Problematika kybernetické bezpečnosti

Řízení rizik bezpečnosti informací

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

22. listopadu 2022, Brno
TLP: GREEN

Pavla Jelečková, Jan Srnec
Odbor kontroly

Národní úřad pro kybernetickou a informační bezpečnost

- **Činnosti NÚKIB**
- Odbor kontroly

NÚKIB

- Vznikl na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
- **Správní orgán pro:**
  - **Kybernetickou bezpečnost**
  - **Ochranu utajovaných informací pro oblasti informačních a komunikačních systémů**
  - **Kryptografickou ochranu**
  - **Problematiku veřejně regulované služby navigačního systému Galileo**

- Vybrané činnosti v oblasti kybernetické bezpečnosti:
  - Určování povinných osob podle ZKB
  - Provádění kontrol dodržování ZKB
  - Provozování Vládního CERT České republiky (GovCERT.cz)
  - Spolupráce s ostatními CERT a CSIRT týmy v ČR i ve světě
  - Příprava zákonů a prováděcích vyhlášek, národních bezpečnostních standardů
  - Osvěta a podpora vzdělávání
  - Příprava a koordinace kybernetických cvičení jak v ČR, tak ve světě
  - Vytyčování národní strategie kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

- Další činnosti:
  - Výkon tzv. příslušného orgánu PRS (Competent PRS Authority), jehož hlavním úkolem je implementace služby PRS navigačního systému Galileo v ČR
  - Bezpečnostní správa provozu služby PRS navigačního systému Galileo
  - Výzkum a vývoj v oblasti šifrování
  - Stanovování ochrany utajovaných informací v oblasti informačních a komunikačních systémů

https://www.nukib.cz/cs/o-nukib/kariera/

VOLNÉ POZICE:

ODBOR BEZPEČNOSTI

- Vedoucí oddělení fyzické bezpečnosti
- Security specialista – analytik / referent odboru bezpečnosti

ODBOR BEZPEČNOSTI INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ:

- Pracovník certifikace kryptografických prostředků - technik
- Pracovník vývoje kryptografických prostředků - specialista vývoje a aplikované kryptografie

ODBOR VLÁDNÍ CERT:

- Analytik síťového provozu
- Forenzní analytik
- Bezpečnostní analytik/analytička
- Koordinační, projektový pracovník CERT
- Incident handler
- Koordinátor penetračních testů/skenů zranitelností

ODBOR KONTROLY:

- Technický specialista informační/kybernetické bezpečnosti

ODBOR INFORMAČNÍCH TECHNOLOGIÍ:

- Administrátor aplikačních systémů
- Security specialista- správce
- Security specialista- analytik
- Klientská podpora-správa IT

ODBOR PRS

- Právní referent bezpečnosti státu – Národní centrum PRS

SEKCE STRATEGICKÝCH AGEND A SPOLUPRÁCE

- Asistent/asistentka odboru

Národní úřad pro kybernetickou a informační bezpečnost

- Činnosti NÚKIB
- **Odbor kontroly**

NÚKIB – Odbor kontroly

Historie

- 2015 vznik pracovní skupiny regulace a auditu
- 2016 vznik oddělení regulace auditu a podpory
- 2018 vznik odboru regulace auditu a kontroly
- 2019 vznik oddělení kontroly
- 2020 vznik odboru kontroly
- -> 2023 stálý růst počtu zaměstnanců

Činnosti Odboru kontroly

- Kontrola v oblasti kybernetické bezpečnosti (u povinných subjektů)
- Metodická podpora v oblasti KB
- „Konzultační a poradenská činnost“ v oblasti kybernetické bezpečnosti pro regulované subjekty
- Provádění interního auditu kybernetické bezpečnosti NÚKIB
- Legislativní, publikační a přednášková činnost
- Další spolupráce napříč NÚKIB

Problematika kybernetické bezpečnosti

- **Normy řady ISO/IEC 27K**
- ISMS

Řada norem ISO/IEC 27k

- Normy specifikující požadavky
  - **ISO/IEC 27000 – Přehled a slovník**
  - **ISO/IEC 27001 – Požadavky**
  - ISO/IEC 27006 – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

- Normy popisující obecné směrnice
  - **ISO/IEC 27002 – Soubor postupů pro opatření bezpečnosti informací**
  - ISO/IEC 27003 – Směrnice pro implementaci systému řízení bezpečnosti informací
  - ISO/IEC 27004 – Měření
  - **ISO/IEC 27005 – Řízení rizik bezpečnosti informací**
  - ISO/IEC 27007 – Směrnice pro audit systém řízení bezpečnosti informací
  - ISO/IEC 27008 – Směrnice pro auditory kontrolních opatření bezpečnosti informací
  - ISO/IEC 27013 – Pokyny pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 2000-1
  - ISO/IEC 20014 – Správa a řízení bezpečnosti informací
  - ISO/IEC TR 27016 – Organizační ekonomika

Řada norem ISO/IEC 27k

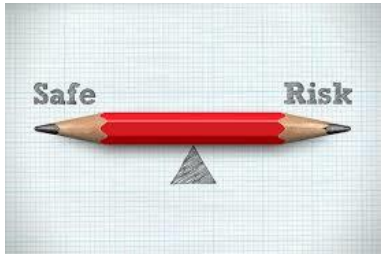
- Normy specifické pro jednotlivá odvětví
  - ISO/IEC 27009 – Požadavky používání ISO/IEC 27 001 ve specifických odvětvích
  - ISO/IEC 27031 - Bezpečnostní techniky - Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace
  - ISO/IEC 27032 - Směrnice pro kybernetickou bezpečnost
  - ISO/IEC 27033-1…6 - Bezpečnost sítě
  - ISO/IEC 27034-1, 2 & 6 - Bezpečnost aplikací
  - ISO/IEC 27035-1 & 2 - Řízení incidentů bezpečnosti informací
  - ISO/IEC 27036-1…4 – Řízení bezpečnosti v dodavatelských vztazích
  - ISO/IEC 27038 - Specifikace pro digitální zpracování dokumentů
  - ISO IEC 27039 - Selection, deployment and operation of intrusion detection [and prevention] systems (IDPS)
  - ISO/IEC 27040 - Storage security
  - ISO/IEC 27041 - Guidance on assuring suitability and adequacy of incident investigative methods
  - ISO/IEC 27042 - Guidelines for the analysis and interpretation of digital evidence
  - ISO/IEC 27043 - Incident investigation principles and processes
  - ISO/IEC 27050 - Electronic discovery

Problematika kybernetické bezpečnosti

- Normy řady ISO/IEC 27K
- **ISMS**

Systém řízení bezpečnosti informací

- **ISMS – „Information Security Management System“**
- ISMS dle řady norem ISO/IEC 27k:
  - **Systematický přístup** k ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací
  - Systematický přístup dosahování cílů organizace
  - Politiky, postupy, směrnice, které organizace řídí, aby zajistila ochranu informačních aktiv
  - **Založený na posuzování rizik**

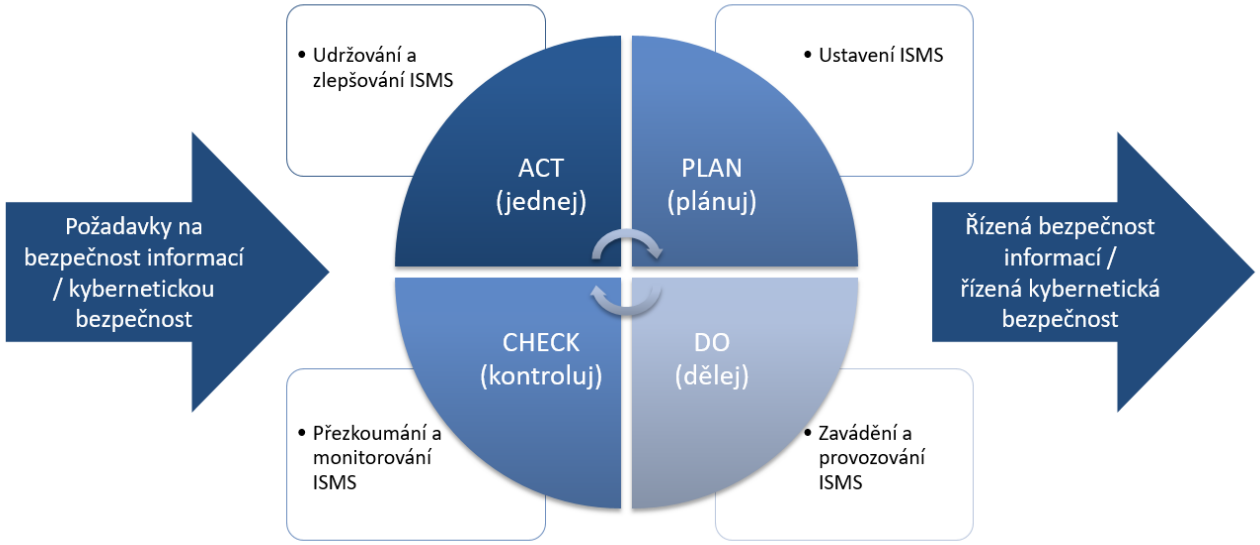


  - Použitelný a aplikovatelný ve všech organizacích bez ohledu na jejich velikost, typ a povahu činností
  - „Best practice“ postup pro efektivní systém řízení bezpečnosti informací v organizaci

- ISMS podle VKB (jedno z organizačních opatření)
  - *„část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat“*

Systém řízení bezpečnosti informací

- Založený na PDCA cyklu



Systém řízení bezpečnosti informací

- Požadavky pro správné zavedení a udržování ISMS v organizaci podle ISO/IEC 27001

Klíčové faktory implementace ISMS

- Nastavení politiky bezpečnosti informací, cílů a činností spojených s cíli
- Viditelná podpora a závazek všech stupňů vedení
- **Aplikace řízení rizik bezpečnosti informací**
- Budování povědomí o bezpečnosti
- Nastavení procesu řízení incidentů
- Zavedení procesu řízení kontinuity činnosti organizace
- Zavedení systému měření pro vyhodnocení výkonnosti bezpečnosti informací

Systém řízení bezpečnosti informací

- **„K čemu nám to bude?“**
- **Úspěšné zavedení ISMS** v organizaci **umožňuje**:
  - Zajistit, že informační aktiva jsou adekvátně chráněna před hrozbami
  - Udržovat strukturovaný komplexní rámec pro:
    - Identifikování a posuzování rizik bezpečnosti informací
    - Výběr a implementaci použitelných opatření
    - Pro měření jejich efektivnosti
  - Neustále zlepšovat prostředí
  - Snížení rizik bezpečnosti informací (snížení pravděpodobnosti incidentů)
  - Zvýšení důvěry v organizaci

Problematika kybernetické bezpečnosti

- **ČSN ISO/IEC 27005 – řízení rizik bezpečnosti informací**

Obsah prezentace

- **Základní charakteristika**
- **Standardy pro řízení rizik**
- **Terminologie**
- **Struktura normy**
  - Proces řízení
  - Stanovení rámce
  - Posouzení rizika
  - Ošetření rizika
  - Akceptace rizika
  - Komunikace rizika
  - Monitorování a přezkoumání rizika

Základní charakteristika normy ISO/IEC 27005

- **Doporučení pro řízení rizik bezpečnosti informací**
- **Nejedná se o konkrétní metodiku**
- **Přístup založen na metodě identifikace rizika aktiv, hrozeb a zranitelností**
- **Univerzální – pro všechny typy organizací**
- **Může být aplikováno na:**
  - Organizaci jako celek
  - Každou samotnou část organizace (např. oddělení, fyzické místo,…)
  - Jakýkoliv informační systém

Základní charakteristika normy ISO/IEC 27005

- **Normy řady ISO/IEC 27xxx vychází od roku 2005**
- **ISO/IEC 27005 - aktuálně 3. vydání**
  - 2008, 2011, 2018
- **Český překlad - ČSN ISO/IEC 27005**
  - 2009, 2013, 2019

Terminologie

- **Riziko -** pravděpodobnost vzniku ztráty
- **Identifikace rizika -** proces hledání, rozpoznání a popsání rizika
- **Vlastník rizika -** ten, kdo je za riziko odpovědný a je oprávněný ho řídit
- **Analýza rizik -** proces pochopení podstaty rizika a stanovení jeho úrovně
- **Řízení rizik -** proces systematického uplatňování politik, řízení a postupů pro analyzování, hodnocení, ošetřování, monitorování a přezkoumávání rizika

Terminologie

- **Hodnocení rizik -** proces porovnání
- **Úroveň rizika -** velikost rizika vyjádřená jako kombinace následků a pravděpodobnosti jejich výskytu
- **Zvládání rizik -** proces modifikace rizika
- **Zbytkové riziko -** riziko, zbývající po ošetření rizik
- **Opatření -** prostředek řízení, který modifikuje riziko

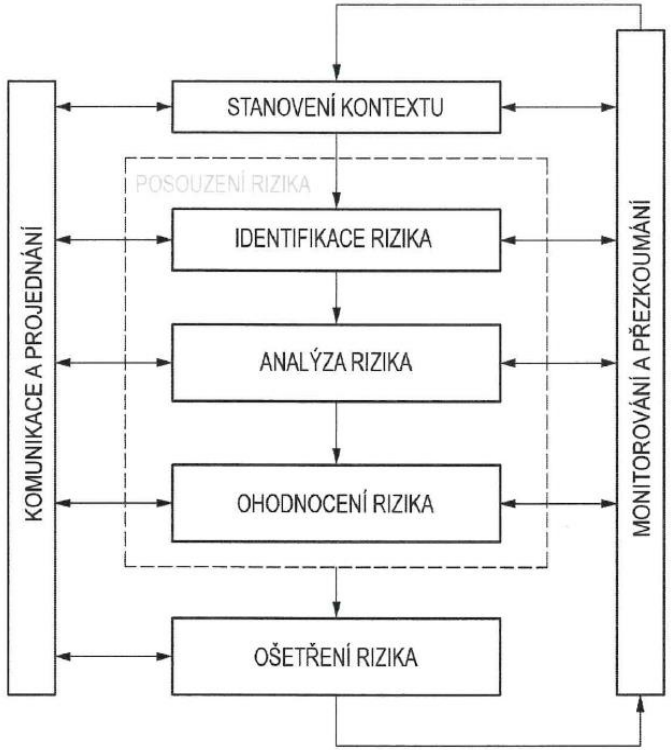
Struktura normy - přílohy

- **A – definuje rozsah a mezní hodnoty**
- **B – identifikace a ocenění aktiv a posouzení dopadu**
- **C – příklady typických hrozeb**
- **D – zranitelnosti a metody pro jejich posouzení**
- **E – příklady přístupů k posouzení rizik**
- **F – omezení pro modifikace rizika**

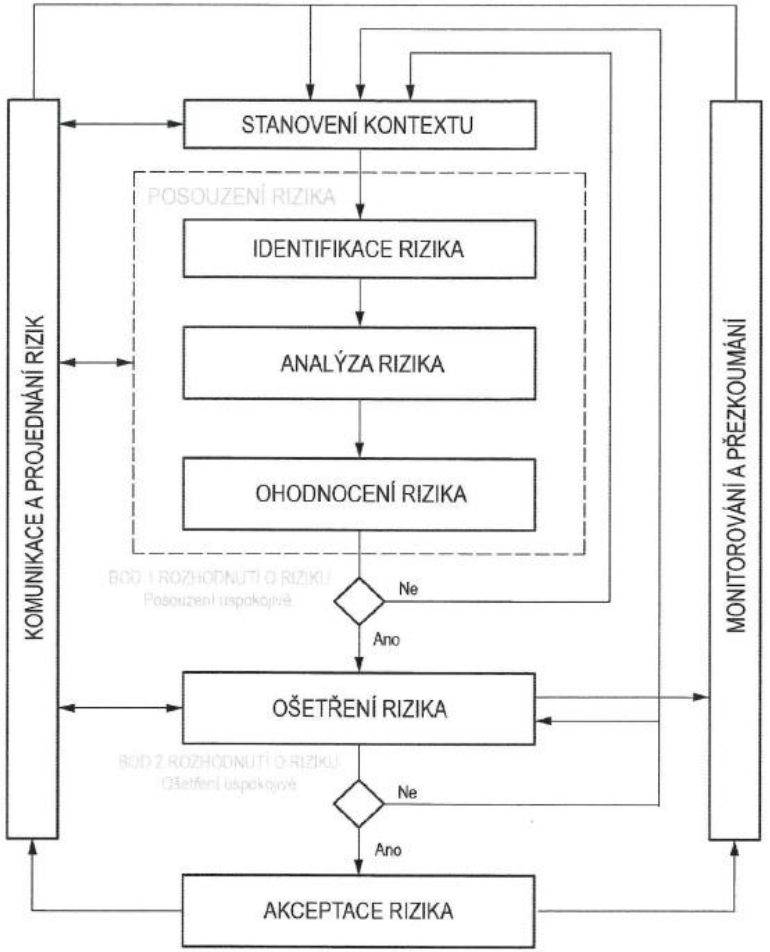
Proces řízení rizik

proces řízení rizik x proces řízení rizik bezpečnosti informací

dle ISO 31000



dle ISO/IEC 27005



Stanovení rámce podle ISO 27001

Rozsah a mezní hodnoty

- Strategické cíle organizace a její strategie a politiky
- Politika bezpečnosti informací organizace
- Celkový přístup k řízení rizik
- Informační aktiva
- Omezení ovlivňující organizaci
- …

Organizace řízení rizik bezpečnosti informací

- Vývoj procesu řízení rizik
- Identifikace a analýza zúčastněných stran
- Definice rolí a odpovědností
- Definice způsobu eskalace rozhodnutí
- …

Stanovení rámce podle ISO 27001

Vstup

- Všechny relevantní informace o organizaci

Výstup

- Specifikace základních kritérií, rozsah a mezní hodnoty a organizace pro proces řízení rizik

Stanovení účelu řízení rizik

- Podpora ISMS, právní shoda, příprava plánu kontinuity,…

Základní kritéria

- Přístup k řízení rizik
- Kritéria hodnocení rizika
- Kritéria dopadu
- Kritéria akceptace rizika

Jak to může prakticky vypadat

- Riziko = hrozba * zranitelnost * dopad
- Riziko = dopad * pravděpodobnost hrozby
- Příp. jiná metoda

- Kritéria akceptace rizika

		Míra dopadu				
		1	2	3	4	5
Míra pravděpodobnosti	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Posouzení rizika

Vstup

- Základní kritéria, rozsah a mezní hodnoty a ustavená organizace pro proces řízení rizik bezpečnosti informací

Výstup

- Seznam posouzených rizik preferovaných dle kritérií pro hodnocení rizika

Identifikování rizik, kvantifikování nebo kvalitativní popsání, stanovení priorit ve vztahu k hodnotícím kritériím rizika cílům relevantním pro organizaci.

Posouzení rizika se skládá z:

- Identifikace rizika
- Analýzy rizika
- Hodnocení rizika

Posouzení rizika

Identifikace rizika

- Identifikace aktiv
- Identifikace hrozeb
- Identifikace existujících opatření
- Identifikace zranitelností
- Identifikace následků

Analýza rizika

- Metodiky analýzy rizika (kvalitativní/kvantitativní)
- Posouzení následků
- Posouzení pravděpodobnosti incidentu
- Určení úrovně rizika

Hodnocení rizika

- Využití znalosti o riziku získané jeho analýzou

Jak to může prakticky vypadat

Aktivum	Hodnota dopadu - důvěrnost	Hodnota dopadu - dostupnost	Hodnota dopadu - integrita	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - důvěrnost	Hodnota rizika - dostupnost	Hodnota rizika - integrita
Aplikační server (HW)	2	3	3	Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů	4	Poškození nebo selhání technického nebo programového vybavení	3	24	36	36
Webový server (HW)	1	2	3	Nedostatečná údržba aktiv	3	Působení škodlivého kódu (například viry, spyware, trojské koně)	4	12	32	48

Posouzení rizika

Vstup

- Seznam rizik preferovaných dle kritérií

Výstup

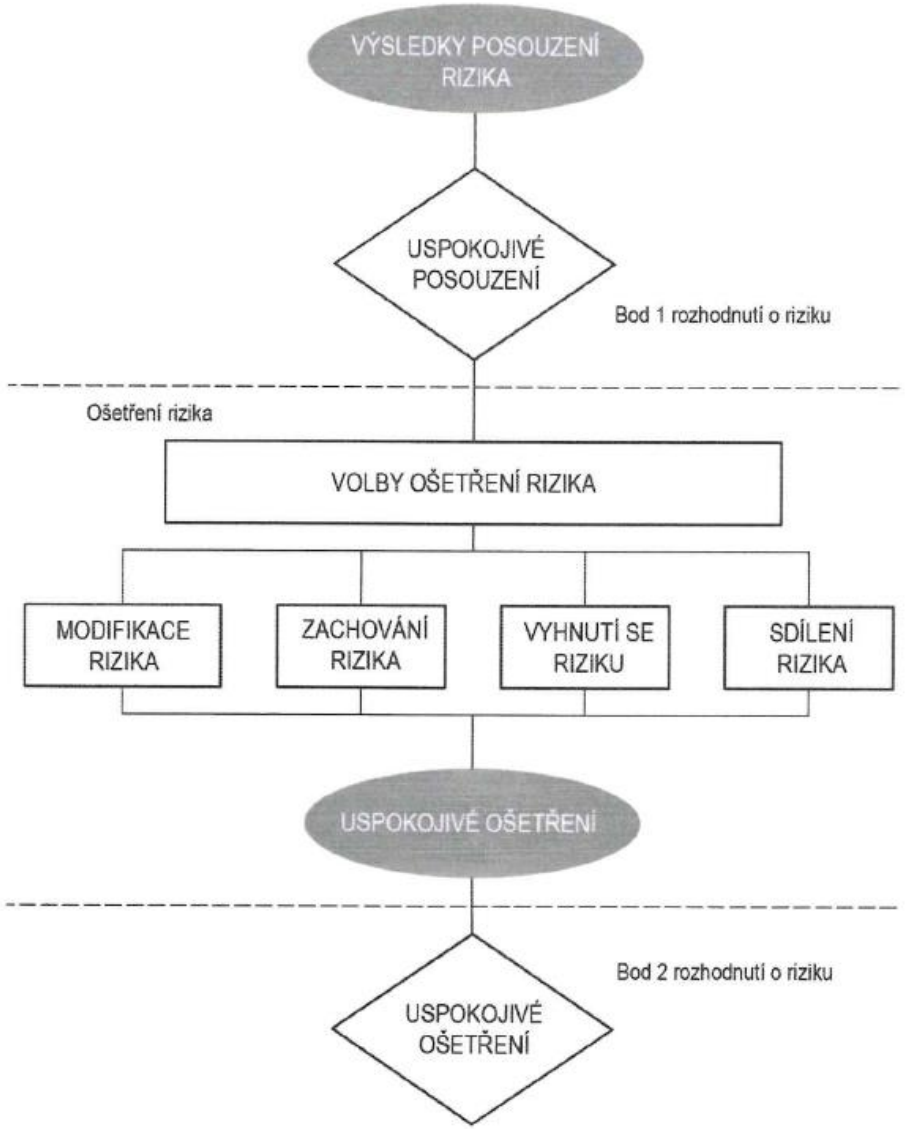
- Plán ošetření rizika, přijetí zbytkových rizik manažery organizace

Výběr opatření ke snížení, zachování, vyhnutí se nebo sdílení rizika, definice plánu ošetření rizika.

Ošetření rizika

- Modifikace rizika
- Zachování rizika
- Vyhnutí se riziku
- Sdílení rizika

Ošetření rizika



Akceptace rizika

Vstup

- Plán ošetření rizika a posouzení zbytkového rizika

Výstup

- Seznam akceptovaných rizik s oprávněním těch, která nesplňují obvyklá kritéria pro akceptaci

Rozhodnutí a oficiální zaznamenání rozhodnutí akceptovat rizika včetně odpovědnosti za tyto rozhodnutí.

Komunikace a konzultace rizika

Vstup

- Všechny informace o riziku obdržené od činností řízení rizik

Výstup

- Trvalé porozumění procesu řízení rizik organizace a výsledky

Sdílení informací mezi osobami přijímajícími rozhodnutí a dalšími zainteresovanými stranami.

Monitorování a přezkoumání rizika

Vstup

- Všechny informace o riziku obdržené od činností řízení rizik

Výstup

- Trvalé propojení řízení rizik s cíli organizace a s kritérii akceptace rizika

Rizika nejsou statická – nutné je neustálé monitorování a přezkoumávání.

Monitorování a přezkoumání rizika

- Monitorování a přezkoumání faktorů rizika
- Monitorování, přezkoumání a zlepšování řízení rizik

ISO/IEC 27005:2018 – Přílohy

- **Přílohy mají informativní charakter**
- **Nejedná se o konečný výčet**
- **Návrh možností, ilustračních příkladů a možných situací**
- **Nutno brát v potaz pouze to, co je relevantní pro organizaci**

Příloha A

Analýza organizace

- Ohodnocení organizace
- Hlavní smysl, strategie, poslání, hodnoty či podnikatelská činnost organizace
- Struktura organizace – divizní, funkční, maticová

Seznam omezení ovlivňující organizaci

- Politická
- Strategická
- Územní
- Funkční

Seznam omezení ovlivňující rozsah působnosti

- Finanční
- Technická
- Environmentální

Příloha B

Příklady identifikace aktiv

- Primární aktiva – informace a procesy
- Podpůrná aktiva – hardware, software, zaměstnanci

Ocenění aktiv

- Kritéria
- Zredukování na obecný základ
- Měřítko
- Závislosti
- Výstup

Posouzení dopadu

- Přímý – náklady na získání, konfiguraci a instalaci nového aktiva
- Nepřímý – náklady na přerušené operace, porušení zákonných či regulatorních povinností

Příloha C

Příklady typických hrozeb

- Úmyslné, náhodné nebo environmentální

Typ	Hrozba
Přírodní událost	Záplavy
	Meteorologické jevy
Fyzická škoda	Požár
	Prach, koroze, zamrznutí
Ohrožení informací	Odposlouchávání
	Krádež zařízení či médií
Technické selhání	Nefunkčnost zařízení či softwaru
Neoprávněná činnost	Poškození dat
	Neoprávněné použití zařízení
Ohrožení funkcí	Chyba při použití
	Zneužití práv
	Odmítnutí činnosti

Příloha C

Zvláštní kategorie - zdroje lidských hrozeb

Původ hrozby	Motivace	Možné následky
Hacker, cracker	Výzva, revolta, peníze	Sociální inženýrství
		Neoprávněný přístup do systému
Terorista	Vydírání, zneužití, zničení, politický zisk	Systémový útok
		Proniknutí do systému
Průmyslová špionáž	Konkurenční výhoda, hospodářská špionáž	Politická výhoda
		Krádež informací
		Obranná výhoda
		Zasahování do osobního soukromí
Nespokojený / nedbalý zaměstnanec	Ego, peněžní zisk, pomsta, špionáž	Zneužití počítače
		Podvod a krádež
		Škodlivý kód
		Sabotáž systému

Příloha D

- **Příklady zranitelností**
- **Metody pro posouzení technických zranitelností**

Typ	Příklady zranitelností	Příklady hrozeb
Hardware	Nedostatečná údržba	Prolomení informačního systému
	Nechráněné uložení	Krádež médií nebo dokumentů
Software	Chybné přidělení přístupových práv	Zneužití práv
	Špatné řízení a správa hesel	Padělání práv
Síť	Nechráněný citlivý provoz	Odposlouchávání
	Špatná kabeláž spojů	Selhání telekomunikačního zařízení
Lokalita	Nedostatek fyzické ochrany budov	Krádež, neoprávněný přístup
Zaměstnanci	Nedostatečné bezpečnostní proškolení	Chyba v použití
	Nedostatek monitorovacích mechanizmů	Nezákonné zpracování dat
Organizace	Nedostatek pravidelných auditů	Zneužití práv
	Nedostatek pravidelného přezkoumání managementem	Neoprávněné použití zařízení

Příloha E

- **Posouzení rizika na obecné úrovni**
- **Podrobné posouzení rizika**

Příloha F

Omezení pro modifikaci rizika

- Časová
- Finanční
- Technická
- Provozní
- Kulturní
- Etická
- Omezení prostředí
- Personální omezení
- Omezení v začlenění nových a existujících opatření

Děkujeme za pozornost

Zdroje

- ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník
- ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky
- ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
- ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací
- ČSN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací
- ČSN ISO/IEC 27 033-2: Informační technologie – Bezpečnostní techniky - Směrnice pro návrh a implementaci bezpečnosti sítě
- Jirásek P., Novák L., Požár J., Výkladový slovník 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)

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.

Pavla Jelečková, Jan Srnec

Odbor kontroly, oddělení kontroly 2

Email: p.jeleckova@nukib.cz, j.srnec@nukib.cz