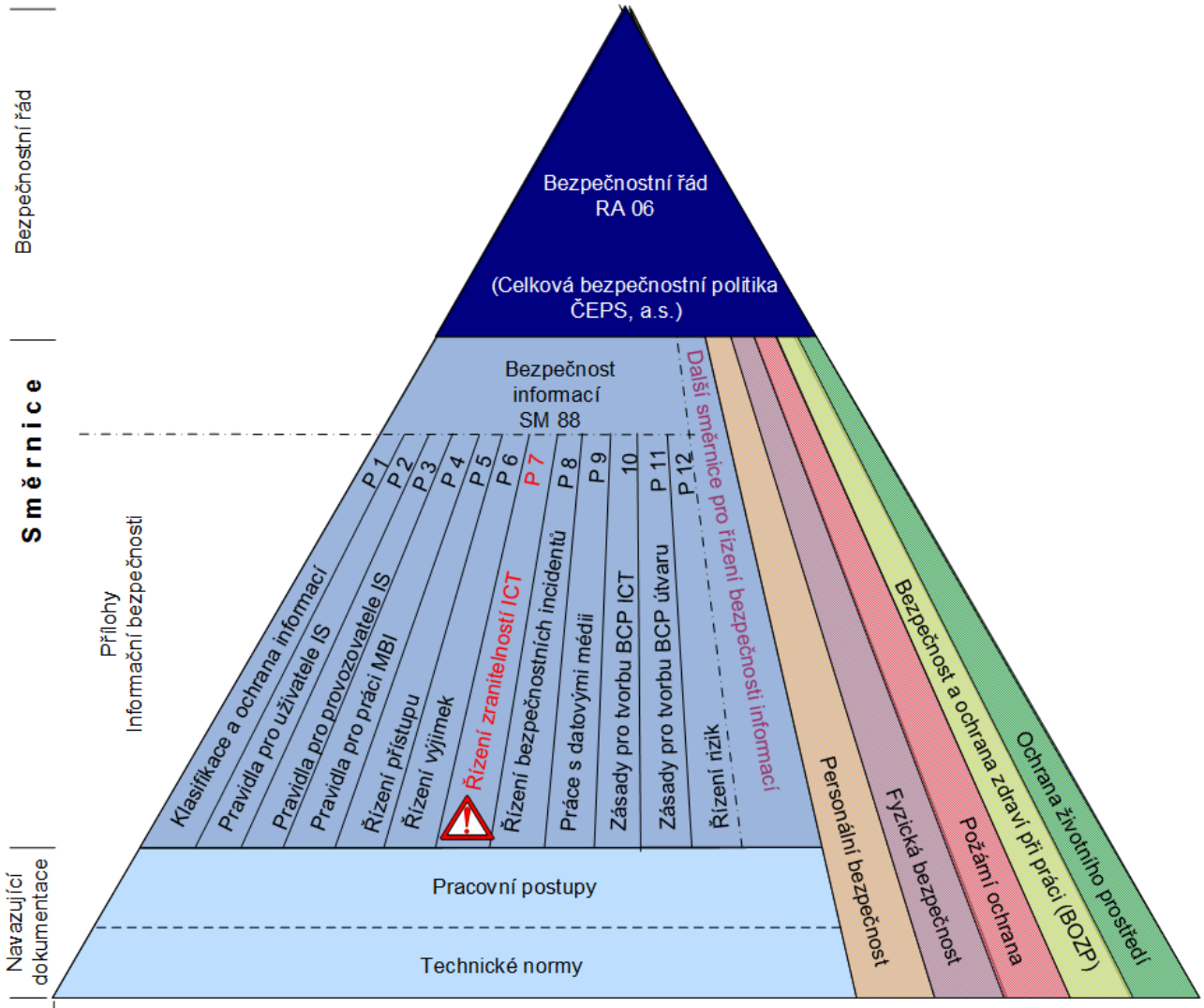
ŘÍZENÍ ZRANITELNOSTÍ ICT

Zařazení a působnost ve struktuře bezpečnostní dokumentace



dokument / působnost	Klasifikace a ochrana informací	Pravidla pro uživatele IS	Pravidla pro provozovatele IS	Pravidla pro práci MBI	Řízení přístupu	Řízení výjimek	Řízení zranitelností ICT	Řízení bezp. incidentů	Práce s datovými médii	Zásady pro tvorbu BCP ICT	Zásady pro tvorbu BCP útvaru	Řízení rizik
uživatel IS	X	X										
provozovatel IS	X	X	X	X	X		X	X	X	X		X
MBI	X	X		X	X	X	X	X	X	X	X	X
vedoucí útvaru	X	X									X	X
personalista	X	X			X							
externí subjekt	X	X	X*)		X*)							

*) *Platí pro externí subjekty v roli správců/administrátorů/vývojářů IS*

Pozn.: Uvedené názvy nejsou přesnými názvy příloh.

OBSAH:

1 ÚČEL, PŮSOBNOST A ODPOVĚDNOST

Dokument *Řízení zranitelností ICT* je samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88“), která stanovuje základní principy, pravidla a požadavky bezpečnosti informací. Tato příloha určuje pravidla, jejichž cílem je snížení bezpečnostních rizik, vyplývajících z neošetřených zranitelností, které jsou obsaženy v prostředcích ICT typu: operační systémy, „krabicové“ programové vybavení, databázové systémy, webové servery, firewally, aktivní síťové prvky apod.

Proces řízení zranitelností ICT produktů definovaný touto přílohou má platnost v rámci úseku *Dispečerské řízení a ICT* a *Provoz a údržba*.

1.1 Role, odpovědnosti a pravomoci

Odpovědný administrátor je zaměstnanec pověřený provozovatelem IS správou a provozem svěřených prostředků ICT:

- podílí se na základě analýzy rizik na roztřídění a určení kritičnosti systémů ICT,
- provádí identifikaci zranitelností a audity konfigurace dle provozních potřeb,
- kontroluje relevanci zranitelností a řeší úkoly dle priorit (instaluje bezpečnostní aktualizace a provádí změny konfigurace ICT v souladu s procesem řízení změn ICT),
- udržuje aktuální seznam aktiv/systémů zahrnutých do procesu řízení zranitelností,
- zpřístupní / poskytne manažerovi informační bezpečnosti informace o aktuálním stavu zranitelností a přijatých protiopatření.

Ředitelé sekcí Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby

- jsou v roli provozovatelů informačních systémů ČEPS,
- odpovídají za vedení seznamu systémů/aktiv zahrnutých do procesu řízení zranitelností ICT.

Vedoucí oddělení Strategie a bezpečnost ICT

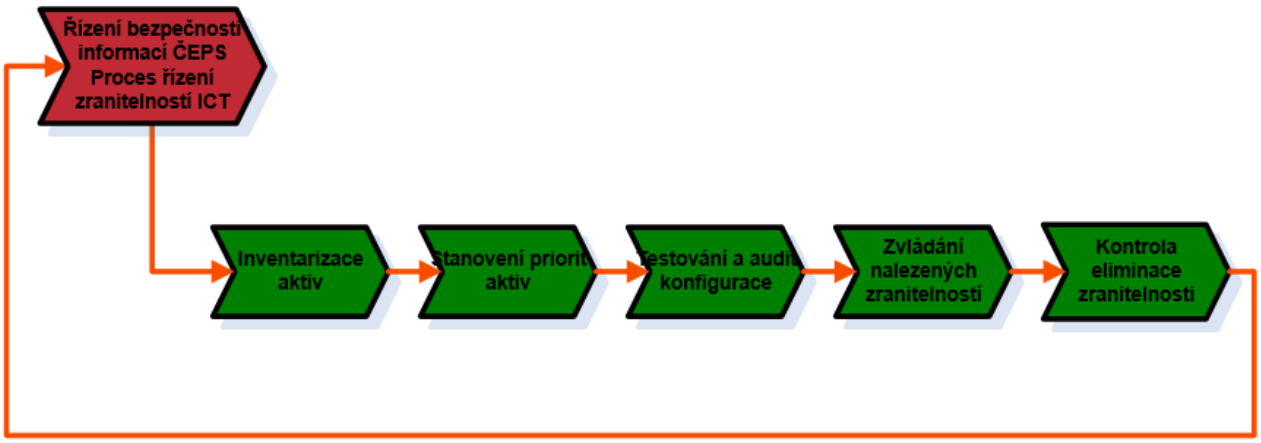
- je v roli manažera bezpečnosti informací,
- rozhoduje sporné případy na základě podkladů poskytnutých specialistou bezpečnosti a odpovědným administrátorem,
- připravuje podklady pro bezpečnostní radu ICT,
- kontroluje realizaci procesu řízení zranitelností ICT.

Specialista bezpečnosti informací:

- podílí se na základě analýzy rizik na roztřídění a určení kritičnosti systémů ICT,
- plánuje testování a audit konfigurace,
- kontroluje výsledky a reporty testování a auditu.

2 PROCES ŘÍZENÍ ZRANITELNOSTÍ ICT

Proces řízení zranitelností ICT obsahuje následující činnosti, které se periodicky opakují v rozsahu odpovídajícímu potřebám ČEPS.



2.1 Inventarizace aktiv

Cílem inventarizace aktiv, jejich identifikace a zatřídění do příslušných skupin a organizačních jednotek je:

- zajistit, aby byly všechny klíčové ICT produkty zahrnuty do systému řízení zranitelností,
- periodicky zjišťovat a aktualizovat jejich stav a analyzovat změny,
- odhalit nepovolená zařízení.

Výstupem inventarizace je:

- aktualizovaný seznam nalezených ICT zařízení, s uvedením přidělených IP adres, verzí operačního systému a detekovaných portů TCP a UDP u každého zařízení,
- schematické mapy síťové topologie detekovaných ICT zařízení, včetně základního popisu pro každé zařízení (aktuálně platná IP adresa, NetBios jméno a DNS jméno a verze operačního systému) včetně jména odpovědného administrátora,

Pokud je identifikováno neoprávněné zařízení postupuje se v souladu s Přílohou č. 8 SM/88.

2.2 Stanovení priorit aktiv ICT

Proces řízení zranitelností je nastaven dle důležitosti jednotlivých ICT aktiv a rizik nalezených zranitelností. Pro každé sledované aktivum musí být stanoven stupeň kritičnosti a ohodnocena míra souvisejícího rizika s každou nalezenou zranitelností. Priority pro odstraňování zranitelností se nastavují dle stupně kritičnosti aktiva a míry rizika zjištěné zranitelnosti.

Vstupem pro určení kritičnosti systémů ICT v organizaci jsou výsledky analýzy rizik. Specialista bezpečnosti ICT, odpovědný administrátor a manažer bezpečnosti informací rozdělí systémy podle úrovně kritičnosti (viz. tabulka níže) do skupin. U systémů, které nebyly do analýzy rizik zahrnuty, bude kritičnost určena ad-hoc a systém bude zahrnut do registru aktiv pro příští analýzu rizik.

V procesu řízení zranitelností ICT musí být zahrnuty typizované systémy, například standardní aplikační, databázové, zálohovací servery uživatelská stanice apod. tak, aby získané informace a účinnost procesu řízení zranitelností byly úplné pro ICT celé společnosti.

Tabulka definující přiřazení míry kritičnosti každému ICT zařízení nebo skupině:

stupeň kritičnosti aktiv	velikost negativního dopadu
1. a 2. stupeň (velmi nízký až nízký)	systémy, u nichž mají potenciální zranitelnosti a jejich řešení **malý vliv** na provoz klíčových procesů ČEPS.
3. stupeň (střední)	systémy, u nichž mají potenciální zranitelnosti a jejich řešení **vliv** na provoz klíčových procesů ČEPS.
4. stupeň (vysoký)	systémy, u nichž mají potenciální zranitelnosti a jejich řešení **podstatný vliv** na provoz klíčových procesů ČEPS.
5. stupeň (nejvyšší)	systémy, u nichž mají potenciální zranitelnosti a jejich řešení **zásadní vliv** na provoz klíčových procesů ČEPS

Výstupem stanovení priorit je seznam skupin zařízení ICT, zahrnutých do procesu řízení zranitelností s přiřazenou mírou kritičnosti pro organizaci a administrátorem ICT odpovědným za eliminaci nalezených zranitelností pro danou skupinu zařízení.

2.3 Identifikace zranitelností

Účelem periodického vyhledávání zranitelností ICT prvků pomocí vzdáleného (network-based) testování zranitelností ICT a bezpečnostního auditu (host-based) konfigurace ICT prvků, systémů a aplikací je včasné odhalení nových zranitelností.

Výsledkem identifikace zranitelností jsou seznamy nových zranitelností, které obsahují následující informace:

- popis každé zranitelnosti, včetně ohodnocení míry rizikovosti a návodu na její odstranění nebo snížení,
- seznam nalezených zranitelností pro každé detekované ICT zařízení a vytvořené skupiny zařízení včetně přehledu o míře rizik,
- přehled o zranitelných ICT zařízeních a skupinách zařízení, s vypočtenou celkovou mírou rizik,
- souhrnné statistické údaje o počtech nalezených zranitelností pro jednotlivé míry rizik, pro jednotlivé ICT zařízení a skupiny zařízení a trendy vývoje počtů zranitelností v čase.

2.4 Zvládání nalezených zranitelností

Na základě výsledků testování a bezpečnostního auditu musí být zajištěn proces zvládání (eliminace) nalezených zranitelností v požadovaných lhůtách a v závislosti na jejich kritičnosti. Základními vstupy pro tento proces jsou míra rizika zranitelnosti příslušného prvku ICT a vazba na odpovědného administrátora.

Nalezené zranitelnosti jsou řešeny v pořadí dle nastavených priorit a ve lhůtě stanovené tabulkou v kap. 3 následujícím způsobem:

Systémy kritičnosti 3

- odpovědný administrátor rozhodne o zálohování systému před provedením nápravného opatření (instalací aktualizace nebo změnou nastavení).

Systémy kritičnosti 4

- odpovědný administrátor musí zálohovat systém před provedením nápravných opatření. Může svolat řešitelský tým, který rozhodne ve stanovené lhůtě o způsobu řešení.

Systémy kritičnosti 5

- odpovědný administrátor svolává řešitelský tým (případně s účastí dodavatele systému) a ve stanovené lhůtě musí být rozhodnuto o způsobu řešení.

Při implementaci nápravných opatření se postupuje v souladu s pravidly pro řízení změn.

Výstupem jsou seznamy otevřených, uzavřených (vyřešených), ignorovaných zranitelností s přiřazenými administrátory a lhůtami pro jejich vyřešení a souhrnné zprávy aktuálních počtů ošetřených a neošetřených zranitelností, rozdělené dle míry rizik a osob odpovědných za jejich eliminaci.

2.5 Kontrola zvládání zranitelností

Pro ověření funkčnosti realizovaných opatření a omezení vzniku chyb lidského faktoru jsou prováděny kontroly zvládání nalezených zranitelností a nastaveny postupy pro případ uplynutí stanovené lhůty pro jejich odstranění.

Výstupem kontrol je seznam ošetřených a neošetřených zranitelností s přiřazenou mírou rizika a lhůtou pro jejich odstranění odpovědným administrátorem. Pokud uplynula stanovená lhůta, musí být k příslušné zranitelnosti zaznamenány důvody, kvůli kterým nebyla odstraněna, a uvedeno rozhodnutí o dalším postupu.

3 LHŮTY PRO ODSTRANĚNÍ ZRANITELNOSTÍ

Následující tabulka uvádí aktuální platné lhůty pro odstranění zjištěných zranitelností na systémech s různou mírou kritičnosti pro organizaci:

Hodnocení kritičnosti zařízení ICT pro klíčové procesy	**Hodnocení rizikovosti nalezených zranitelností ICT**				
	rizikovost 5 (velmi vysoká)	**rizikovost 4 (vysoká)**	**rizikovost 3 (střední)**	**rizikovost 2 (nízká)**	**rizikovost 1 (velmi nízká)**
kritičnost 5 (velmi vysoká)	2 dny	5 dní	10 dní	bez lhůty	bez lhůty
kritičnost 4 (vysoká)	5 dní	7 dní	14 dní	bez lhůty	bez lhůty
kritičnost 3 (střední)	10 dní	14 dní	21 dní	bez lhůty	bez lhůty

Údaje v tabulce znamenají nejzazší lhůtu v kalendářních dnech, do kdy musí být **rozhodnuto o způsobu řešení dané zranitelnosti či o tom, že se nejedná o zranitelnost**. Implementace musí být provedena (je-li známé řešení) bez zbytečného odkladu.

Odstranění zranitelnosti musí respektovat proces řízení změn. U odstranění zranitelností rizikovosti 4 a 5 na systémech stupně kritičnosti 4 a 5 se jedná o urgentní změnu, které musí být umožněn zrychlený proces řízení změn.

4 SEZNAM SYSTÉMŮ/AKTIV ZAHRNUTÝCH DO PROCESU ŘÍZENÍ ZRANITELNOSTÍ ICT

Seznam musí obsahovat minimálně následující položky:

DNS/netbios name	IP adresa(y)	Odpovědný administrátor	Síťový segment (LAN/DMZ/WAN)	Stupeň kritičnosti

Aktuální seznam systémů/aktiv má charakter citlivé interní informace a jeho vlastníkem je ředitel příslušné sekce „Energetické řídící a informační systémy“ nebo „ICT služby “. Seznam je udržován v elektronické podobě a je zpřístupněn odpovědnému administrátorovi (administrátorům) a manažerovi informační bezpečnosti.

5 PŘECHODNÁ USTANOVENÍ

Do doby zajištění technických prostředků a podmínek pro automatizované testování zranitelností má provozovatel informačních systémů ČEPS povinnost postupovat v co největší možné míře v souladu s touto směrnicí při zachování zásad v této směrnici obsažených.