NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

SYSTÉM A ROZSAH ISMS

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIŘAZENO • BRNO • 31. KVĚTNA 2022

VERZE DOKUMENTU: 1.0

SYSTÉM A ROZSAH ISMS

Podpůrný materiál

Obsah

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Úvod

Jednou ze základních tezí zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“ nebo „zákon“), je jeho orientace na určený nebo identifikovaný informační nebo komunikační systém. Povinnosti plynoucí ze zákona o kybernetické bezpečnosti tak nedopadají na veškeré systémy dané organizace, ale zaměřují se pouze na ty informační a komunikační systémy, které mají vzhledem k účelu zákona daný význam. Zabezpečení těchto systémů, stejně tak jako i další povinnosti plynoucí ze zákona o kybernetické bezpečnosti, jsou tak řešeny ve vztahu k nim.

Hlavním cílem tohoto podpůrného materiálu je sdělit čtenářům, jak správně porozumět pojmům informační a komunikační systém a jak je následně uchopit pro praktické použití při zajišťování kybernetické bezpečnosti. Důležitost pochopení základních pojmů informační a komunikační systém reflektuje také skutečnost, že na tyto pojmy přímo navazují pojmy informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém a informační systém základní služby, resp. tyto pojmy navazují na hlavní kategorie systémů na které dopadá zákon o kybernetické bezpečnosti.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 653

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1 Manažerské shrnutí

V první části se tento podpůrný materiál věnuje právnímu výkladu zmíněných pojmů, v kapitole 3.4 je následně praktická ukázka jak s těmito pojmy pracovat.

V zákoně o kybernetické bezpečnosti je pojem informační nebo komunikační systém vymezen vždy službou, pro kterou existuje.

Informační nebo komunikační systém je tvořen aktivy, tedy jak technickým a programovým vybavením, komunikačními prostředky, objekty, zaměstnanci a dodavateli, stejně tak jako informacemi, které zpracovává a službami (procesy), které tento informační nebo komunikační systém poskytuje. Tato aktiva podporují výkon předmětné služby v daném rozsahu a kvalitě, přičemž se nezohledňuje důležitost daného aktiva pro její zajištění – všechna, i ta nejméně důležitá aktiva, jsou součástí informačního nebo komunikačního systému, pokud slouží k zajištění jeho funkčnosti a poskytování předmětné služby v požadované kvalitě.

U takto určených aktiv je dále zohledněna důležitost prostřednictvím hodnocení aktiv a rizik, které je počátečním předpokladem pro následné systematické zavádění přiměřených bezpečnostních opatření, kterému předchází především správné stanovení rozsahu systému řízení bezpečnosti informací v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“ nebo „vyhláška“).

2 Základní teze

2.1 Pojem „systém“ v tomto dokumentu

Když se řekne slovo „systém“, každý si vybaví něco jiného. Zákon o kybernetické bezpečnosti používá slovo „systém“ především ve dvou významech které jsou vysvětleny dále.

2.1.1 Informační nebo komunikační systém

Prvním významem, který je pro tento podpůrný materiál stěžejní a se kterým pracuje především zákon o kybernetické bezpečnosti jako takový, je význam ve smyslu *„informační nebo komunikační systém“*, tedy ve smyslu označující uspořádání jednotlivých aktiv (prvků) a jejich propojení do hierarchického celku zajišťujícího přímou funkčnost požadovaných služeb (procesů) v požadované kvalitě.

Prvním dílčím cílem tohoto dokumentu je dosáhnout správného pochopení toho, co je určeným nebo identifikovaným[1] informačním nebo komunikačním systémem podle zákona o kybernetické bezpečnosti a pomoci tak povinným osobám se správným praktickým použitím těchto pojmů.

Pojem určený nebo identifikovaný informační nebo komunikační systém se v tomto smyslu vztahuje na hlavní část povinných osob podle § 3 písm. c) až f) zákona o kybernetické bezpečnosti – správce nebo provozovatele informačních nebo komunikačních systémů kritické informační infrastruktury, významných informačních systémů, nebo informačních systémů základní služby.

2.1.2 Systém řízení bezpečnosti informací

Druhým významem, kterým se bude tento podpůrný materiál zabývat, je význam ve smyslu *„systém řízení bezpečnosti informací“* (dále jen „ISMS“, z akronymu anglického „Information Security Management System“), který souvisí nejen se zákonem, ale i s vyhláškou o kybernetické bezpečnosti. ISMS se rozumí ta část systému řízení organizace založená na přístupu k rizikům informačního nebo komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.

Druhým dílčím cílem tohoto dokumentu je přiblížit správný způsob stanovení rozsahu ISMS, a to právě s ohledem na určený nebo identifikovaný informační nebo komunikační systém.

> Sousloví *„určený nebo identifikovaný systém“* v tomto dokumentu tedy označuje *„informační systém“* nebo *„komunikační systém“*.

[1] U systému kritické informační infrastruktury nebo informačního systému základní služby dochází k určení systému Úřadem autoritativně. V případě významného informačního systému tomu tak není, ten se stává významným informačním systémem v okamžiku objektivního naplnění zákonné definice, u takto určeného sytému je tedy vhodné používat spíše pojem „identifikace“, než pojem „určení“. Problematice identifikace významných informačních systémů se věnuje podpůrný materiál „Průvodce identifikací významného informačního systému“, umístěný na www.nukib.cz

Pojem *„ISMS“* nebo sousloví *„rozsah ISMS“*, označuje *„systém řízení bezpečnosti informací“, zkráceně „SŘBI“ nebo „rozsah systému řízení bezpečnosti informací“.*

3 Informační nebo komunikační systém v zákoně o kybernetické bezpečnosti

Pro správnou aplikaci a praktické použití pojmu „*informační nebo komunikační systém*“ je potřeba znát odpovědi na tři základní otázky:

1) Čím je „*informační nebo komunikační systém*“ vymezen?
2) Co „*informační nebo komunikační systém*“ tvoří?
3) Jaká je vazba mezi tím, co „*informační nebo komunikační systém*“ vymezuje a co jej tvoří?

Odpověďmi na tyto otázky se zabývají následující podkapitoly.

Pochopení a aplikace těchto tří otázek je pro správné pochopení pojmu „*informační nebo komunikační systém*“ stěžejní. Protože pojem „*informační nebo komunikační systém*“ jako takový není v zákoně o kybernetické bezpečnosti definován, budou odpovědi na tyto otázky společně tvořit praktickou definici.

Proč je to důležité?

Zákon o kybernetické bezpečnosti vztahuje ke správnému pochopení a vymezení určeného nebo identifikovaného informačního nebo komunikačního systému v organizaci téměř všechny povinnosti. Bezpečnostní opatření se zavádějí a provádějí v rozsahu nezbytném pro zajištění kybernetické bezpečnosti určeného nebo identifikovaného informačního nebo komunikačního systému. Kybernetické bezpečnostní incidenty se hlásí Národnímu úřadu pro kybernetickou a informační bezpečnost, pokud se stanou v určeném nebo identifikovaném informačním nebo komunikačním systému. Provozovatelem informačního nebo komunikačního systému může být pouze taková osoba, která funkčnost technických a programových prostředků zajišťuje na prostředcích tvořících informační nebo komunikační systém.

3.1 Čím je „*informační nebo komunikační systém*“ vymezen?

Pojem „*informační systém*“, ani „*komunikační systém*“ není v zákoně o kybernetické bezpečnosti výslovně definován. Je tedy nutno hledat výklad tohoto pojmu tak, aby byl v souladu s použitím těchto pojmů v zákoně.

Přestože v zákoně o kybernetické bezpečnosti legální definice *„informačního nebo komunikačního systému“* chybí, lze si v zákoně povšimnout společných znaků v rámci různých použití těchto pojmů. Hlavním společným jmenovatelem vymezení tohoto pojmu je služba, pro

kterou daný „*informační nebo komunikační systém*“ existuje.[2] Je tomu tak, ať už jde v případě informačního nebo komunikačního systému kritické informační infrastruktury o službu, na kterou by mělo narušení funkce tohoto systému závažný dopad, v případě významného informačního systému o službu, k jejímuž zajištění je tento informační systém využívaný, nebo v případě informačního systému základní služby o službu, jejíž poskytování je na fungování tohoto informačního systému závislé.

„*Informační nebo komunikační systém*“ je tedy v zákoně o kybernetické bezpečnosti vždy vymezen službou, pro kterou existuje.

Praktická aplikace vymezení systému pomocí služby

V případě určení informačního nebo komunikačního systému kritické informační infrastruktury nebo informačního systému základní služby se pro stanovení určené služby použije znění odvětvových kritérií příslušných prováděcích právních předpisů a zároveň v procesu určování těchto systémů Úřad autoritativně vystupuje.

V případě identifikace významných informačních systémů je nutné, aby vymezení systému prostřednictvím služby učinil sám orgán veřejné moci. V případě významných informačních systémů uvedených v § 2 odst. 1 vyhlášky č. 360/2020 Sb., o významných informačních systémech[3], jsou stanoveny typové významné informační systémy prostřednictvím služby a jsou tak přímo definovány. V případě posuzování naplnění určujících kritérií podle § 3 odst. 1 této vyhlášky, o významných informačních systémech se tento přístup použije obdobně s tím rozdílem, že službu, jejíž výkon informační systém zajišťuje, orgán veřejné moci identifikuje a nadefinuje sám podle skutečného účelu posuzovaného systému a jím zajišťovaných činností.

3.2 Co „informační nebo komunikační *systém*“ tvoří?

Společným vymezujícím prvkem „*informačního nebo komunikačního systému*“ je tedy služba. To však pro pochopení pojmu v celé jeho šíři nestačí – není totiž zřejmé, z čeho se daný informační nebo komunikační systém skládá, resp. co je těmi konkrétními aktivy, které podporují danou službu v požadované kvalitě.

Ani v případě pojmu „*komunikační systém*“, neexistuje zákonná definice, lze však ale konstatovat, že přestože existuje mnoho definic informačního nebo komunikačního systému, jen málo z nich se spokojí s označením informačního systému jako prostého výčtu technického nebo

[2] Tj. organizace si nepořizují, nevyvíjejí a neudržují systémy bez konkrétního cíle – systém má organizace vždy za určitým účelem, aby poskytoval organizaci určitou službu. Je tomu tak vždy, nehledě na to, zda je to služba pro interní nebo externí potřeby organizace, nebo zda byla správa systému organizaci uložena zákonem, nebo si jej organizace pořídila z vlastního rozhodnutí atd.

[3] *Vyhláška, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.*

programového vybavení, bez uvedení dalších prvků, jako např. procesů, informací, uživatelů apod.

Vyhláška o kybernetické bezpečnosti, která je prováděcím právním předpisem k zákonu o kybernetické bezpečnosti, stanovuje mimo jiné obsah a rozsah bezpečnostních opatření, které musí povinné orgány a osoby podle zákona zavést a provádět v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich určeného nebo identifikovaného systému. Tato bezpečnostní opatření se pak v rámci procesu daného vyhláškou vztahují k tzv. aktivům.

Vyhláška o kybernetické bezpečnosti tato aktiva definuje, přičemž je dělí na tzv. primární aktiva, kterými rozumí informace a služby, které systém zpracovává nebo poskytuje, a tzv. podpůrná aktiva, kterými se rozumí technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, a jejichž selhání může mít dopad na systém, a dále také zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti systému.

Vedle toho je potřeba zmínit, že k výše uvedenému může přispět také např. definice pojmu provozovatel informačního nebo komunikačního systému podle zákona o kybernetické bezpečnosti, která vztahuje naplnění definičních znaků provozovatele informačního nebo komunikačního systému k tomu, kdo zajišťuje funkčnost podpůrných aktiv tedy *„technických a programových prostředků tvořících určený nebo identifikovaný systém*“. I např. zde je tedy nutné mít na paměti, že kromě technických a programových prostředků tvoří tento *„systém*“ i jeho další, jiné, součásti jako např. objekty, zaměstnanci, dodavatelé apod.

Je tedy patrné, že pojem *„informační nebo komunikační systém“* je tvořen jak technickým a programovým vybavením a komunikačními prostředky,[4] **tak objekty, zaměstnanci a dodavateli, stejně tak jako informacemi, které systém zpracovává a službami (procesy), které určený nebo identifikovaný systém poskytuje** (důraz je kladen na službu, kterou je systém vymezen, nicméně součástí služby jako primárního aktiva je nutno chápat i s ní související „procesy“)**.**

Přestože legální definici informačního a komunikačního systému zákon o kybernetické bezpečnosti neobsahuje, lze ji analogicky interpretovat i obdobnými legálními definicemi obsaženými v právních předpisech České republiky.

„Informačním systémem veřejné správy (se rozumí) funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností. Informační činností (se

[4] Uvedeným technickým vybavením, komunikačními prostředky a programovým vybavením budou například aplikační software, virtualizační software, operační systémy, databáze, servery (aplikační, databázové atd.), firewally, všechny druhy koncových zařízení (pracovních stanice, ale také tiskárny, senzory, čidla apod.), stejně tak jako nosiče pro uchování dat nebo komunikační infrastruktura tvořená komunikačními kabely a kabeláží.

rozumí) získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů veřejné správy prostřednictvím technických a programových prostředků."[5]

„Informačním systémem nakládajícím s utajovanými informacemi se (…) rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací."[6]

„Komunikačním systémem nakládajícím s utajovanými informacemi se (…) rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy."[7]

Uvedené analogické definice potvrzují, že určený nebo identifikovaný systém se neskládá jen z technických a programových prostředků, ale jedná se o skutečně komplexní množinu různých vzájemně propojených částí.

3.3 Jaká je vazba mezi tím, co *„informační nebo komunikační systém"* vymezuje a co jej tvoří?

Jak již víme, *„informační nebo komunikační systém"* je vymezen službou a tvořen aktivy, a to jak technickým a programovým vybavením a komunikačními prostředky, objekty, zaměstnanci a dodavateli, stejně tak jako informacemi, které systém zpracovává a službami, které určený nebo identifikovaný systém poskytuje. Z výše uvedeného však zatím nevyplývá, která aktiva organizace danou službu podporují a která už ne, tj. jaký je vztah mezi vymezením „*informačního nebo komunikačního systému*" prostřednictvím služby a aktivy, ze kterých se může „*informační nebo komunikační systém*" skládat.

Vyhláška o kybernetické bezpečnosti k primárním aktivům uvádí, že se jedná o takové informace nebo služby, které zpracovává nebo poskytuje informační a komunikační systém. V případě podpůrných aktiv se jedná o technická aktiva, zaměstnance a dodavatele, podílející se na provozu, rozvoji, správě nebo bezpečnosti tohoto systému. U technických aktiv se pak blíže jedná o takové technické vybavení, komunikační prostředky a programové vybavení systému a objekty, ve kterých jsou systémy umístěny, jejichž selhání může mít dopad na systém.

[5] § 2 písm. b) a § 2 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy
[6] § 34 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací
[7] § 35 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací

S ohledem na výše uvedené je však potřeba konstatovat, že definice technického aktiva daná v § 2 písm. k) vyhlášky o kybernetické bezpečnosti, není na tomto místě dána zcela správně. Problematickou je prostřední část definice, která stanovuje, že se jedná o takové technické vybavení, komunikační prostředky a programové vybavení *„informačního a komunikačního systému*“ a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém. Problémem je, že technická aktiva je možné a mnohdy dokonce nutné identifikovat i nad rámec určeného nebo identifikovaného informačního nebo komunikačního systému, nikoliv pouze v rámci takového systému. Možnost identifikace podpůrných, tzn. i technických aktiv, nad rámec určeného nebo identifikovaného informačního nebo komunikačního systému je podmínkou při stanovování rozsahu ISMS.

Přestože se rozsahu ISMS věnuje blíže až následující kapitola, je pro potřeby pochopení informačního nebo komunikačního systému nutno už zde konstatovat, že opačný přístup by se neslučoval s ustanoveními vyhlášky o kybernetické bezpečnosti, dle kterých si povinná osoba stanoví rozsah ISMS, ve kterém určí organizační části a aktiva, jichž se ISMS týká, a následně pro takto stanovený rozsah ISMS zavede přiměřená bezpečnostní opatření.

Pokud by povinná osoba mohla stanovit rozsah ISMS v otázce technických aktiv pouze v rámci aktiv daných pro systém jako takový, stanovovala by rozsah ISMS, v rámci kterého bude následně zavádět bezpečnostní opatření, maximálně na tu množinu aktiv, z nichž se daný informační nebo komunikační systém skládá. Záměr daný vyhláškou byl přitom zcela zjevně opačný – stanovení rozsahu ISMS by mělo přinést povinné osobě možnost stanovit množinu aktiv, pro která bude zavádět bezpečnostní opatření tak, aby se jednalo minimálně o ta aktiva, která tvoří systém, a navíc ještě taková, která jsou potřeba, aby byla bezpečnost dostatečně zajištěna.

V tuto chvíli tedy můžeme přijmout, že existuje takové technické a programové vybavení, komunikační prostředky, objekty, zaměstnanci, dodavatelé, které jsou součástí systému, a takové, které jsou nad rámec toho součástí rozsahu ISMS stanoveného podle vyhlášky o kybernetické bezpečnosti. Jak ovšem poznat ta aktiva, která jsou součástí systému? Také jinak, která konkrétní aktiva jsou součástí systému, která aktiva jsou nad to pouze součástí rozsahu ISMS, a která aktiva v organizaci nejsou součástí ani systému, ani rozsahu ISMS.

V rámci otázky, jaká je vazba mezi tím, co „informační nebo komunikační systém“ vymezuje a co jej tvoří, se bude tedy jednat o taková aktiva [technické a programové vybavení, komunikační prostředky, objekty, zaměstnance, dodavatele, informace a služby(procesy)], které přímo podporují výkon předmětné služby v daném rozsahu a kvalitě.

Je potřeba mít na paměti, že v případě kritické informační infrastruktury by narušení fungování informačního nebo komunikačního systému mělo závažný dopad na službu pro kterou byl systém určen, tedy přeneseně na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. V případě významného informačního systému by došlo k ohrožení výkonu činnosti

orgánu veřejné moci a v případě informačního systému základní služby by došlo k omezení poskytování základní služby závislé na daném systému. Služba je funkční, pokud k těmto negativním jevům nedojde. Proto veškerá aktiva, tak jak jsou vyjmenována výše, která by mohla tyto negativní jevy způsobit, a to nejen samostatně, ale i v souhrnu, jsou a musí být součástí určeného nebo identifikovaného systému.

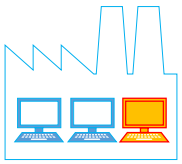
Jak je z výše uvedeného patrné, přestože je určený nebo identifikovaný informační nebo komunikační systém vždy vymezen službou, která se v průběhu času nemění, je to, co jej tvoří v čase neustále proměnné.

3.4 ISMS a stanovení jeho rozsahu

Zavedení ISMS patří mezi stěžejní organizační bezpečnostní opatření pro zajištění kybernetické bezpečnosti daného systému a jehož základ je upraven v § 3 vyhlášky o kybernetické bezpečnosti, přičemž jeho filozofie prostupuje celou vyhláškou.

Dle vyhlášky o kybernetické bezpečnosti je rozsah ISMS nutno stanovit dokumentovanou formou a s ohledem na požadavky dotčených stran a organizační bezpečnost. Smyslem stanovení rozsahu je určit organizační části a aktiva, jichž se ISMS týká, tedy fyzický perimetr, organizační celky, zainteresované osoby (zaměstnanci, dodavatelé a další) a technologie. Dokumentované stanovení rozsahu ISMS je nezbytné pro následnou přezkoumatelnost, případnou potřebu jeho rozšíření, či pro zajištění jeho jednotného výkladu v organizaci.

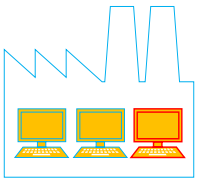
Pevně daným je specifický požadavek zákona o kybernetické bezpečnosti, reprezentován povinností povinné osoby zabezpečovat určený nebo identifikovaný systém spadající do působnosti zákona o kybernetické bezpečnosti. Tímto je dán minimální rozsah ISMS (viz Obrázek 1).



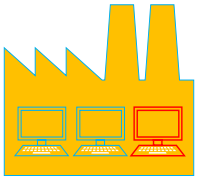
Obrázek 1: Hypoteticky možný minimální rozsah ISMS odpovídající rozsahu určeného informačního nebo komunikačního systému

Vedle nutnosti stanovit rozsah ISMS, má ale povinná osoba podle § 4 odst. 2 zákona o kybernetické bezpečnosti zavést ISMS (a další bezpečnostní opatření) **v rozsahu nezbytném pro zajištění kybernetické bezpečnosti** daného systému. Z toho vyplývá, že tato povinnost povede **k tomu, že povinná osoba v souladu s § 3 písm. a) vyhlášky o kybernetické bezpečnosti** zohlední požadavky dalších dotčených stran a požadavky organizační bezpečnosti, a **zvolí rozsah ISMS na větší část aktiv povinné osoby, než jsou aktiva určeného nebo identifikovaného**

systému (viz Obrázek 2). To pak může vést také k tomu, že do rozsahu ISMS zahrne všechna aktiva v organizaci (viz Obrázek 3).



Obrázek 2: Rozsah ISMS stanovený na určený informační nebo komunikační systém a aktiva, zajišťující zabezpečení jeho kybernetické bezpečnosti



Obrázek 3: Rozsah ISMS stanovený na celou organizaci

Z výše uvedené logiky lze také odvodit, že **pokud by povinná osoba stanovila rozsah ISMS na menší množinu aktiv, než která tvoří určený nebo identifikovaný systém, neměla by následně možnost dosáhnout požadavku § 4 odst. 2 zákona o kybernetické bezpečnosti a došlo by tak k jeho porušení.**

Jakmile povinná osoba stanoví rozsah ISMS, zavádí pro takto stanovený rozsah na základě cílů, bezpečnostních potřeb a hodnocení rizik přiměřená bezpečnostní opatření.

3.4.1 Ilustrační příklad možného stanovení rozsahu ISMS v organizaci

Nejmenovaná organizace spravující např. významný informační systém za účelem zajištění výkonu spisové služby, bude mít rozsah ISMS stanoven nejen na aktiva přímo související se zajištěním služby samotného výkonu spisové služby (např. servery), ale i na aktiva zajišťující např. zabezpečení serverovny. Rozsah ISMS bude tedy rozšířený o taková aktiva, která se na výkonu služby významného informačního systému přímo nepodílejí, nicméně jsou nezbytná pro zajištění její bezpečnosti v širším kontextu – pokud budou servery zabezpečené, ale do serverovny bude umožněn volný přístup, může dojít k úmyslnému či neúmyslnému přerušení poskytování služby např. vytržením přívodního kabelu elektrické energie při neopatrném pohybu v prostorách objektu. Rozsah ISMS tedy nebude stanoven na celou organizaci, ale pouze na nezbytná aktiva podílející se na zajištění výkonu uvedené spisové služby.

Při stanovení rozsahu ISMS je nezbytné neopomenout žádnou z kategorií podpůrných aktiv. U jakéhokoliv systému je tedy potřeba do rozsahu ISMS zahrnout, mimo aktiva přímo související se zajištěním funkčnosti konkrétního systému, i např. zaměstnance pracující s tímto systémem, nebo např. dodavatele, kteří zabezpečují jeho funkčnost, dodávají aktualizace či se podílí na jeho provozu.

Do rozsahu ISMS tedy zcela jistě spadají podpůrná aktiva typu lokality, zaměstnanci, dodavatelé a podpůrné technologie (např. dodávky energií, kamerový systém, systém řízení přístupu na základě např. čipových karet, EZS, helpdesk, detekční nástroje, systém pro monitoring sítě a další).

> Správné stanovení rozsahu ISMS je ve vztahu k systematickému zavádění bezpečnostních opatření dle vyhlášky o kybernetické bezpečnosti stěžejní (viz kapitola 2.1.2). Při stanovování rozsahu ISMS je potřeba určit organizační části a aktiva, jichž se ISMS týká a dále je nutno postupovat s ohledem na požadavky dotčených stran a organizační bezpečnost. Jedině takto bude zajištěno vhodné stanovení rozsahu ISMS a budou moct být implementována všechna bezpečnostní opatření vedoucí k zajištění kybernetické bezpečnosti určeného nebo identifikovaného informačního nebo komunikačního systému.

4 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: (WHITE)	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
31. května 2022	0.1	Odbor kontroly	Vytvoření dokumentu