NÚKIB

NEPŘIMĚŘENÉ NÁKLADY

vysvětlení pojmu

Verze 2.3, platná ke dni 22.12.2022

Obsah

Úvod

Tento dokument poskytuje možný výklad pojmu „přiměřenosti“, resp. nepřiměřenosti při zavádění bezpečnostních opatření z pohledu finančních nákladů, se kterým je možné se setkat ve vztahu k zavádění povinností ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“ nebo „ZKB“), resp. vyhlášky 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“). Jednotnou hodnotu nepřiměřených nákladů nelze jednoznačně určit pro všechny subjekty, neboť každý subjekt má hodnotu hranice nepřiměřených nákladů rozdílnou – vychází se přímo z konkrétní analýzy rizik daného subjektu.

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

E-mail: regulace@nukib.cz

Upozornění:

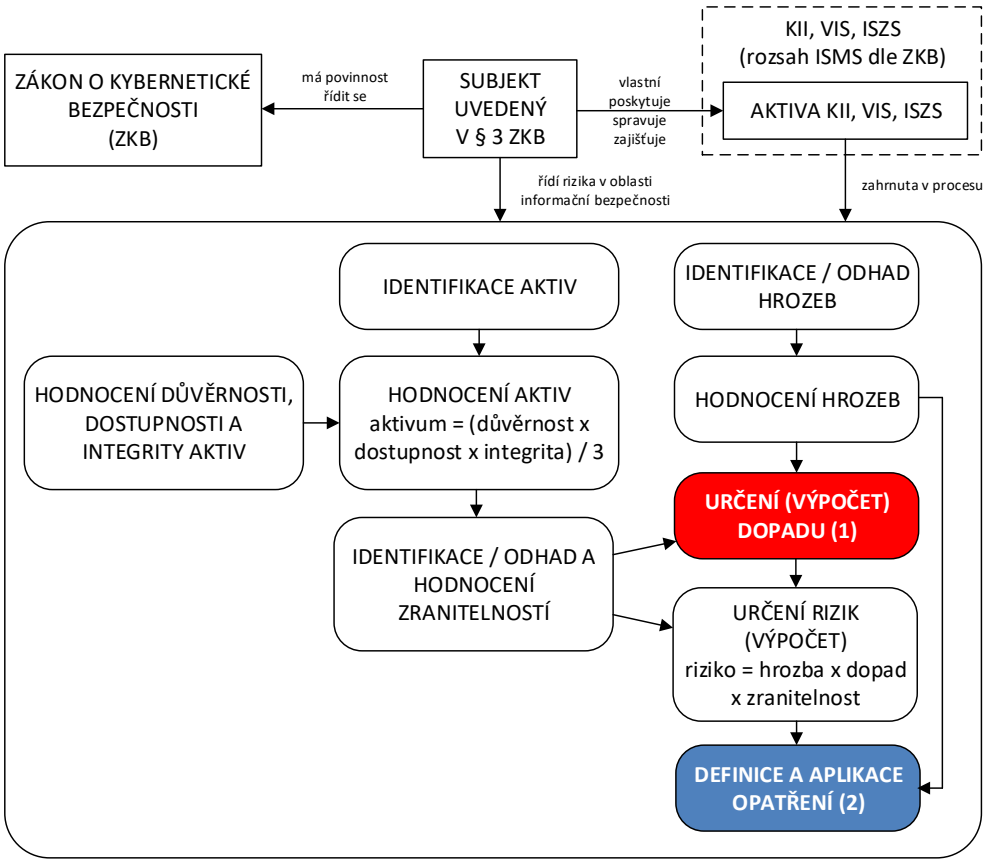
Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Nepřiměřené náklady

Při stanovování nákladů je nejprve důležité stanovit si rozsah systému řízení bezpečnosti informací (dále jen „ISMS“). To znamená zaměřit se jednak na ta aktiva, která jsou součástí kritické informační infrastruktury (dále jen „KII“), významného informačního systému (dále jen „VIS“), případně informačního systému základní služby (dále jen „ISZS“), jednak na aktiva, která sice nejsou součástí určeného systému, nicméně jejich ochrana je nezbytná pro zajištění bezpečnosti určeného systému. Pro jednotlivé správce a provozovatele informačních nebo komunikačních systémů, by to měl být snadný úkol, neboť právě oni by měli znát dokonale architekturu svých informačních a komunikačních technologií (dále jen „ICT“) a dokáží určit, který prvek (aktivum) ICT architektury do ISMS zahrnout a který nikoliv.[1]

Po stanovení rozsahu ISMS je nutno provádět proces řízení rizik, zahrnující analýzu rizik, kdy jsou mimo jiné zjištěny hodnoty důležitosti jednotlivých aktiv, hodnoty hrozeb, zranitelností a dopadů. Subjekt sám musí vědět, jaký případný dopad má daný účinek hrozby a zranitelnosti. Následně se určí výpočtem hodnota rizik a poté jsou definována opatření proti rizikům, kde rovněž musí konkrétní subjekt znát náklady jednotlivých opatření.

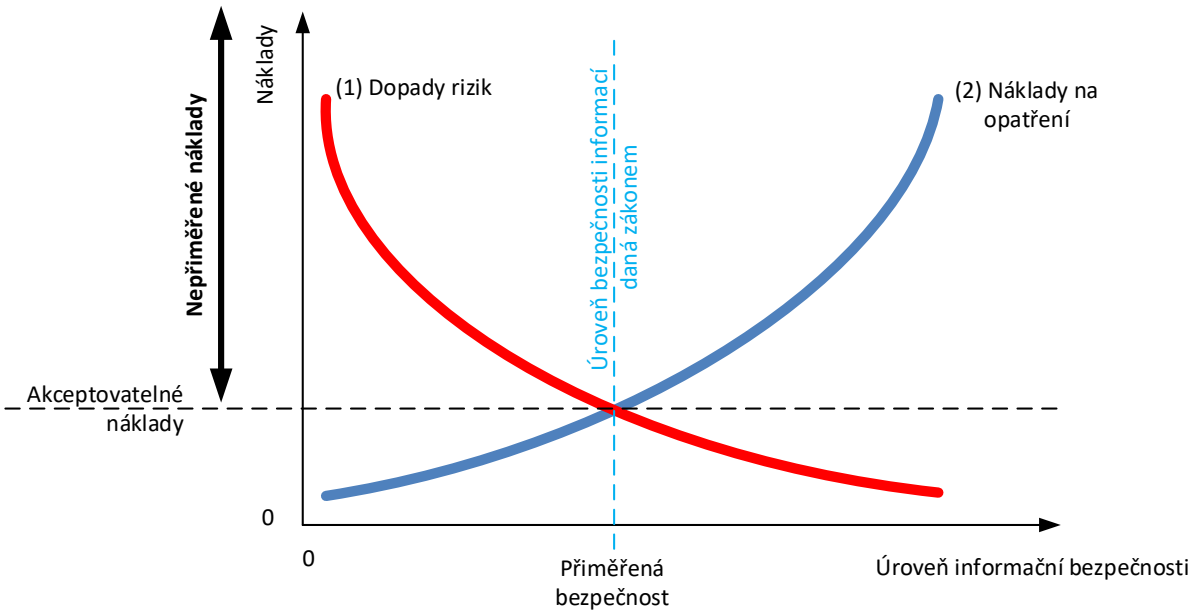
[1] V rámci kontrol dodržování zákona o kybernetické bezpečnosti bude docházet i ke kontrolám rozsahu ISMS.



Obrázek č. 1: Stanovení systému ISMS

Po provedení celkové analýzy rizik si následně subjekt promítne do grafu náklady (svislá osa) a úroveň informační bezpečnosti (vodorovná osa), kde vynáší křivku dopadu a křivku nákladů na opatření. Průnikem křivek dostane subjekt hodnotu přiměřené bezpečnosti a akceptovatelných nákladů.

Na následujícím obrázku je zachyceno odvození nepřiměřených nákladů. Vychází se z obecně známého grafu přiměřené bezpečnosti s tím, že zákon o kybernetické bezpečnosti zde hraje regulační roli a stanovuje minimální úroveň informační bezpečnosti.



Obrázek č. 2: Odvození nepřiměřených nákladů

1.1 Příklad č. 1

Představme si orgán veřejné moci, který je správcem informačního systému (dále jen „IS“). Náklady na pořízení tohoto IS činily 1.000.000 Kč. Z důvodu, že správce IS nedodržel doporučení dodavatele pro provoz systému a zároveň nedisponoval smlouvou o servisní podpoře, jejíž součástí jsou pravidelné aktualizace takového systému, se systém stává velmi zranitelným.

Zranitelnosti zneužil útočník, který získal pomocí SQL injection kontrolu nad celou databází IS, došlo k odcizení a následnému smazání dat z databáze serveru. Jelikož nebylo dodrženo technické doporučení dodavatele pro provoz IS, databáze nebyla redundantní a prostředí pro provoz IS mělo i další nedostatky. Poslední záloha dat byla starší 6 měsíců.

Správce IS se dostává do ztrát na úrovni nepřiměřených nákladů:

- První možností nápravy je zaplacení servisního poplatku na tento rok (z důvodu aktualizace systému a obnovení databáze do továrního stavu) a převedení veškerých záznamů z papírové podoby opět do systému, takovéto řešení je vyčísleno na 6.000.000 Kč.

- Druhou možností je zaplatit dodavateli IS servisní poplatek na tento rok za aktualizaci IS a za následné obnovení dat pomocí speciálních technologií (kompletní rekonstrukce IS), cena tohoto řešení činí 1.500.000 Kč.

Opatření proti tomuto riziku však bylo prosté – mít pravidelně aktualizovaný celý systém (servisní poplatky činí 156.000 Kč ročně) a dbát na doporučení dodavatele IS, s čímž souvisí dodatečné pořízení hardwarového a softwarového vybavení a přenastavení stávajících síťových aktivních prvků (zejména firewallů a routerů) a databázových oprávnění (zhruba 235.000 Kč).

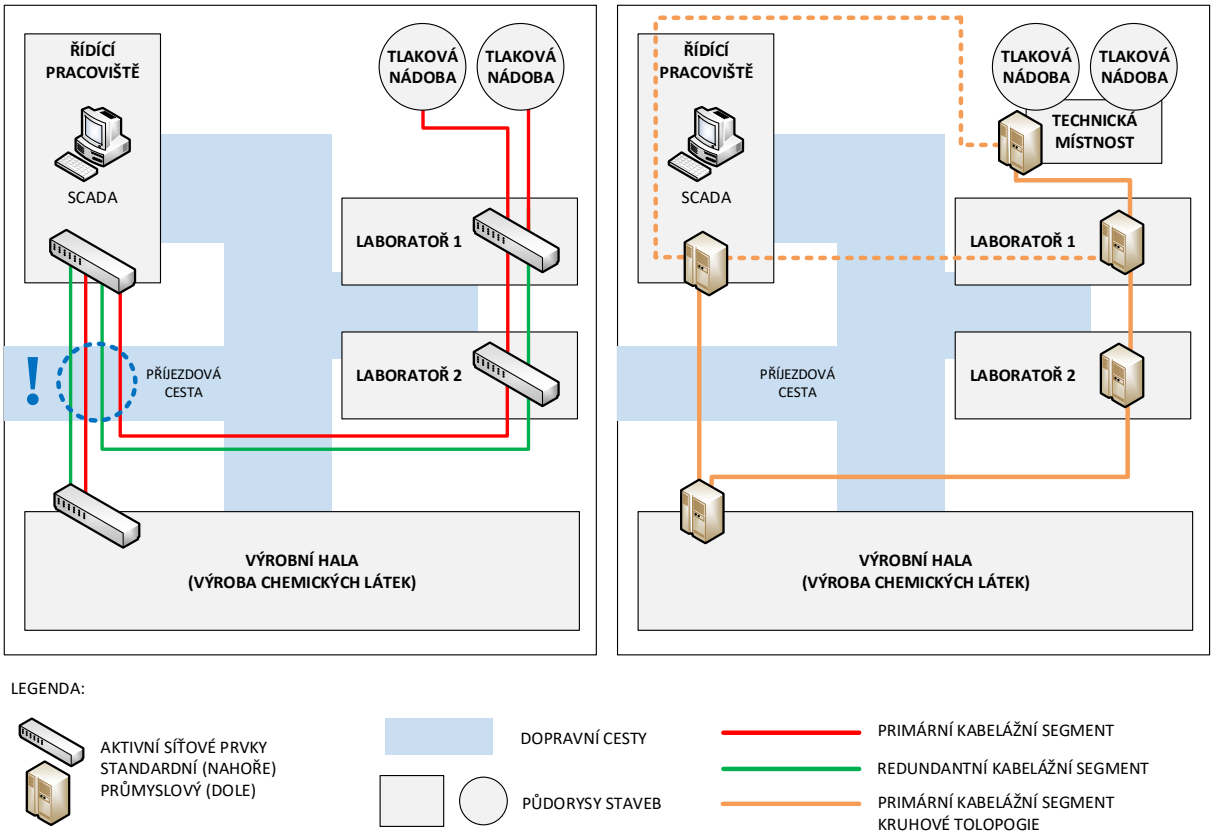
1.2 Příklad č. 2

Tento příklad je velmi zjednodušený. Představme si síť chemických továren (společnost), která se chystá vybudovat novou chemickou továrnu na svém pozemku za městem. Na obrázku č. 3 vlevo je prvotní návrh síťové topologie, který kopíruje topologii jiné továrny této společnosti v jiné zemi. V tomto případě uvažujeme, že taková továrna bude prvkem kritické infrastruktury, neboť součástí továrny jsou velké zásobníky zemního plynu. Vedení továrny se musí řídit zákonem o kybernetické bezpečnosti.

V prvotním projektovém návrhu jsou použity standardní síťové aktivní prvky, a navíc je zde viditelná další zranitelnost, a to zejména v místě, kdy veškerá kabeláž prochází takřka jedním bodem v zemi pod příjezdovou cestou. Z toho nám vyplývá hrozba přerušení kabelážních segmentů, které spojují SCADA systém s laboratořemi a výrobní halou, obsahující jednotlivé řízené stroje na výrobu chemikálií (RTU jednotky). Riziko by mohlo způsobit značný

ekonomický dopad pro společnost (přímé ztráty, sankce za ohrožení veřejnosti), ale zejména by mohlo mít nepříznivý vliv na zdraví občanů nedalekého města (nepřiměřené náklady).

Naštěstí je celý projekt v přípravné fázi, a proto je možné jej přehodnotit, aniž by společnost vynaložila dodatečné náklady na restrukturalizaci síťové infrastruktury. Na obrázku č. 3 vpravo je nový návrh projektu, kde se počítá s použitím průmyslových síťových aktivních prvků, které jsou do tohoto prostředí přímo určeny, v topologii kruhu. Díky zdokonalené funkci RSTP těchto aktivních prvků je dosaženo redundance a doba výpadku komunikace v případě přerušení jedné z tras je snížena na minimum. Aplikace takového opatření nám navýší původní rozpočet na ICT infrastrukturu továrny o 12 %, zároveň nám sníží riziko ze stupně „kritické“ na stupeň „nízké“.



Obrázek č. 3: Půdorysné schéma síťové topologie chemické továrny, bez přihlédnutí k rizikům (vlevo) a s přihlédnutím k rizikům (vpravo) – aplikace opatření

2 Seznam zkratek

ICS	Industrial Control Systém (průmyslový řídící systém)
ICT	informační a komunikační technologie
ISMS	Information Security Management Systém (systém řízení bezpečnosti informací)
ISZS	informační systém základní služby
KII	kritická informační infrastruktura
RSTP	Rapid Spanning Tree Protocol
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition (≈ dispečerské řízení a sběr dat)
SQL	Structured Query Language
VIS	významný informační systém

3 Použité zdroje

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

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)

ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 74s.

ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. 52s.

ONDRÁK, V., SEDLÁK, P., MAZÁLEK, V., *Problematika ISMS v manažerské informatice.* Brno: Akademie nakladatelství CERM, 2013. ISBN 978-80-7204872-4.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
2015	1.0	NCKB	Vytvoření dokumentu
12. 11. 2018	2.0	Odb. regulace	Grafická i textová revize dokumentu
28. 1. 2019	2.1	Odb. regulace	Změna kontaktních údajů
1. 10. 2020	2.2	Odb. regulace	Revize dokumentu
22. 12. 2022	2.3	Odb. regulace	Změna kontaktních údajů a revize dokumentu