odst. 2 ZoKB umožňuje, aby sdružení CZ.NIC vlastním jménem a na vlastní odpovědnost vykonávalo i další hospodářskou činnost v oblasti kybernetické bezpečnosti, která není přímo upravena zákonem o kybernetické bezpečnosti. Podmínkou však je, že tato další hospodářská činnost nenaruší plnění úkolů národního CSIRT.

Sdružení CZ.NIC je povinno při plnění povinností národního CSIRT týmu postupovat nestranně.

Dle ustanovení § 18 ZoKB se provozovatelem národního CERT se může stát pouze právnická osoba,

a) která splňuje podmínky uvedené v odstavci 2 a

b) se kterou Úřad uzavřel veřejnoprávní smlouvu podle § 19.

(2) **Provozovatelem národního CERT může být pouze právnická osoba, která**

a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací,

b) provozuje nebo spravuje informační systémy nebo služby a sítě elektronických komunikací[5] anebo se na jejich provozu a správě podílí, a to nejméně po dobu 5 let,

c) má technické předpoklady v oblasti kybernetické bezpečnosti,

d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,

e) nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky,

f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,

g) není zahraniční osobou podle jiného právního předpisu a

h) nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele národního CERT postupovat podle § 17 odst. 3.

(3) **Zájemce prokazuje splnění podmínek předložením**

a) čestného prohlášení v případě odstavce 2 písm. a) až d), g) a h) a

b) potvrzení orgánu Finanční správy České republiky a Celní správy České republiky v případě odstavce 2 písm. e).

(4) **Z obsahu čestného prohlášení podle odstavce 3 písm. a) musí být zřejmé, že uchazeč splňuje příslušné předpoklady. Potvrzení podle odstavce 3 písm. b), že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky, nesmí být starší než 30 dnů. Za účelem prokázání podmínky uvedené v odstavci 2 písm. f) si Úřad vyžádá výpis z evidence Rejstříku trestů podle jiného právního předpisu[6].**

(5) **Provozovatel národního CERT vykonává činnosti podle § 17 odst. 2 písm. a) až c), e) a g) až l) bezúplatně. Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 nezbytné náklady.**

(6) **Úřad zveřejní na svých internetových stránkách údaje o provozovateli národního CERT, a to jeho obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.**

Toto ustanovení stanoví obecné podmínky pro výběr provozovatele národního CERT. Současně je upraven způsob založení jeho závazku k provozování národního CERT formou veřejnoprávní smlouvy uzavřené s NBÚ. Užití institutu veřejnoprávní smlouvy odpovídá předpokladu, že provozovatelem národního CERT bude osoba soukromého práva. Závazky provozovatele národního CERT vykonávat činnosti uvedené v tomto zákoně mají sice převážně charakter soukromoprávní, ve vztahu k poskytovatelům služeb elektronických komunikací, subjektům zajišťující sítě elektronických komunikací a subjektům zajišťující významné sítě však bude provozovatel národního CERT vystupovat jako subjekt, prostřednictvím jehož činnosti tyto povinné osoby plní některé své zákonné povinnosti, typicky povinnost oznamovat kontaktní údaje a v případě subjektů zajišťujících významné sítě též povinnost hlásit výskyt kybernetických bezpečnostních incidentů.

Vzhledem k tomu, že národní CERT je pracovištěm velkého významu pro systém kybernetické bezpečnosti České republiky, vyžaduje se, aby měl jeho provozovatel sídlo na území České republiky. S ohledem na bezpečnostní expozici národního CERT tedy není možno vnímat tento požadavek jako diskriminační vůči osobám se sídlem v ostatních státech Evropské unie. Bezúhonnost, transparentní vlastnická struktura a neexistence splatných finančních závazků vůči státu jsou v případě spolupráce státu a osoby soukromého práva standardně požadovanými formálními podmínkami. Zákon rovněž formuluje materiální podmínky výkonu funkce provozovatele národního CERT, přičemž se požaduje, aby provozovatel národního CERT prokázal faktické schopnosti, zkušenosti a technické možnosti schopnost vykonávat činnosti uložené mu tímto zákonem, jakož i schopnost pracovat v součinnosti se zahraničními subjekty působícími na úseku kybernetické bezpečnosti. Zákon dále požaduje, aby provozovatel národního CERT vykonával činnosti svěřené mu tímto zákonem nestranně, bez ohledu na jeho případný smluvní či jiný vztah s povinnými osobami.

K § 18 odst. 5

Toto ustanovení reaguje na rozšíření kompetencí provozovatele národního CERT v § 17 a rozšiřuje adekvátně okruh činností, jež provozovatel národního CERT vykonává bezplatně.

K § 18 odst. 5

Legislativně technická úprava z důvodu rozšíření kompetencí provozovatele národního CERT. Pro zajištění důsledného naplňování povinností vyplývajících ze směrnice a následně ze zákona o kybernetické bezpečnosti se zakotvuje povinnost národního CERT vynaložit na zajištění výkonu kompetencí adekvátní finanční prostředky.

K odst. 1) a 2)

Provozovatelem národního CERT týmu je sdružení CZ.NIC.

Ustanovení § 18 ZoKB definuje podmínky, za kterých se může subjekt stát provozovatelem národního CERT.

Provozovatelem národního CERT může být pouze **právnická osoba**[7]**, se níž NÚKIB** (či dříve NBÚ) **uzavřel veřejnoprávní smlouvu**[8] (dle § 19 ZoKB), a **která splňuje následující podmínky:**

a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací,

Dle § 2 písm. b) ZoOUI je *„zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.“*

b) provozuje nebo spravuje informační systémy nebo služby a sítě elektronických komunikací anebo se na jejich provozu a správě podílí, **a to nejméně po dobu 5 let,**

c) má technické předpoklady v oblasti kybernetické bezpečnosti,

d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,

Požadavek na provozování některého ze systémů uvedených pod písmenem c), na existenci technických předpokladů v oblasti kybernetické bezpečnosti a členství v nadnárodní organizaci působící v oblasti kybernetické bezpečnosti dává státu garanci, že se daná osoba dostatečně dlouho a kvalitně věnuje problematice kybernetické bezpečnosti, řešení incidentů aj. De facto jde o prokázání faktické schopnosti, zkušenosti a technické možnosti vykonávat činnosti uložené mu ZoKB.

e) nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani **v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky,**

f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,

Neexistence splatných finančních závazků vůči státu, stejně jako prokázání bezúhonnosti je v případě spolupráce státu a osoby soukromého práva standardně požadovanou formální podmínkou pro uzavření smlouvy.

Zákon o kybernetické bezpečnosti se v § 18 odst. 2 písm. f) dopouští faktické nepřesnosti, která je způsobena novelizací zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. V tomto zákoně byly původně v § 7 vymezeny ty trestné činy, jichž se může dopustit právnická osoba. V současné účinné právní úpravě je v § 7 uvedeno negativní vymezení trestných činů.

Ustanovení § 7 TOPO (s účinností od 1. 12. 2016) stanoví, že právnická osoba může být trestně odpovědná za spáchání všech trestných činů s výjimkou trestných činů v tomto ustanovení taxativně uvedených.

Vedle vymezení okruhu trestných činů je třeba v případě trestně právní odpovědnosti právnických osob řešit i otázku přičitatelnosti. Přestože právnická osoba je fiktivní konstrukt, právo obecně ve vztahu k právnickým osobám uznává jejich způsobilost právně (tedy i protiprávně) jednat, včetně toho, že se jim přičítá zavinění. Zavinění jakožto podmínka trestní odpovědnosti se právnické osobě přičítá, jestliže nastaly okolnosti dle § 8 odst. 2 zákona o trestněprávní odpovědnosti právnických osob.

Dle § 8 odst. 1 zákona o TOPO se trestným činem spáchaným právnickou osobou rozumí protiprávní čin spáchaný v jejím zájmu nebo v rámci její činnosti, jednal-li tak

a) statutární orgán nebo člen statutárního orgánu, anebo jiná osoba ve vedoucím postavení v rámci právnické osoby, která je oprávněna jménem nebo za právnickou osobu jednat,

b) osoba ve vedoucím postavení v rámci právnické osoby, která u této právnické osoby vykonává řídící nebo kontrolní činnost, i když není osobou uvedenou v písmenu a),

c) ten, kdo vykonává rozhodující vliv na řízení této právnické osoby, jestliže jeho jednání bylo alespoň jednou z podmínek vzniku následku zakládajícího trestní odpovědnost právnické osoby, nebo

d) zaměstnanec nebo osoba v obdobném postavení (dále jen „zaměstnanec“) při plnění pracovních úkolů, i když není osobou uvedenou v písmenech a) až c),

jestliže lze právnické osobě jednání výše uvedené osoby přičítat podle § 8 odst. 2 TOPO.

g) není zahraniční osobou podle jiného právního předpisu,

Za zahraniční osobu se dle § 3024 OZ považuje fyzická osoba s bydlištěm nebo právnická osoba se sídlem mimo území České republiky.

Vzhledem k významnosti národního CERT týmu v oblasti kybernetické bezpečnosti ČR je požadováno, aby provozovatel tohoto týmu měl sídlo na území ČR. Tento požadavek nelze vnímat jako diskriminaci vůči jiným osobám se sídlem v jiném členském státu Unie.

h) nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele národního CERT postupovat podle § 17 odst. 3 ZoKB.

K odst. 3) a 4)

Právnická osoba, která se chce stát provozovatelem národního CERT, prokazuje splnění podmínek předložením čestného prohlášení [v případě § 18 odst. 2 písm. a) až d), g), h) ZoKB] a potvrzením orgánu Finanční správy České republiky a Celní správy České republiky [v případě § 18 odst. 2 písm. e) ZoKB].

Z obsahu čestného prohlášení musí být zřejmé, že uchazeč splňuje příslušné předpoklady. Potvrzení, že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky, **nesmí být starší než 30 dnů.**

Z důvodu **prokázání té skutečnosti, že právnická osoba nebyla pravomocně odsouzena za spáchání trestného** činu **si NÚKIB vyžádá výpis z evidence Rejstříku trestů.**

K odst. 5)

Provozovatel národního CERT **vykonává činnosti uvedené v § 17 odst. 2 ZoKB bezúplatně**. Výjimkou z podmínky bezplatnosti jsou pouze následující činnosti:

§ **poskytuje orgánům a osobám** uvedeným v § 3 písm. a), b) a h) ZoKB **metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,**

§ **provádí hodnocení zranitelností** v oblasti kybernetické bezpečnosti.

Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 ZoKB nezbytné náklady.

K odst. 6)

Z důvodu možnosti kontaktovat provozovatele národního CERT týmu jsou údaje o tomto provozovateli zveřejněny na internetových stránkách NÚKIB. Zveřejněny jsou následující informace: obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.

3.1.2 Vládní CERT

Vládní CERT jako součást Úřadu

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až g),

b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až g),

c) vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,

d) poskytuje orgánům a osobám uvedeným v § 3 písm. c) až g) metodickou podporu a pomoc,

e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,

f) přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje,

g) přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje,

h) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje,

i) poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů,

j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

k) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

l) přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost,

m) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[9] **a**

n) spolupracuje s týmy CSIRT jiných členských států.

Vládní CERT je součástí NBÚ, respektive Národního centra kybernetické bezpečnosti, jež je organizačním celkem NBÚ, který zajišťuje jeho činnost. Vládní CERT je koncipován jako centrální veřejnoprávní pracoviště a veřejnoprávní „single point of contact" pro oblast kybernetické bezpečnosti. Jeho činnost zahrnuje příjem kontaktních údajů od vybraných povinných osob, příjem informací o kybernetické bezpečnostní situaci, a to zejména příjem povinných a iniciativních hlášení kybernetických bezpečnostních incidentů a dalších údajů o kybernetické bezpečnostní situaci od tuzemských a zahraničních orgánů veřejné moci a spolupracujících subjektů a jejich vyhodnocování. Vládní CERT dále poskytuje součinnost vybraným typům povinných osob při výskytu kybernetického bezpečnostního incidentu, zajišťuje součinnost s ostatními orgány a subjekty zajišťujícími kybernetickou bezpečnost v České republice a ve spolupracujících nebo spojeneckých státech a rovněž provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.

K § 20 písm. a), b), d) a e)

Mezi subjekty, se kterými komunikuje a s nimiž spolupracuje vládní CERT, se doplňují nové povinné subjekty - provozovatelé základních služeb a správci a provozovatelé informačních systémů základních služeb.

K § 20 písm. c)

Mezi informační systémy, u nichž vládní CERT vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech, se doplňují informační systémy, na jejichž provozování je závislé poskytování základních služeb.

K § 20 písm. i)

Legislativně technická úprava vyplývající z potřeby doplnění nových písmen do tohoto ustanovení.

K § 20 písm. j) a písm. k) až n)

Vládní CERT na základě směrnice v tomto ustanovení získává nové kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který upravuje hlášení kybernetických bezpečnostních incidentů.

Vládní CERT podle zákona ve znění tohoto návrhu: přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je, poskytuje dotčeným subjektů metodickou podporu, pomoc a součinnost, působí jako kontaktní místo, provádí hodnocení zranitelnosti v oblasti kybernetické bezpečnosti, předává NBÚ údaje o incidentech, plní roli týmu CSIRT podle směrnice, spolupracuje s jinými týmy CSIRT, komunikuje s příslušnými orgány jiných členských států a v neposlední řadě přijímá dobrovolná hlášení o kybernetických bezpečnostních incidentech.

Tím naplňuje požadavky přílohy I směrnice:

- *Monitorování incidentů na vnitrostátní úrovni - § 20 písm. b), c), f), g), l).*
- *Vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám – § 20 písm. d), e), i), n).*
- *Reakce na incidenty - § 20 písm. d), e).*
- *Poskytování dynamické analýzy rizik a incidentů a přehledu o situaci - § 20 písm. j).*
- *Účast v síti CSIRT - § 20 písm. m).*

Tím, že vládní CERT, který je součástí NBÚ, plní roli týmu CSIRT, bude i naplňovat požadavky směrnice na účast týmu CSIRT v síti CSIRT podle článku 12 směrnice. Účast zástupců národního CERT bude ponechána na jejich uvážení.

Směrnice stanoví ve svém článku 9, že každý členský stát zřídí jeden nebo více týmu CSIRT, neřeší však, že by se měli zástupci všech týmů CSIRT členského státu povinně účastnit práce sítě CSIRT. Postačuje tak plně účast alespoň jednoho týmu CSIRT, což naplní zástupci vládního CERT. Ustanovení upravuje postup vládního CERT v případě, že má nahlášený kybernetický bezpečnostní incident významný

dopad na kontinuitu poskytování základních služeb, nebo dopad na poskytování digitálních služeb v jiném členském státu Evropské unie. V takovém případě se v souladu s čl. 14 odst. 5, potažmo čl. 16 odst. 6 směrnice zakotvuje oprávnění vládního CERT informovat o daném incidentu příslušné orgány jiných členských států.

Směrnice předvídá ve svém čl. 20 situaci, kdy subjekt, který nebyl určen jako provozovatel základních služeb a není ani poskytovatelem digitálních služeb, zaregistruje napadení bezpečnosti jeho informačních systémů a má snahu tuto situaci řešit. V tomto případě může tento kybernetický bezpečnostní incident dobrovolně nahlásit vládnímu CERT a ve spolupráci s ním situaci řešit. Vládní CERT v tomto případě hlášení zpracuje, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje přiměřeně, jako když je mu nahlášen kybernetický bezpečnostní incident u provozovatele základních služeb.

Na základě zákona o kybernetické bezpečnosti **jsou v ČR povinně zřízeny dva týmy** typu CERT/CSIRT, **a to národní a vládní**.

Provozovatelem národní CERT je právnická osoba s níž NÚKIB (dříve NBÚ) uzavřel veřejnoprávní smlouvu (viz § 19 ZoKB).

Vládní CERT (**GovCERT.CZ** – blíže viz https://www.govcert.cz/) je zřízen na základě zákona jakožto součást Národního úřadu pro kybernetickou a informační bezpečnost (dříve v gesci NBÚ).

Dle zákona o kybernetické bezpečnosti vládní CERT:

- **přijímá oznámení kontaktních údajů** od orgánů a osob uvedených v § 3 písm. c) až g) ZoKB,
- **přijímá hlášení o kybernetických bezpečnostních incidentech** od orgánů a osob uvedených v § 3 písm. c) až g) ZoKB,
- **vyhodnocuje údaje** o kybernetických bezpečnostních **událostech** a kybernetických bezpečnostních **incidentech** z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,
- **poskytuje orgánům a osobám** uvedeným v § 3 písm. c) až g) ZoKB **metodickou podporu a pomoc,**
- **poskytuje součinnost** orgánům a osobám uvedeným v § 3 písm. c) až g) ZoKB **při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,**

Řešení bezpečnostních incidentů patří k hlavním činnostem vládního týmu. Při nahlášení kybernetického bezpečnostního incidentu je vládní tým GovCERT.CZ připraven pomoci IT specialistům po technické stránce, včetně poskytnutí rad pro další preventivní opatření. V případě, že dojde ke zjištění, že některý z incidentů cílí na více subjektů, je vládní tým GovCERT.CZ připraven koordinovat společný postup na jeho řešení.[10]

- **přijímá podněty a údaje** od orgánů a osob uvedených v § 3 ZoKB a od jiných orgánů a osob **a tyto** podněty a údaje **vyhodnocuje,**
- **přijímá údaje od provozovatele národního CERT** a tyto údaje vyhodnocuje,
- **přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí**, a tyto údaje vyhodnocuje,
- **poskytuje podle údaje z evidence incidentů** (viz § 9 odst. 4 ZoKB) provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů,
- **provádí hodnocení zranitelností** v oblasti kybernetické bezpečnosti,
- **informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad** na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,
- **přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3 ZoKB**; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost,
- **plní roli týmu CSIRT** podle čl. 9 NIS,
- **spolupracuje s týmy CSIRT jiných členských států**.

Vedle povinností explicitně stanovených zákonem o kybernetické bezpečnosti si vládní CERT stanovil i další úkoly[11], mezi které patří:

- **Sdílení dat**

GovCERT.CZ získává v rámci spolupráce s různými nadnárodními organizacemi, které se zabývají kybernetickou bezpečností, množství reportů a dat, které se týkají potenciálně infikovaných informačních systémů v ČR. Tyto informace v rámci proaktivní činnosti poskytuje dalším subjektům. Sdílená data jsou rozdělena do následujících projektů:

· **BotnetFeed** – pomocí tohoto nástroje jsou zpracovávána data z převzatých C&C serverů o koncových stanicích zapojených do sítí botnetů. Pro identifikaci případně nakaženého počítačového systému je správci IP rozsahu předána IP adresa a informace o botnetu, do kterého je začleněna.

· **IHAP** (Incident Handling Automation Project)**, MDM** (Malicious Domain Manager) – v rámci těchto projektů jsou sbírány fragmenty indikátorů kompromitace (IoC) z různých serverů. Mezi nejčastější indikátory patří phishing, útoky hrubou silou, ids alerty, spam, pokusy o skenování, zneužívání zranitelností, výskyt malware a mnoho dalších typů. Na základě těchto dat jsou připravovány krátké reporty, které vždy obsahují IP adresu kompromitovaného stroje a stručné shrnutí, o jaký typ incidentu se jedná.

· **Shadowserver** – projekt je zaměřen na průběžné vyhledávání relevantních informací o zranitelnostech v kyberprostoru a o výskytech těchto zranitelností na konkrétních IP adresách.

- **Nasazování Honeypotů**
- **Penetrační testování**

Jedná se o legální pokus o průnik do testovaných systémů. Výsledkem je zpráva o chybách v zabezpečení testovaného subjektu, která je určena výhradně jeho vlastníkovi, který na základě zprávy učiní příslušná bezpečnostní opatření.

Další možností je provedení skenování zranitelností podle OWASP (Open Web Application Security Project).

- **Informační HUB**

Na webových stránkách govcert.cz je možné nalézt informace, rešerše, analýzy a články týkající se aktuálních hrozeb a zranitelností se vztahem k systémům v České republice. Uvedené dokumenty jsou doplňovány o pravidelné měsíční bulletiny shrnující významné bezpečnostní incidenty v CŘ i zahraničí.

- **Vzdělávání a výzkumná činnost**

Forenzní laboratoř a SCADA laboratoř

---

[1] Čl. 9 NIS

[2] *Kdy nás kontaktovat.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/

[3] *Služby CSIRT.CZ.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://csirt.cz/page/2764/sluzby/

[4] Všechny úkoly jsou převzaty z: *Služby CSIRT.CZ.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://csirt.cz/page/2764/sluzby/

[5] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[6] Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů.

[7] Dle § 20 odst. 1 OZ se právnickou osobou rozumí *„**organizovaný útvar, o kterém zákon stanoví, že má právní osobnost, nebo jehož právní osobnost zákon uzná.** Právnická osoba může bez zřetele na předmět své činnosti mít práva a povinnosti, které se slučují s její právní povahou.“* Stát se v oblasti soukromého práva považuje za právnickou osobu. (§ 21 OZ).

Právnickou osobou může být osoba soukromého či veřejného práva podle toho v jakém zájmu je právnická osoba ustanovena (§ 144 OZ). Z pohledu občanského práva jsou právnickou osobou korporace (viz § 210 a násl. OZ), fundace (viz § 303 a násl. OZ) a ústavy (viz § 402 a násl.).

[8] Využití institutu veřejnoprávní smlouvy dle § 160 a násl. SŘ odpovídá předpokladu, že provozovatelem národního CERT bude osoba soukromého práva.

[9] Viz čl. 9 NIS

[10] *Poskytované služby.* [online]. [cit. 1. 8. 2018]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

[11] Všechny úkoly jsou převzaty z: *Poskytované služby.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

3.2. Polsko

Právní rámec pro týmy CSIRT/CERT v Polsku

Zákon ze dne 5. července 2018 o národním systému kybernetické bezpečnosti rozlišuje 3 národní CSIRT:

- CSIRT GOV - tým pro řešení počítačových bezpečnostních incidentů působící na národní úrovni, v jehož čele stojí vedoucí Agentury pro vnitřní bezpečnost.

- CSIRT MON - Tým pro reakci na počítačové bezpečnostní incidenty, který působí na národní úrovni a je veden ministrem národní obrany.

- CSIRT NASK - Tým pro řešení počítačových bezpečnostních incidentů působící na národní úrovni, v jehož čele stojí Vědecká a akademická počítačová síť - Národní výzkumný ústav.

Zákon dále uvádí následující subjekty, které jsou součástí národního systému kybernetické bezpečnosti:

- provozovatelé základních služeb;

- poskytovatelé digitálních služeb;

- odvětvové týmy kybernetické bezpečnosti;

- subjekty sektoru veřejných financí uvedené v článku 1. 9 bodech 1-6, 8, 9, 11 a 12 zákona ze dne 27. srpna

- 2009 o veřejných financích (Sbírka zákonů z roku 2017, položka 2077 a z roku 2018, položka 62, 1000 a 1366);

- výzkumné ústavy;

- Polská národní banka;

- Bank Gospodarstwa Krajowego;

- Úřad technické inspekce;

- Polská agentura pro leteckou navigaci;

- Polské akreditační centrum

- Státní fond pro ochranu životního prostředí a vodní hospodářství a provinční fondy pro ochranu životního prostředí a vodní hospodářství;

- obchodně právní společnosti plnící úkoly veřejné služby ve smyslu čl. 1 odst. 2 zákona ze dne 20. prosince 1996 o obecním řízení (Sb. zákonů 2017, položka 827 a 2018, položka 1496);

- subjekty poskytující služby kybernetické bezpečnosti;

- příslušné orgány pro kybernetickou bezpečnost;

- Jednotné kontaktní místo pro kybernetickou bezpečnost;

- Vládní zmocněnec pro kybernetickou bezpečnost;

- Vysoká škola kybernetické bezpečnosti.

Úkoly, způsoby činnosti a další předpisy subjektů polského systému kybernetické bezpečnosti jsou stanoveny v zákoně.

3.3. Portugalsko

Under construction

3.4. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) was adopted by the European Parliament.
- The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
  - Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
  - cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
  - a culture of security across sectors that are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.
- Členské státy přistoupily různě k implementaci NIS.
- Legislativní rámec CSIRT/CERT týmů v ČR je částečně stanoven zákonem o kybernetické bezpečnosti. Tento zákon stanoví podmínky pro existenci národního a vládního CSIRT/CERT týmu, avšak na druhou stranu nijak neomezuje vznik a existenci jiných CSIRT/CERT týmů.
  - Na základě zákona o kybernetické bezpečnosti jsou v ČR povinně zřízeny dva týmy typu CERT/CSIRT, a to národní a vládní. Každý z těchto týmů má zákonem (§ 17 a násl. ZoKB) přesně stanovená práva a povinnosti.
- Legislativní rámec CSIRT/CERT týmů v Polsku
- Legislativní rámec CSIRT/CERT týmů v Portugalsku

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- kybernetická bezpečnost
- CSIRT/CERT
- NIS directive
- ENISA
- Constituency
- Národní a vládní CSIRT/CERT
- Spolupráce týmů

KONTROLNÍ OTÁZKY

- Existuje hierarchie mezi CSIRT/CERT týmy?
- Jak je definováno pole působnosti CSIRT/CERT týmu?
- Kdo je to vládní CSIRT/CERT tým?
- Kdo je to národní CSIRT/CERT tým?
- Jaké jsou role a úkoly dalších CSIRT/CERT týmů?
- Jak je to s konstituencí CSIRT/CERT týmů ve vaší zemi?

4. Závěr

Žijeme v době, kdy jsou informační a komunikační technologie již neodmyslitelně propojeny s každým aspektem našeho bytí. Určitým paradoxem je, že de facto nemáme možnost se tomuto prostupu a vzájemné interakci s ICT vyhnout, což nás současně činí více zranitelnými.

S tím, jak roste objem dat a informací ukládaných v jednotlivých ISP, začínají být stále více řešeny i otázky jejich efektivního zabezpečení, předávání či vymazání, a to nejen na základě smlouvy uzavřené mezi poskytovatelem dané služby a koncovým uživatelem, ale i na základě nově vznikajících právních předpisů.

Státy, organizace, ale i jednotlivci si čím dál více uvědomují, že informace a data představují významný potenciál, který je ve stále větší míře napadán kybernetickými útoky ať již s cílem zcizení, poškození, znepřístupnění, či vymazání dat.

Pokud chceme v současné společnosti žít a využívat její benefity, není možné se od ICT oprostit a rozhodně nemá smysl tyto technologie přestat využívat. Je třeba se začít učit, jak tyto technologie a služby využívat, jak se vyhnout či alespoň eliminovat následky způsobené kybernetickými útoky.

Řadě negativních událostí se lze vyhnout, pokud budou jedinci i organizace respektovat alespoň základní principy kybernetické bezpečnosti.

V kyberprostoru, stejně jako ve světě reálném, neexistuje jedna bezpečnost a jedno zabezpečení, které by bylo možné univerzálně aplikovat na každého. Pokud chceme řešit bezpečnost, je třeba ji řešit komplexně a je třeba individualizovat.

Informační a komunikační technologie jsou oborem, který se nejdynamičtěji a nejmasivněji vyvíjí. Oblasti, kterým bychom v této souvislost měli věnovat extrémní pozornost, jsou bezpečnost a edukace uživatelů.

5. Seznam literatury

1. *2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

2. *Analýza rizik.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

3. ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440

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

5. *CIA triad methodology.* [online]. [cit. 10. 7. 2018]. Dostupné z: *https*://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

6. *Computer Security Incident Handling Guide* [online]. [cit. 13. 8. 2018], s. 6. Dostupné z: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

7. *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.

8. *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.

9. *Cyberthreat.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat

10. *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10. 12. 2017]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

11. *ENISA CSIRT maturity assessment model* [online], 2019. VERSION 2.0. Athens, Greece: European Union Agency for Network and Information Security (ENISA) [cit. 2021-03-16]. ISBN 978-92-9204-292-9. Dostupné z: https://www.enisa.europa.eu/publications/study-on-csirt-maturity/at_download/fullReport, p. 6

12. EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

13. FRANK, Libor. *Bezpečnostní studia.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

14. FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

15. HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, availability.* [online]. [cit. 13. 1. 2018]. Dostupné z: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

16. *Hrozba.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

17. HSU, D. Frank a D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 S. ISBN 978-0-8232-4456-0. s 41.

18. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 23. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

19. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. s. 21 a násl.

20. KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21. 7. 2018]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

21. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016.

22. *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29. 6. 2018]. Dostupné z: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

23. *Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma.* [online]. [cit. 29. 6. 2017]. Dostupné z:http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

24. MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

25. MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - provádění kontrol technického stavu technických zařízení.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

26. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

27. *Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/

28. *POŽÁR, Josef. Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 37.

29. POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

30. PROSISE, Chris a Kevin MANDIVA. *Incident response & komputer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 13

31. Před čím chránit? – Bezpečnostní hrozby, události, incidenty. *[online]. [cit. 6. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit*

32. *Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

33. RAK, Roman. Homo sapiens versus security. ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

34. SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570039

35. SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570035

36. SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570047

37. SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570040

38. *Směrnice NIS.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

39. SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23. 9. 2014)

40. ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vyd. Praha: C. H. Beck, 2012, s. 2308

41. ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 20 a násl.

42. *Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin.* [online]. [cit. 29. 6. 2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin

43. *The complete breadth of CGI Cyber Security services.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://mss.cgi.com/service-portfolio

44. *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

45. VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení při nevojenských krizových situacích*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 1. 7. 2018]. Dostupné z: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx

46. WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

47. *WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

48. WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s.

49. *Základní pojmy.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

50. ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10. 7. 2018]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

51. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf