Jan Kolouch, Pavel Bašta a kol.

CyberSecurity

Edice CZ.NIC

CYBERSECURITY

doc. JUDr. Jan Kolouch, Ph.D.
Bc. Pavel Bašta
Andrea Kropáčová
Bc. Martin Kunc

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2019
Kniha vyšla jako 20. publikace v Edici CZ.NIC.
ISBN 978-80-88168-34-8

CZ.NIC | SPRÁVCE DOMÉNY CZ

Právní stav byl zohledněn ke dni 1. 7. 2018.

Autorský kolektiv
doc. JUDr. Jan Kolouch, Ph.D., autor kapitol:
předmluva autorů, 1, 2, 3, 4, závěr, seznam literatury; spoluautor kapitol: 5, 6
Bc. Pavel Bašta, autor kapitol: 5, 6; spoluautor kapitol: 1, 1.3.3, 1.4.
Andrea Kropáčová, autorka kapitoly 7
Bc. Martin Kunc, autor kapitol: 6.4, 6.5

ISBN 978-80-88168-34-8

— Jan Kolouch, Pavel Bašta a kol.

CyberSecurity

— Edice CZ.NIC

Předmluva vydavatele

Vážení čtenáři,

pokaždé, když vidím novou knihu v naší edici, mám pocit dobře vykonané práce. Ne, nejsem autorem, editorem nebo grafikem těchto knih, na jejich vzniku se nepodílím prakticky žádnou činností, ale i tak ten pocit mám. Jsem rád, že Edice CZ.NIC existuje a pomáhá spatřit světlo světa spoustě výborných knih, které by to (možná) bez nás měly s cestou ke čtenáři složitější.

Speciálně mám ale radost vždy, když jde o knihu z oblasti bezpečnosti. Měl jsem tu čest psát již předmluvu ke knize CyberCrime, kterou jsme v naší edici vydávali v roce 2016. V letošním roce jsme se pokusili na tuto knihu volně navázat – s rozšířeným týmem autorů a novým, z trochu jiného úhlu pohledu pojatým obsahem.

K osvědčenému autorovi, vysokoškolskému pedagogovi a ostřílenému odborníkovi na kybernetickou kriminalitu Janu Kolouchovi se připojili moji kolegové z prostředí bezpečnostních týmů, kteří dali knize další rozměr.

Kniha se tak z mého pohledu ještě více posunula z oné pomyslné knihovny na pracovní stůl (jak jsem o tom psal před dvěma lety) a já věřím, že bude užitečná jak pro běžné uživatele, kteří budou potřebovat radu, návod nebo vhodný postup při řešení každodenních problémů bezpečnosti, tak i pro odborníky, kteří v ní najdou inspiraci pro své další vzdělávání.

Ostatně udělejte si obrázek sami – přeji příjemně a užitečně strávené chvíle při práci s knihou.

Martin Peterka, CZ.NIC
Praha, 23. října 2018

Předmluva autorů

Předmluva autorů

„Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.“ [1]

Dnešní společnost se v průběhu posledních 20 let stala na informačních a komunikačních technologiích[2] natolik závislá, že okamžitý kolaps těchto technologií a služeb na ně navázaných by pro značnou část lidstva byl spojen s téměř apokalyptickými následky, ne nepodobnými těm uvedeným v románu Ondřeje Neffa - Tma.[3]

V tomto románu je apokalypsa spojena s masivním a dlouhotrvajícím výpadkem, respektive zdánlivým koncem elektrické energie. Co by však pro lidstvo znamenal okamžitý a nečekaný výpadek ICT?

Jsme přesvědčeni, že ještě před deseti či patnácti lety by nemožnost připojení se k Internetu a dalším ICT službám znamenala pouze to, že bychom se věnovali jiné práci, či udělali víc „skutečné práce“.

V současné době je otázkou, co bychom mohli dělat? Nezapnuli bychom počítač ani textový editor, ve kterém píšeme tuto knihu, nikomu bychom se nedovolali, nebyli bychom schopni si užitečné odkazy dohledat na Internetu (ok… na https://www.google.com/), nedomluvili bychom se se svým editorem a rozhodně bychom Vám nijak nebyli schopni předat informace, které se do této knihy snažíme zachytit.

Další otázkou je, zda by vůbec byly poskytovány služby, na které jsme zvyklí a bez kterých si svůj život už neumíme představit. Mezi tyto služby je zcela bezpochyby možné zařadit distribuci elektřiny, vody, telekomunikační služby, zdravotní péči, zajištění bezpečnosti občanů a státu, dopravu (řízení provozu, ale i hromadnou dopravu), finanční transakce (včetně běžných plateb, výběru z bankomatů atd.), přístup k informacím (televizní zpravodajství, ale samozřejmě i Seznam.cz, Google.com) aj.

Nedávné útoky ransomwarem[4] WannaCry, Petya (respektive mutací tohoto malware – Petrwap či Win32/Diskcoder.C Trojan) ukázaly zranitelnost a zejména závislost „vyspělého a moderního“

1: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 474

2: Dále jen: **ICT** či informační a komunikační technologie, **IT** či informační technologie, **IS** či informační systémy. Pojem **ICT** v sobě zahrnuje jednak počítačové systémy (viz dále), tak i technologie (např. optické, metalické kabely aj.) umožňující vzájemnou interakci těchto systémů.

3: NEFF, Ondřej. *Tma.* Praha: Plus. ISBN 978-80-259-0279-0

4: Blíže k pojmu ransomware viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 221 a násl. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

světa na ICT a zároveň prezentovaly nedostatečnost zabezpečení vitálních systémů před kybernetickými útoky. Právě WannaCry, byť se jednalo o klasický ransomware útok, kterých jsou denně desítky, dokázal zcela zastavit provoz 16 nemocnic ve Velké Británii.[5] Petrwap pak způsobil značné problémy zejména na Ukrajině, kdy řada ukrajinských společností (mimo jiné se jednalo o energetické společnosti, letiště v Kyjevě, banky aj.) nemohla vykonávat svoji běžnou činnost či ji musela zcela zastavit. *„V důsledku tohoto útoku mají některé banky problémy s prováděním bankovních operací"*, oznámila ukrajinská centrální banka. Různé antivirové společnosti pak oznamovaly země, jež byly tímto útokem přímo dotčeny. Podle antivirové společnosti ESET byly mezi nejvíce napadenými zeměmi vedle Ukrajiny i Itálie, Izrael, Srbsko, ale také Česká republika.[6] Společnost Kaspersky Lab pak tento okruh zemí dále rozšířila o Polsko, Německo, Francii, USA, Velkou Británii, Austrálii, Rusko aj.[7]

Otázkou pak zůstává, jestli jsme skutečně „vyspělí a moderní"? Možná by bylo lepší nás označit za „trendy a in" a především **neustále připojené**. Velmi rychle jsme si začali zvykat na nové a nové technologie, jejich vylepšení a nadstavby v podobě Internet of Things[8] (do budoucna Internet of Everything), které vlastně ani v řadě případů skutečně nepotřebujeme.

5: Viz např.: *UK hospitals hit with massive ransomware attack*. [online]. [cit. 27. 6. 2076]. Dostupné z: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin
U.K. Hospitals Hit in Widespread Ransomware Attack. [online]. [cit. 27. 6. 2017]. Dostupné z: https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
Masivní kyberútok zasáhl ve stovce zemí. Ochromil nemocnice i Telefóniku. [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.cnews.cz/ransomware-wanacryptor-wcry-wannacry

6: *Šíří se staronový vir vyděrač. Výkupné neplaťte, adresa je nefunkční.* [online]. [cit. 28. 6. 2017]. Dostupné z: https://technet.idnes.cz/kyberneticky-hackersky-utok-ve-svete-ransomware-fbq-/sw_internet.aspx?c=A170627_172510_tec-kratke-zpravy_pka

7: *RANSOMWARE IS ONE OF THE WORLD'S FASTEST GROWING TYPES OF MALWARE.* [online]. [cit. 28. 6. 2017]. Dostupné z: https://go.kaspersky.com/Anti-ransomware-tool.html

8: Dále jen **IoT**, či Internet věcí. Typicky se jedná o zařízení (počítačové systémy), které sbírají a vyměňují si data s jinými počítačovými systémy. Předpokladem je, že jsou tato zařízení připojena k počítačovému systému, či počítačové síti. Příkladem může být:

- komunikace mezi televizí a žárovkou - pokud bude televize schopna navázat kontakt se žárovkou, bude možné zajistit optimální nastavení světla žárovky ve vztahu k aktuálnímu nastavení jasu televize;
- předávání informací z osobní váhy do telefonu či přímo lékaři;
- předání informací z wearables („nositelná" elektronika, čidla aj.) umístěného v oblečení, botách do počítačového systému pro výpočet ušlých kroků, spálených kalorií aj.
- sledování pozice GPS a předávání této informace;
- sledování množství potravin v lednici a případný automatický nákup chybějících potravin aj.

Bližší informace naleznete např. na:
What is Internet of Things. [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

„Ještě než jsem se přestěhoval do své vily na šesti kolech, byl můj byt ten nejlepší kamarád. Lednička vždycky věděla, na co mám právě chuť. Šampaňské bylo pokaždé vychlazené na tu správnou teplotu s přesností na desetinu stupně. Sama vyhazovala prošlé potraviny a sama nakupovala čerstvé. Pračka hlásila šatní skříni, kdy má pořídit nové oblečení podle poslední módy. Postel mě sama uspávala i budila podle mozkových vln. Záchodová mísa průběžně analyzovala tělesný odpad, a když něco nebylo v pořádku, přivolala lékařského medibota a nařídila ledničce, co mám jíst a pít pro zdraví. Všechno bylo tak propojené a perfektní, že jsem si nakonec začal připadat jako další domácí spotřebič. A tak jsem oprášil starý vojenský kufr po tátovi ukrývající skoro zapomenuté nářadí. Z útrob jsem vytáhl kladivo a všem těm chytrým přístrojům vymlátil wi-fi anténky.“

Být nad věcí internetu věcí[9]

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.[10]

Je třeba si uvědomit, že čím více budeme závislí na ICT 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.[11]

V této souvislosti je třeba připomenout citát ***Scientia est potentia*** (***vědění je moc, v poznání a znalostech je síla, vědění je síla***). V případě ICT a služeb s nimi spojených je třeba poznat, co tyto technologie a služby představují, co činí a k čemu slouží.[12]

Internet of Things (IoT). [online]. [cit. 15. 7. 2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

9: STANČÍK, Petr. *100 miliard neuronů.* [online]. [cit. 16. 8. 2018]. Dostupné z: https://backendstories.skoda-kariera.cz/assets/files/library/b01/100_MILIARD_NEURONU_-_PETR_STANCIK.pdf s. 133

10: 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

11: *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

12: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 474

V současnosti by rezignace na využívání ICT znamenala izolaci jedince či organizace od zbytku společnosti, v řadě případů i nemožnost „fungování“ tohoto jedince ve společnosti či státě, který tyto technologie využívá, případně vyžaduje, aby jej využívaly i osoby, které se v jeho teritoriu nacházejí (např. datové schránky, které jsou povinné pro určité subjekty; různé formy e-identit aj.).

Pokud chceme v současné společnosti žít a využívat její benefity, není možné se od ICT oprostit a rozhodně nemá smysl tyto technologie přestat využívat.

Informační a komunikační technologie jsou oborem, který se nejdynamičtěji a nejmasivněji vyvíjí, avšak otázkám bezpečnosti či zabezpečení není věnována taková pozornost jako například tomu, jaký bude design výrobků, kapacita úložného prostoru, možnosti telekomunikace s dalšími zařízeními aj.

Kniha, kterou právě čtete, se primárně snaží věnovat problematice kybernetické bezpečnosti. Ale tak, jako nebylo možné se při řešení problematiky kyberkriminality vyhnout kybernetické bezpečnosti, ani u kybernetické bezpečnosti nelze opomenout problematiku kyberkriminality. Tyto dvě oblasti jsou bezprostředně spjaty a bezpečnostní opatření v řadě případů odráží útoky, které mají ve své podstatě kriminální povahu.

Naší snahou je v této knize představit základní principy, které by každá osoba, která využívá ICT, měla respektovat a případně si je měla modifikovat v závislosti na činnosti či účelu, za kterým tyto technologie využívá. Dále pak načerpat informace o činnosti bezpečnostních týmů typu CERT, CSIRT[13] v kyberprostoru, jejich možnostech a limitech.

Samostatná pozornost je také věnována výkladu některých právních norem, které s problematikou kybernetické bezpečnosti bezprostředně souvisejí. Půjde především o novelizovaný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)[14], ve znění pozdějších předpisů; Nařízení Evropského parlamentu a Rady (EU) 2016/697 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[15] a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) aj.

Výklad zákona o kybernetické bezpečnosti a prováděcích vyhlášek k tomuto zákonu je podán formou komentáře.

13: **CERT** (**C**omputer **E**mergency **R**esponse **T**eam) či **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam). Dále jen **CERT** a **CSIRT**. Blíže viz kap. 7 CERT/CSIRT týmy

14: Dále jen zákon o kybernetické bezpečnosti či **ZoKB**

15: Také známé jako GDPR (**G**eneral **D**ata **P**rotection **R**egulation) či Obecné nařízení o ochraně osobních údajů. Dále jen **GDPR**.

Tato kniha byla pro autory skutečným oříškem, neboť je mnohem složitější psát knihu o kybernetické bezpečnosti, respektive o tom, jak byste si měli zabezpečit svoje prvky ICT, jak se chovat bezpečně on-line aj. než psát knihu o kybernetických útocích a právní odpovědnosti za ně.[16] Ten zásadní problém totiž spočívá v tom, že 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.

Na základě výše uvedeného jsme se rozhodli tuto knihu koncipovat tak, aby informace v ní obsažené mohli využít jak běžní uživatelé (např. při tvorbě a správě hesel; nastavování VPN aj.), tak IT odborníci, kteří se chtějí vzdělat i v problematice kybernetické bezpečnosti. Nedílnou součástí této publikace jsou i doporučení, rady, postupy, případně nástroje využitelné jak uživateli, tak právě i správci jednotlivých ICT systémů. Tyto rady a doporučení vycházejí zejména ze zkušeností pracovníků CSIRT.CZ a CZ.NIC-CSIRT při řešení kybernetických útoků.

Tato kniha shrnuje naše názory a zkušenosti, které jsme získali v oblasti kybernetické bezpečnosti, kybernetické kriminality a edukace uživatelů.

Identifikační údaje osob použité v příkladech (IP adresy, e-mailové schránky apod.) byly v některých případech pozměněny, na druhou stranu monografie obsahuje celou řadu reálných případů z praxe, u nichž z důvodu objektivnosti byly zachovány informace o skutečných aktérech či detailech útoku.

Kdykoli rádi přivítáme jakoukoli zpětnou vazbu od čtenářů této knihy. Vy jste totiž ti, kteří dokáží odhalit chyby a prohřešky, které jsme přehlédli. Také budeme rádi, pokud nás upozorníte na témata, která vás zajímají více.

Za jakoukoli Vaši zpětnou vazbu jsme vděční.

16: Viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8 [online]. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Tuto knihu jsme se rozhodli vydat pod Creative Commons licencí: CC BY ND.[17]

Závěrem bychom chtěli poděkovat všem těm, kdo se o výslednou podobu této knihy zasloužili. Náš dík patří Evě Cvrkové, Martinu Peterkovi, JUDr. Josefu Součkovi, CSc., Mgr. Janu Nejedlému, všem kolegům z CESNET CERTS a CSIRT.CZ jakož i dalším odborníkům, s nimiž jsme měli tu čest spolupracovat a diskutovat.

Děkujeme všem, kdo byli ochotni číst a připomínkovat rukopis této knihy. Díky za Vaše připomínky a náměty.

Poslední a největší dík patří našim rodinám, které nám umožnily a umožňují dělat to, co nás baví.

Za autory

Jan Kolouch
jan.kolouch@cesnet.cz

17: Bližší informace o creative commons licencích dále naleznete např. na:
https://creativecommons.org/licenses/by-nd/3.0/cz/
https://cs.wikipedia.org/wiki/Creative_Commons

Obsah

Předmluva vydavatele **5**

Předmluva autorů **9**

Seznam zkratek **25**

I Základní terminologie **33**

1 Kyberprostor (Cyberspace) **35**

2 Pojem kybernetické bezpečnosti a pojmy související **39**
2.1 Kybernetická bezpečnost 39
2.2 Principy kybernetické bezpečnosti 45
2.2.1 Triáda CIA 45
2.2.2 Prvky kybernetické bezpečnosti 56
2.2.3 Životní cyklus kybernetické bezpečnosti 63
2.3 Riziko, aktivum, zranitelnost 68
2.3.1 Riziko 68
2.3.2 Aktivum 72
2.3.3 Zranitelnost 72
2.4 Kybernetické hrozby, události, incidenty a útoky 73
2.4.1 Kybernetická hrozba 74
2.4.2 Kybernetická bezpečnostní událost 80
2.4.3 Kybernetický (bezpečnostní) incident 81
2.4.4 Kybernetický útok (Cyber Attack) 82
2.4.5 Kyberkriminalita (Cybercrime) 83

II Legislativa **85**

3 Legislativní základ kybernetické bezpečnosti **87**
3.1 Legislativní vývoj kybernetické bezpečnosti v ČR 87
3.2 Právní normy vztahující se ke kybernetické bezpečnosti 94
3.2.1 Dokumenty EU/ES sloužící k harmonizaci právních úprav při řešení problematiky kybernetické bezpečnosti 95
3.2.2 Právní normy ČR 98
3.3 Exkurze do práv a povinností vyplývajících z některých právních norem 99
3.3.1 GDPR 101
3.3.1.1 Místní působnost GDPR 104
3.3.1.2 Osobní údaj 104

3.3.1.3 Zpracování osobních údajů 109
3.3.1.4 Zabezpečení osobních údajů 111
3.3.1.5 Posouzení vlivu na ochranu osobních údajů (DPIA) 112
3.3.2 ePrivacy 113
3.3.2.1 Působnost ePrivacy 114
3.3.2.2 Základní terminologie ePrivacy 115
3.3.2.3 Zpracování dat 118
3.3.3 Občanský zákoník 120
3.3.3.1 Ochrana soukromí 121
3.3.3.2 Právní jednání 123
3.3.3.3 Náhrada škody 123
3.3.4 Trestní zákoník 124

4 Zákon o kybernetické bezpečnosti 129
4.1 Příčiny vzniku ZoKB 130
4.2 Základní cíle a principy ZoKB 133
4.3 Komentář k ZoKB 138
§ 1 Předmět úpravy 138
§ 2 Vymezení pojmů 142
Kybernetický prostor 148
Kritická informační infrastruktura 150
Bezpečnost informací 154
Významný informační systém 154
Správce informačního systému 164
Správce komunikačního systému 164
Provozovatel informačního nebo komunikačního systému 164
Významná síť elektronických komunikací 167
Základní služba. Informační systém základní služby.
Provozovatel základní služby 167
Digitální služba 189
Příslušný orgán 197
§ 3 198
Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací 200
Orgán nebo osoba zajišťující významnou síť 205
Správce a provozovatel informačního systému kritické informační infrastruktury 208
Správce a provozovatel komunikačního systému kritické informační infrastruktury 208
Správce a provozovatel významného informačního systému 216
Správce a provozovatel informačního systému základní služby 222

Provozovatel základní služby 228
Poskytovatel digitální služby 233
§ 3a Zástupce poskytovatele digitálních služeb 237
§ 4 Bezpečnostní opatření 241
§ 4a 248
§ 5 250

Organizační opatření 253
Systém řízení bezpečnosti informací 253
Řízení rizik 259
Bezpečnostní politika 264
Organizační bezpečnost 266
Stanovení bezpečnostních požadavků pro dodavatele 274
Řízení aktiv 275
Bezpečnost lidských zdrojů 276
Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému 277
Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému 277
Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů 278
Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů 279
Řízení kontinuity činností 280
Kontrola a audit kritické informační infrastruktury a významných informačních systémů 281

Technická opatření 281
Fyzická bezpečnost 282
Nástroj pro ochranu integrity komunikačních sítí 285
Nástroj pro ověřování identity uživatelů 285
Nástroj pro řízení přístupových oprávnění 287
Nástroj pro ochranu před škodlivým kódem 288
Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů 289
Nástroj pro detekci kybernetických bezpečnostních událostí 290
Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí 291
Aplikační bezpečnost 292
Kryptografické prostředky 292
Nástroj pro zajišťování úrovně dostupnosti informací 293
Bezpečnost průmyslových a řídicích systémů 294

§ 6 294
§ 6a 295
§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident 299
§ 8 Hlášení kybernetického bezpečnostního incidentu 302
§ 9 Evidence 311
§ 10 314
§ 10a 316
§ 11 Opatření 319
§ 12 Varování 323
§ 13 Reaktivní a ochranné opatření 325
§ 14 330
§ 15 331
§ 15a 334
§ 16 Kontaktní údaje 335
§ 17 Národní CERT 340
§ 18 Provozovatel národního CERT 348
§ 19 Veřejnoprávní smlouva 353
§ 20 Vládní CERT 356
§ 21 Stav kybernetického nebezpečí 361
§ 21a Úřad 367
§ 22 367
§ 22a Určení provozovatele základní služby a informačního systému základní služby 374
§ 22b 379
§ 23 Kontrola 381
§ 24 Nápravná opatření 384
§ 24a Kontrola činnosti Úřadu 386
§ 24b 388
§ 24c 388
§ 25 Přestupky 389
§ 26 393
§ 27 Společné ustanovení k přestupkům 394
§ 28 Zmocňovací ustanovení 394
§ 29 Přechodná ustanovení 395
§ 30 396
§ 31 397
§ 32 398
§ 33 Společná ustanovení 399
§ 35 Změna zákona o elektronických komunikacích 401
§ 37 Změna zákona o provozování rozhlasového a televizního vysílání 402
§ 38 Účinnost 402

III Kyberbezpečnost prakticky **405**

5 Fyzická bezpečnost **411**
5.1 Zajištění perimetru 411
5.2 Kontrola přístupu 412
5.3 Vnitřní bezpečnost 415
5.4 Ochrana počítačových systémů 416
5.4.1 Opatření proti krádeži počítačových systémů 417
5.4.2 Ochrana před rozebráním a úpravou počítačových systémů 418
5.4.3 Ochrana před připojením cizích periferií k počítačovým systémům 420

6 Bezpečnost sítí a služeb **425**
6.1 Ochrana sítí 425
6.1.1 Rozdělení sítě jako základní prvek zajištění bezpečnosti 426
6.1.1.1 DMZ 426
6.1.1.2 VLAN 427
6.1.2 Ochrana sítě LAN 429
6.1.2.1 DHCP protokol 429
6.1.2.2 ARP protokol 431
6.1.2.3 DNS 435
6.1.2.4 IEEE 802.1X 438
6.1.2.5 Bezdrátové sítě 439
6.1.2.6 IPv6 451
6.1.3 Ochrana na rozhraní sítí 455
6.1.3.1 Access Control List (ACL) 455
6.1.3.2 Firewall 455
6.1.3.3 Proxy server 458
6.1.3.4 Intrusion Detection System (IDS) a Intrusion Prevention System (IPS) 460
6.1.3.5 Security Information and Event Management (SIEM) 461
6.1.3.6 Antivir, Antispam 462
6.2 Aplikační bezpečnost 462
6.2.1 Řízení přístupů 462
6.2.2 Ověřování uživatelů 463
6.2.3 Hesla 464
6.2.4 Logy a logování 475
6.2.5 Zabezpečení důvěrnosti a integrity přenášených dat 476
6.2.6 Zranitelnosti 478
6.3 Ochrana koncových počítačových systémů 480
6.4 Vzdálený přístup k počítačovým systémům 481
6.5 Paměťová média 484
6.6 Správa a dohled nad počítačovou sítí 485

6.7 Přenosné počítačové systémy 487
6.8 Bezpečnost lidských zdrojů 489
6.9 Reakce na incident 490
6.9.1 Hlášení bezpečnostních incidentů 492
6.9.2 Interní hlášení bezpečnostních incidentů 492
6.9.3 Řešení bezpečnostních incidentů 493
6.10 Možnosti využití dalších informačních zdrojů o incidentech 495
6.10.1 Malicious Domain Manager 496
6.10.2 Cyber Threat Intelligence Project - PROKI 497

7 CERT/CSIRT týmy 505
7.1 Historie 505
7.2 CERT a CSIRT týmy 506
7.3 Jak vzniká CERT/CSIRT tým 508
7.4 Spolupráce CERT/CSIRT infrastruktury 510
7.5 Hierarchie CERT/CSIRT týmů? 512
7.6 Národní a vládní CERT/CSIRT týmy 513
7.7 Situace v ČR a ve světě 514
7.8 Národní CSIRT České republiky 515
7.9 Vládní CERT České republiky 516
7.10 Na který CERT/CSIRT tým se obrátit? 516

Závěr 519

Seznam použitých pramenů a dalších zdrojů 523

Rejstřík 541

Summary 560

Seznam zkratek

Seznam zkratek

Zkratka	Význam
AES	Advanced Encryption Standard
API	Application Programming Interface
APT	Advanced Persistent Threat
BYOD	Bring Your Own Device
C&C	Command-and-Control
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CCTV	Closed Circuit Television
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
Data retention	plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DNS	Domain Name System (hierarchický systém doménových jmen)
Dodatkový protokol	Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě
DoS, DDoS	Denial of Service, Distributed Denial of Service
DPIA	Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů)
eIdas	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
ENISA	The European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací)
EULA	End User Licence Agreement (smlouva uzavřená typicky mezi uživatelem a ISP)
EZS	elektronický zabezpečovací systém či elektronická zabezpečovací signalizace

GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/697 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HIDS	Host-based Intrusion Detection System
HMAC	Hashed Message Authentication Mode
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol (internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML)
IaaS	Infrastructure as a Service
IAP	Internet Access Provider
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	informační a komunikační technologie
IDS	Intrusion Detection System
IoE	Internet of Everything (Internet všeho)
IoT	Internet of Things (Internet věcí)
IP	Internet Protocol
IPS	Intrusion Prevention System
Ipv4, IPv6	Internet Protocol verze 4, 6
IS	informační systém / systémy
ISMS	Information Security Management System
ISP	Internet Service Provider (specificky k českému právu je využíván pojem poskytovatel služeb informační společnosti)
IT	informační technologie
KZ, krizový zákon	Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol (protokol definovaný pro ukládání a přístup k datům na adresářovém serveru)
LIR	Local Internet Registry
Listina	Zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod
NBÚ	Národní bezpečnostní úřad
NIDS	Network Intrusion Detection System

NIS	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	operační systém
OZ, občanský zákoník	Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
PaaS	Platform as a Service
PC	Personal Computer (osobní počítač)
PCO	pult centralizované ochrany
PROKI	PRedikce a Ochrana Před Kybernetickými Incidenty
PTK	Pairwise Transient Key
RDP	Remote Desktop Protokol
RIR	Regional Internet Registry
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equal
SIEM	Security Incident and Event Management (nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí)
SLA	Service-Level Agreement
SMTP	Simple Mail Transfer Protocol (internetový protokol určený pro přenos zpráv elektronické pošty)
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office/Home Office
SQL	Structured Query Language
SŘ, správní řád	Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TI	Trusted Introducer
TKIP	Temporal Key Integrity Protocol
TLP	Traffic Light Protocol
TLS	Transport Layer Security

TOPO, zákon o trestní odpovědnosti právnických osob	Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů
TŘ, trestní řád	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
TZK, trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
Úmluva o kyberkriminalitě	Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001
UPS	Uninterruptible Power Supply (záložní zdroj elektrického napájení)
URL	Uniform Resource Locator (jednotná adresa zdroje)
Úřad	V kap. 4 a násl. je v textu zákona používán pojem Úřad pro označení NBÚ či NÚKIB (v závislosti na době)
Ústava	Ústava České republiky ze dne 16. 12. 1992 jako součást ústavního pořádku České republiky pod č. 1/1993 Sb., ve znění ústavních zákonů č. 347/1997 Sb., č. 300/2000 Sb., č. 395/2001 Sb., č. 448/2001 Sb. a č. 515/2002 Sb.
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA, WPA2	Wi-Fi Protected Access
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key
WPS	Wi-Fi Protected Setup
XML	eXtensible Markup Language
XSS	Cross-Site Scripting
ZoBČR	Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky
ZoEK, zákon o elektronických komunikacích	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně dalších zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

ZoKB, zákon o kybernetické bezpečnosti	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
ZoOU, zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
ZoOUI, zákon o ochraně utajovaných informací	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
ZoP, zákony o přestupcích	Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich Zákon č. 251/2016 Sb., o některých přestupcích
ZoS	Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů
ZoZT, zákon o znalcích a tlumočnících	Zákon č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů
ZSIS, zákon o některých službách informační společnosti	Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů

1 Základní terminologie

I Základní terminologie

1 Kyberprostor (Cyberspace)

Chceme-li se věnovat problematice kybernetické bezpečnosti, kybernetických útoků, incidentů, ochrany digitálních dat aj., je nezbytně nutné nejprve vymezit ono pomyslné hrací pole, ve kterém se tyto „útočné a obranné" akce odehrávají.

Vlastní pojem kyberprostor (cyberspace) poprvé použil v roce 1982 v povídce „*Jak vypálit Chrom*"[18] William Gibson. Ten následně v románu Neuromancer uvedl, že kyberprostor je:

„*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …*"

William Gibson: Neuromancer (1984)

Do obecného povědomí se ale pojem kyberprostor začíná dostávat až po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation): **„A Declaration of the Independence of Cyberspace."**[19]

Pokud bychom chtěli nalézt definici kyberprostoru v některém ze slovníků, pak Oxford dictionary k termínu cyberspace uvádí, že jde o „*fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě.*"[20] Český Výkladový slovník kybernetické bezpečnosti nedefinuje pojem kyberprostor, ale specificky uvádí pouze pojem „*Český kyberprostor*"[21], kterým se rozumí „*kyberprostor pod jurisdikcí České republiky*".

Jsme přesvědčeni o tom, že ani jeden z výše uvedených slovníků nedefinuje kyberprostor tak, aby bylo možné pochopit komplexnost tohoto prostředí.

18: v originále: Burning Chrome (1982)

19: Blíže viz BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23. 9. 2014]. Dostupné z: https://www.eff.org/cyberspace-independence.

Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

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

21: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 37. [online]. [cit. 10. 7. 2018]. Dostupné z:
https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

Kyberprostor je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy[22], které jsou do této sítě připojeny a které v ní interagují. Vlastní interakce uvedených systémů samozřejmě není možná bez zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů).

Tím je vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor.

Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb, atd.), se adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození či zániku kyberprostoru jako takového.

Kyberprostor je také možné definovat jako prostor kybernetických aktivit, či jako prostor vytvořený informačními a komunikačními technologiemi. Tento prostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném. Obecně je sice možné konstatovat, že na kyberprostor lze aplikovat standardní kritéria[23], která jsou uplatňována v návaznosti na skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).[24]

Kyberprostor je dnes mnohými státy považován za pátou doménu či sféru (a to ne jen pro účely války) po zemi, vodě, vzduchu a vesmíru. Tomuto prostoru je nejen ze strany státních organizací věnována stále větší a vetší pozornost.

Mezi **znaky kyberprostoru** je možné zařadit jeho **decentralizovanost**, **globálnost**, **otevřenost**, **bohatost na informace**, **interaktivnost** a možnost ovlivňování mínění skrze uživatele. Podstatným rysem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje, že projev světa virtuálního může mít a má dopady ve světě reálném.

Pokud jde o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) zákona o kybernetické bezpečnosti, kde je uvedeno, že „***kybernetickým prostorem je digitální prostředí***

22: Blíže viz § 2 odst. 2 ZoKB, případně: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 57 a násl.

23: Viz např. kap. 3.3.4 Trestní zákoník

24: Blíže viz REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 218

umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací."

Dle našeho názoru jednu z velmi zdařilých definic kyberprostoru přináší dokument Cyberspace Operations: Concept Capability Plan 2016–2028, který definuje **kyberprostor jako prostor složený ze tří vrstev:**[25]

1) **fyzické**,
2) **logické** a
3) **sociální**.

Tyto vrstvy se pak skládají z celkem pěti komponent.

Ad 1) Fyzická vrstva
Tato vrstva zahrnuje pojem „**geographic component**" a pojem **fyzické síťové komponenty**. Pojem „geographic component" nemá v našem jazyce přesný ekvivalent, nicméně je jím myšleno přesné umístění síťových prvků ve fyzickém světě. Pojem fyzické síťové komponenty pak zahrnuje infrastrukturu v podobě kabelů, řídících prvků sítě (switch, router) a dalšího zařízení.

Toto rozdělení fyzické vrstvy má svou logiku. Zatímco geopolitické hranice mezi státy mohou být v kyberprostoru snadno překročeny, v reálném světě zde stále existují omezení, která vyplývají z podstaty našeho fyzického světa.

Pokud tuto myšlenku převedeme do světa kyberútoků a incidentů, znamená to, že mohu jako útočník poškodit prvek fyzické vrstvy buď vzdáleně, například tím, že znám jeho konkrétní zranitelnost, kterou lze vzdáleně napadnout, nebo jej mohu poškodit přímo v reálném světě, pokud se mi k němu podaří fyzicky dostat a zaútočit na něj například s použitím fyzické síly. Dopad v kyberprostoru bude stejný, ale provedení samotného útoku je značně odlišné.

Ad 2) Logická vrstva
Tato vrstva obsahuje **logické síťové komponenty**, čímž jsou myšlena logická propojení mezi síťovými uzly. Ta jsou realizována prostřednictvím síťových komunikačních protokolů. Uzly mohou být počítače, telefony a další síťová zařízení.

Ad 3) Sociální vrstva
Tato vrstva se skládá z komponent nazvaných „**kyberosobnost**" a **osobnost**.

25: *Cyberspace Operations: Concept Capability Plan 2016–2028*. [online]. [cit. 18. 2. 2018], s. 8–9 Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

Komponenta „kyberosobnost“ zahrnuje identifikaci osoby na síti, jako je e-mailová adresa, IP adresa, číslo telefonu a další. Komponenta osobnost se skládá ze skutečných osob připojených k síti. Jedna individualita pak může mít více „kyberosobností“, například různé e-maily na různých zařízeních, a jedna „kyberosobnost“ může být ve skutečnosti více různých skutečných osob, využívajících například jeden společný sdílený účet.

Kyberprostor je také možné definovat podle dostupnosti a dohledatelnosti dat pro běžného uživatele. Podle tohoto dělení lze kyberprostor rozdělit na služby a data dostupná pomocí Internetu, na služby a data dostupná pouze v rámci konkrétních sítí a zařízení a na služby a data záměrně skrytá a dostupná s využitím speciálních nástrojů.

Obvykle se pro tyto kategorie používají názvy:

1) **Surface Web**,
2) **Deep Web** a
3) **Dark Web**.

Deep a Dark Weby jsou také souhrnně označovány jako **D4rkN3ts – Darknets**. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.[26]

Na terminologii, která používá k rozdělení kyberprostoru pojem *web,* se bohužel podepsal fakt, že pro většinu laické veřejnosti platí jednoduchá rovnice:

KYBERPROSTOR = INTERNET = **WEB**

Nicméně kyberprostor se netýká pouze webových stránek, ale všech počítačových systémů, služeb, uživatelů a dat, jež se v tomto prostoru pohybují.

26: Srov. Např. *The dark Web explained.* [online]. [cit. 20. 7. 2016]. Dostupné z:
https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
či *Surface Web, Deep Web, Dark Web – What's the Difference.* [online]. [cit. 20. 7. 2016]. Dostupné z:
https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

2 Pojem kybernetické bezpečnosti a pojmy související

„Objev jaderné energie nepřinesl nové problémy. Pouze učinil naléhavějším nutnost vyřešit existující problémy."

Albert Einstein

V této kapitole se pokusíme vymezit některé základní pojmy, které jsou důležité pro pochopení problematiky kybernetické bezpečnosti. Záměrně jsme si pro úvod do této kapitoly vybrali citát Alberta Einsteina, neboť právě tento citát vystihuje základní problém kybernetické bezpečnosti, kterým je samotné pochopení tohoto relativně nového fenoménu a aplikování „starých bezpečnostních pravidel" na tento „nový" jev, jakož i vytvoření podmínek a prostředků pro řešení problémů, které je možné označit jako kybernetické útoky.

Vzhledem k zaměření a rozsahu knihy není možné vysvětlit veškeré pojmosloví související s kybernetickou bezpečností a ICT, k tomuto účelu slouží specializované slovníky.[27] Na tomto místě budou vysvětleny základní pojmy, které budou v dalších částech této monografie využívány. Další pojmy pak jsou samostatně vymezeny v kapitole 4.3, která se věnuje výkladu zákona o kybernetické bezpečnosti.

2.1 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." [28]

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.

27: Jedná se například o:
HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. 456 s. či JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-436-6. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

28: *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

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.[29]

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." [30]

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[31] jako takovým.

Bezpečnost

Definic pojmu **bezpečnost (security)**[32] existuje celá řada, avšak neexistuje žádná jednotná, obecně akceptovaná definice. Většina definic pojmu bezpečnost je uváděna spíše v odborné literatuře, než v legislativě samotné.[33]

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."* [34]

29: Viz kap. 2.4 Kybernetické hrozby, události, incidenty a útoky

30: *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

31: Viz kap. 1 Kyberprostor (Cyberspace)

32: 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 i aktivního zabezpečení, zajištění či ochrany a pojem **safety** je využíván zpravidla k vyjádření pasivní bezpečnosti, bezpečí, charakteristice stavu či vlastnosti určitého objektu.

33: 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.

34: 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

Požár definuje *„bezpečnost jako vlastnost nějakého objektu nebo subjektu, která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.“* [35]

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.[36]

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?**[37]

Ideálním cílem bezpečnosti je vytvoření stavu „absolutního bezpečí“. Tento stav je ale utopií, protože jej není možné reálně dosáhnout,[38] 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

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

36: 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/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

37: 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

38: Viz WAISOVÁ, Šárka. *Bezpečnost: vyvoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. 159 s. ISBN 80-86898-2-10

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**.[39]

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.[40]

3) Dle Jiráska a kol. představuje **kybernetická bezpečnost (Cyber Security)** „***souhrn** právních, organizačních, technických a vzdělávacích **prostředků směřujících k zajištění ochrany kybernetického prostoru.***“ [41]

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***

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

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

41: 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/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

***a odolného kyberprostoru v České republice**, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.*“ [42]

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.[43]

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“.[44]

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**[45] Evropské agentury ENISA[46]: „*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*

42: *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

43: 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.

44: 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

45: *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

46: The European Union Agency for Network and Information Security

paradigma ‚CIA' triády[47] *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[48] 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.*"

Zákon o kybernetické bezpečnosti ani prováděcí vyhlášky k tomuto zákonu vlastní pojem kybernetické bezpečnosti nevymezují. To, co je v těchto právních předpisech vymezeno, však umožňuje pochopit základy a principy kybernetické bezpečnosti, jakož je i následně aplikovat.

Zákon samotný určuje povinné subjekty, které mají povinnost zavést bezpečnostní opatření. A následně těmto subjektům také definuje jejich práva a povinnosti.[49]

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,**

47: Blíže viz kap. 2.2 Principy kybernetické bezpečnosti

48: 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

49: Blíže viz § 3 a násl. ZoKB

- **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.

2.2 Principy kybernetické bezpečnosti

Při uplatňování kybernetické bezpečnosti dochází k implementaci následujících principů, které jsou také nazývány triády kybernetické bezpečnosti.[50]

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).

2.2.1 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**[51], 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.

50: 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

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

Velmi často je triáda CIA vztahována primárně právě k informacím.

Toto užší pojetí vyplývá zejména z vlastní definice **informační bezpečnosti**, 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.[52] Mezi základní normy informační bezpečnosti patří:

- ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
- ČSN 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[53] 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.*"

52: Blíže viz § 5 ZoKB a ISMS - Systém řízení bezpečnosti informací

53: 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

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.“* [54]

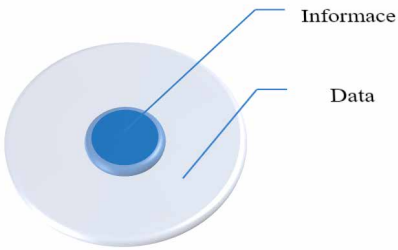
Wiener tvrdí, že *„informace je název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.“* Dále také uvádí, že informace není ani hmotou ani energií, ale samostatnou fyzikální kategorií.[55]

Smejkal uvádí, že za informaci je možné považovat *„každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.“* [56]

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.[57]

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.[58]



54: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

55: 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.

56: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 36

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

58: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

Data a informace jsou v rámci kyberprostoru přenášeny pomocí počítačových systémů[59], jež jsou nedílnou součástí kybernetické či informační bezpečnosti.

Na základě výše uvedeného jsme přesvědčeni, že je třeba triádu CIA[60] uplatňovat ne jen 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[61]:**

    - **Přísně tajné (Top secret)** - neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážnou újmu zájmům České republiky.

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

60: 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

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

- **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 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.).[62]

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**

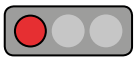
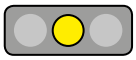
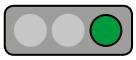
V rámci komunity kybernetické bezpečnosti vznikla v minulosti potřeba sdílet informace a data (typicky o kybernetických útocích), která mají citlivou povahu. Z tohoto důvodu byl v National Infrastructure Security Coordination Centre[63] vytvořen na počátku roku 2000 **protokol TLP** (***Traffic Light Protocol***).[64] 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.

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

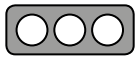
63: V současnosti Centre for Protection of National Infrastructure - CPNI

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

Protokol TLP je nejvhodněji vymezen v následující tabulce, která byla převzata z US-CERT[65]:

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.**

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

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).“ [66]

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)[67]

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.

66: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 19

67: Dále jen vyhláška o kybernetické bezpečnosti či **VoKB**.

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[68] 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.“*

68: 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

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).“ [69]

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	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
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 jsou 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 jsou 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.

69: ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. s. 22

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 jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Dostupnost (Availability)

Dle Výkladového slovníku kybernetické bezpečnosti[70] 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.[71]

„O zničení (destruction) určitých informací se v informační bezpečnosti hovoří jako o narušení jejich dostupnosti (availability).“ [72]

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.

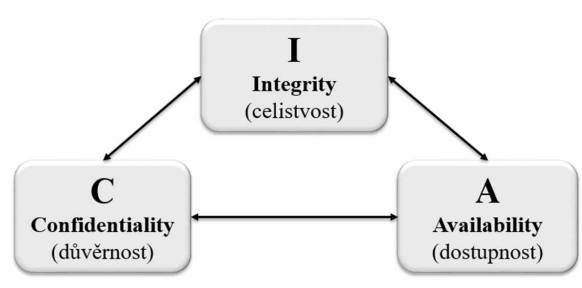
70: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 43. [online]. [cit. 10. 7. 2018]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

71: 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

72: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 24

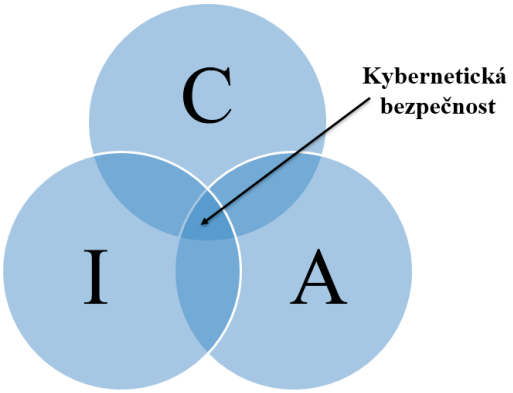
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. 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[73]

2.2.2 Prvky kybernetické bezpečnosti

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

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

- **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.*“

„*Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů.*“

Bruce Schneier[74]

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),

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

- **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."
„Amatéři hackují systémy, profesionálové ‚hackují' lidi."

Bruce Schneier[75]

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."

„Pokud se domníváte, že technologie dokáže vyřešit vaše bezpečnostní problémy, nerozumíte problémům a nerozumíte technologii."

Bruce Schneier[76]

75: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570035 Překlad autora.
76: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570040 Překlad autora.

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[77], IDS/IPS[78], honeypot[79] 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[80] a na základě této analýzy případně doplnit či modifikovat existující 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.).[81]

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

77: Firewall je systém obsahující pravidla, dle kterých se řídí datové toky v rámci síťových technologií.

78: **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**.

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

80: Blíže viz kap. 2.3.2 Aktivum. V tomto případě jsou aktivem míněny technologie a aplikace, které jsou v organizaci využívány.

81: Blíže viz kap. 6.1 Ochrana sítí

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."

*„Mantrou dobrého bezpečnostního inženýra je: ‚**Bezpečnost není produkt, ale proces.**' Je to víc než navrhnout silnou kryptografii do systému; je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala."*

Bruce Schneier[82]

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,

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

- 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.[83]

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

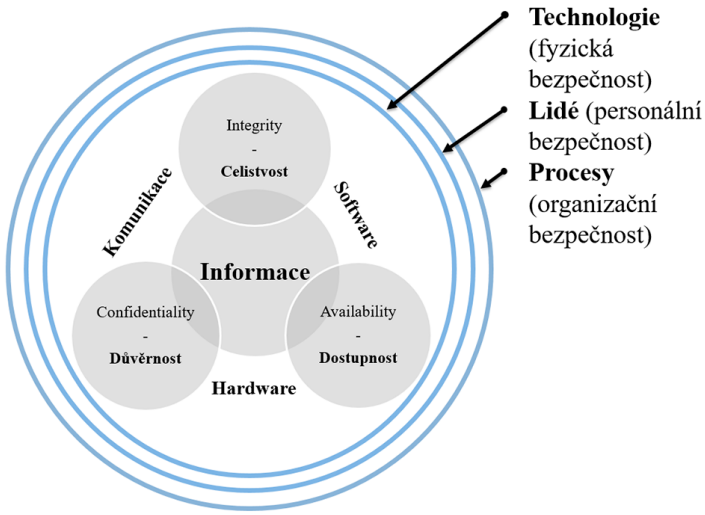
Pokud se organizace rozhodne implementovat pravidla kybernetické bezpečnosti, pak je samozřejmě vhodné udržovat hardware i software aktualizovaný, dodržovat pravidla, která jsou nastavena pro přístup k jednotlivým systémům aj.

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.

83: 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.

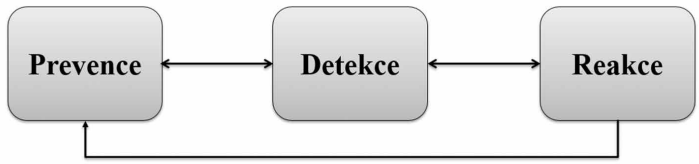


Obrázek 4: Triáda CIA doplněná o technologie, lidi a procesy[84]

2.2.3 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.[85]

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

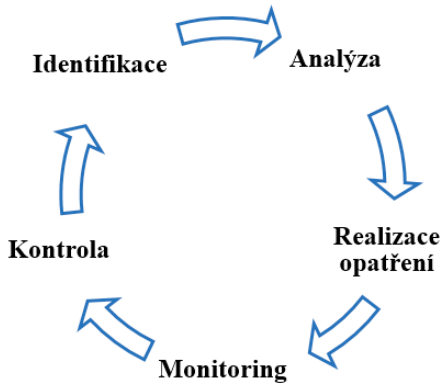
84: Předlohou grafu byl graf zveřejněný v: *CIA triad methodology*. [online]. [cit. 10. 7. 2018]. Dostupné z: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

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

Obrázek 6: Životní cyklus kybernetické bezpečnosti dle kybez.cz[86]

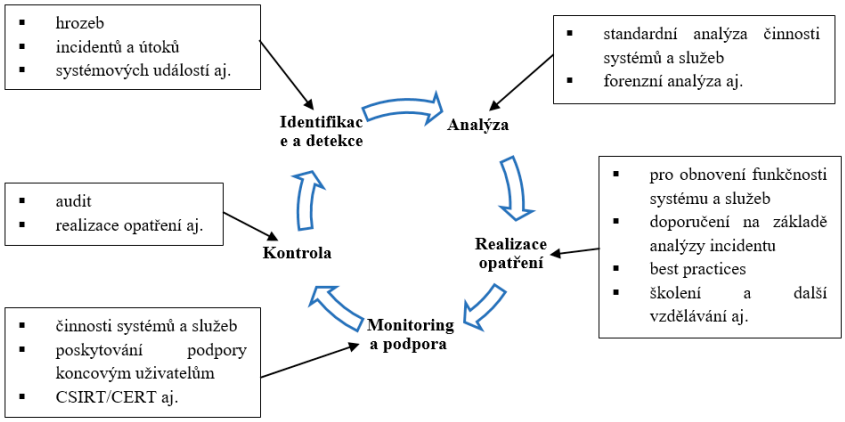
Při řešení kybernetické bezpečnosti neexistuje žádný „záchytný bod", v rámci kterého by bylo možné říci: *„Zvládli jsme to! Jsme chráněni proti kybernetickým útokům či hrozbám. Jsme kyberneticky bezpeční."*

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

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



Obrázek 8: Životní cyklus kybernetické bezpečnosti

Vlastní znázornění životního cyklu kybernetické bezpečnosti může být značně komplexnější.[87]

Obrázek 9: Příklad řešení kybernetické bezpečnosti

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

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[88], 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 % [89]

- oběťmi jsou organizace působící ve:
  - zdravotnictví – 24 %
  - veřejném sektoru (typicky státní správa a samospráva aj.) – 14 %

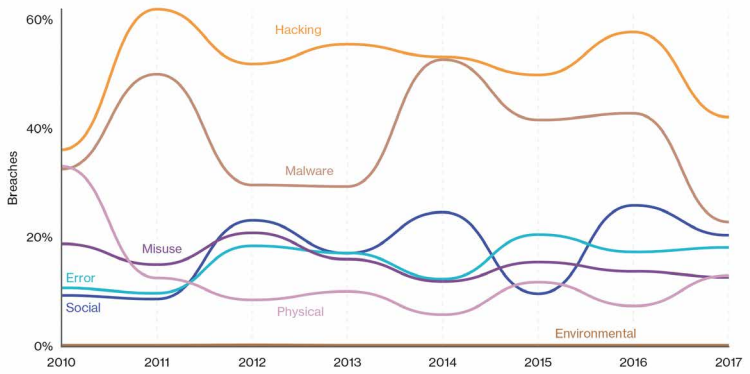
- motiv útoku:
  - **obohacení se – 76%**
  - zisk dat a informací (špionáž) – 13 %

- **68 % útoků bylo odhaleno až po několika měsících, či po delší době**

88: *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

89: V rámci jednotlivých útoků zpravidla dochází ke kombinování technik a nástrojů.

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



Obrázek 10: Typy útoků použitých k narušení bezpečnosti[90]

Dle zprávy Národního úřadu pro kybernetickou a informační bezpečnost[91] ***„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.“* [92]

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,

90: *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

91: Dále jen **NÚKIB**

92: *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

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."[93]

2.3 Riziko, aktivum, zranitelnost

2.3.1 Riziko

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.*" [94]

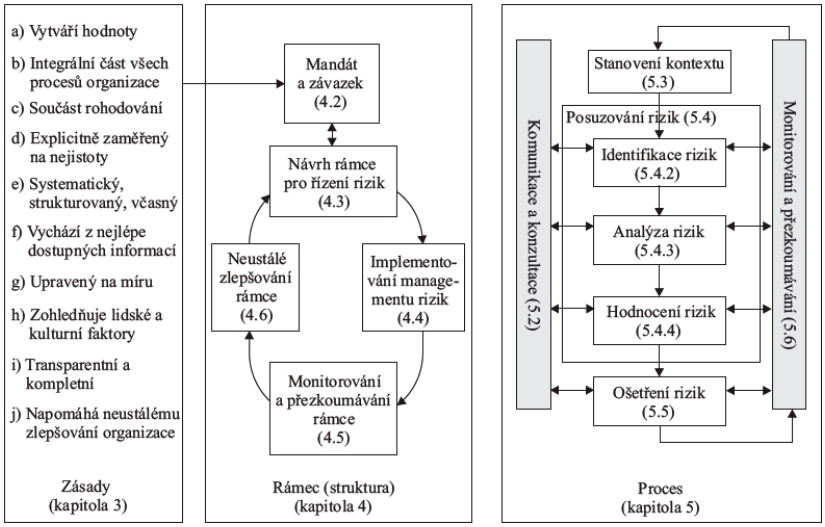
Riziko je také možné definovat jako **potenciál, že se hrozba stane reálnou a využije zranitelnosti aktiva**.[95] Dle čl. 4 odst. 9 NIS se **rizikem** rozumí „***jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.***" V 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.

93: *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

94: 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

95: Blíže viz § 2 písm. f) VoKB
K pojmu aktiva viz kap. 2.3.2 Aktivum



Obrázek 11: Vazby mezi principy, rámcem a procesem managementu rizik[96]

Valášek a kol.[97] 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:

96: 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

97: 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

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:[98]

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.[99]

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.

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

99: Viz kap. 2.4.2 Kybernetická bezpečnostní událost a 2.4.3 Kybernetický (bezpečnostní) incident

2.3.2 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.

2.3.3 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 (blíže viz kap. 2.4.1 - konkrétně klasifikace hrozeb).

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.[100]

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.

2.4 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.

100: 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

2.4.1 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.*“ [101]

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.*“ [102]

S tímto základním pojmem pak bezprostředně souvisí i pojem **bezpečnostní hrozba** (Information security threat)[103], 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.*“ [104]

Vedle dvou výše uvedených pojmů definují autoři ve výkladovém slovníku i pojmy **aktivní hrozba, pasivní hrozba a pokročilá a trvalá hrozba.**[105]

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

102: 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

103: 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.

104: 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

105: Tamtéž s. 16, 81 a 87

Oxford dictionary uvádí, že **kybernetickou hrozbou je možnost škodlivého pokusu o poškození nebo narušení počítačové sítě nebo systému.**[106] Přičemž za systém je v tomto kontextu považován počítačový systém.

Kybernetickou hrozbu lze také definovat jako akt směřující ke změně[107] informace, aplikací či systému samotného.

Jirovský vymezuje čtyři skupiny základních hrozeb a zároveň charakterizuje jejich vztah:[108]

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.[109]
4) **Nelegitimní použití** je užití informací neautorizovaným subjektem či neoprávněným způsobem.[110]

Uvedený vztah je nejlépe znázorněn na následujícím obrázku.

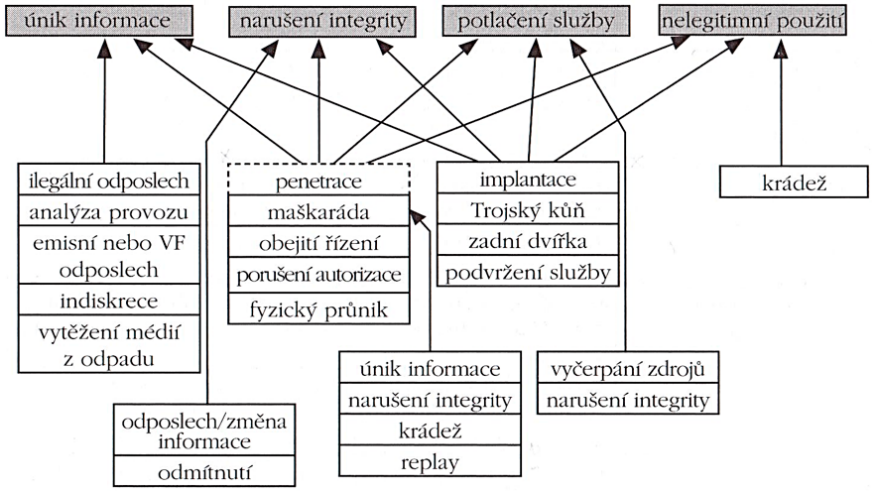
106: *Cyberthreat.* [online]. [cit. 6. 7. 2018]. Dostupné z:
https://en.oxforddictionaries.com/definition/cyberthreat Překlad autora.

107: Změnou je míněna i krádež informace, její zničení, či zmaření jejího užití.

108: 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.

109: 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.

110: Například dojde k napadení zpoplatněného systému a využívání jeho služeb bez platby za služby.



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**

- **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.).[111]

  - **z nedbalosti.**
    Mezi kybernetické hrozby způsobené z nedbalosti je možné zařadit například:
    - omylem smazaná data,

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

    - 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.

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

- **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**

- **hrozby vnitřní** (zdroj hrozby se nachází uvnitř organizace)
- **hrozby vnější** (zdroj hrozby se nachází mimo organizaci)[112]

3) **Cíle hrozby**

- **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.

- **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.

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

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

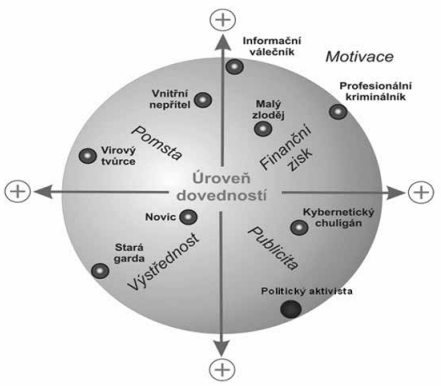
4) **Motivace**

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.[113]

Další členění útočníků dle motivace představuje i Rak[114], 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

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

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

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).

2.4.2 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.[115]

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).*"[116]

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.*"[117]

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.

115: PROSISE, Chris a Kevin MANDIVA. *Incident response & computer 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.

116: 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

117: *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 Překlad autora.

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.*

2.4.3 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.“* [118]

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.“* [119]

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.**

118: 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

119: *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

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.*

2.4.4 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.“* [120]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru[121], 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**[122] definovat jako **jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.

120: 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

121: 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.

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

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.

2.4.5 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).

„Proč nám skvělá technika, která šetří práci a usnadňuje život, dosud přinesla tak málo štěstí? Odpověď je prostá: protože jsme se jí nenaučili rozumně užívat."

Albert Einstein