ZÁKLADNÍ OTÁZKY KYBERNETICKÉ BEZPEČNOSTI PODNIKŮ V OBORU ENERGETIKA A TEPLÁRENSTVÍ

Tento materiál navazuje na článek **Kybernetická bezpečnost** (Cyber-Security), zveřejněný v publikaci ČSZE „Energetika kolem nás“ a klade si za cíl:

a) **Poskytnout managementu firem základní informace o této problematice v rozsahu umožňujícím její uchopení v širších souvislostech**. Přesahujících jádro problému (kterým je samotná ochrana před možným kybernetickým útokem) a poskytujících základní opory v procesu stanovení střednědobých a dlouhodobých cílů v této oblasti, jako nedílné součásti firemní strategie. V tomto směru proto materiál není primárně určen specialistům v oboru IT, ICT a samotné kybernetické bezpečnosti, ale je zacílen na TOP management (Decision-makers). Členům firemního vedení by měl usnadnit vnímání této problematiky ve správných proporcích ve vztahu k ostatním otázkám, vnímaným tradičně „přednostní“ optikou. Jako je modernizace výrobních a přenosových technologií, rozvoje lidských zdrojů, ochrany životního prostředí, obchodního rozvoje atd.

b) Vzhledem k problematice kybernetické bezpečnosti je toto sdělení zaměřeno především na **osoby odpovědné za opatření kybernetické bezpečnosti v souvislosti s rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), odboru regulace, o určení provozovatelů základní služby**. Sama skutečnost, nezařazení do této kategorie však nezbavuje management společnosti obecné odpovědnosti za bezpečnost podniku v kybernetickém prostoru.

c) **Každému čtenáři pak poskytnout srozumitelnou základní orientaci v této problematice.** Neboť kybernetická ochrana není jen věcí vedení firmy (alokace nezbytných finančních zdrojů; nastavení určité vnitropodnikové organizační kultury), ale každého zaměstnance (od disciplinovaného užívání koncového zařízení IS a kompatibilních ICT periferií po obecný přístup k ochraně informací). Pokud materiál poslouží jako zdroj informací studentům odborných škol, budeme rádi.

Naším zájmem je poskytnou vám informace, pojednávající problematiku kybernetické bezpečnosti v širších souvislostech. Na jedné straně si uvědomujeme obecnou tendenci vnímat tuto problematiku přes prizma značné nepřístupnosti pro velkou část lidí. Mimo jiné pro obtížnou orientaci v pojmovém aparátu (převážně odvozeného z angličtiny). Tím se proto problematika kybernetické bezpečnosti stává doménou „specialistů“ (toto konstatování je zcela proto pejorativního podtextu, naopak, nic proti specialistům, jejich úloha je nezastupitelná). Praxe však ukazuje, že zaujetí postoje ve smyslu … „kybernetická bezpečnost, no dobře a co já s tím, to je věc „specialistů“…, je špatně. Naopak zdůrazňujeme a tímto materiálech chceme dosáhnout pochopení, že kybernetická bezpečnost tvoří plně integrovanou součást firemní strategie a managementu, jeho součástí jsou bezpečnostní procesy a bezpečnostní management v širším slova smyslu. Kybernetická bezpečnost se musí stát obecně přijímanou součástí firemní kultury. Varujeme před jejím „tunelovým viděním“. Tomu jsme přizpůsobili strukturu tohoto materiálu, který členíme do následujících oddílů takto:

1. Úvod do problematiky – základní souvislosti
2. Vybrané základní pojmy kybernetické bezpečnosti
3. Opatření kybernetické bezpečnosti
4. Kybernetická bezpečnost v širším kontextu
5. Jak k problému kybernetické bezpečnosti přistoupit

1.
Úvod do problematiky – základní souvislosti

Pod pojmem kybernetická bezpečnost rozumíme **souhrn právních, organizačních, technických a vzdělávacích prostředků, směřujících k zajištění ochrany kybernetického prostoru** (tedy digitálního prostředí, umožňujícího vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací). [1] Zajistit přiměřenou úroveň ochrany kybernetického prostoru v rámci něhož se podnik pohybuje, nabývá na stále větším významu. Je to dáno zejména těmito skutečnostmi:

Technickým rozvojem energetických oborů – výroba elektrické energie a výroba tepla i všechny procesy spojené s jejich distribucí ke koncovým uživatelům, jsou stále ve větší míře nasyceny elektronickými řídicími a komunikačními systémy. Podstatné omezení jejich funkčnosti či vyřazení by vedlo k vážnému narušení dodavatelského řetězce, hospodářským ztrátám, chaosu ve veřejné správě a široké škále negativních dopadů na život velkých skupin obyvatelstva. Od omezení vnímané kvality života až po jeho fatální ohrožení.

Mírou provázanosti dodavatelsko-odběratelského řetězce. Každý výrobce elektřiny i tepla je životně závislý na síti subjektů finančního kapitálu, dodavatelů různých věcných komodit a služeb, provozovatelích přenosových a distribučních soustav. Tato míra provázanosti přesahuje v řadě případů regionální i národní rámec. V případě, že by kterýkoli z těchto článků byl ochromen kybernetickým útokem, bude to mít důsledky různé úrovně kritičnosti i pro ostatní.

Místem energetiky a souvisejících podpůrných aktivit, jako součástí kritické infrastruktury (v regionálním, národním i nadnárodním (EU) smyslu). **Energetika patří mezi tzv. základní služby.** Základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností. [2]

Kybernetický útok se stal běžným nástrojem v rukou různých aktérů. Nejen ve světě obecné kriminality (vydírání; bankovní kriminalita; sabotování výkonu institucí státní správy apod.), ale i ve světě politického soupeření (včetně vojenskopolitické konfrontace; tzv. kybernetická válka a její nástroje), hospodářského soupeření, a to až po globální úroveň.

2.
Vybrané základní pojmy kybernetické bezpečnosti

Tak jako v každém oboru, ani v oblasti kybernetické bezpečnosti, se nevyhneme specifickému pojmosloví. Jeho zvládnutí, alespoň na elementární úrovni je nezbytným předpokladem pochopení problematiky a komunikace o ní. Není posláním tohoto materiálu zabíhat do podrobností a ani k tomu není prostor. Proto se omezujeme jen na výklad pojmů, se kterými budeme v následujícím textu pracovat a které jsou podmínkou pro jeho pochopení. Zájemce o hlubší vhled do problematiky pak podrobněji zorientuje závěrečný oddíl textu – Právní a odborné normy a další metodické opory.

Základním předpokladem funkčního a efektivního přístupu k této problematice, je nechápat kybernetickou bezpečnost jako „stav“, cíl našeho úsilí, po jehož dosažení si můžeme říci „hotovo“. **Kybernetická bezpečnost je permanentně otevřený proces s mnoha proměnnými**.

---

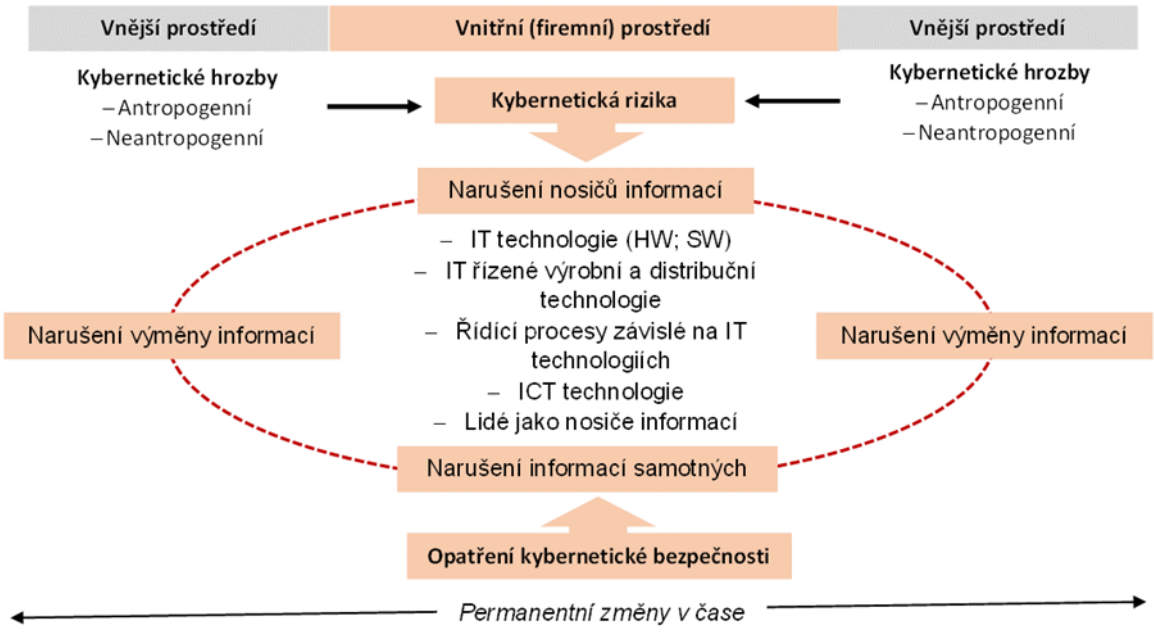
[1] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015

[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti; **v tomto textu také „ZKB“**), §2

Základní služba
Provozovatelem základní služby je orgán nebo osoba, která poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) podle § 22a; pro účely plnění informační povinnosti podle příslušného předpisu Evropské unie[8]) se za provozovatele základní služby považují též orgány a osoby uvedené v § 3 písm. c) a d). [3]

Vnější a vnitřní prostředí
Vnější prostředí zahrnuje široké spektrum subjektů, s nimiž si firma vyměňuje zdroje, zboží, informace a služby a v místně specifické míře regulace sdílí *globální kybernetický prostor*.

Schéma č.1
Kybernetická bezpečnost jako otevřený proces



Strukturu schéma č.1 využijeme pro účely tohoto materiálu jako selektivní nástroj výběru pojmů a následné struktury pojednání dalších dílčích témat.

Kybernetický prostor [4], jako digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. *Vnitřní prostředí* je tvořeno lidmi a specifickým vnitřním kybernetickým prostorem. Specifika tohoto prostoru plynou z konkrétní míry, způsobu organizace a technického řešení digitalizace vnitřních procesů. Mezi vnějším a vnitřním prostředím existuje řada vazeb. Z pohledu kybernetické bezpečnosti jsou právě tyto vazby (informační „brány“ mezi jednotlivými, podmíněně samostatnými okruhy vnitřního digitálního prostředí) zdrojem možného ohrožení. Klíčovým prvkem vnějšího i vnitřního prostředí jsou lidé. Jejich znalosti, návyky a motivace, do značné míry determinují celkovou úroveň kybernetické bezpečnosti.

Kontext

[3] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015
[4] Tamtéž

Tento pojem je důležitý pro správné definování smyslu a cílů kybernetické bezpečnosti, identifikaci hrozeb, analýzu z nich pramenících rizik, jejich prioritizaci a od toho odvozenou volbu optimalizovaného výčtu bezpečnostních opatření. Činit tak bez ohledu na vnitřní a vnější kontext je znakem formálního přístupu, mechanického převzetí „vzorů“ a v konečném důsledku to nepovede k dosažení požadované úrovně ochrany. Základní body stanovení vnitřního a vnějšího kontextu stanovuje norma.[5] Stanovení kontextu je východiskem pro proces managementu rizik.[6]

Kybernetické hrozby

Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.[7] Na webových stránkách Ministerstva vnitra ČR jsou kybernetické hrozby definovány takto: kybernetické hrozby a informační kriminalita zahrnují širokou škálu negativních fenoménů různého stupně závažnosti, ke kterým dochází v prostředí informačních technologií - od kybernetické špionáže, hackerství a DDoS[8] útoků, přes stále častější internetové podvody a krádeže (ohrožení internetového bankovnictví, krádeže dat z kreditních karet, falešné e-shopy, zneužívání osobních údajů atd.) a další formy kriminálních či nežádoucích aktivit (šíření dětské pornografie, prodej drog na internetových tržištích a praní špinavých peněz s pomocí virtuálních měn, stalking, internetová šikana, spam atd.) až po projevy extremismu a zneužívání internetu k teroristickým aktivitám a propagandě (včetně např. zveřejňování návodů na konstrukci výbušnin atd.). Hrozby v kybernetickém prostoru představují proto jednu z klíčových výzev současnosti.[9] Hrozby obecně členíme takto:

a) Antropogenní hrozby – tj. hrozby pramenící z lidských aktivit (neznalost; opomenutí; omyl; nepřátelský úmysl; teroristický útok; vojenský útok apod.).
b) Neantropogenní hrozby
   - Enviromentální – kolaps informačního systému v důsledku působení přírodních sil (např. sluneční bouře; úder blesku; záplava…)
   - Technologické – např. kolaps informačního systému v důsledku jeho zastaralosti (operační systém; HW; SW); Blackout[10] apod.

Hlavní kybernetické hrozby[11]

- Škodlivý kód (Malware)
- Útoky na webové bázi (Web based attacks)
- Útoky na webové aplikace (Web application attacks)
- Síť infikovaných počítačů (Botnets)
- Odepření služby (Denial of Service)
- Fyzická krádež / ztráta / poškození (Physical Theft / Loss / Damage)

---

[5] ČSN/EN 31010 – Management rizik – Techniky posuzování rizik

[6] tamtéž

[7] tamtéž

[8] **DoS útok** (**D**enial **o**f **s**ervice; česky odepření služby) je typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům. Může k tomu dojít zahlcením obrovským množstvím požadavků či využitím nějaké chyby, která sice útočníkovi neumožní službu ovládnout, ale umožní ji učinit nefunkční. Podtypem útoku DoS je tzv. **DDoS útok** (**D**istributed **D**enial **o**f **S**ervice), při kterém je pro zahlcení cílové služby využito velké množství počítačů z různých geografických lokalit ("distribuovaných"). Často je tento útok veden bez vědomí majitelů útočících počítačů a jedná se o důsledek napadení a úspěšného infikování těchto systémů.

[9] Dostupné on line: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?qn=Y2hudW09Mw_%3d%3d [cit. Autor 7.3.2022, 08:15]

[10] „Co se týče blackoutu, není v současné Evropě otázkou zda, ale kdy. Zdrojová připravenost se začíná vytrácet …“ IN: Drábová, D.: Blackout přijde. Otázkou je pouze kdy. Dostupné on line: https://iuhli.cz/blackout-prijde-otazkou-je-pouze-kdy/ [cit. Autor; 7.3.2022, 14:51]

[11] Dostupné on line: Dokumentace IZS – Hasičský záchranný sbor České republiky (hzscr.cz) [cit. Autor; 7.3.2022; 10:15]

- Interní hrozby zasvěcených (Insider threat)
- Rybaření (Phishing)
- Nevyžádaná pošta (Spam)
- Bezpečnostní díry (Exploit kits)
- Narušení dat (Data breaches)
- Krádež identity (Identity Theft)
- Únik informací (Information Leakage)
- Zašifrování dat (Ransomware)
- Kybernetická špionáž (Cyber espionage)

Vyhláška o kybernetické bezpečnosti vyjmenovává mimo jiné následující hrozby: [12]
- porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů
- škodlivý kód (například viry, spyware, trojské koně)
- narušení fyzické bezpečnosti
- přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
- pochybení ze strany zaměstnanců
- nedostatek zaměstnanců s potřebnou odbornou úrovní
- cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
- napadení elektronické komunikace (odposlech, modifikace)

Kybernetická rizika

Přes vysokou frekvenci užívání pojmu riziko, nepanuje v jeho definování naprostá shoda.[13]
Pro potřeby tohoto materiálu definujeme riziko takto:
Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko také představuje účinek nejistoty na dosažení cílů nebo pravděpodobnost výskytu nežádoucí události s nežádoucími následky.[14]

V tomto materiálu pracujeme s těmito základními složkami rizika:

a) **Hrozba – HRxy**
Hrozba je vždy konkrétní. V níže uvedeném vzorci má vždy hodnotu (1) a tedy se do stanovení celkové míry rizika nepromítá. Činí jej však konkrétním (riziko „čeho“).

b) **Celková míra rizika - ΣM_{Rz}**
Tato hodnota vyplyne z korelace jednotlivých složek rizika. Výpočet □MRz umožňuje stanovit reálné cíle politiky kybernetické bezpečnost organizace, definovat bezpečnostní priority a promítnout je do harmonogramu realizace bezpečnostních opatření. Korelaci složek rizika, jako celkovou míru rizika (váhu), stanovíme podle následujícího vzorce.

$$\Sigma M_{Rz} = HR_{xy} \bullet M_{Pr} \bullet M_{Zr} \bullet M_{Kr}$$

c) **Míra pravděpodobnosti – M_{Pr}**

[12] Vyhláška 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)

[13] Výkladový slovník kybernetické bezpečnosti definuje riziko takto: (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. V některých materiálech (zejména v překladech z angličtiny, je s pojmy „hrozba“ a „riziko“ dokonce pracováno jako se synonymy).

[14] S využitím: Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. Ministerstvo vnitra ČR – Odbor bezpečnostní politiky a prevence kriminality. Praha 2016. Dostupné on line: https://www.mvcr.cz/webpm/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx [cit. Autor, 8.3.2022, 13:11]

Je hodnotou vyjadřující, s jako pravděpodobností lze předpokládat, že se daná konkrétní hrozba naplní. Obecná pravděpodobnost plyne z četnosti naplnění určité hrozby ve zvoleném časovém intervalu. Vývoj této hodnoty vyjadřuje určitý obecný trend a jako takový zakládá výchozí úroveň naší pozornosti, kterou eliminaci/omezení pravděpodobnosti naplnění dané hrozby věnujeme. Konkrétní pravděpodobnost naplnění určité hroby plyne z posouzení vnějšího a vnitřního kontextu (naše atraktivita jako cíle na straně jedné a míra naší zranitelnosti na straně druhé).

d) **Míra zranitelnosti – M_{Zr}**
Je negativní hodnotou síly přijatých obranných opatření. Čím silnější jsou přijatá bezpečnostní opatření, tím klesá míra pravděpodobnosti naplnění určité konkrétní hrozby. Vyhláška o kybernetické bezpečnosti v této souvislosti hovoří o následujících skutečnostech, zvyšujících zranitelnost: [15]
- zastaralost informačního a komunikačního systému
- nedostatečné bezpečnostní povědomí uživatelů a administrátorů
- nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování
- nedostatečná ochrana aktiv
- nevhodná bezpečnostní architektura
- nedostatečná míra nezávislé kontroly

e) **Míra kritičnosti utrpěných následků – M_{Kr}**
Vyjadřuje závažnost dopadu naplnění konkrétní hrozby na naše zájmy (naplnění firemních cílů; schopnost naplnit společenské závazky ve všech uvažovaných rovinách – k vlastním zaměstnancům, akcionářům; k ostatním dotčeným subjektům – firmám, institucím a občanům; v lokálním, regionálním, národním i mezinárodním měřítku; výše nákladů na odstranění následků; dopadů na pověst firmy).

Posouzení kybernetických rizik
Celkový proces identifikace rizika, analýzy rizika a hodnocení rizika.[16] Posouzení rizika umožňuje odpovědným pracovníkům lépe chápat rizika, která by mohla ovlivnit dosahování cílů organizace, optimalizovat způsob jejich ošetření a řízení.[17] Tento proces zahrnuje:[18]
- Identifikaci aktiv, vazeb a závislostí mezi nimi
- Identifikaci hrozeb a jejich vazby k jednotlivým aktivům
- Stanovení metodiky pro identifikaci a hodnocení rizik
- Vyhodnocení rizik a stanovení bezpečnostních priorit
- Stanovení kritérií pro akceptovatelnost rizik
- Zpracování Plánu zvládání rizik

Informace
Každý znakový projev, který má smysl pro komunikátora i příjemce.[19]

[15] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

[16] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015

[17] ČSN/EN 31010 - Management rizik – Techniky posuzování rizik

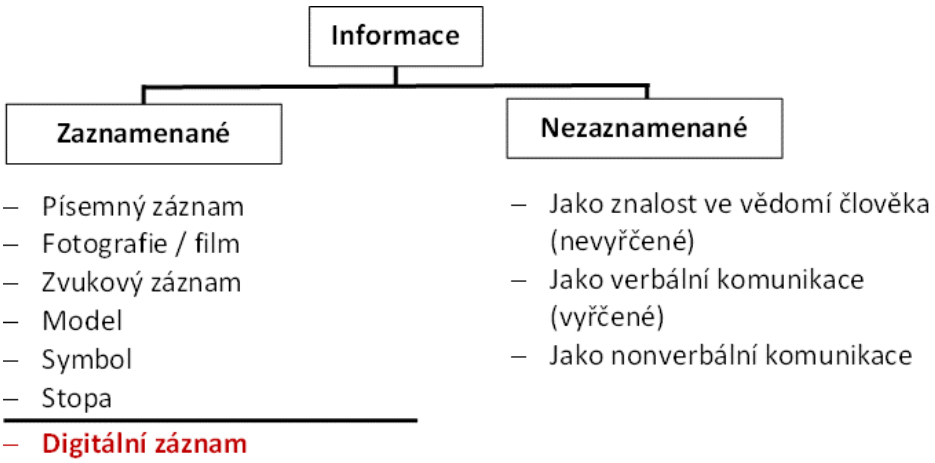
[18] Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

[19] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015

Informace mají různou formu záznamu (digitální[20]; listinnou; obrazovou; model; ústní sdělení apod.) a požívají různou míru normativní ochrany (klasifikované[21]; neklasifikované). Z uvedeného je patrné, že informační bezpečnost je širší pojem než kybernetická bezpečnost. V podnikové praxi je nutno tuto skutečnost důsledně zohlednit (touto problematikou se budeme šířeji zabývat ve 4. oddílu tohoto materiálu).

Informační systém
Funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky. Tyto prostředky tvoří síť elektronických komunikací přenosové systémy,

Schéma č.2
Možné formy záznamu informace[22]



popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.[23] Základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví. Mezi základní služby patří energetika. Informační sítě, na kterých jsou služby v oblasti energetiky (v souvislosti s předmětným zaměřením tohoto materiálu – elektroenergetika a teplárenství) tvoří informačním systémem základní služby.[24]

Opatření kybernetické bezpečnosti

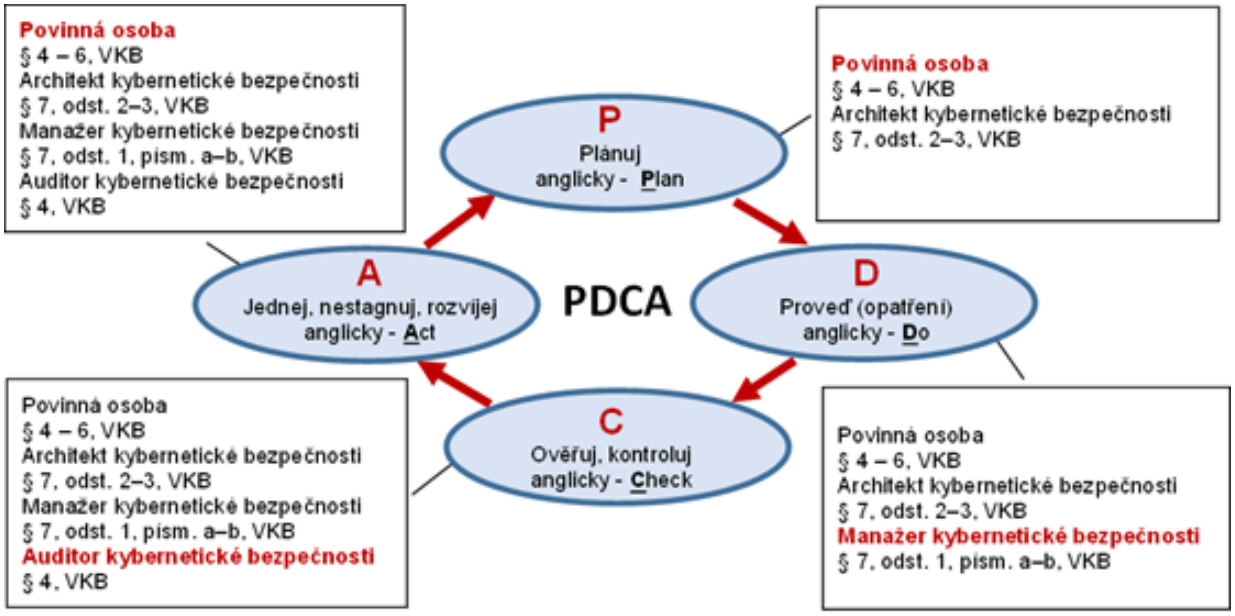
[20] Právě tyto jsou předmětem kybernetické bezpečnosti
[21] Utajované informace podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; zvláštní skutečnosti podle zákona 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon); osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů; obchodní tajemství podle zákona č. č. 89/2012 Sb., Občanský zákoník a další.
[22] S využitím ČSN EN ISO/IEC 27000, čl. 3.2.1
[23] Tamtéž
[24] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Prostředky modifikující riziko, včetně politik, strategií, postupů, směrnic, obvyklých postupů (praktik) nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy.[25]

Zavádění bezpečnostních opatření – PDCA model

Osvědčeným procesním modelem budování bezpečnostního systému, zavádění systému bezpečnostních opatření kybernetické bezpečnosti nevyjímaje je model PDCA (z anglického **P**lan-**D**o-**C**heck-**A**ct – Plánuj-proveď-ověř-jednej). Uvedené čtyři základní kroky se cyklicky opakují, čím je dosahováno soustavného zvyšování účinnosti systému bezpečnostních opatření. V rámci cyklu periodicky se opakujících kroků se mění zapojení nositelů jednotlivých rolí. Přičemž role povinné osoby, zastoupené oprávněnými zástupci[26] a vrcholovým managementem společnosti, je ve všech fázích cyklu zachováno na úrovni „vrcholové odpovědnosti". Tato odpovědnost je distribuována, společně s pravomocemi, soustavou bezpečnostní dokumentace. Povinnosti osob zastávajících jednotlivé role v řízení systému kybernetické bezpečnosti organizace stanovuje předpis.[27]

Schéma č.3
Zavádění a zdokonalování systému bezpečnostních opatření kybernetické bezpečnosti



Bezpečnostní politika organizace

Bezpečnostní politika představuje soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv. [28]

[25] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015

[26] Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění zákona č. 458/2016 Sb., zákona č. 33/2020 Sb. a zákona č. 163/2020 Sb.

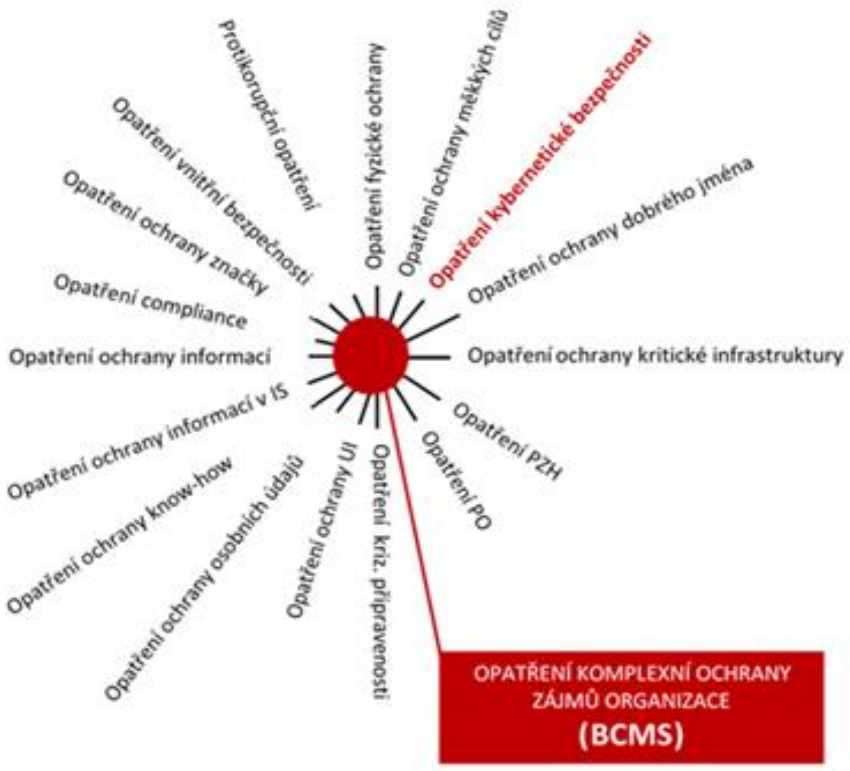
[27] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

[28] Tamtéž

Schéma č.4
Struktura Bezpečnostní politiky organizace

Bezpečnostní politika je proto klíčovým dokumentem, stanovujícím základní úkoly kybernetické bezpečnosti a způsob jejich naplňování v organizaci. Kybernetické hrozby představují pro organizace sektoru energetiky aktuálně velmi závažnou bezpečnostní výzvu. Nejsou to však jediné hrozby, kterými organizace čelí.

Schéma č.5
Kybernetická bezpečnost ve vazbě na další bezpečnostní hrozby a opatření k přiměřenému omezení jejich dopadů

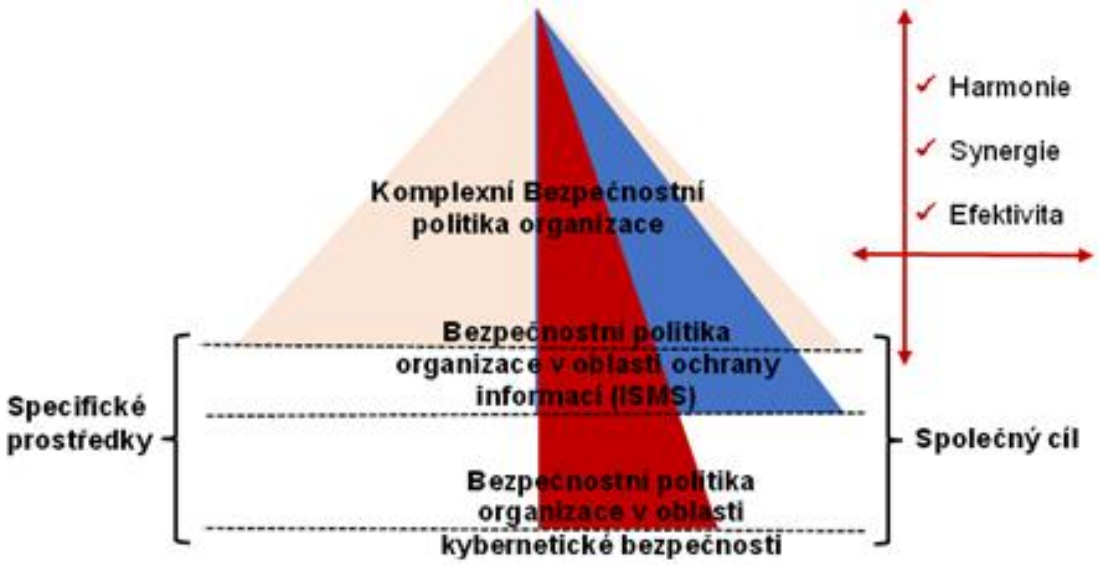


Zohlednění těchto skutečností se může promítnout do struktury komplexní bezpečnostní politiky organizace. Bezpečnostní politika zajištění kybernetické bezpečnosti organizace pak může být jednou z bezpečnostních politik. To samozřejmě klade důraz na vzájemné provázání bezpečnostních opatření, s důrazem na maximalizaci jejich synergií. Bezpečnostní politika může mít rovněž rozdílný rozsah a formu:

a) Z hlediska rozsahu:
   - Komplexní bezpečnostní politiky, v rámci, které zaujímá kybernetická bezpečnost místo samostatného oddílu
   - Specializovaného dokumentu, řešícího jen problematiku kybernetické bezpečnosti

b) Z hlediska formy:
   - Dokumentu určeného pro práci vedení organizace, bezpečnostního managementu a specialistů v oblasti kybernetické bezpečnosti
   - Dokumentu nazvaného např. Bezpečnostní politika organizace v oblasti ochrany před kybernetickými hrozbami, který je výborem, sestaveným z pohledu potřeb jeho motivační funkce a určeného všem zaměstnancům. Zdůrazňujícího vůli vedení chránit organizaci před dopady kybernetických hrozeb, závazek všech zaměstnanců se na tomto úsilí podílet v rozsahu plynoucího z jejich pracovního zařazení a odpovědnost každého za dodržování stanovených bezpečnostních postupů.

Schéma č.6
Možná předmětná struktura Bezpečnostní politiky organizace



Strukturu a obsah Bezpečnostní politiky organizace stanoví právní předpis takto[29]

- Politika systému řízení bezpečnosti informací
- Politika řízení aktiv
- Politika organizační bezpečnosti
- Politika řízení dodavatelů
- Politika bezpečnosti lidských zdrojů
- Politika řízení provozu a komunikací
- Politika řízení přístupu
- Politika bezpečného chování uživatelů
- Politika zálohování a obnovy a dlouhodobého ukládání
- Politika bezpečného předávání a výměny informací
- Politika řízení technických zranitelností
- Politika bezpečného používání mobilních zařízení
- Politika akvizice, vývoje a údržby
- Politika ochrany osobních údajů
- Politika fyzické bezpečnosti
- Politika bezpečnosti komunikační sítě
- Politika ochrany před škodlivým kódem
- Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
- Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Politika bezpečného používání kryptografické ochrany
- Politika řízení změn
- Politika zvládání kybernetických bezpečnostních incidentů
- Politika řízení kontinuity činností

Bezpečnostní dokumentace kybernetické bezpečnosti

[29] Příloha č. 5 k vyhlášce 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)

Řízení a účinnost opatření, která nejsou zdokumentována nelze prokázat. Právní předpis stanoví rozsah bezpečnostní dokumentace kybernetické bezpečnosti takto:[30]

a) Bezpečnostní politika
b) Bezpečnostní dokumentace
- Zpráva z auditu kybernetické bezpečnosti
- Zpráva z přezkoumání systému řízení bezpečnosti informací
- Metodika pro identifikaci a hodnocení aktiv a pro hodnocení rizik
- Zpráva o hodnocení aktiv a rizik
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik
- Plán rozvoje bezpečnostního povědomí
- Evidence změn
- Hlášené kontaktní údaje
- Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

c) Další doporučená dokumentace
- Topologie infrastruktury.
- Přehled síťových zařízení.

3.
Opatření kybernetické bezpečnosti

Zákon[31] tuto obecnou definici obsahově specifikuje takto:

(1) **Bezpečnostními opatřeními jsou**
a) organizační opatření
b) technická opatření.
(2) **Organizačními opatřeními jsou**
a) systém řízení bezpečnosti informací,
b) řízení rizik,
c) bezpečnostní politika,
d) organizační bezpečnost,
e) stanovení bezpečnostních požadavků pro dodavatele,
f) řízení aktiv,
g) bezpečnost lidských zdrojů,
h) řízení provozu a komunikací,
i) řízení přístupu osob,
j) akvizice, vývoj a údržba,
k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
l) řízení kontinuity činností a
m) kontrola a audit.
(3) **Technickými opatřeními jsou**
a) fyzická bezpečnost,
b) nástroj pro ochranu integrity komunikačních sítí,
c) nástroj pro ověřování identity uživatelů,

[30] Příloha č. 5 k vyhlášce 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)

[31] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

d) nástroj pro řízení přístupových oprávnění,
e) nástroj pro ochranu před škodlivým kódem,
f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
g) nástroj pro detekci kybernetických bezpečnostních událostí,
h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
i) aplikační bezpečnost,
j) kryptografické prostředky,
k) nástroj pro zajišťování úrovně dostupnosti informací a
l) bezpečnost průmyslových a řídících systémů.

Prováděcí předpis[32] k tomu zákonu pak stanoví podrobnější strukturu těchto opatření.

4.
Kybernetická bezpečnost v širším kontextu

Potřeba chápat kybernetickou bezpečnost v zájmu její účinnosti a efektivity v širším kontextu, již byla v tomto materiálu vzpomenuta. Detailnější pojednání těchto souvislostí však bylo potlačeno. V zájmu zachování centra pozornosti na problematiku kybernetické bezpečnosti v užším slova smyslu. Tedy v rozsahu explicitně definovaném souborem citovaných norem. V tomto oddílu se zaměříme na hlavní širší souvislosti, jejichž reflexi považujeme rovněž za mimořádně důležitou. Jedná se o problematiku normativně ukotvených bezpečnostních procesů, jejichž předmětné zaměření se relevantním způsobem vztahuje k ochraně informací, nebo ochraně klíčových zájmů organizace, které mohou být ohrožovány ze strany nedostatečného řešení informační bezpečnosti. Zmíníme se jen o nejdůležitějších:

- Systém řízení bezpečnosti informací
- Systém ochrany utajovaných informací
- Systém ochrany dodavatelsko – odběratelského řetězce
- Ochrana kontinuity podnikání

Jejich vztah z pohledu sledovaného téma – kybernetické bezpečnosti podniků energetického sektoru, koncentrovaně vyjadřuje schéma č.7 na následující straně. Prostřednictvím tohoto schéma usilujeme o transparentní podchycení základních souvislostí:

- Míru komplexnosti ochrany oprávněných zájmů organizace v uvedených normativně ukotvených systémech bezpečnostních opatření.
- Váhu opatření kybernetické bezpečnosti v uvedených normativně ukotvených systémech bezpečnostních opatření.

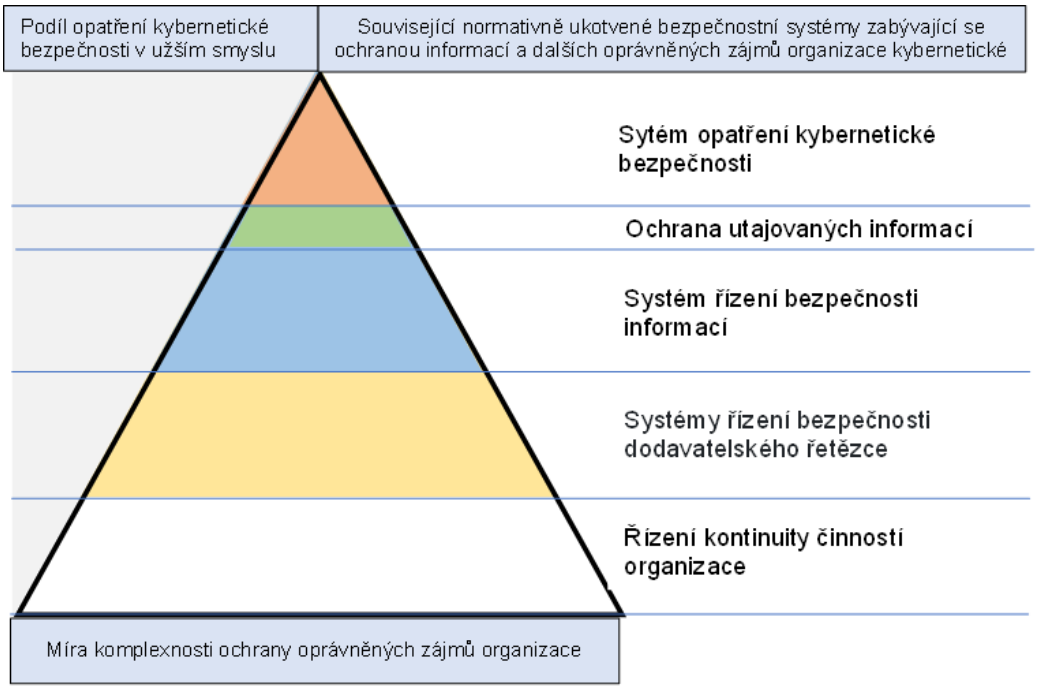
1. Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (ISMS – **I**nformation **S**ecurity **M**anagement **S**ystem), představuje zdokumentovaný systém, ve kterém jsou chráněna definovaná informační aktiva, jsou řízena rizika bezpečnosti informací a zavedená opatření jsou kontrolována. Pojem primárně zavedla norma ISO/IEC 17799 (mezinárodní norma převzatá z Britského standardu BS 7799-1:1999), publikovaná Mezinárodní organizací pro normalizaci (ISO) v roce 2000. Novější revidovaná verze je součástí nové řady norem týkající se bezpečnosti informací, které jsou současně plně kompatibilní s ostatními normami rodiny ISO.[33]

Schéma č.7
Kybernetická bezpečnost v širších souvislostech

[32] Vyhláška 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)

[33] ČSN EN ISO/IEC 27000 - Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací - Přehled a slovník



ISMS je systém sestávající z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby permanentně byla zachována účinnost systému opatření, v zájmu dosahování cílů organizace. Je založen na následujících základních **principech**:

- principu potřebnosti (nutnosti);
- principu jasně definované odpovědnosti;
- principu vědomí o shodě zájmů a postupů zúčastněných stran (managementu; zaměstnanců; partnerů);
- principu řízení rizik;
- principu začlenění bezpečnostních opatření mezi základní prvky sítí a systémů;
- principu aktivní prevence informačních incidentů;
- principu permanentního opakování posuzování bezpečnosti informací a provádění **modifikací dle potřeby (procesní model PDCA).**

Z uvedeného vyplývá vztah mezi systémem bezpečnostních opatření kybernetické bezpečnosti a systémem bezpečnostních opatření řízení bezpečnosti informací (ISMS), jako:

- systémů shodných cílů, principů a postupů;
- jako užšího (opatření kybernetické bezpečnosti) a širšího (ISMS);
- jako systémů užívajících převážně shodných technických a režimových opatření, částečně se lišících v souboru organizačních opatření;
- jako systémů plně kompatibilních, vzájemně se podporujících a dosahujících žádoucích synergií.

Proces ustavení, monitorování, udržování a zlepšování ISMS zahrnuje:

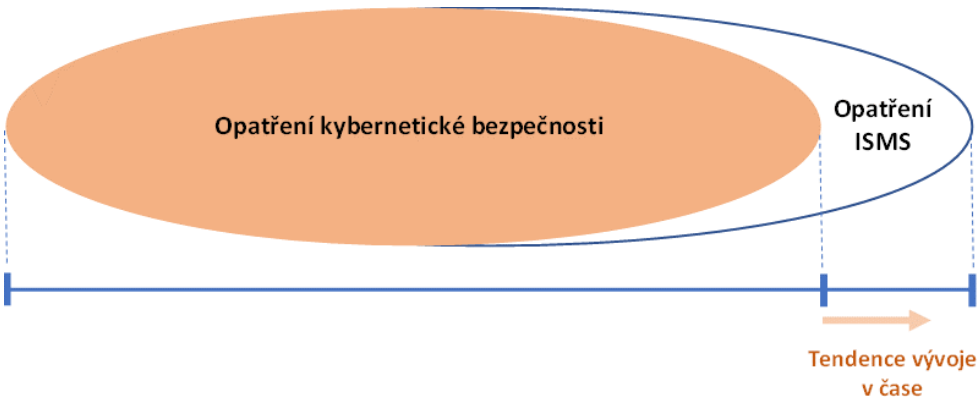
- identifikaci informačních aktiv, jejich valuaci z pohledu potřeb organizace, právních norem, vnějšího a vnitřního kontextu, reálných bezpečnostních hrozeb;
- posouzení rizik a stanovení bezpečnostních priorit organizace:
- výběr a implementaci příslušných bezpečnostních opatření k omezení rizik na akceptovatelnou úroveň a zvládnutí neakceptovatelných rizik;

– cyklický monitoring, testování a posuzování účinnosti opatření a zvyšování jejich efektivnosti v závislosti na vývoji bezpečnostní situace a od ní odvozených bezpečnostních potřeb organizace.

Bezpečnostní dokumentace ISMS[34]

a) Bezpečnostní politika organizace (Politiky bezpečnosti informací)
b) Interní směrnice bezpečnosti informací:
   – rámce řízení (odpovědnosti; komunikace);
   – pravidla pro užívání mobilních zařízení a bezpečná organizace práce na dálku;
   – bezpečnost lidských zdrojů;
   – řízení aktiv;
   – klasifikace informací;
   – řízení přístupu a odpovědnosti uživatelů;
   – fyzická bezpečnost a bezpečnost prostředí;
   – bezpečnost provozu;
   – bezpečnost komunikací;
   – akvizice, vývoj a údržba systémů;
   – řízení dodávek služeb dodavatelů;
   – řízení incidentů bezpečnosti informací.
c) Postupy a závěry přezkoumání bezpečnosti informací.

Schéma č.8
Vztah mezi systémy opatření kybernetické bezpečnosti a ISMS



Systém opatření ochrany informací v rámci ISMS je „širší“. Zahrnuje opatření ochrany informací, zaznamenaných v jiné než digitální formě, opatření ochrany informací

[34] S využitím: ČSN ISO/IEC 27001 - Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky Příloha A (normativní)

v komunikačních prostředcích (telefony; mobilní telefony) a opatření zaměřená proti ústnímu vyzrazení informací. Hranice mezi těmito systémy je neostrá a obsah opatření se do jisté míry prolíná. Trend vývoje těchto systémů v čase, vzhledem v postupu digitalizace, vede k rozšíření systému kybernetické ochrany. V praxi je možné přistoupit ke společnému souboru bezpečnostní dokumentace (od Politik po zdokumentování opatření), jak pro Systém řízení bezpečnosti informací (ISMS), tak pro systém kybernetické bezpečnosti.

2. Systém ochran utajovaných informací

Ochrana utajovaných informací není normativně podchycena normami opatření kybernetické bezpečnosti, ani ISMS. Z tohoto pohledu tvoří relativně autonomní podsystém bezpečnosti informací s vlastní normativní základnou.[35]

3. Systémy řízení bezpečnosti dodavatelského řetězce[36]

Tyto procesy jsou řízeny dle normy ČSN ISO 28000.Předmětem této mezinárodní normy je specifikace požadavků na systém managementu bezpečnosti, přičemž zahrnuje kritické aspekty pro zajištění bezpečnosti dodavatelského řetězce. Management bezpečnosti je spojen s celou řadou dalších aspektů řízení obchodní činnosti (business management). Tyto aspekty zahrnují veškeré činnosti, jež organizace provádí, řídí a mají dopad na bezpečnost dodavatelského řetězce. **Tedy i aspekty informační a kybernetické bezpečnosti. Dodavatelský řetězec** norma definuje jako propojený řetězec zdrojů a procesů, které začínají shromažďováním surovin až po dodávku produktů nebo služeb koncovému uživateli prostřednictvím různých druhů dopravy/dodávky. **Informace explicitně nezmiňuje**. Z kontextu je však nepochybné, že v průběhu této směny zainteresované strany sdílí velký objem informací, převážně v kybernetickém prostoru. Z toho plynou potenciální hrozby:

- zneužití informačních kanálů kybernetickému útoku a tím poškodit jednu nebo více zainteresovaných stran (přenos škodlivého kódu);
- hrozba přenosu škodlivého kódu z informačních kanálů obchodního styku na informační systémy spravují životně důležité provozní systémy.

Z toho plynou potřeby zabezpečení těchto informačních toků. Obtížnost naplnění tohoto požadavku vzrůstá úměrně zapojení společnosti v národním, evropském a globálním měřítku. V národním a evropském měřítku poskytuje přiměřenou ochranu důsledné dodržování shora pojednaných norem kybernetické bezpečnosti a ISMS. V tomto rámci je nezbytné:

- v národním a evropském měřítku uplatnit důsledný, smluvně zakotvený, deklarovaný, případně ověřovaný požadavek na implementaci opatření kybernetické bezpečnosti;
- v rámci komunikace v globálním měřítku se musí kontext, tedy lokalita a informační důvěryhodnost partnera, promítnout v analýze rizik a síle přijatých bezpečnostních opatření.

Každá norma ISO je certifikovatelná. Jedním z možných opatření posílení bezpečnostních opatření ve vzájemném styku, je akceptace certifikátu shody, vydaného důvěryhodnou certifikační autoritou: Řada nadnárodních firem proto u svých klíčových dodavatelů a odběratelů požaduje certifikáty shody vydané nadnárodními certifikačními autoritami s vysokým koeficientem důvěryhodnosti.

---

[35] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů; Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů; Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů

[36] ČSN ISO 28000 (010381) - Specifikace pro systémy managementu bezpečnosti dodavatelských řetězců

Řízení kontinuity činností organizace

Pojem řízení kontinuity činností – má dva významy:

a) ve smyslu krizového managementu jako „procesy a/nebo postupy k zajištění nepřetržitého chodu organizace“[37], proces „prevence, zmírňování a zotavení se z přerušení“.
b) ve smyslu mezinárodních standardů Systém řízení kontinuity činností organizace (Business Continuity Management System, BCMS)[38]

Ochrana informací ve smyslu BCMS zahrnuje:[39]

- zajištění ochrany prioritních činností před narušením;
- stabilizování, pokračování, obnovení a zotavení prioritních činností po narušení;
- zmírnění, odezvu a zvládání dopadů.

Kroky vedoucí z zavedení BCMS

- Porozumění organizaci
- Identifikace hrozeb, analýza rizik a stanovení bezpečnostních priorit (rozsahu BCP – Plánu zachování kontinuity)
- Vytvoření Politik BCM
- Plán opatření BCM a jeho implementace
- Testování, auditování, udržování a zvyšování účinnosti
- Certifikace BCMS

5.
Jak k problému kybernetické bezpečnosti přistoupit?

Vzhledem k cílům, které portál ČSZE sleduje a omezenému prostoru, nemohou být ambice tohoto materiálu ničím více, než poskytnout základní orientaci v problematice kybernetické bezpečnosti a zorientovat v relevantních zdrojích. Pokud se nám to podařilo, v což doufáme, jsme tomu rádi. Samozřejmě si však uvědomujeme, že jsme uspokojí jen část čtenářů. Ucelenou odpověď na základní otázku, kterou jsme užili pro název tohoto oddílu a kterou jste si pravděpodobně také položili – no dobře a jak dál? – můžeme pomoci zodpovědět jen cestou dále uvedených návodných doporučení. Nejedná se o žádné „knížecí rady“, byt tak mohou působit. V každém případě jsme přesvědčeni o tom, že jsou pro vás užitečné.

1. Pokud za Vás nerozhodla norma a nejste „povinnými subjekty“ a pokud Vás k tomu nenutí obchodní partneři, musíte se rozhodnout, zda a v jakém rozsahu se problémem zabývat. V této souvislosti doporučujeme:
   - Prvotně vycházet z reálných hrozeb a od nich odvozených rizik. Dopady mimořádných událostí a náklady spojené s odstraněním následků, jsou vždy násobně vyšší než náklady prevence.
   - Respektovat skutečnost, že nic a bezpečnost zvlášť, není zadarmo. Něco stojí. Peníze a velké organizační úsilí. Proto se řiďte zásadou přiměřenosti a hledejte optimální řešení z pohledu „náklad-výkon“.
   - Hledat optimálního řešení. To předpokládá odbornost a schopnost využít nejlepší praxe v oboru, tedy i potřebnou zkušenost.

[37] Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015

[38] ČSN EN ISO 22301:2013, Ochrana společnosti - Systémy managementu kontinuity podnikání – Požadavky; BS 25999-1:2006, Business continuity management – Part 1: Code of practice; BS 25999-2:2007, Business continuity management – Part 2: Specification; Business continuity management: Good practice guid Jirásek, P.; Novák, L.; Požár, J.: Výkladový slovník kybernetické bezpečnosti. Policejní akademie ČR v Praze. Praha 2015elines .

[39] Krůček, P.: Dostupné on line: https://www.krucek.cz/kontinuita-podnikani-z-pohledu-bezpecnosti-informaci/ [cit. Autor, 13.3.2022, 20:30]

- Neposuzovat problém izolovaně. Respektovat co nejširší souvislosti. Bezpečnost je systém. V jeho rámci se jednotlivé „specializované bezpečnosti“ (včetně kybernetické) vzájemně prolínají. Hledejte vždy maximum možných synergií.
- Rozhlédněte se. Neřešte věc jen v dimenzi vašeho podniku. V kybernetickém prostoru nejste nikdy sami. Identifikujte síť vazeb s dodavateli a odběrateli. A tam, kde by od partnerů hrozilo nebezpečí, přizpůsobte tomu přiměřené bariéry a vyvíjejte na ně tlak, aby i oni implementovali dostatečná bezpečnostní opatření. A to i v tom případě, že nejsou „osobou povinou“ a z tohoto pohledu se jim mohou zdát náklady kybernetické bezpečnosti „nadbytečné“. Nebojte se využít obchodních nástrojů, včetně uplatnění vašeho práva na periodický audit.
- Nejste-li sami ve vedení společnosti, snažte se ho získat. Vůle vedení společnosti, deklarovaná v bezpečnostní politice, je alfa-omega úspěchu.

2. Projdete-li vším shora uvedeným, můžete zjistit, že úkol je nad vaše síly. Nemáte dostatek odborníků. Nebojte se outsourcingu. Zejména v oblasti:
   - Konzultační podpory
   - Vstupních analýz v oblasti kybernetické bezpečnosti a shora uvedených souvisejících oblastí
   - Projektování a řízení implementace bezpečnostní opatření
   - Zajištění externího auditora kybernetické bezpečnosti
   - Školení managementu i zaměstnanců

3. Neváhejte se obrátit na autora tohoto materiálu.

PhDr. Zdeněk Hais
M: +420 736 473 349
E: haisz@fsc-ov.cz

Autor disponuje 30letou praxí v managementu společností, poskytujících soukromé bezpečnostní služby, služby facility managementu, poradenství a specializovaného odborného vzdělávání a výcviku. Je členem Bezpečnostní sekce Hospodářské komory ČR. V současné době pracuje jako manažer podpory významných klientů společnosti F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s. a jako znalec její Znalecké kanceláře.