Principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro oblast ochrany civilního letectví před protiprávními činy

Úvod

V této příručce jsou uvedeny principy, postupy a požadavky v oblasti kybernetické bezpečnosti zejména pro subjekty, které se neřídí zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a podílejí se na ochraně civilního letectví před protiprávními činy. Příručka je rozdělena na dvě části, první část je zaměřena zejména na řízení a zavedení oblasti kybernetické bezpečnosti z pohledu vrcholového managementu. Součástí první části je rovněž stanovení odpovědnosti, vytvoření bezpečnostní politiky, zpracování dokumentace a stanovení rolí, které budou přiděleny osobě nebo osobám odpovědným za kybernetickou bezpečnost. Druhá část je zaměřena na základní principy a postupy v technické oblasti a slouží jako podpůrný návod pro minimální zabezpečení daného subjektu.

Příručka zaměřená na ochranu informačních a komunikačních systémů by měla sloužit pro veškeré subjekty, které se podílejí na ochraně civilního letectví před protiprávními činy a nemají s oblastí kybernetické bezpečnosti žádné nebo minimální zkušenosti. Příručka je určena i subjektům, kteří s ochranou informačních nebo komunikačních systémů začínají nebo již začaly uvažovat o její implementaci. Ochrana informačních a komunikačních systémů je povinná pro veškeré subjekty, které se neřídí výše zmíněným zákonem. Nastavení těchto procesů a postupů musí být implementováno v bezpečnostním programu každého subjektu a následně bude nedílnou součástí kontrolní činnosti Úřadu pro civilní letectví.

V druhé části jsou popsány základní informace a doporučení pro nastavení minimální ochrany informačních nebo komunikačních systémů. V této části jsou také vysvětlené základní pojmy v oblasti kybernetické bezpečnosti, jejich řešení a doporučení.

Oblast kybernetické bezpečnosti bude součástí kontrolní činnosti Úřadu pro civilní letectví (dále jen „Úřad“) od 1. ledna 2022. Každý subjekt je povinný od tohoto data nastavit ochranu informačních a komunikačních systémů v rámci oblasti výkonu činnosti, která souvisí s ochranou civilního letectví před protiprávními činy.

Úroveň nastavených postupů a procesů je na uvážení každého subjektu vzhledem k rozsahu jeho vykonávané činnosti.

I. Nastavení procesů z hlediska řízení organizace

Základním principem této části je popsání postupů a procesů z hlediska zavedení kybernetické bezpečnosti u subjektů, jež se podílejí na ochraně civilního letectví před protiprávními činy. V této části jsou uvedeny postupy pro stanovení odpovědnosti, vytvoření bezpečnostní politiky a bezpečnostní dokumentace. Dále jsou také zmíněna doporučení a stanovení odpovědností jednotlivých osob v oblasti kybernetické bezpečnosti.

Systematický přístup ke zvyšování kybernetické bezpečnosti musí být nedílnou součástí při zavádění bezpečnostních opatření a musí být podporováno vrcholovým vedením tak, aby byla zajištěna ochrana informačních a komunikačních systémů na té nejvyšší úrovni.

Cílem nastavení těchto procesů je včasná identifikace a ochrana kritických částí systému a dat. Zvyšování povědomí v oblasti kybernetické bezpečnosti, nastavení procesů, postupů a ochrany informačních a komunikačních systémů je povinné zejména pro tyto oblasti:

- databáze schválených agentů, známých odesílatelů, schválených dodavatelů palubních zásob a známých dodavatelů a dalších subjektů v oblasti zasilatelského řetězce;
- přístupová databáze osob do neveřejných prostorů subjektů, ve kterých se manipuluje anebo ukládají letecké zásilky, palubní zásoby anebo letištní dodávky, přístupová databáze osob jiných než cestujících do neveřejného prostoru letiště, SRA/CSRA;
- naprogramování a elektronické ovládání vjezdových/přístupových bran a vstupů, elektronický systém kontroly vstupu, včetně poplachového systému (EZS, EPS);
- čtečky palubních lístků;
- CCTV systém včetně uložiště záznamů;
- systém pro spojení cestujících a zapsaných zavazadel;
- čtečky e-pasů;
- bezpečnostní vybavení včetně jejich výstupů a síťových systémů;
- databáze personálních dat obsahující údaje o odborných či průběžných odborných přípravách bezpečnostních pracovníků apod.;
- zabezpečení úložišť, pracovních a serverových stanic a sítí, kde jsou uloženy dokumenty obsahující citlivé informace (bezpečnostní program, protokoly z kontrolní činnosti atd.);
- systém pro odbavení cestujících včetně jeho úložiště;
- informační systémy pro cestující včetně ovládání těchto systémů.[1]

Veškeré postupy a procesy zaměřené na ochranu informačních a komunikačních systémů musí být uvedeny v bezpečnostním programu každého subjektu, který se podílí na ochraně civilního letectví před protiprávními činy. Jednotlivé postupy a procesy budou podléhat kontrolní činnosti ze strany Úřadu.

[1] Evropská komise. *Prováděcí nařízení Komise (EU) 2019/1583 ze dne 25. září 2019, kterým se mění prováděcí nařízení (EU) 2015/1998*, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti, pokud jde o opatření o kybernetické bezpečnosti. Dostupný také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?toc=OJ%3AL%3A2019%3A246%3ATOC&uri=uriserv%3AOJ.L_.2019.246.01.0015.01.CES

1. Osoba odpovědná za kybernetickou bezpečnost

Základním předpokladem je zajištění osoby odpovědné za kybernetickou bezpečnost, tato osoba by měla podléhat dohodě o zachování mlčenlivosti minimálně v podobě doložky k pracovní smlouvě. Osoba odpovědná za kybernetickou bezpečnost musí mít znalosti v oblasti informačních a komunikačních systémů minimálně na uživatelské úrovni.

Osoba odpovědná za kybernetickou bezpečnost musí absolvovat on-line školení a dále musí zabezpečit proškolení ostatních zaměstnanců formou on-line školení a splnění testu. On-line školení a testy jsou pod záštitou NÚKIB.

Jedná se zejména o tato školení:

- Základy kybernetické bezpečnosti – „Dávej kyber“ – určené pro zaměstnance
- Kurz pro manažery kybernetické bezpečnosti – určené pro osoby odpovědné za tuto oblast

Osoba odpovědná za kybernetickou bezpečnost je povinna zajistit odebrání přístupových oprávnění u veškerých účtů zaměstnanců (např. při ukončení pracovního vztahu).

Osoba odpovědná za kybernetickou bezpečnost musí mít ověření spolehlivosti nebo ověření fyzických osob minimálně stupně Důvěrné. Plán pro zavedení bezpečnostních opatření v oblasti kybernetické bezpečnosti

Plán pro zavedení bezpečnostních opatření by měl sloužit jako přehledový dokument pro zajištění ochrany informačních a komunikačních systémů a může obsahovat tyto oblasti:

- Seznam bezpečnostních opatření, která musí být zavedena
- Zdroje, ze kterých bude čerpáno
- Časový harmonogram pro zavedení
- Klasifikace úrovně ochrany informací
- Řízení dodavatelů
- Školení
- Změny a jejich následky
- Kontinuita činností
- Auditní činnost

V plánu zavádění bezpečnostních opatření musí být zohledněny také bezpečnostní incidenty, aktuality v oblasti vydávané NÚKIB, zohlednění výsledku interního auditu, ale i kontrolní činnosti v rámci dozorového orgánu. Je doporučeno zpracovávat plán pro zavedení bezpečnostních opatření v oblasti kybernetické bezpečnosti vždy na následující kalendářní rok. Plán by měl obsahovat doporučení pro stanovení dostupnosti dat. Zajištění dostupnosti dat je důležité zejména při řešení nestandardních situací, podporu, postupy pro obnovu po havárii a zálohování.

Součástí plánu by mělo být správné rozvržení a identifikace nutné ochrany systému v návaznosti na citlivost informací. Klasifikace úrovně ochrany informací může být rozdělena dle následující tabulky.

Tabulka č. 1 Úroveň hodnocení informací

Úroveň	Důvěrnost	Integrita	Dostupnost
1	Informace jsou veřejně přístupné nebo byly určené ke zveřejnění. Narušení důvěrnosti neohrožuje oprávněné zájmy organizace.	Narušení integrity neohrožuje oprávněné zájmy organizace.	Narušení dostupnosti není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu.
2	Informace nejsou veřejně přístupné a tvoří know-how organizace.	Narušení integrity informace může vést k poškození oprávněných zájmů organizace.	Narušení dostupnosti by nemělo překročit dobu několika hodin. Výpadek je nutné řešit bez zbytečného odkladu, protože vede k ohrožení oprávněných zájmů organizace.
3	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie.	Narušení integrity vede k poškození oprávněných zájmů organizace.	Narušení dostupnosti není přípustné a i krátkodobá nedostupnost vede k vážnému ohrožení oprávněných zájmů organizace.

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Součástí plánu by mělo být rozvržení činností na denní běžné úrovni, ale také nastavení postupů při mimořádných událostech.

Plán určený pro běžný provoz, jehož součástí jsou mimo jiné postupy v případě ztráty dat, jejich dostupnost, důvěrnost a integrita slouží zejména pro zajištění včasného obnovení denního provozu například při výpadku. Součástí tohoto plánu mohou být zejména tyto oblasti:

- Minimální úroveň užívání
- Doba obnovení chodu – Recovery Time Objective „RTO“ – Doba pro obnovení minimální úrovně poskytovaných služeb IKS (doba obnovení standardního provozu)
- Bod obnovení dat – Recovery Point Objective „RPO“ – časové období pro zpětné obnovení dat po selhání systému, zejména do jaké úrovně je možné obnovit data a o která data lze přijít[2]

Plán využívaný při mimořádných událostech by měl vycházet z plánu určeného pro běžný denní provoz a měl by obsahovat konkrétní posloupnosti a činnosti nutné pro obnovu chodu informačního nebo komunikačního systému.

[2] *Minimální bezpečnostní standard*. NÚKIB, NAKIT, MVČR. Metodiky, doporučení a standardy. [online]. c2020 [cit. 21. 09. 2021]. Dostupný z www: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

2. Řízení externích dodavatelů

V případě, kdy je osoba odpovědná za kybernetickou bezpečnost a osoba odpovědná za auditní činnost v oblasti kybernetické bezpečnosti zajišťována externími dodavateli, je důrazně doporučováno nevyužívat stejného externího dodavatele pro obě funkce z toho důvodu, aby byla zajištěna nestrannost a nezávislost daného subjektu.

V případě využití externího dodavatele pro zajištění ochrany informačních a komunikačních systémů daného subjektu je doporučováno vyvarovat se tzv. vendor lock-in. (*Vendor-lock in nebo také proprietární uzamčení, což znamená uzamčení zákazníka v závislosti na konkrétním dodavateli. Přechod k jiným dodavatelům je značně ztížen a zákazník tak zůstává závislý na daném dodavateli).*

Činnost externích dodavatelů musí být smluvně zajištěna. Příklady oblastí, které musejí být smluvně zajištěny, jsou dále uvedeny v Minimálním bezpečnostním standardu NÚKIB.

3. Školení a spolupráce s dalšími subjekty

Všichni zaměstnanci musí absolvovat příslušná školení v oblasti kybernetické bezpečnosti. Osoby odpovědné za tuto oblast musí neustále zvyšovat povědomí svých zaměstnanců. Dále je nutné poučit osoby, administrátory a uživatele o jejich právech, seznámit je s bezpečnostní politikou, trvale rozvíjet a kontrolovat dodržování stanovených postupů.

Školení zaměstnanců je doporučováno provádět minimálně 1x za rok. Součástí náborového, ale i průběžného školení musí být příprava na neobvyklé situace spojené s ochranou informačních a komunikačních systémů. Školení musí být v souladu s výkonem pracovní činnosti daného zaměstnance. V případě, kdy zaměstnance zastává specializovanou pracovní pozici, musí tomu odpovídat příslušné školení.

4. Identifikování změn

Každá změna musí být včas identifikována a veškeré procesy a postupy musí vést k eliminaci narušení správné funkčnosti informačního nebo komunikačního systému.

Změny musejí být řešeny včasným odhalením, evidencí, vyhodnocením a koordinováním na přijatelné úrovni vzhledem k dennímu provozu. Veškeré dopady plánovaných, ale i nenadálých změn musejí být zváženy a bezpečnostní politiky musí být aktualizovány. Dále je doporučováno provádět testování změn a zajištění možného navrácení do původního stavu.

5. Nezávislý audit a kontrolní činnost

Cílem nezávislého auditu je včasné odhalení nedostatků a odhalení potencionálních oblastí ke zlepšení. Výsledky nezávislého auditu se předkládají vrcholovému vedení a dále je nutné tyto výsledky zohlednit v plánu zavádění bezpečnostních opatření a také v bezpečnostní dokumentaci.

Nezávislý audit je nutné provádět vždy po dvou letech a následně při vzniku mimořádné události nebo na základě uvážení vrcholového vedení. Audit je možné provádět vlastními zaměstnanci vyškolenými v této oblasti nebo lze využit i externího dodavatele. V případě využití vlastních zaměstnanců je nutné zajistit jejich nezávislost. V případě využití externího dodavatele je nutné dohlížet na průběh auditu taktéž osobou, která je v kontrolované organizaci zaměstnána.

Cílem nezávislého auditu je posouzení souladu zejména s bezpečnostní dokumentací, právními předpisy, smluvními závazky, praxí a bezpečnostní politikou.

Nastavení procesů a postupů v oblasti kybernetické bezpečnosti může být předmětem nebo součástí kontrolní činnosti Úřadu. Osoba odpovědná za kybernetickou bezpečnost je povinna poskytnout veškerá data a údaje na žádost kontrolního pracovníka Úřadu.

II. Nastavení procesů z hlediska řízení technických postupů

Tato část je zaměřena na zabezpečení informačních a komunikačních systémů z pohledu technického zaměření. V prvé řadě je nutné zajistit soubor opatření proti poškození nebo krádeži těchto systémů. Je nutné stanovit pravidla pro návštěvy, které musí být identifikovány, zaznamenány do příslušné evidence a po celou dobu doprovázeny odpovědnou osobou.

Fyzické zabezpečení může být zajišťováno pomocí kamerových systémů nebo bezpečnostní agenturou, která zajistí nepřetržitý dozor. Prostory pro informační a komunikační systémy a jejich komponenty by měly být klimatizovány a zabezpečeny proti neoprávněnému přístupu. Přístupy do systému musí podléhat přístupovým oprávněním a každý uživatel musí mít jedinečný identifikátor (veškeré identifikátory musí být řízeny a evidovány včetně práv a oprávnění určených osob). Přístupová oprávnění musí být aktualizována. Každý uživatelský účet musí disponovat minimálně možností změnou a obnovení hesla.

Dále musí být nastavené takové postupy u každého subjektu, aby byla zajištěna registrace, autentizace a identifikace všech uživatelů. V celém systému musí být nastavená taková opatření, aby při poruše jednoho komponentu, nedošlo k výpadku celého systému *(Single Point of Failure).* Další povinností každého subjektu je nastavení procesů a postupů pro kontrolu softwaru a hardwaru v dané organizaci jako jsou například antivirové programy, kontrola využívání soukromých zařízení zaměstnanců, která jsou přinášena a připojována do počítačové sítě na pracovišti, kontrola připojovaných USB zařízení apod.

Pro přístup z veřejné sítě do interní počítačové sítě subjektu je doporučováno využívat zabezpečené šifrované připojení mezi dvěma sítěmi nebo mezi konkrétním uživatelem a sítí známé též jako VPN *(například pro připojení do počítačové sítě subjektu z home office apod.).*

Minimální úroveň pro nastavení hesla

Další oblastí k zajištění ochrany informačních a komunikačních systémů je nastavení přístupových hesel, minimální požadavky pro vytváření hesel, případně s využitím vícefázové autentizace (uživatel poskytne dva nebo více důkazů potvrzující jeho identitu a pravost) a to v závislosti na finančních zdrojích subjektu. Pro administrátorské účty nebo účty vyžadující vyšší úroveň zabezpečení je doporučováno nastavení přísnějších požadavků pro nastavení hesla.

Minimální úroveň pro nastavení hesla:

- minimální délka hesla – 10 znaků
- zákaz používání stejného hesla
- maximální doba platnosti – 18 měsíců
- zamčení účtu po 10 neplatných pokusech
- jednorázové prvotní heslo, které musí být změněno v určitém časovém limitu[3]

[3] *Minimální bezpečnostní standard*. NÚKIB, NAKIT, MVČR. Metodiky, doporučení a standardy. [online]. c2020 [cit. 21. 09. 2021]. Dostupný z www: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

6. Prevence proti škodlivému kódu *(malware)*

Cílem tohoto opatření je zajištění informačního nebo komunikačního systému proti škodlivému kódu. Je důležité správně identifikovat prostředí v síti, kde je nutné tyto softwary instalovat a pravidelně je aktualizovat. Veškerá získaná data z těchto bezpečnostních nástrojů (antivirus, firewall, proxy, router, switch apod.) musí být neustále vyhodnocována a ukládána pro následnou analýzu a zvyšování ochrany informačních a komunikačních systémů každého subjektu. Pravidelné testování těchto nástrojů by mělo být nedílnou součástí zajištění ochrany IKS.

Instalování jiných programových vybavení, které nejsou schválené osobou odpovědnou za kybernetickou bezpečnost nebo příslušným IT oddělením by mělo být zakázáno. Dále je vhodné seznámit zaměstnance s postupy při obdržení e-mailů s potencionální hrozbou od neznámých odesílatelů, sdílet základní informace pro nastavení hesel a jejich ochraně, adekvátně řešit problémy s připojením nebo zakázat navštěvování nezabezpečených webů apod.

Dále by měly být stanoveny postupy při vzniku kybernetických bezpečnostních incidentů, jejich analýza a řádná evidence. Všichni uživatelé musí být seznámeni s tím, jak postupovat v případě nestandardní situace, která by mohla ovlivnit běžný provoz v dané organizaci.

Osoba odpovědná za kybernetickou bezpečnost musí znát přesné postupy, jak danou situaci vyřešit, případně na koho se obrátit. Veškeré incidenty by měly být řešeny okamžitě, dále by měly být řádně evidovány a vyhodnocovány za účelem jejich eliminace při další takové události. Za incident je považováno nejen narušení integrity či důvěrnosti, ale i nedostupnost služby.

Řešením bezpečnostních incidentů na národní úrovni se zabývá vládní tým CERT, který zajišťuje prvotní pomoc a slouží jako zdroj informací při vzniku nestandardních situací. CERT slouží zejména pro jiné orgány na území České republiky, organizace, ale také pro občany. Dále je možné incidenty hlásit národnímu týmu CSIRT, který slouží zejména pro hlášení incidentů, které mohou mít zásadní vliv na fungování celého státu. Národní CSIRT plní úlohu CERT, spolupracuje se subjekty na území České republiky a udržuje zahraniční vztahy se světovými týmy CERT.[4]

Faktory, které ovlivňují zranitelnost sítě, mohou být například chyby v systému (bugy), které mohou být zneužity malwarem. Dalším faktorem může být nepřiměřené oprávnění uživatelů, proto je doporučováno nastavit rozdílná oprávnění pro uživatele a administrátory. Jedním z nejvýznamnějších faktorů, které mohou ovlivnit zranitelnost IKS je homogenita systému, což znamená, že veškeré počítače fungují na stejném operačním systému.

[4] *Minimální bezpečnostní standard*. NÚKIB, NAKIT, MVČR. Metodiky, doporučení a standardy. [online]. c2020 [cit. 21. 09. 2021]. Dostupný z www: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

Logování

Logování je záznam aktivity uživatele v informačním nebo komunikačním prostředí. Logování je používáno za účelem analýzy a případnému vyloučení, zda došlo v systému k chybě. Logování napomáhá k rychlému a spolehlivému vyřešení daného incidentu a jeho příští eliminaci. Log obsahující citlivé informace by měl být přepsán, aby byla zajištěna jeho nedostupnost.

V případě, že došlo k nestandardní situaci, logy pomáhají určit příčinu a také poskytují informace, jak k dané chybě došlo.

Veškeré výstupy a záznamy by měly podléhat kontrolní činnosti. Přístup k veškerým záznamům musí být chráněn. Veškeré záznamy musí být ukládány a měly by být k dispozici při vzniku mimořádné události a při řešení incidentů. Za incidenty je možné považovat zejména:

- přihlašování a odhlašování uživatelů
- automatická varovná nebo chybová hlášení
- změny v přístupových oprávněních
- zahájení a ukončení činnosti aplikací

Obsahem logu jsou zejména tyto informace:

- datum a čas
- síťové identifikátory
- identifikátor uživatele
- typ události
- úspěšnost nebo neúspěšnost činnosti[5]

V každé organizaci je dále doporučováno provádět testování za účelem ověření bezpečnosti daného systému. Bezpečnostní testy nebo také testy zranitelnosti mohou být zaštitovány i externími dodavateli. Veškerá data musí být chráněna, kontrolována a o každém testu musí být zpracován záznam. Pro účely testování by měla sloužit neprovozní data nebo data pozměněná.

Dále je každý subjekt odpovědný za nastavení postupů k ochraně webových aplikací proti nejčastějším útokům jako jsou například Injection útoky, únik informací, špatná autentizace, nezabezpečené kryptografické úložiště, vzdálené spuštění nebo nedostatečně zabezpečená komunikace mezi systémy.

[5] *Minimální bezpečnostní standard*. NÚKIB, NAKIT, MVČR. Metodiky, doporučení a standardy. [online]. c2020 [cit. 21. 09. 2021]. Dostupný z www: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

7. Šifrování dat a disků

Cílem tohoto opatření je zajištění ochrany informací od jejich vzniku. Vzhledem k rozsahu činnosti daného subjektu je doporučováno zavádět takové kryptografické metody, aby bylo možné zajistit bezpečnost informačních nebo komunikačních systémů na přijatelné úrovni.

Citlivá data by měla podléhat šifrování a přístup k nim by měly mít pouze oprávněné osoby. NÚKIB zpracovává doporučení ohledně kryptografických algoritmů, které jsou veřejně přístupné. Zavádění kryptografických metod je doporučováno zejména u subjektů s širším rozsahem vykonávané činnosti a na základě dostupnosti finančních zdrojů každého subjektu.

8. Zálohování dat

Veškerá data informačního nebo komunikačního systému musí být zálohována. Každý subjekt je povinný nastavit takové procesy a postupy, které budou odpovídat rozsahu jeho činnosti. Osoba odpovědná za kybernetickou bezpečnost musí být s problematikou zálohování dat seznámena a musí data kdykoliv zpřístupnit Úřadu nebo osobě, která provádí nezávislý audit.

Pro zajištění dostatečné úrovně ochrany IKS musí záloha citlivých dat podléhat šifrování a přístup k ní musí mít pouze oprávněné osoby.

Zálohování by mělo být prováděno na dvou různých médiích, z toho alespoň jedno médium by mělo být fyzické (např. HDD, USB flash disk apod.) nebo je možné využít metodu 3-2-1 – viz. obrázek č. 1.

Dále je doporučováno nastavit přiměřená ochranná opatření k zajištění kybernetické bezpečnosti při využívání cloudových služeb. Pravidla pro poskytovatele cloudových služeb a externí dodavatele by měla být totožná.

Obrázek č. 1 Zálohování dat pomocí metody 3-2-1

Zdroj: https://www.cb-nn.com/co-byste-delali-kdybyste-prisli-o-vsechna-sva-data/

9. Rozdělení komunikace s externími informačními nebo komunikačními systémy

Cílem je zabezpečení komunikace s externími informačními systémy. Komunikací s externími informačními systémy se rozumí zabezpečená komunikace například mezi jednotlivými subjekty nebo orgány státní správy.

Pro jednodušší orientaci je možné přenos dat rozdělit do skupin na základě citlivosti poskytovaných informací. Citlivá data by měla podléhat šifrování například pomocí end-to-end metody, což je metoda využívaná pro přenos dat mezi odesílatelem a příjemcem a je chráněna například proti odposlechu.[6]

V případě přenosu méně citlivých informací je možné využít šifrování dat a autorizaci uživatele v rámci IKS. V každém případě komunikace mezi jednotlivými informačními a komunikačními systémy musí být zabezpečena minimálně na povinné úrovni se zabezpečením koncových bodů.

Komunikace s externími informačními subjekty by měla být zabezpečena vzhledem k rozsahu, velikosti a potřebě daného subjektu se zajištěním minimální ochrany dat. Komunikace mezi jednotlivými systémy nemusí být vždy šifrovaná, zde je na uvážení každého subjektu, jaké postupy a procesy zabezpečení komunikace nastaví vzhledem k rozsahu vykonávané činnosti a dostupnosti finančních zdrojů.

[6] *Minimální bezpečnostní standard*. NÚKIB, NAKIT, MVČR. Metodiky, doporučení a standardy. [online]. c2020 [cit. 21. 09. 2021]. Dostupný z www: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/>.

Zkratky

NÚKIB	Národní úřad pro kybernetickou bezpečnost
MBS	Minimální bezpečnostní standard
IKS	Informační nebo komunikační systém
SRA	Bezpečnostní vyhrazený prostor
CSRA	Kritický vyhrazený prostor
EZS	Elektronický zabezpečovací systém
EPS	Elektrická požární signalizace
CCTV	Closed-circuit television, uzavřený tel. okruh
RTO	Recovery Time Objective
RPO	Recovery Point Objective
USB	Universal Serial Bus
HDD	Hard Disk Drive, pevný disk
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ÚCL	Úřad pro civilní letectví
VPN	Virtuální soukromá síť