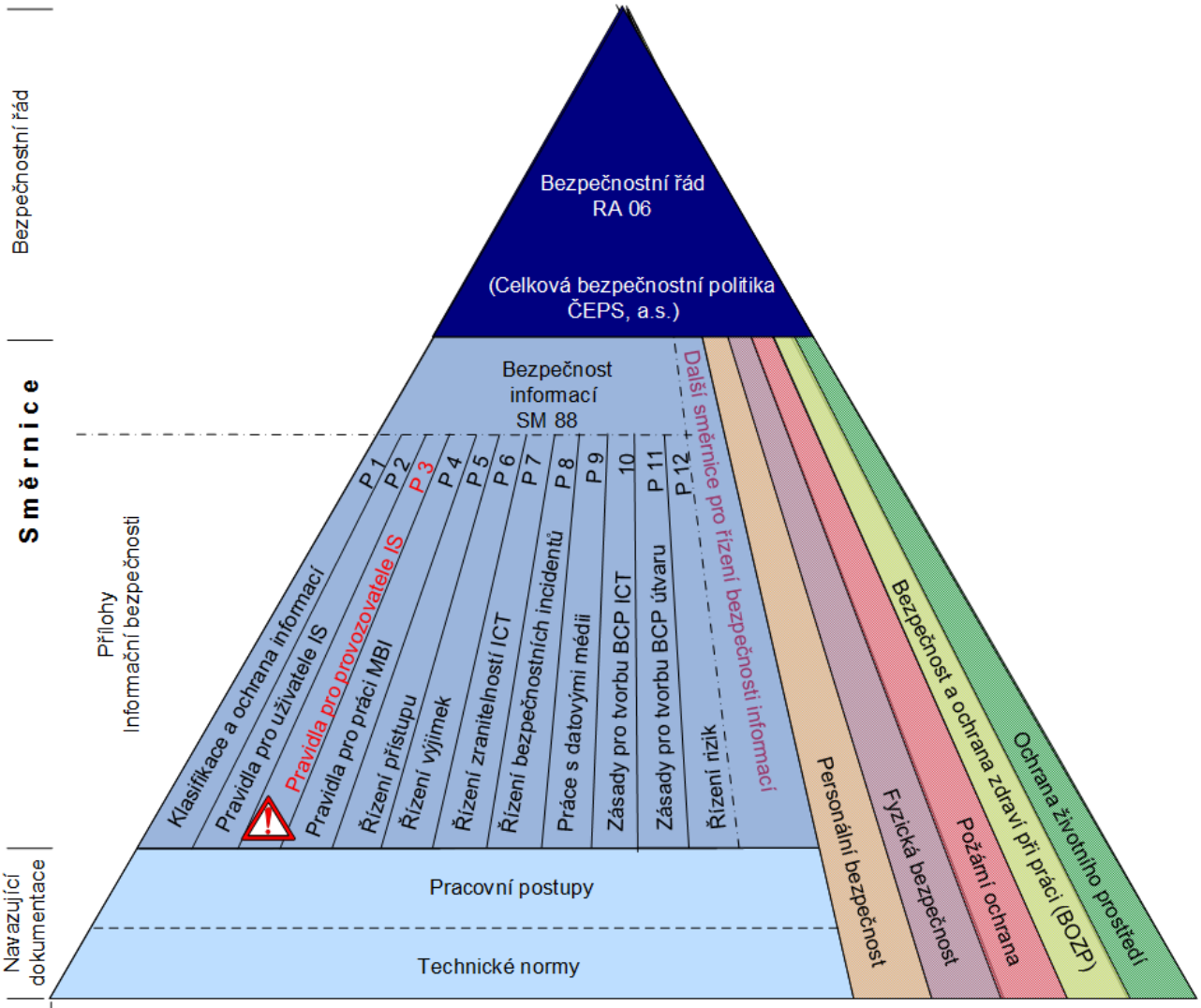
PRAVIDLA BEZPEČNOSTI INFORMACÍ PRO SPRÁVCE A ADMINISTRÁTORA IS

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 A PŮSOBNOST

Dokument „*Pravidla bezpečnosti informací pro provozovatele a administrátora IS" je* samostatnou přílohou směrnice *Bezpečnost informací* (dále „SM/88"), která stanovuje základní principy, pravidla a požadavky bezpečnosti informací v ČEPS. Tato příloha určuje pravidla pro dodržování bezpečnosti informací pro provozovatele a administrátory informačních systémů společnosti.

Příloha je závazná pro všechny zaměstnance ČEPS v roli provozovatele nebo administrátora informačního systému a dále pro externí subjekty konající práce v IS/ICT ČEPS v rozsahu daném smluvním vztahem.

1.1 Role, odpovědnosti a pravomoci

Administrátor IS je povinen:

- zajistit bezpečnost aktiv v oblasti své působnosti
- zajistit soulad bezpečnosti svěřeného aktiva s interní bezpečnostní dokumentací (především dodržovat bezpečnostní politiky konfiguračních standardů prvků IS/ICT, patch managementu a ustanovení směrnic SM/88, SM/96, SM/103, SM/104 a dalších)
- udržovat aktuální evidenci svěřených aktiv
- spolupracovat při hodnocení rizik, hodnocení stavu bezpečnosti informací a při bezpečnostních auditech
- spolupracovat při zavádění a realizaci bezpečnostních opatření při ochraně osob, majetku, informací, prostředí a pro zajištění kontinuity a obnovy činností společnosti
- předcházet vzniku bezpečnostních incidentů a aktivně postupovat při oznamování, odhalování a likvidaci jejich následků
- spolupracovat při provádění bezpečnostních auditů, analýz zranitelností a penetračních testů.

Ředitelé sekcí *Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby* jsou v roli provozovatelů informačních systémů ČEPS ve své působnosti a jsou povinni zajistit:

- evidenci a aktuálnost evidence aktiv IS včetně určení vlastníků těchto aktiv v rámci své odpovědnosti
- dokumentaci a aktuálnost dokumentace infrastruktury ICT
- dokumentaci služeb ICT, které jsou poskytovány v rámci ČEPS[1] a pro kritickou službu identifikaci prostředků IT, které se na ní podílí
- klasifikaci služeb a souvisejících prostředků ICT v souladu s Přílohou č. 1 SM/88
- zpracování a dodržování pracovních postupů ve své působnosti
- vytvoření konfiguračních standardů zařízení infrastruktury IS/ICT
- implementaci a monitorování technických bezpečnostních opatření pro přístup externích subjektů v souladu se smlouvou.

Ředitelé sekcí *Energetické řídící a informační systémy, ICT služby a Řízení provozu a údržby* jsou oprávněni od manažera bezpečnosti informací (MBI) vyžadovat:

- provedení odpovídajícího hodnocení rizik bezpečnosti informací pro výše uvedenou klasifikaci služeb

[1] Služby ve smyslu ISO/IEC 20000, např. Dispečerský řídicí systém, Energetický obchodní systém, SAP, úložiště dat (sdílené disky) apod.

- provedení mimořádného hodnocení bezpečnostních rizik, analýzy zranitelnosti nebo penetračních testů pro vybraná aktiva ICT
- definici bezpečnostních požadavků konfiguračního standardu pro výše uvedenou standardizaci konfigurace
- seznam bezpečnostních výjimek.

Externí subjekty podílející se na správě prostředků ICT ČEPS jsou povinni seznámit se s touto přílohou SM/88 a s další dokumentací a dodržovat jejich ustanovení. Vztahují se na ně odpovědnosti role Administrátor IS.

Identifikace a posouzení rizik plynoucích z přístupu externích subjektů je v odpovědnosti MIB a je prováděna v souladu s požadavky SM/88.

1.2 Definice základních pojmů a zkratek

Administrátor IS – zaměstnanec pověřený provozovatelem IS správou a provozem svěřeného informačního systému nebo zařízení ICT infrastruktury.

DMZ – demilitarizovaná zóna.

IDS/IPS – Intrusion Detection System (systém detekce průniků do IS)/ Intrusion Prevention System (systém prevence průniků do IS).

Prostředky ICT (Prvky IS/ICT) – technické prostředky (servery, koncové stanice, síťové prvky, datová úložiště, záložní zdroje napájení a další zařízení infrastruktury ICT), operační systémy a aplikační software.

Provozovatel IS – útvar zajišťující provoz informačních systémů tak, aby odpovídajícím způsobem a se stanovenou spolehlivostí podporoval procesy společnosti (sekce Energetické řídící a informační systémy, sekce ICT služby a sekce Řízení provozu a údržby).

Služba ICT – služba poskytovaná vnitřním zákazníkům provozovatelem IS. Podporuje podnikové procesy při využití informačních technologií (pomocí zaměstnanců, procesů a prostředků ICT) a měla by být definována v dohodě o úrovni služeb.

2 ŘÍZENÍ AKTIV A KLASIFIKACE INFORMACÍ

2.1 Odpovědnost za aktiva

Administrátor IS může být vlastníkem aktiva společnosti nebo může být pověřen[2] k jeho správě.

2.2 Klasifikace informací a aktiv

Klasifikaci informací provádí jejich vlastník v souladu s Přílohou č. 1 SM/88 a uživatelé informací jsou povinni se při práci s informacemi řídit tam uvedenými pravidly.

Služby ICT a prostředky (HW, SW) pro zpracování informací přebírají nejvyšší klasifikační stupeň zpracovávaných informací.

Za klasifikaci aktiva odpovídá jeho vlastník. Hodnoty klasifikace aktiva IS jsou stanoveny jako maximální hodnoty důvěrnosti, dostupnosti a integrity ze všech služeb ICT, které dané aktivum podporuje.

[2] Pověření může vyplývat z pracovního zařazení, nemusí být explicitní.

3 BEZPEČNOST LIDSKÝCH ZDROJŮ

Bezpečnost lidských zdrojů ve vztahu k bezpečnosti informací je uvedena ve směrnici SM/88 (kap. 8) a v interní dokumentaci odboru Personalistika (SM/99 *Personální bezpečnost*).

4 FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

Fyzická bezpečnost ve vztahu k bezpečnosti informací je uvedena ve směrnici SM/88 (kap. 9) a v interní dokumentaci připravené odborem Bezpečnostní činnosti (SM/85 *Fyzická bezpečnost*).

5 ŘÍZENÍ PROVOZU IS/ICT

5.1 Provozní dokumentace ICT

Provozní dokumentace IS/ICT se zpracovává formou pracovních postupů, technických norem nebo směrnic v souladu s RA/01 nebo podle vnitřních pravidel příslušných sekcí ICT. Za tvorbu a aktualizaci této dokumentace odpovídá provozovatel IS.

Postupy používané při poskytování služeb ICT musí být dokumentovány např. formou pracovních postupů. Typickým příkladem jsou zálohovací plány, plány obnovy systému po havárii, plány pravidelné údržby systémů, apod.

Dokumentace IS a infrastruktury ICT

Administrátoři jsou povinni vytvářet a udržovat aktuální evidenci zařízení a dokumentaci ke všem spravovaným systémům a zařízením. Tato dokumentace musí obsahovat informace o infrastruktuře ICT a o konfiguraci systémů nebo zařízení a o provedených změnách. Detailnost dokumentace je závislá na kritičnosti systému.

Konfigurační standardy (včetně patch managementu) musí být vytvořeny, uplatňovány a aktualizovány pro prvky a zařízení nebo skupiny prvků a zařízení implementovaných ve struktuře IS/ICT:

- koncové stanice (standardní uživatelské, technologická a speciální PC nebo notebooky) včetně schváleného internetového prohlížeče
- servery (fyzické i virtuální)
- disková úložiště, zálohovací a archivační systémy
- síťové prvky
- apod.

Kde je to možné, musí být bezpečnostní nastavení vynucováno prostředky, které daný systém umožňuje.

Evidence koncových zařízení, jejich konfigurační standard a způsob přidělování (pracovních stanic, notebooků, PDA a dalších uživatelských zařízení) je řízena směrnicí SM/96 *Nákup, evidence a používání ICT vybavení.*

Evidence serverů, jejich konfigurační standard a způsob provozu je řízen směrnicí SM/103 *Nákup, evidence a používání ICT infrastruktury*. Evidence serverů musí obsahovat alespoň informace o:

- HW i SW konfiguraci serveru, tzv. *konfigurační standard*
- všech provozních aktivitách (logy nebo provozní deník, včetně data, času a jména administrátora, který zásah provedl)
- instalovaném software (aplikace, databáze, atd.)
- požadavcích a realizaci zálohování dat i systému

- klasifikačním stupni informací, které jsou na serveru uloženy nebo zpracovávány
- konfiguraci instalovaného bezpečnostního software fyzickém umístění
- administrátorech zodpovědných za provoz serveru a aplikací.

Evidence síťových prvků musí obsahovat alespoň informace o:

- HW i SW konfiguraci zařízení, tzv. *konfigurační standard*
- vazbě na zařízení a systémy, které se v případě poruchy síťového prvku stanou nedostupné pro zajištění provozu příslušnými sekcemi ICT
- fyzickém umístění
- provozních aktivitách dle pracovních postupů příslušných sekcí ICT
- administrátorech odpovědných za provoz zařízení.

K evidencím smí přistupovat pouze:

- administrátoři – možnost čtení i zápisu pro záznamy o systémech, které jsou v jejich správě
- manažer bezpečnosti informací a pověření specialisté, možnost čtení, kde to systém umožňuje, nebo na vyžádání
- interní auditoři – na vyžádání
- další zaměstnanci, kteří informace potřebují k plnění svých pracovních povinností (např. HelpDesk) – přístupy jsou definované popisem pracovního místa.

Výjimky z výše uvedených pravidel, zejména výjimky způsobené technickým omezením nebo omezenou pracovní kapacitou specialistů ICT, musí být schváleny ředitelem příslušné sekce ICT a uděleny manažerem bezpečnosti informací dle ustanovení Přílohy č. 6 SM/88.

5.2 Řízení změn

Řízení změn je definováno SM/104 *Procesy sekce ICT služby*.

Všechna zařízení pro zpracování informací společnosti podléhají změnovému řízení. Za změny ve smyslu ustanovení tohoto článku nejsou považovány rutinní provozní zásahy. Každé změně s dopadem na bezpečnost informací musí předcházet analýza hodnotící bezpečnostní a provozní dopady. O důležitosti změny a o provedení analýzy rozhoduje administrátor zařízení, kterého se změna týká. Na základě provedené analýzy musí být vypracován postup/harmonogram, který zajistí minimalizaci výpadků poskytovaných služeb při realizaci změny. Analýza dopadů i harmonogram musí být dokumentovány.

Oddělení Strategie a bezpečnost ICT se z pohledu bezpečnosti informací v rámci procesu řízení změn v ICT podílí na schvalování každé změny, která naplňuje alespoň jeden z předpokladů:

- rozsahem znamená zásah do celého informačního systému nebo jeho významné části
- týká se zařízení v DMZ
- týká se bezpečnostních nastavení koncových stanic, serverů nebo síťových prvků
- týká se zařízení pracoviště Homebankingu
- týká se zařízení zpracovávajících informace klasifikované stupněm „CITLIVÉ INTERNÍ“.

5.3 Oddělení povinností

Dopady selhání lidského faktoru na bezpečnost informací společnosti je nutno minimalizovat. Všechny provozní a kontrolní odpovědnosti musí být oddělené:

- zaměstnanci odboru Interní audit a procesy ČEPS a oddělení Strategie a bezpečnost ICT provádějící audit IS nesmějí mít přidělena oprávnění umožňující provádět změny nastavení zařízení ve správě sekcí ICT a sekce Řízení provozu a údržby (provozovatele IS)
- vývojáři nesmějí provádět administraci provozních serverů, které jsou ve správě provozovatele IS
- administrátoři nesmějí mít přidělena oprávnění umožňující editaci auditních záznamů (logů)
- administrátoři nesmějí mít přidělena oprávnění umožňující manipulaci s daty na spravovaných zařízeních, pokud tato oprávnění nepotřebují k plnění svých pracovních povinností nebo neexistuje možnost oddělení těchto práv vzhledem k architektuře systému
- administrátoři (ani jiní uživatelé) nesmějí mít přidělena administrátorská oprávnění k zařízením, která nespravují a nenesou za jejich provoz odpovědnost
- administrátoři nesmějí používat privilegovaný účet pro jinou než administrátorskou činnost.

Výjimky z výše uvedených pravidel, zejména výjimky způsobené technickým omezením, architekturou systémů, omezenou pracovní kapacitou nebo specifikou pracovních povinností specialistů ICT, musí být schváleny ředitelem příslušné sekce ICT a uděleny manažerem bezpečnosti informací dle ustanovení Přílohy č. 6 SM/88.

5.4 Oddělení vývoje, testování a provozu

Z vývojového ani testovacího prostředí nesmí být možné ovlivnit nebo narušit provozní prostředí. Testování nových verzí systémů, aplikací i zařízení se nesmí provádět v provozním prostředí. Testy smí být prováděny pouze s testovacími daty.

Akceptační kritéria bezpečnosti informací nutná pro uvedení systémů ICT do provozu specifikují zaměstnanci provozních útvarů a specialisté bezpečnosti informací ze sekcí ICT a oddělení Strategie a bezpečnost ICT.

Nové verze systémů nebo aplikací a nová zařízení pro zpracování informací smí být nasazena až potom, co je testováním potvrzeno splnění předem definovaných akceptačních kritérií.

Provozní servery nesmí obsahovat překladače a systémové utility, které nejsou nezbytné pro jejich správu nebo provoz.

Počet administrátorů jednotlivých zařízení nebo zařízení ve funkčním celku musí být minimalizován na nejnižší možný počet, který zajistí výkon všech potřebných úkonů a dostatečnou zastupitelnost.

Výjimky z výše uvedených pravidel musí být schváleny ředitelem příslušné sekce a uděleny manažerem bezpečnosti informací dle ustanovení Přílohy č. 6 SM/88.

5.5 Řízení dodávek služeb externího subjektu

Dodávky služeb

Základní povinnosti pro řízení dodávek realizovaných externím subjektem jsou stanoveny směrnicí SM/88.

Administrátoři aplikací a zařízení pro zpracování informací, ke kterým přistupují pracovníci externího subjektu, jsou v rámci svých pravomocí povinni se ujistit, že:

- byla podepsána smlouva nebo prohlášení o ochraně informací (NDA)
- administrátoři externího subjektu splňují požadavky tohoto dokumentu.

V opačném případě nesmí být pracovníkům externího subjektu přístup přidělen.

Na základě smluvního vztahu musí administrátoři pro pracovníky externího subjektu zajistit:

- přidělení logických a fyzických přístupových práv v souladu s Přílohou č. 5 SM/88
- zápis do auditních záznamů (logů) v souladu s ustanoveními v kap. 9.

Monitorování služeb

Administrátoři aplikací nebo zařízení pro zpracování informací ČEPS musí zajistit, že zařízení je externím subjektem spravováno v souladu se všemi bezpečnostními požadavky platnými pro obdobná zařízení spravovaná zaměstnanci společnosti.

Administrátoři provozovatele IS ČEPS jsou povinni zajistit splnění požadavků:

- dodávka zařízení, jeho správa nebo poskytovaná služba je na požadované úrovni a kvalitě i v souladu se smluvními podmínkami
- kvalita a úroveň poskytované služby je pravidelně (nebo průběžně) monitorována a kontrolována
- řízení změn na zařízeních nebo v poskytovaných službách je prováděno v souladu s touto přílohou (kap. 5.2)
- činnosti a přístupy pracovníků externích subjektů jsou zaznamenávány v souladu s touto přílohou (logování činností, pracovní záznamy, provozní deník apod.)
- všechny záznamy jsou pravidelně (nebo dle potřeby) kontrolovány tak, aby byla odhalena narušení nebo pokusy o narušení bezpečnosti informací
- zranitelnosti zařízení ICT jsou řízeny v souladu s Přílohou č. 7 SM/88
- zařízení je monitorováno
- bezpečnostní incidenty jsou řízeny v souladu s Přílohou č. 8 SM/88.

5.6 Plánování a přejímání systémů

Řízení kapacit

Zajištění dostupnosti, požadované výkonnosti a spolehlivosti IS ČEPS musí být řízené a v souladu se současnými i budoucími potřebami společnosti. Administrátoři musí brát při výběru software i hardware v úvahu známé zranitelnosti všech jeho verzí v historii.

Přejímání systémů a zařízení

Pro předávání významných aplikací do provozu musí existovat pracovní postup stanovující kroky a podmínky, které musí být splněny před nasazením systému, aplikace nebo zařízení do provozu. Za vypracování postupu před nasazením změny do provozu odpovídá provozovatel systému, kontroluje ředitel příslušné sekce ICT.

Pro uvedení nových systémů nebo zařízení do provozu jsou provozovatel IS a jeho administrátoři povinni zajistit alespoň:

- převzetí a akceptaci provozní dokumentace včetně specifikace bezpečnosti informací, plánů kontinuity a obnovy
- implementaci a akceptaci všech opatření bezpečnosti informací vyplývající z:
    - řídící bezpečnostní dokumentace
    - hodnocení rizik, pokud bylo součástí dodávky
    - jiných specifických požadavků stanovených oddělením Strategie a bezpečnost ICT
- provedení a úspěšné splnění akceptačních testů
- školení uživatelů i administrátorů v požadovaném rozsahu
- splnění dalších podmínek specifikovaných v projektu, smlouvě a související dokumentaci.

Je-li nový systém dodáván a implementován externím subjektem, platí pro akceptaci stejná pravidla jako pro systémy dodávané nebo implementované interně. Smlouva o implementaci musí obsahovat podmínky úspěšného ukončení akceptačních testů. Probíhá-li implementace v samostatných etapách, musí být stanovena akceptační kritéria pro každou etapu.

5.7 Ochrana proti škodlivým programům

Administrátoři mohou na uživatelské koncové stanice a provozní systémy instalovat pouze otestovaný a schválený software (SM/96).

Proti šíření škodlivých programů musí být instalován antivirový a antispywareový software s centrálním managementem. V případě nutnosti mohou administrátoři nainstalovat i další software pro detekci a odstranění škodlivých programů. O trvalé instalaci takového software se rozhoduje v procesu řízení změn v ICT. Nainstalovaný obranný software musí být na všech zařízeních pravidelně aktualizován. Pokud software poskytuje automatickou aktualizaci, musí být na všech zařízeních zapnuta. Databáze signatur musí být aktualizována s frekvencí, stanovenou správcem antivirového software.

Administrátorům je zakázáno bezdůvodně měnit nastavení antivirové ochrany a schváleného obranného SW nebo jej vypínat. Při vypnutí antivirové ochrany a obranného SW se další činnost řídí pracovními postupy příslušných sekcí ICT. Antivirový software musí být instalován na všech uživatelských stanicích a serverech.

Administrátoři jsou povinni nastavení antivirové kontroly konfigurovat takovým způsobem, aby ji uživatelé nemohli svévolně vypínat. Uživatelé s administrátorskými oprávněními nesmějí měnit nastavení antivirového programu ani dalšího bezpečnostního softwaru (personální FW).

5.8 Zálohování a archivace

Zálohování dat a softwarového vybavení je zajišťováno zaměstnanci odpovědnými za provoz daného IS. Způsoby a pravidla pro zálohování dat, informací a softwarového vybavení jsou stanoveny v průběhu implementace příslušného IS nebo provozní dokumentací zpracovanou provozovateli IS.

Zálohy a archivy musí podléhat stejné klasifikaci a ochranným opatřením jako jejich nejvýše klasifikovaná předloha (zdroj).

5.9 Správa bezpečnosti sítě

Síťová opatření

Síťová infrastruktura musí být dostatečně podrobně zdokumentována a dokumentace musí odpovídat skutečnému stavu (musí být aktualizována). Administrátoři síťové infrastruktury zajišťují bezpečný a spolehlivý provoz počítačových sítí společnosti a jsou povinni zajistit splnění požadavků a pravidel:

- každé propojení interní sítě společnosti s veřejnými datovými sítěmi musí být schváleno ředitelem sekce ICT služby a manažerem bezpečnosti informací
- instalovat zařízení do počítačové sítě společnosti smějí pouze pověření administrátoři provozovatele IS nebo externího subjektu s patřičnou smlouvou
- všechny body propojení sítě společnosti s veřejnými datovými sítěmi musí být monitorovány IDS/IPS

- pro autentizaci vzdálené administrace používat protokolu a serveru RADIUS, TACACS+ nebo podobných, přistupovat vzdáleně pomocí protokolu ssh, nebo využívat jinou bezpečnou technologii schválenou manažerem bezpečnosti informací
- využívat prvků autentizace u routovacích protokolů a dalšího zabezpečení, které dovoluje implementace těchto protokolů.

Internetová brána pro uživatele

Uživatelé (zaměstnanci společnosti i externích subjektů) mohou přistupovat k Internetu pouze přes centrální přístupovou bránu (proxy server) nebo přes centrálně spravovaný personální firewall (při použití nástroje na vypnutí proxy serveru).[1] Administrátoři IS/IT jsou povinni:

- nastavit prostupy pouze pro povolené protokoly na povolených portech:
  - http (80), https (443), ftp (20,21)
  - další dle výjimky udělené manažerem bezpečnosti informací
- umožnit komunikaci uživatelů s bránou pouze z interní sítě společnosti
- umožnit správu brány pouze z interní sítě společnosti

v případě použití přístupu přes centrální bránu, zajistit logování přístupu uživatelů k internetu a způsobu využívání Internetu alespoň v rozsahu

  - přihlašovací jméno z Active Directory nebo jiné jednoznačné určení uživatele
  - datum a čas
  - požadované URL nebo IP adresy.

Administrátoři jsou povinni tyto logy uchovávat minimálně po dobu jednoho roku a na vyžádání je poskytnout řediteli příslušné sekce ICT, případně manažerovi bezpečnosti informací nebo auditorovi.

Změny v síťové infrastruktuře

Významné změny v síťovém modelu musí být schváleny v procesu řízení změn ICT. Před realizací takových změn musí být ohodnocena rizika změny a sestaven havarijní plán pro případ neúspěchu implementace změny nebo musí být nová infrastruktura budována paralelně se stávající.

Změnou v síťovém modelu se rozumí:

- změna proti pravidlům a požadavkům bezpečnostní dokumentace (SM/88 včetně relevantních příloh)
- změna oproti pravidlům a požadavkům na provoz v DMZ a v dalších bezpečnostně citlivých oblastech síťové infrastruktury
- modifikace propojení nebo struktury jednotlivých síťových segmentů či vytvoření nových
- změna v IP plánu
- změny, které mohou mít dopady na funkčnost bezpečnostních prvků, např.:
  - v evidenci síťových prvků a prostupů mezi síťovými segmenty či sítěmi
  - v konfiguraci IDS/IPS zařízení
- zavádění nových technologií
- jiné změny, které administrátoři síťové infrastruktury považují za významné.

Bezpečnost bezdrátových sítí

[1] Týká se notebooků při práci mimo lokality ČEPS

Požadavky na bezpečnost bezdrátových sítí musí být stanoveny vhodnou dokumentací (konfigurační standard) a schváleny ředitelem příslušné sekce ICT a manažerem bezpečnosti informací. Administrátoři síťové infrastruktury jsou povinni v rámci svých pracovních kompetencí zajistit pro bezdrátové sítě alespoň splnění požadavků:

- přístupové body musí být konfigurovány tak, aby autentizace připojovaných zařízení probíhala před zahájením spojení
- bezdrátová zařízení musí být autentizována před připojením do sítě ČEPS
- uživatelé přistupující k bezdrátové síti musí být autentizováni
- komunikace v rámci bezdrátových sítí musí být šifrována
- pro zařízení bezdrátové sítě musí být vypracován konfigurační standard.

5.10 Bezpečnost při zacházení s médii

Zásady práce při zacházení s médii stanovuje Příloha č. 9 SM/88. Klasifikace informací a manipulační postupy s médii musí být v souladu s ustanoveními v Příloze č. 1 SM/88.

5.11 Elektronická pošta a web

Elektronická pošta

Základní pravidla pro elektronickou poštu jsou uvedena v kap. 3.4 Přílohy č. 1 a kap. 3.9 a 3.10 Přílohy č. 2 SM/88.

Administrátoři poštovních serverů jsou povinni zajistit:

- antivirovou a antispamovou kontrolu mailových zpráv – všechny příchozí i odchozí maily (z a do internetu) musí být zkontrolovány na přítomnost virů
- ochranu poštovních serverů proti napadení z veřejných datových sítí, administrátoři jsou povinni používat pouze schválených protokolů,
- konfiguraci všech poštovních serverů tak, aby poskytovaly služby pouze autentizovaným oprávněným uživatelům
- ochranu poštovních schránek uživatelů.

K poštovní schránce má přístup pouze její vlastník. V odůvodněných případech a pouze se souhlasem přímého nadřízeného zaměstnance smí být ke schránce uživatele umožněn přístup i jiným osobám. O toto nastavení musí být požádáno příslušným vedoucím zaměstnancem prostřednictvím aplikace Helpdesk. Další činnost se řídí pracovními postupy sekce ICT služby.

Obdobná pravidla platí pro zřízení hromadné poštovní schránky.

Veřejně přístupné systémy (webové aplikace)

Veřejně přístupné systémy (např. webové servery a informační portály pro zákazníky, přístupné z veřejných datových sítí) musí být umístěny v DMZ nebo jinak zabezpečeny. Administrátoři i externí subjekty spravující veřejně přístupné systémy jsou povinni je instalovat a konfigurovat dle požadavků stanovených v tomto dokumentu a v příslušných konfiguračních standardech.

5.12 Monitorování

Pořizování auditních záznamů (logů)

Administrátoři zařízení, systémů a aplikací pro zpracování informací jsou povinni zajistit zaznamenávání událostí (logování) na systémové i aplikační úrovni. Veškeré aktivity související s monitorováním a zaznamenáváním událostí musí být v souladu s obecně závaznými právními

předpisy a interní bezpečnostní dokumentací. **Nikdy nesmí být součástí záznamů heslo nebo PIN**.

Monitorování používání systémů a aplikací

Monitorování uživatelských stanic

Logování musí být zapnuto na všech uživatelských stanicích. Záznamy jsou tvořeny pro tři kategorie událostí:

- systémové
- aplikační
- bezpečnostní.

Bezpečnostní záznamy smí být dostupné pouze uživatelům zařazeným ve skupině *Administrators* (nebo v příslušné globální skupině). Bezpečnostní záznamy musí obsahovat události alespoň rozsahu:

- přihlášení a odhlášení od pracovní stanice a systému - úspěšné i neúspěšné
- správa uživatelů a skupin - úspěšné i neúspěšné
- použití uživatelských práv – pouze neúspěšné.

Velikost souborů pro auditní záznamy na pracovních stanicích musí být nastavena nejméně na 4096 kB. Starší události budou přepisovány novými až po dosažení limitu. Pokud je uživatel pracovní stanice zařazen ve skupině *Administrators*, má zakázáno měnit nastavení definované dle předchozího odstavce.

Popsaný rozsah logování je nutno dodržet pro všechny operační systémy používané na pracovních stanicích.

Monitorování serverů a síťových zařízení

Logování musí být zapnuto na všech serverech a síťových zařízeních. Provozovatel IS zodpovědný za správu serveru nebo síťového prvku stanoví ve spolupráci se specialisty ICT bezpečnosti z oddělení Strategie a bezpečnost ICT pravidla a rozsah logování v závislosti na typu, službách a klasifikaci zařízení.

Velikost souborů pro auditní záznamy musí být nastavena v souladu s konfiguračním standardem zařízení (nejméně 20480 kB). Starší události budou přepisovány novými až po dosažení limitu. Před dosažením limitu musí být provedena archivace logu pro jeho uchování po předepsanou dobu.

Monitorování aplikací

Aktivity uživatelů na aplikační úrovni jsou zaznamenávány v souladu s požadavky provozní dokumentace monitorované aplikace. Rozsah záznamů, bezpečnostní požadavky na jejich ochranu a přístup k nim i požadavky na zálohování a archivaci mohou být obdobné jako při monitorování pracovní stanic nebo serverů.

Ochrana auditních záznamů (logů)

Auditní záznamy jsou administrátoři povinni uchovávat po dobu stanovenou provozní dokumentací, nebo dle ustanovení platné legislativy.

Auditní záznamy musí být klasifikovány vyšším nebo stejným klasifikačním stupněm jako informace, které daný systém nebo zařízení zpracovává.

Provozní deník

Pracovní aktivity administrátorů na klíčových zařízeních a systémech je nutno zaznamenávat do provozního deníku zařízení alespoň v rozsahu:

- datum a čas

- popis zásahu
- identifikace administrátora.

Hlášení událostí a incidentů

Všechny chyby, selhání nebo jiná provozní narušení včetně událostí a incidentů bezpečnosti informací, které administrátor IS řeší, musí být hlášeny, vyhodnocovány a řešeny v souladu s Přílohou č. 8 SM/88. Provozovatel IS poskytuje manažeru bezpečnosti informací měsíční přehled výskytu bezpečnostních incidentů.

Synchronizace hodin

Všechny servery a pracovní stanice musí mít pravidelně (nejméně jednou za den) synchronizován systémový čas se zdrojem přesného času.

5.13 Mobilní výpočetní nebo komunikační zařízení a práce na dálku

Při práci s mobilním výpočetním nebo komunikačním zařízením administrátoři musí:

- dodržovat v roli uživatelů zařízení ustanovení kap. 3.12 Přílohy č. 2 SM/88
- nastavovat na uživatelské notebooky a další mobilní zařízení pouze oprávnění USER (výjimky pro technologické notebooky nebo notebooky s aplikacemi vyžadujícími vyšší úroveň oprávnění musí být schváleny manažerem bezpečnosti informací dle ustanovení Přílohy č. 6 SM/88)
- konfigurovat uživatelské notebooky tak, aby mimo prostory společnosti byl zajištěn bezpečný přístup k datům společnosti přes centrální internetovou proxy bránu nebo prostřednictvím aplikace Internet proxy přepínač pro přímý přístup k internetu a to v případě, že uživatel nepřistupuje do vnitřní sítě společnosti.
- důsledně dodržovat při instalaci těchto zařízení doporučení konfiguračních standardů
- při práci na dálku a vzdáleném přístupu do infrastruktury společnosti používat předepsaným způsobem:
  - pouze schválené zařízení
  - pouze schválené způsoby přístupu
- zajistit, že zařízení používaná pro práci na dálku mimo prostory společnosti nezůstanou nikdy bez dozoru.

6 POŘÍZENÍ, VÝVOJ A ÚDRŽBA INFORMAČNÍCH SYSTÉMŮ

6.1 Bezpečnostní požadavky informačních systémů

Požadavky na bezpečnosti informací musí být součástí každého projektu nebo úkolu, při kterém je pořizován, vyvíjen, udržován nebo měněn informační systém nebo zařízení pro zpracování informací. Tyto požadavky se projednávají v rámci procesu řízení změn ICT.

Bezpečnostní požadavky systémů musí splňovat obecně závazné právní předpisy vztahující se na informace zpracovávané v těchto systémech a musí splňovat požadavky stanovené interní dokumentací.

6.2 Kontrola správného zpracování v aplikacích

Všechny nově implementované systémy a aplikace musí splnit předem stanovená akceptační kritéria (kap. 5.6). Aplikace vyvíjené na zakázku (externím subjektem nebo interně), musí mít vždy implementovány kontroly parametrické správnosti vstupních dat (délka vstupních řetězců, povolené znaky apod.). Všechny komponenty informačního systému, které si vyměňují zpracovávaná data s jinými na aplikační vrstvě, musí při všech výměnách dat potvrzovat jejich úplnost a integritu a stejné potvrzení vyžadovat.

6.3 Kryptografická opatření

Administrátoři informačních systémů využívajících kryptografická opatření (algoritmy, bezpečnostní protokoly, správu klíčů, speciální software a hardware) musí při celém jejich životním cyklu (od instalace, konfigurace, provozu, výroby a distribuce klíčů až po ukončení funkčnosti) postupovat v souladu s dodanou dokumentací a s interními bezpečnostními požadavky.

Minimální požadavky na kryptografické algoritmy pro ochranu prvků kritické informační infrastruktury jsou definovány v příloze 3 vyhlášky č. 316/2014 Sb. . o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Symetrické algoritmy

V případě blokových šifer se přednostně využívají algoritmy AES nebo 3DES schválené v normách FIPS. Pokud nejsou tyto algoritmy k dispozici, doporučují se algoritmy Blowfish, CAST nebo IDEA. Za minimální bezpečnou délku klíče se považuje 80 bitů. Pro 3DES se doporučuje nastavit délku 112 bitů a pro ostatní symetrické algoritmy 128 bitů. Kde je to možné a účelné (s ohledem na rychlost) i vyšší.

Použití jiných algoritmů musí být schváleno manažerem informační bezpečnosti.

Asymetrické algoritmy

Přednostně musí být použit algoritmus RSA s délkou modulu alespoň 1024 bitů. Lze použít i algoritmus DSA (minimálně 1024/160 bitů) a ECC (minimálně 160 bitů).

Použití jiných algoritmů musí být schváleno manažerem informační bezpečnosti.

Hashovací funkce

Přednostně se využívají algoritmy schválené v normách FIPS třídy SHA-2 (SHA-256, SHA-384 nebo SHA-512). Z dalších hashovacích funkcí lze použít Whirpool.

Nasazení jiných hashovacích funkcí musí být schváleno ředitelem příslušné sekce ICT a manažerem informační bezpečnosti. Za implementaci schválených kryptografických opatření odpovídá příslušný ředitel sekce ICT.

6.4 Bezpečnost systémových souborů

Plný přístup k systémovým souborům je umožněn pouze administrátorům koncových stanic, serverů, síťových prvků a ostatních zařízení, která spravují. Na servery a technologická zařízení mají přístup pouze jejich administrátoři. Běžným uživatelům není povoleno se na tyto zařízení přihlašovat. Jiný přístup se projednává v procesu řízení výjimek bezpečnosti informací (Příloha č. 6).

Změny provozního programového vybavení musí být řízeny v souladu s pravidly uvedenými v kap. 5.1.

6.5 Řízení zranitelností ICT

Řízení, správa a kontrola technických zranitelností je upravena Přílohou č. 7 SM/88.

6.6 Profylaxe

Provozovatel IS je odpovědný za zpracování plánu pro preventivní diagnostiku a údržbu prvků IS v souladu s jejich aktuálním stavem, kritičností a stavem provozního prostředí. Preventivní údržba musí být prováděna plánovaně tak, aby neohrozila provoz obchodních a informačních systémů společnosti.

7 ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Povinnosti uživatelů i administrátorů a příslušné postupy pro zvládání bezpečnostních incidentů jsou uvedeny Příloze č. 8 SM/88.

8 ŘÍZENÍ KONTINUITY ČINNOSTÍ ORGANIZACE

Řízení kontinuity činností se realizuje v souladu s obecně závaznými právními předpisy a interní dokumentací v souladu s Přílohami č. 10 a č. 11 SM/88.

Administrátoři systémů a zařízení spolupracují při návrhu a testování plánu obnovy ICT (havarijní plány) se specialisty bezpečnosti informací. V případě vzniku havarijní události odstraňují škody a obnovují funkčnost systémů a zařízení v souladu s postupy definovanými v plánech obnovy ICT. Za vytvoření havarijních plánů a plánů obnovy odpovídá provozovatel IS.

9 SOULAD S POŽADAVKY

Administrátoři systémů a zařízení jsou povinni dodržovat obecně závazné právní předpisy, pravidla a bezpečnostní opatření definovaná interní bezpečnostní dokumentací a ustanoveními této přílohy, která se týkají ochrany důležitých informací organizace, osobních údajů a ochrany duševního vlastnictví (autorská a patentová práva).