Příloha č. 4

Pravidla pro provozovatele IS

OBSAH

ČÁST I. ÚVODNÍ USTANOVENÍ

Tato příloha se týká výhradně externích subjektů, které pro MD zajišťují provoz IS a těch zaměstnanců MD, kteří jsou v roli administrátorů IS MD a jejich nadřízených (jedná se vesměs o zaměstnance, které řídí ředitel Odboru ICT).

Kapitola 1 DEFINICE POJMŮ A ZKRATEK

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

DMZ: demilitarizovaná zóna (speciální typ počítačové sítě, která se využívá ke zvýšení bezpečnosti komunikace s vnějším prostředím a plní roli firewallu).

HelpDesk: kontaktní místo pro všechny uživatele IS MD pro případ potíží nebo požadavků.

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

Informační aktivum: jakákoli informace nebo prostředek pro práci s ní, který má pro MD nějakou hodnotu.

Informační systém (IS): informační infrastruktura, soustava aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací.

Incident: jakákoli odchylka od popsaného stavu, resp. výpadek služby.

Bezpečnostní incident: událost v IS, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky.

OTP: jednorázové heslo (One Time Password).

Podpůrné informační aktivum: technické informační aktivum, zaměstnanci a dodavatelé, podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému

Provozovatel IS: subjekt, zajišťující provoz daného informačního systému tak, aby odpovídajícím způsobem a se stanovenou spolehlivostí podporoval procesy MD (provozovatelem interních IS MD je Odbor ICT).

Správce informačního systému: vedoucí zaměstnanec, který určuje účel zpracování informací a podmínky provozování informačního systému.

Technické informační aktivum: fyzická informační aktiva (především hardware ICT), programová informační aktiva (především aplikační a databázový SW), telekomunikační a další technické a podpůrné služby.

Vlastník (garant) informačního aktiva: vedoucí zaměstnanec, který odpovídá za zajištění rozvoje, použití a bezpečnosti informačního aktiva.

Kapitola 2 ROZSAH PŮSOBNOSTI

Tato příloha BPI MD stanovuje základní pravidla/principy/zásady, povinnosti a odpovědnosti provozovatelů (resp. administrátorů a jejich nadřízených) IS MD.

ČÁST II. ORGANIZACE BEZPEČNOSTI INFORMACÍ

Kapitola 1 ROLE, ODPOVĚDNOSTI A PRAVOMOCI

Ředitel Odboru ICT:

- řídí dokumentaci infrastruktury ICT,
- definuje pravidla pro evidenci informačních aktiv v rozsahu služeb, poskytovaných Odborem ICT,
- definuje pravidla pro dokumentaci služeb IS MD včetně zálohování,
- zajišťuje implementaci a monitorování bezpečnostních opatření v rozsahu služeb, poskytovaných Odborem ICT,
- řídí rizika služeb, poskytovaných Odborem ICT,
- řídí technické zranitelnosti,
- vede a průběžně aktualizuje seznam bezpečnostních výjimek v souladu s požadavky Přílohy č. 6 BPI MD.

Administrátor IS (není podstatné, zda se jedná o zaměstnance MD nebo externího subjektu):

- průběžně aktualizuje evidenci svěřených informačních aktiv v souladu s BPI MD,
- zajišťuje zabezpečení všech svěřených informačních aktiv v souladu s BPI MD,
- předchází vzniku bezpečnostních incidentů/problémů a aktivně postupovat při oznamování, odhalování a likvidaci jejich následků,
- spolupracuje při analýzách rizik, hodnocení stavu informační bezpečnosti a při bezpečnostních auditech,
- spolupracuje při zavádění a realizaci bezpečnostních opatření,
- spolupracuje při zajištění kontinuity činností a plánů obnovy po havárii,
- spolupracuje při provádění bezpečnostních auditů, analýz zranitelností a penetračních testů.

Kapitola 3 ODDĚLENÍ POVINNOSTÍ

Provozovatel zajistí dodržování pravidla neslučitelnosti provozních, bezpečnostních a kontrolních rolí. Dále zajistí, aby:

- pracovníci vývoje nebyli oprávněni provádět administraci provozních serverů, které byly předány do správy provozovatele IS,
- administrátoři neměli oprávnění umožňující editaci vzdálených auditních záznamů (logů),
- administrátoři neměli oprávnění umožňující manipulaci s daty na spravovaných zařízeních, pokud tato oprávnění nepotřebují k plnění svých pracovních povinností (pracovní povinností je míněn i zásah provedený na zdokumentovanou žádost vlastníka informačního aktiva) nebo neexistuje možnost oddělení těchto práv vzhledem k architektuře systému,
- administrátoři neměli administrátorská oprávnění k zařízením, která nespravují a nenesou za jejich provoz odpovědnost,
- administrátoři nemohli používat privilegovaný účet pro jinou než administrátorskou činnost s výjimkou účtů pro správu koncových stanic.

Kapitola 4 VÝJIMKY Z USTANOVENÝCH PRAVIDEL

Výjimky z pravidel stanovených touto přílohou BPI MD (v důsledku technického omezení, architektury systému, omezenou pracovní kapacitou nebo specifikou pracovních povinností specialistů ICT), musí být předem zdokumentovaným způsobem schváleny Manažerem KB.

ČÁST III. HODNOCENÍ PODPŮRNÝCH INFORMAČNÍCH AKTIV

Vlastník podpůrného informačního aktiva provádí jeho hodnocení. Stupeň hodnocení podpůrného informačního aktiva musí odpovídat hodnocení primárního informačního aktiva s nejvyšším stupněm hodnocení, na jehož zpracování se dané podpůrné informační aktivum podílí.

ČÁST IV. ŘÍZENÍ PŘÍSTUPU

Kapitola 1 POŽADAVKY NA ŘÍZENÍ PŘÍSTUPU

Všem uživatelům mohou být přidělena pouze taková oprávnění, která potřebují k vykonávání svých pracovních povinností. Při přidělování uživatelských práv platí zásada „co není povoleno, je zakázáno“.

Administrátor je oprávněn přidělit uživateli oprávnění, pokud jsou splněny tyto podmínky:

- přidělení uživatelského oprávnění bylo schváleno správcem IS v souladu s Přílohou č. 5 BPI MD,
- nastavení umožňuje jednoznačné určení zodpovědnosti za prováděné operace,
- přidělování a využívání přístupových práv musí být vedeny auditní záznamy (logy) v souladu s požadavky této přílohy BPI MD,
- pokud jsou pro řízení přístupu použity biometrické prostředky, musí být použity v souladu s platnou legislativou.

Administrátoři jsou povinni alespoň 1x měsíčně kontrolovat přístupová oprávnění. Případné zjištěné „non-compliance“ stavy (např. existence účtu zaměstnance, který již na MD nepracuje) musí administrátoři neprodleně řešit.

Součástí této kontroly musí být dále identifikace dlouhodobě nevyužívaných účtů (účet nebyl použit déle než 120 dní). Dlouhodobě nevyužívané standardní uživatelské účty mají být zrušeny, dočasně zneplatněny a podobně. Možnost zrušení nebo potřebu ponechání aktivního dlouhodobě nevyužívaných technologických účtů musí administrátorovi odsouhlasit správce IS.

Pro potřeby přístupů dodavatelů za účelem podpory nebo řešení problémů (neplatí pro externisty v rolích administrátorů systémů, na ty se vztahují stejné požadavky jako na zaměstnance MD ve stejných rolích) mohou být vytvořeny účty, pomocí kterých mohou zaměstnanci dodavatele přistupovat k systémům. Tyto účty musí splňovat požadavky uvedené v ČÁSTI IV, Kapitole 3 (*„Správa a řízení přístupu uživatelů“*). Pokud je nutné vytvořit pro potřeby podpory účet, který bude sdílen více pracovníky jednoho dodavatele, musí takový účet splnit tyto podmínky:

- s dodavatelem je podepsána platná smlouva,
- jsou dodržena všechna ustanovení této přílohy BPI MD,
- účet je implicitně (defaultně) zablokován a odblokovává se pouze pro dobu nezbytnou k vyžádanému zákroku,
- uživatelské účty nesmějí být sdíleny více dodavateli.

Při konfiguraci systému musí administrátor nastavit politiku pro uživatelská hesla, která bude kontrolovat dodržování požadavků Vyhlášky o kybernetické bezpečnosti (Správa identit).

Pokud dojde k uzamčení účtu z důvodu velkého počtu neúspěšných přihlášení, musí být účet uzamčen minimálně 30 minut nebo do zásahu administrátora.

Administrátor systému komunikujícího s Internetem a sdílejícího autentizaci s důvěryhodnými systémy ve vnitřní síti, které slouží mj. i pro autentizaci (např. AD), je povinen zajistit, že při dosažení nejvyššího povoleného počtu neúspěšných přihlášení bude pouze blokováno další

přihlášení, nikoliv však uzamčení účtu na úrovni důvěryhodných autentizačních služeb ve vnitřní síti.

Je povoleno použití stejných hesel k serverům patřícím ke stejné službě a zároveň zpracovávajícím informace stejné klasifikace.

Hesla se nesmějí v systému vyskytovat v otevřené (nešifrované) podobě. Administrátoři jsou povinni používat pro šifrování hesel nejsilnější algoritmus, který je v distribuci systému dostupný, pokud to negativně neovlivní chod systému, přičemž mohou využít i silnější algoritmy dodávané mimo standardní distribuci systému.

Je-li to technicky možné, jsou administrátoři povinni umožnit (případně upřednostnit) silnou autentizaci – např. použití interních autentizačních služeb nebo jednorázových hesel zasílaných odděleným komunikačním kanálem.

V případě použití jednorázového hesla, musí být toto heslo generováno off-line (nezávisle na komunikačním kanálu použitém k přihlašování) k tomu určeným zařízením, nebo musí být uživateli doručeno bezpečným kanálem fyzicky odděleným od komunikačního kanálu použitého k přihlašování a musí splňovat následující parametry:

- maximální doba platnosti OTP od jeho vydání/zaslání: 5 minut, nebo vyžádání nového OTP (co nastane dříve),
- minimální délka: 11 znaků (z množiny 0-9), nebo 7 znaků (z množiny a-z + 0-9).

Kapitola 2 ŘÍZENÍ PŘÍSTUPU K SÍŤOVÝM SLUŽBÁM

Pro řízení přístupu uživatelů k pracovním stanicím musí být vytvořeny a aplikovány skupinové politiky Active Directory. Tyto politiky specifikuje Odbor ICT.

Na pracovních stanicích je zakázáno sdílet celé disky i jednotlivé adresáře kromě standardního systémového sdílení.

Na uživatelských stanicích je zakázáno sdílení tiskáren, všechny tiskárny používané více zaměstnanci musí být připojeny k lokální síti pomocí tiskového (print) serveru. Tiskárny umístěné ve společných prostorách MD (chodby, openspace a podobně) musí být vybaveny autentizačními mechanismy pro uživatele. Administrátoři jsou povinni zabezpečit funkčnost těchto mechanismů, tak aby nedocházelo ke spouštění tiskových úloh bez přítomnosti oprávněných uživatelů.

Na standardních serverech nesmí být uživatelům povoleno přihlášení k operačnímu systému. Uživatelé se mohou přihlašovat pouze ke službám, které jsou serverem nabízeny dle provozní dokumentace a stanovení účelu serveru.

K technologickým stanicím mají uživatelé zakázaný přístup, mohou k nim přistupovat pouze jejich administrátoři, případně pověření technici.

K bezpečnostním prvkům mohou přistupovat pouze jmenovitě určení administrátoři, Manažer KB, Architekt KB a případně jmenovitě pověření uživatelé.

Kapitola 3 SPRÁVA A ŘÍZENÍ PŘÍSTUPU UŽIVATELŮ

3.1 Zřízení a zrušení uživatelského účtu

Administrátoři mohou zřídit či zrušit uživatelský účet pouze na základě schváleného požadavku. Každý uživatelský účet musí mít unikátní ID v rámci systému, kde je zřízen, které odpovídá jmenné konvenci Odboru ICT.

Administrátoři jsou povinni minimálně 1x měsíčně (doporučeno je po 1. dnu v měsíci) kontrolovat přidělení přístupových oprávnění uživatelům, kteří již nejsou zaměstnanci MD, jsou dlouhodobě

nepřítomni, resp. s nimi byla ukončena spolupráce jako s externisty. Pokud administrátor zjistí přidělení oprávnění takovému uživateli, musí okamžitě účet zneplatnit.

3.2 Zřízení přístupu uživatele

Administrátoři jsou oprávněni uživatelským účtům nastavit přístupová oprávnění pouze na základě schváleného požadavku.

Jakékoliv změny v nastavení přístupových oprávnění mohou administrátoři provádět pouze na základě schválených požadavků, nebo při řešení havarijních situací (je-li to nezbytné pro vyřešení situace), nebo pokud ponechání přístupových práv ohrožuje provoz/stabilitu systému. O změně přístupových práv, která nebyla provedena na základě schváleného požadavku nebo nebyla hlášena jako bezpečnostní incident, musí administrátoři bez zbytečného odkladu informovat dotčeného uživatele a/nebo jeho nadřízeného.

Je zakázáno zřizování hromadných/skupinových uživatelských účtů, případně sdílení těchto účtů. Takovéto účty jsou administrátoři povinni smazat/zakázat okamžitě při jejich detekci a jejich existenci hlásit jako bezpečnostní incident.

Přístupová oprávnění musí být definována jako vazba na pracovní pozici zaměstnance (definuje nadřízený zaměstnanec), v případě změny pracovní pozice musí administrátoři odpovídajícím způsobem změnit i přístupová oprávnění uživatelského účtu zaměstnance.

3.3 Řízení privilegovaných přístupových práv

Privilegovaný přístup k prvku IS může mít přidělen pouze pracovník, který je pověřen administrací (obdobně platí i pro účty umožňující částečnou administraci, např. backup). Seznam pracovníků s administrátorskými resp. privilegovanými oprávněními musí být součástí provozní dokumentace.

Administrátorské účty se nesmějí používat pro činnosti nesouvisející s administrací. Pro běžnou agendu musí administrátor využívat neprivilegovaného účtu, pro jednotlivý administrativní zásah je doporučeno používat příkazy pro spuštění aplikace s jinými právy, než je aktuální login (‘runas‘ resp. ‘su do‘), případně bezpečné (např. „ssh“) připojení ke službě vyhrazené na daném serveru pro administraci umožňující pouze lokální připojení. Toto ustanovení se nevztahuje na uživatelské účty, které mají přidělená administrátorská práva pro pracovní stanice.

Pro administraci i jakoukoliv jinou činnost je zakázáno přímé přihlašování k implicitním (defaultním) systémovým účtům určeným pro administraci. Musí být vytvořen účet pro každou fyzickou osobu provádějící administraci, která následně použije utilitu ‘runas‘ resp. ‘su do‘, případně použije bezpečné (např. „ssh“) připojení ke službě vyhrazené na daném serveru pro administraci umožňující pouze lokální připojení.

Administrátoři jsou povinni účelně používat všechny dostupné mechanismy pro řízení přístupu (např. ACL či nastavení packet filtru na síťovém rozhraní). Pokud je to technicky možné, jsou povinni využívat přidaných hodnot trusted systémů.

Administrátoři jsou povinni využívat možnosti nastavovat práva ke zdrojům OS (např. práva zapisovat do registrů, skupina wheel u UNIXu a podobně), pokud je takové nastavení účelné.

3.4 Řízení chráněných autentizačních informací uživatelů

Všechny systémy musí, je-li to technicky možné, při prvním přihlášení uživatele vynucovat změnu prvotního hesla (=hesla, které bylo uživateli předáno správcem systému). Stejná změna hesla musí být vynucena i při každém novém vygenerování hesla (např. při zapomenutí hesla uživatelem). Předání takového hesla musí být realizováno odděleným komunikačním kanálem (např. nové heslo k webovému portálu nesmí být posláno emailem, ale může být zasláno SMSkou na mobil uvedený

v oficiálním telefonním seznamu). Heslo nesmí být mezi administrátory sdíleno, musí být uchováváno v tajnosti a při předávání nesmí být dostupné třetí osobě.

Administrátor je po instalaci systému/síťového prvku a jakéhokoliv dalšího zařízení či softwaru vždy povinen neprodleně změnit výchozí autentizační informace výrobce.

3.5 Odpovědnost uživatelů

Odpovědnosti uživatelů jsou definovány v Příloze č. 3 BPI MD.

3.6 Řízení přístupu k systémům a aplikacím

Administrátoři jsou povinni používat netriviální hesla, jež respektují požadavky na sílu hesla stanovené v ČÁSTI IV, Kapitole 2 této přílohy BPI MD („Pravidla řízení přístupu“).

Administrátoři jsou povinni chránit hesla před kompromitací a minimalizovat všechna rizika související s jejich vyzrazením.

Administrátoři jsou povinni ukládat šifrovací klíče chráněné pomocí „passphrase“, pokud klíč neslouží pro automatický provoz.

Administrátoři jsou povinni, pokud je to technicky možné, zajistit běh služeb pod jinými oprávněními, než má superuživatel („root“, resp. „administrator“).

Administrátoři jsou povinni používat „access control“ listy a další mechanismy řízení oprávnění ať už k souborovým systémům nebo k aplikacím, pokud je to účelné, a zároveň, pokud je to technicky možné, jsou povinni využívat přidaných hodnot „trusted“ systémů. Administrátoři jsou povinni zajistit, aby k jimi spravovaným serverům nebylo možné přistupovat jinak, než definovaným a schváleným způsobem (např. vypnutí nepoužívaných služeb a „daemonů“, využití interních firewall systémů a podobně).

U serverů, kde je to technicky možné, s uživatelskými účty, které mohou díky svému nastavení umožnit vykonání nějaké systémové úlohy, je administrátor povinen nastavit limity takovému uživateli, které omezí využití CPU, RAM, místa na disku a podobně.

Administrátoři jsou povinni zajistit monitoring přístupu a činnosti externistů v roli podpory k informačním aktivům MD – v případě vzdáleného přístupu externistů (po síti) logováním, v případě fyzického přístupu k zařízení zajištěním odborného dozoru po celou dobu zásahu.

3.7 Bezpečné postupy přihlášení

Administrátoři jsou povinni, je-li to technicky možné, implementovat takovou politiku pro přihlášení, která zajistí:

- heslo nebude při zadáváni, resp. ani v jiných případech, zobrazeno,
- heslo nebude přenášeno (např. mezi uživatelským SW a serverem) v nešifrované podobě,
- informování uživatele o špatném přihlášení, které mu neposkytne žádné informace či nápovědu pro uhodnutí přihlašovacího jména či hesla (doporučujeme uvádět pouze "špatné uživatelské jméno či heslo" a kontakt na pracovníka uživatelské podpory),
- automatické odhlášení uživatele a/nebo uzamčení pracovní stanice po 15 minutách nečinnosti.

Administrátoři jsou povinni zajistit ochranu proti „brute force“ (hrubý útok automatickým opakovaným přihlášením a podobně) a dalším technickým útokům na hesla, viz minimální požadavky na nastavení politiky pro hesla, definované v ČÁSTI IV, Kapitole 2 této části (Pravidla řízení přístupu“) a požadavky na logování přístupů definované v ČÁSTI VI, Kapitole 4 této přílohy BPI MD („Monitorování“).

Pro SSH autentizaci administrátorů k systémům není povoleno používání pouze jména + hesla.

3.8 Použití privilegovaných obslužných programů

Administrátoři jsou povinni zajistit, aby uživatelé mohli přistupovat ke zdrojům jimi spravovaných systémů pouze v rozsahu stanoveném schválenými přístupovými oprávněními. Zejména jsou administrátoři povinni zamezit uživatelům v přístupu k systémovým adresářům a souborům a zajistit, aby všechny uživatelem spouštěné programy pracovaly výhradně pod účtem uživatele.

3.9 Řízení přístupu ke zdrojovému kódu programu

Ke zdrojovým kódům programů mohou přistupovat pouze pracovníci pověření vývojem (případně pracovníci provádějící audit zdrojového kódu).

Zdrojový kód nesmí být umístěn na provozních serverech; zdrojový kód aktuálně testovaných aplikací může být v případě potřeby ve výjimečných případech umístěn na testovacích serverech.

Vývojáři nesmějí být zároveň administrátory provozních serverů.

ČÁST V. KRYPTOGRAFICKÁ OPATŘENÍ

Administrátoři IS, které využívají některá kryptografická opatření (algoritmy, bezpečnostní protokoly, klíčové hospodářství, speciální software a hardware), musí při jeho celém životním cyklu (od instalace, konfigurace, provozu, výroby a distribuce klíčů a jiných směnných prvků (např. tokenů pro bezpečné uložení certifikátů) až po likvidaci tohoto systému) postupovat v souladu s dodanou dokumentací a minimálními požadavky, které jsou uvedeny v této příloze BPI MD. Dále pak je vhodné brát v potaz hodnocení bezpečnosti příslušného řešení resp. další dokumenty, které se zabývají aspekty kryptografické ochrany.

Při výběru algoritmů a síly mechanismů se administrátoři řídí minimálními požadavky uvedenými v této kapitole a výsledky hodnocení a příslušnými doporučeními.

Kapitola 1 GENERÁTORY NÁHODNÝCH ČÍSEL

MD preferuje použití fyzikálního generátoru náhodných čísel. V případě provozování takovéhoto generátoru je potřeba zajistit statistické testování na kvalitu výstupu a test funkčnosti generátoru.

V případě použití pseudonáhodného generátoru (PRNG – Pseudo-Random Number Generator) náhodných čísel je potřeba zajistit vhodný nepredikovatelný způsob náhodného a dostatečně velkého počátečního nastavení („seed“). Množina všech reálně dosažitelných počátečních nastavení musí být tak velká, aby nedávala útočníkovi možnost získat výsledky takovéhoto pseudonáhodného generátoru.

Kapitola 2 SYMETRICKÉ ALGORITMY ASYMETRICKÉ ALGORITMY A HASHOVACÍ FUNKCE

Výběr šifrovacích algoritmů a hashovacích funkcí se řídí aktuálními doporučeními Národního úřadu pro kybernetickou a informační bezpečnost.

Použití jiných algoritmů a funkcí musí být schváleno jako výjimka v souladu s Přílohou č. 6 BPI MD.

Kapitola 3 SPRÁVA KLÍČŮ A CERTIFIKÁTŮ

Při výběru symetrického a asymetrického algoritmu je potřeba vždy doplnit popis životního cyklu použitého klíče a jeho distribuce. Tento popis musí být v tomto minimálním rozsahu: generování klíče, uložení klíče, vlastnictví klíče, přístup ke klíči, požadavky na jeho použití (např.

u symetrické šifry uvést omezení na objem šifrovaných dat), uvést zda je možné provést obnovu klíče a pokud ano, tak za jakých podmínek, postup při kompromitaci klíče.

Za správu klíčů a certifikátů odpovídá garant certifikátu. Tj. každá dvojice klíčů asymetrické kryptografie a každý klíč symetrické kryptografie má svého garanta. Jeho povinností je:

- zajistit bezpečné uložení kopie klíče / klíčů,
- podílet se na rozhodnutí, které klíče a certifikáty je možné nasadit pro určitou aplikaci,
- zajistit používání klíčů a certifikátů ve shodě s certifikační politikou vydávající certifikační autority,
- bezpečné předání klíčů správcům serverů, respektive aplikací,
- kontrolovat využívání klíčů a certifikátů,
- vést přehled, kde jsou jednotlivé klíče a certifikáty používány a komu byly předány,
- vést přehled o platnosti certifikátů a zajistit jejich včasnou obnovu,
- v případě potřeby zajistit odvolání certifikátu.

ČÁST VI. BEZPEČNOST PROVOZU

Kapitola 1 PROVOZNÍ POSTUPY A ODPOVĚDNOSTI

1.1 Dokumentace provozních postupů

Veškeré provozní postupy musí být dokumentovány. Provozní postupy musí jednoznačně popisovat všechny rutině prováděné zásahy tak, jak mají být prováděny v podmínkách MD. Nedílnou součástí těchto postupů jsou i havarijní plány a plány obnovy systému po havárii.

Všechna zařízení v IS MD musí být (jako podpůrná informační aktiva) identifikována a evidována. Tato evidence musí být klasifikována přinejmenším bezpečnostním klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU“.

Evidence pracovních stanic musí obsahovat minimálně následující údaje:

- informace o HW i SW konfiguraci stanice (včetně konfigurace síťových připojení a standardních aplikací),
- informace o všech provozních aktivitách (včetně data a času a jména administrátora, který zásah provedl),
- informace o konfiguraci softwaru instalovaného nad rámec standardních instalací,
- informace o přidělení stanice konkrétnímu uživateli (včetně zdůvodnění/účelu).

Evidence serverů musí obsahovat minimálně následující údaje:

- informace o HW i SW konfiguraci serveru (včetně konfigurace síťových připojení a běžících služeb/“daemonů“),
- informace o všech provozních aktivitách (včetně data a času a jména administrátora, který zásah provedl),
- informace o instalovaném software (aplikace, databáze …),
- informace o požadavcích a realizaci zálohování dat i systému,
- informace o klasifikačním stupni informací, které jsou na serveru uloženy nebo zpracovávány,
- informace o konfiguraci instalovaného bezpečnostního software a nastavení auditování událostí,
- informace o fyzickém umístění,
- informace o administrátorech zodpovědných za provoz serveru i jednotlivých aplikací.

Evidence síťových prvků („huby“, „switche“, „routery“, „firewally“ …) musí obsahovat minimálně následující údaje:

- informace o konfiguraci HW i SW zařízení včetně informací o nastavení auditování událostí,
- informace o fyzickém umístění,
- informace o všech provozních aktivitách (včetně data a času a jména administrátor, který zásah provedl),
- informace o administrátorech zodpovědných za provoz zařízení.

Součástí evidencí prvků IS musí být ke každému prvku i seznam jeho administrátorů. K těmto evidencím mohou přistupovat pouze:

- administrátoři – možnost čtení i zápisu pro záznamy o systémech, které jsou v jejich správě,
- zaměstnanci v oblasti bezpečnosti (Manažer KB a jím pověření zaměstnanci) – možnost čtení pro všechny záznamy a možnost zápisu relevantních informací (např. informace o bezpečnostních testech),
- auditoři – možnost čtení pro všechny záznamy,
- a další zaměstnanci, kteří informace potřebují ke své práci (např. HelpDesk) – přístupy definované po domluvě s administrátory daného zařízení/systému na základě pracovních povinností.

1.2 Řízení změn

Všechna zařízení pro zpracování informací a změny na nich prováděné podléhají změnovému řízení v odpovědnosti Odboru ICT. Za změny ve smyslu ustanovení této kapitoly nejsou považovány rutinní provozní zásahy.

Každé změně musí předcházet analýza jejího dopadu na provoz a musí se k ní vyjádřit administrátoři zařízení/systémů, kterých se dotýká. Na základě této analýzy musí realizátor změny vypracovat harmonogram, který zajistí minimalizaci výpadků jednotlivých komponent systému a jím poskytovaných služeb. Analýza dopadů i harmonogram musí být dokumentovány, kromě případů, kdy se nejedná o změny zásadního charakteru na spravovaném(ých) zařízení(ch) – určuje administrátor. Požadovanou dokumentaci zajistí žadatel změny, ostatní pracovníci (např. administrátoři) jsou povinni poskytnout potřebné součinnosti.

Pokud změna svým rozsahem znamená zásah do podstatné části IS, dotýká se zařízení v DMZ, dotýká se zařízení nebo systémů provozujících bezpečnostní technologie, případně se dotýká zařízení zpracovávajících informace klasifikované bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ“, musí změnu kromě provozních útvarů odsouhlasit i Manažer KB.

1.3 Plánování kapacit

Plánování kapacit jednotlivých komponent IS je odpovědností Odboru ICT. Organizační jednotky, případně externí subjekty, odpovídají za monitorování provozu systému tak, aby zajistily včasnou detekci vzniklých problémů se zdroji (disková kapacita, operační paměť propustnost sítě a podobně). Součástí provozních doporučení je i plánování budoucí spotřeby kapacit s ohledem na plánování a řízení změn na MD. Při plánování kapacit musí být zohledněny i aplikace/systémy, které pro ukládání dat využívají externí datová úložiště (např. „cloudové“ systémy).

Administrátoři musí brát při výběru software (i hardware) v úvahu počet a stav řešení známých zranitelností všech jeho verzí v historii.

1.4 Princip oddělení prostředí vývoje, testování a provozu

Vývojové, testovací a provozní prostředí musí být odděleny. Testování nových verzí software (resp. nového hardware) nesmí probíhat v provozním prostředí. Tyto testy nesmějí být prováděny nad ostrými daty. Pokud takové testování není možné, musí případné výjimky schválit administrátoři provozních zařízení, vlastnící dat a Manažer KB. Testování nad osobními údaji je možné pouze po jejich anonymizaci.

Nový hardware či software může být nasazen až poté, co jsou splněny předem definované podmínky. Tyto podmínky definují zaměstnanci Odboru ICT, případně je upřesňují pro konkrétní HW či SW a schvaluje je Manažer KB.

Na provozních serverech nesmí být instalovány překladače a systémové utility, které nejsou nezbytné pro správu.

Pracovníci vývoje nesmějí mít administrátorský přístup k provoznímu prostředí. Pokud to z technických či provozních důvodů není možné, musí případné výjimky schválit administrátoři provozních zařízení, Manažer KB a musí být navržena kompenzační opatření.

Kapitola 2 OCHRANA PŘED ŠKODLIVÝM KÓDEM

Jako ochrana proti škodlivým programům musí být instalován antivirový software s centrálním managementem. V případě potřeby mohou administrátoři instalovat i další software pro detekci škodlivého kódu. Takový software musí být schválen Manažerem KB a Odborem ICT.

Administrátorům je zakázáno vypínat bezdůvodně antivirovou ochranu. O vypnutí musí být vytvořen záznam v příslušné provozní dokumentaci. Antivirový software musí být instalován na všech uživatelských stanicích a relevantních serverech (servery s operačním systémem Windows, „fileservery“, mailové „gatewaye“ a další, pro které příslušné SW nástroje existují, resp. jsou přínosné).

Nastavení antivirové kontroly pro uživatele jsou administrátoři povinni konfigurovat takovým způsobem, aby ji uživatelé nemohli svévolně vypínat.

Administrátoři mohou na provozní systémy instalovat pouze software, který odpovídá požadavkům stanoveným v odstavci 5.4 („Instalace softwaru na provozní systémy“).

Administrátoři odpovídají za to, že veškerý software na serverech i pracovních stanicích je instalován, konfigurován a spravován tak, aby pravděpodobnost napadení škodlivým programem byla minimalizována. To znamená zejména:

- požadování autentizace pro každé spojení se serverem či stanicí ze sítě (interní i veřejné),
- zakázání všech vzdálených spojení se servery i stanicemi, která nejsou potřebná pro výkon činnosti, dohled či správu,
- vypnutí všech voleb („features“), které nejsou potřebné pro provoz serveru či pracovní stanici, resp. pro práci uživatelů,
- bezpečné nastavení všech programů komunikujících po síti,
- pravidelná aktualizace v závislosti na nově objevených chybách a zranitelnostech.

Administrátoři jsou dále povinni provádět pravidelné kontroly jimi spravovaných zařízení na přítomnost škodlivého kódu.

Kapitola 3 ZÁLOHOVÁNÍ

Požadavky na četnost/frekvenci, dostupnost záloh a dobu jejich uchování stanoví vlastník zpracovávaných informací v závislosti na dopadech nedostupnosti či ztráty dat. Veškeré zálohy musí podléhat obdobným ochranným opatřením jako původní data a musí být klasifikovány klasifikačním stupněm stejným nebo vyšším, jako jejich nejvýše klasifikovaná předloha.

Administrátoři zodpovědní za zálohování jsou (kromě jiného) povinni:

- zajistit dostatečnou zálohovací kapacitu,
- pravidelně (doporučeno alespoň 1x za rok) kontrolovat životnost použitých zálohovacích médií dle specifikací výrobce (média s končící životností nahradit),
- pravidelně (doporučeno alespoň 1x za rok) kontrolovat čitelnost zálohovaných dat

- pravidelně (doporučeno alespoň 1x za rok) provádět testovací obnovu dat.

Kapitola 4 MONITOROVÁNÍ

Požadavky na provozní monitoring prvků IS musejí respektovat právní předpisy (např. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů).

4.1 Požadavky na auditní záznamy

Administrátoři jsou povinni nastavit na spravovaných systémech logování minimálně dle požadavků této přílohy BPI MD. Pro konkrétní systémy může být správcem IS požadováno logování nad rámec této přílohy BPI MD. Každý záznam v logu musí obsahovat minimálně tyto informace:

- datum a čas, kdy k události došlo,
- ID uživatele (či automatu),
- zdroj (IP adresa, lokální konzole a podobně),
- vlastní auditní informaci.

V logovacích souborech nesmí být při chybných i úspěšných přihlášeních zaznamenáváno heslo.

Administrátoři jsou povinni při vzdáleném on-line logování zajistit zasílání definovaných (domluvených při přípravě on-line logování) záznamů v případě, že v definované době nedošlo k žádné události, která by auditní záznam vygenerovala („keep alive“); tato doba je minimálně 300 sekund, pro konkrétní systémy může být na základě klasifikace zpracovávaných informací zkrácena.

Veškeré uvažované změny v nastavení logování (vynucené změnami v provozu zařízení, jeho upgradem/nahrazením, či z jiných důvodů) jsou administrátoři povinni bez prodlení oznámit Manažerovi KB; v případě použití vzdáleného logování i pracovníkům odpovědným za provoz systémů pro sběr těchto logů.

V případě, že z technických (případně jiných) důvodů není možné zajistit logování podle požadavků této přílohy BPI MD, případně další řídící dokumentace, jsou administrátoři povinni tuto skutečnost ohlásit Manažerovi KB a zažádat o výjimku.

Výpadek auditních funkcí požadovaných touto přílohou BPI MD musí být řešen jako bezpečnostní incident.

4.2 Monitorování uživatelských aplikací

Všechny aplikace musí umožňovat nastavení logování v níže uvedeném rozsahu. Pro záznam auditních událostí mohou aplikace využívat prostředky operačního systému či jiného instalovaného SW.

Bezpečnostní log aplikace musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- informace o přihlášení a odhlášení uživatelů i administrátorů,
- informace o změnách v metodě zabezpečení (včetně nastavení politiky pro logování),
- informace o provedených změnách dat,
- informace o přístupech uživatelů k informacím klasifikovaným stupněm „CHRÁNĚNÉ“,
- informace o importech a exportech dat.

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na klasifikačním stupni informací, se kterými aplikace pracuje. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.3 Monitorování uživatelských stanic

Logování musí být zapnuto na všech uživatelských stanicích. Bezpečnostní log může být dostupný (pokud to je technicky možné, tak jen pro čtení) pouze uživatelům zařazeným ve skupině „administrators“ (resp. v příslušné globální skupině). Bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- přihlášení a odhlášení,
- správa uživatelů a skupin,
- připojení a odpojení externích zařízení,
- změny v metodě zabezpečení,
- použití uživatelských práv.

Velikost těchto logů musí být nastavena minimálně na 16384 kB, staré události budou přepisovány novými až v případě potřeby.

Je-li na uživatelské stanici instalován jiný operační systém než standardní Windows, je jeho administrátor povinen zajistit logování událostí na úrovni popsané v této kapitole.

4.4 Monitorování standardních serverů a technologických stanic

Logování musí být zapnuto na všech serverech. Správce IS ve spolupráci s Manažerem KB stanoví pravidla a rozsah logování v závislosti na službách poskytovaných serverem.

Bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v tomto rozsahu:

- informace o přihlášení a odhlášení,
- informace o změnách v metodě zabezpečení (včetně nastavení politiky pro logování),
- připojení a odpojení externích zařízení,
- informace o změně identity („su“/“runas“),
- informace o spouštění a zastavování služeb/“daemonů“,
- informace o změně systémového data,
- informace o vypnutí/restart systému.

4.5 Monitorování serverů v DMZ

Všechny servery v DMZ musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových“ filtrů,
- informace o neúspěšném přístupu ke službě z“ tcp wrapperu“,
- informace od procesů obsluhujících aplikační vrstvu („http“, „smtp“, a podobně).

Logovaná musí být minimálně IP adresa a čas přístupu, ale pokud je to možné, i další informace (např. kompletní hlavičky paketů).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na službách poskytovaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.6 Monitorování serverů zpracovávajících „CHRÁNĚNÉ“ informace

Všechny servery, které pracují s informacemi klasifikovanými bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ“ musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových“ filtrů,
- informace o neúspěšném přístupu ke službě z „tcp wrapperu“,

- relevantní informace z aplikačního SW (pokud si administrátor není jist relevancí informací pro centrální logování, určí ji ve spolupráci s Manažerem KB nebo jím pověřenou osobou).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na informacích zpracovávaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.7 Monitorování síťových prvků

Všechny síťové prvky musí logovat následující události:

- úspěšné i neúspěšné pokusy o přihlášení/odhlášení k síťovému prvku,
- změny v konfiguraci,
- výpadky dostupnosti zařízení a síťových tras.

4.8 Monitorování bezpečnostních zařízení

Všechny bezpečnostní prvky musí vzdáleně logovat události vyžadované pro logování standardních serverů a navíc také:

- informace o odmítnutých paketech z interních „packetových“ filtrů,
- informace o neúspěšném přístupu ke službě z „tcp wrapperu“,
- všechny zásahy do konfigurace i do všech dalších součástí systému (např. změny v datových souborech).

Administrátor stanoví na základě dohody s Manažerem KB pravidla a rozsah logování v závislosti na službách poskytovaných serverem. Vlastní nastavení auditních pravidel musí být schváleno Manažerem KB nebo jím pověřenou osobou.

4.9 Ochrana auditních záznamů

Administrátoři jsou povinni auditní záznamy klasifikovat dle Bezpečnostní politiky MD a dále je vzhledem ke klasifikačnímu stupni odpovídajícím způsobem chránit. Pro klasifikaci platí, že logy musí být klasifikovány přinejmenším stupněm „PRO VNITŘNÍ POTŘEBU“.

Auditní záznamy jsou administrátoři povinni uchovávat minimálně po dobu jednoho roku, nebo dle ustanovení platné legislativy, pokud tato stanoví delší čas. Kratší dobu uchovávání logů lze stanovit pouze v případě vzdáleného logování událostí do centrálního systému pro sběr logů (případně SIEM), nebo výjimkou udělenou Manažerem KB nebo jím pověřenou osobou.

Administrátoři jsou povinni na vyžádání Manažera KB zajistit vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) na jimi spravovaných zařízeních. Konkrétní způsob realizace vzdáleného logování bude stanoven dle možností monitorovaného zařízení s maximalizací využití nástrojů na zařízení instalovaných.

K auditním záznamům mohou přistupovat pouze:

- administrátoři zodpovědní za provoz zařízení, které logy vytváří,
- administrátoři systému pro zpracování logů (pouze pro logy v takovém systému archivované),
- Manažer KB, Architekt KB a bezpečnostní správci jednotlivých IS (dále jen pracovníci v oblasti bezpečnosti) pouze čtení,
- auditoři (pouze v rámci auditu a se souhlasem Manažera KB) - pouze čtení.

Je-li to technicky možné, mohou mít přístupová práva pro zápis do auditních záznamů pouze pracovníci pověření jejich archivací nebo mazáním starých logů.
Pro zajištění důvěryhodnosti logů musí být dodrženy následující požadavky na oddělení rolí:

- administrátoři provozních zařízení (síťových prvků, serverů, aplikací) nesmí mít přístup k logům uchovávaným v centrálním systému pro sběr logů,
- administrátoři centrálního systému pro sběr logů (případně SIEM) nesmí mít administrátorský přístup k provozním zařízením (mohou však mít přístup pro čtení),
- administrátoři serverů a aplikací nesmějí mít administrátorský přístup k síťovým prvkům a nesmějí mít přístup k IDS,
- administrátoři sítě nesmějí mít, je-li to technicky možné (IDS není součástí síťových prvků) k IDS,
- administrátoři síťových prvků nesmějí mít administrátorský přístup k provozním serverům a aplikacím.

4.10 Logy o činnosti administrátorů a operátorů

Činnosti privilegovaných účtů musí být zaznamenávány do logů. Logy, je-li to technicky a organizačně možné, musejí být chráněny proti narušení ze strany těchto privilegovaných uživatelů. Za nastavení takového logování, je-li technicky možné, odpovídají administrátoři provozních zařízení.

4.11 Synchronizace hodin

Všechny servery, pracovní stanice a další prvky infrastruktury, které používají systémový čas, musí mít pravidelně (minimálně jednou za den) synchronizován systémový čas s centrálním časovým serverem MD nebo jiným zdrojem přesného času, schváleným Odborem ICT.

Kapitola 5 ŘÍZENÍ A KONTROLA PROVOZNÍHO SOFTWARU

5.1 Nasazení do provozu

Administrátoři jsou povinni instalovat a udržovat optimalizovanou sadu komponent systému. Optimalizovanou sadou komponent se rozumí pouze komponenty nezbytné pro poskytování služby, pro kterou je prostředek určen, administraci a provozní či bezpečnostní dohled systému. Administrátoři jsou povinni zajistit nespouštění nepotřebných služeb nebo démonů.

Předávání aplikací, systémů, upgrade a nových verzí do provozu se realizuje v souladu s pracovními postupy Odboru ICT. Do provozního prostředí je instalují administrátoři příslušných zařízení, systémů či aplikací.

Pro uvedení nově implementovaných systémů do provozu musí být splněny minimálně tyto podmínky:

- předaná dokumentace včetně bezpečnostní specifikace, havarijních plánů a plánů obnovy je akceptována,
- je akceptován bezpečnostní model (domluvené/stanovené bezpečnostní požadavky specifikované touto přílohou BPI MD, případně další požadavky, uplatněné ze strany MD v rámci daného projektu),
- úspěšné provozní testy,
- úspěšné bezpečnostní testy,
- školení uživatelů i obsluhy (je-li potřebné/účelné – rozhodují administrátoři, resp. uživatelé),
- další podmínky specifikované v zadání či řízené dokumentaci.

Splnění výše uvedených podmínek musí potvrdit Architekt KB a schválit Manažer KB.

Je-li nový systém dodáván a implementován externím subjektem, platí po akceptaci stejná pravidla jako pro systémy dodávané/implementované interně.

Smlouva o implementaci musí obsahovat podmínku úspěšného ukončení akceptačních testů před zaplacením implementace (resp. podstatné části této platby).

V případě, že implementace probíhá v samostatných etapách, musí být stanovena akceptační kritéria pro každou etapu.

Administrátoři mohou převzít do provozu pouze zařízení, jehož bezpečnost byla prověřena bezpečnostními testy. Tyto testy musí obsahovat minimálně „scan" na zjištění existence známých zranitelností; případné další testy, které stanoví Manažer KB. Bezpečnostní „scan" provádí Manažer KB nebo jím schválený partner. V případě nasazení mnoha prvků se shodným nastavením, je možné provést testy pouze na vybraném vzorku zařízení.

Je-li to technicky možné, jsou administrátoři povinni nahradit nebo přejmenovat implicitní (defaultní) systémové účty („root", „administrator", „guest", ...). Účty, které slouží pro správu systému, musí mít netriviální hesla a politika pro jejich používání musí splňovat minimálně podmínky stanovené touto přílohou BPI MD.

5.2 Provoz

Administrátoři jsou povinni vytvořit provozní dokumentaci všech spravovaných systémů, která bude obsahovat informace o konfiguraci systému a jejích změnách. Veškeré změny v konfiguraci spravovaných zařízení jsou administrátoři povinni, je-li to účelné, zaznamenávat i do havarijních plánů a plánů obnovy systému po havárii.

Jedno konkrétní zařízení nebo skupinu zařízení ve funkčním celku nesmí spravovat více dodavatelů nebo odborů MD. 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 administrátorů.

Vzdálená správa zařízení, která pracují s informacemi klasifikovanými bezpečnostním klasifikačním stupněm „CHRÁNĚNÉ" a zařízeními umístěnými v DMZ, musí probíhat šifrovaně podle požadavků této přílohy BPI MD (ČÁST VII, Kapitola 1, Odstavec 1.1).

Administrátoři jsou povinni udržovat otevřené pouze porty nezbytné pro zajištění chodu služeb serverů a dalších zařízení ICT. Administrátoři jsou povinni zakázat v systému všechny porty, které nejsou nezbytné pro zajištění chodu služeb serverů, uživatelských stanic a síťových prvků.

Při správě zařízení umístěných v DMZ jsou administrátoři povinni řídit se ustanoveními zvláštního předpisu stanovujícím požadavky na provoz zařízení v DMZ.

Administrátoři jednotlivých zařízení jsou povinni umožnit/zajistit instalaci a konfiguraci bezpečnostního SW definovaného Manažerem KB a potřebné komunikační prostupy. V případě, že je instalace takového SW nemožná z provozních důvodů, musí tuto skutečnost administrátor prokázat. Za průkazné jsou považovány výstupy z nástrojů pro monitoring systému, známé/zdokumentované problémy s kompatibilitou konkrétních SW komponent a výstupy z provedených testů.

5.3 Pravidelné kontroly

Administrátoři jsou povinni pravidelně (doporučeno je jednou měsíčně) najít soubory, které nevlastní žádný uživatel. Administrátor zjistí důvod, proč v systému takové soubory existují, a provede nápravu (smazání, určení vlastníka, příp. jiná činnost).

Administrátoři jsou povinni minimálně jednou měsíčně provést analýzu bezpečnostních logů spravovaných systémů a prověřit případné nalezené anomálie, zda se nejedná o narušení bezpečnosti systému, případně přípravu k útoku na systém. Odhalení útoku nebo přípravy na něj musí být hlášeno a řešeno jako bezpečnostní incident.

Administrátoři jsou povinni pravidelně (doporučeno je jednou měsíčně) kontrolovat TCP i UDP porty ve stavu „listen“. Detekce takového portu, který není uveden v provozní dokumentaci, musí být hlášena a řešena jako bezpečnostní incident. Kontrola TCP i UDP portů se netýká uživatelských stanic.

Administrátoři jsou povinni využívat nástroje pro kontrolu integrity souborového systému.

Manažer KB nebo jím pověřený zaměstnanec je oprávněn provádět v součinnosti s administrátorem namátkové testování zranitelností a slabin. S výsledky těchto testů musí být administrátoři seznámeni a jsou povinni se k nim vyjádřit.

5.4 Instalace softwaru na provozní systémy

Instalaci software na provozní zařízení mohou provádět pouze administrátoři zodpovědní za jeho provoz.

Administrátor odpovídá za to, že na pracovní stanice, servery a další zařízení v jeho správě je instalován pouze software splňující následující podmínky:

- software je potřebný pro výkon činností, správu, dohled, bezpečnost zařízení, bezpečnost IS nebo informačních aktiv MD,
- software je legálně zakoupený, případně se jedná o freeware (i pro komerční použití, např. SW pod GNU licencí a podobně), anebo SW vytvořený interně,
- software je schválen Odborem ICT a není zamítnut Manažerem KB,
- software je schválen administrátorem daného zařízení.

Před instalací software jsou administrátoři povinni ověřit konzistenci a pravost instalačních balíčků (např. kontrola CRC - Cyclic redundancy check – cyklického redundantního součtu, je-li SW stahován z/pomocí veřejné datové sítě, jedná se o originální datový nosič od výrobce neumožňující modifikaci dat a podobně).

Pokud nedošlo ke konkrétnímu pověření bezpečnostního správce, administrátoři jsou při správě svěřených zařízení povinni, zajistit, kromě jiného, i bezpečnost zařízení a informací na něm zpracovávaných či uchovávaných.

Kapitola 6 SPRÁVA A ŘÍZENÍ TECHNICKÝCH ZRANITELNOSTÍ

Administrátoři jsou povinni sledovat informace o zranitelnostech a využívat služeb pro sledování zranitelností, které jsou v této oblasti poskytovány. Administrátoři jsou povinni zajistit instalaci relevantních bezpečnostních SW oprav pro daný systém neovlivňujících negativním způsobem běh služeb a aplikací.

Pokud bezpečnostní „patch“ negativně ovlivňuje provoz zařízení, musí být jeho (ne)nasazení konzultováno s Manažerem KB tak, aby byla zvážena vhodná kompenzační, případně detekční opatření. Záznam do provozní dokumentace musí být proveden i v případě, že „patch“ instalován nebude. Tento záznam musí obsahovat detailní informace o tom, která komponenta zařízení a proč instalaci „patche“ neumožňuje, a dále pak patření přijatá pro minimalizaci rizik plynoucích z neinstalování „patche“. Pro instalaci bezpečnostních „patchů“ musí být minimálně jednou měsíčně vyhrazena časová okna v SLA daného systému.

Nápravná opatření, která jsou administrátorům uložena, mohou být aplikována až na základě souhlasu Manažera KB.

Software na servery a technologická PC mohou instalovat pouze jejich administrátoři a k tomu pověření pracovníci. Na uživatelské stanice mohou instalovat SW i pověření uživatelé, kteří mají přidělena příslušná oprávnění, musí však dodržet ustanovení této přílohy BPI MD.

Kapitola 7 AUDITY IS

Administrátoři jsou povinni poskytnout nezbytné součinnosti pracovníkům provádějícím audit nebo kontrolu podle schváleného plánu auditů a plánu testů (neplánovanou kontrolu musí schválit Manažer KB nebo ředitel Odboru ICT). Bezpečnostní testy jsou prováděny podle pracovního postupu, který definuje Manažer KB.

Pracovníci provádějící audit/testy musí mít přístup pouze pro čtení. Je-li pro provedení auditu/testů potřebné vyšší přístupové oprávnění, musí být tato skutečnost s administrátory předem konzultována a přístupová oprávnění schválena Manažerem KB. Přístup k auditním záznamům je možný pouze podle pravidel stanovených touto přílohou BPI MD nebo se souhlasem Manažera KB. Konfigurační a systémové soubory mohou být zpřístupněny pouze jako izolované kopie.

Úspěšné provedení penetračních testů (napadení testovaného systému) není považováno na bezpečnostní incident. Penetrační test bez předchozího informování administrátorů, Manažera KB a ředitele Odboru ICT je bezpečnostním incidentem vždy.

ČÁST VII. BEZPEČNOST KOMUNIKACÍ

Obecné bezpečnostní požadavky na správu síťových prvků se řídí příslušnými ustanoveními této přílohy BPI MD.

Kapitola 1 SPRÁVA BEZPEČNOSTI SÍTĚ

Jakékoliv propojení interní sítě s veřejnými datovými sítěmi musí být schváleno administrátory síťové infrastruktury a Manažerem KB. Instalovat komunikační zařízení do sítě MD smějí pouze administrátoři síťové infrastruktury.
Provoz mezi veřejnými sítěmi nebo sítěmi třetích stran a sítí MD musí být řízen pomocí firewallů. Konfigurace FW musí vycházet z principu, co není dovoleno, je zakázáno. Povolené prostupy skrz FW musí být součástí provozní dokumentace; pro každý prostup musí být uveden důvod jeho zřízení.

Služby, poskytované ze sítě MD do prostředí Internetu (webové servery, ftp servery, VPN a podobně) musí být umístěny v DMZ.

Vybrané body propojení sítě MD s veřejnými datovými sítěmi nebo sítěmi třetích stran a rozhraní mezi vybranými bezpečnostními zónami musí být monitorovány a/nebo řízeny IDS/IPS.

Administrátoři síťové infrastruktury jsou povinni zajistit potřebné propojení pro bezpečnostní monitoring a vyhodnocování dat IDS/IPS. Nasazování jednotlivých komponent systému IDS/IPS je realizováno dle potřeb MD a schválených zdrojů pro tuto oblast.

Při komunikaci je zakázáno využívat sdíleného média na linkové vrstvě modelu OSI, pokud to nevynucuje technologie.

1.1 Nastavení síťových prvků a jejich vzájemná komunikace

Administrátoři „routerů“ i „firewallů“ jsou povinni nastavovat základní filtrační pravidla, která vyplývají z RFC (popisujících konkrétní protokoly a podobně).

Pro správu síťových prvků musí být vytvořena fyzicky (nebo na úrovni VLAN) oddělená management síť.

Administrátoři síťových zařízení jsou povinni pro autentizaci vzdálené administrace používat protokolu a serveru „RADIUS“, „Diameter“, „TACACS+“ nebo podobných, případně přistupovat vzdáleně pomocí protokolu „ssh“ tam, kde je to možné, nebo využívat jinou bezpečnou technologii schválenou Manažerem KB.

Administrátoři jsou povinni využít prvků autentizace u „routovacích“ protokolů a dalšího zabezpečení, které dovoluje implementace těchto protokolů.

1.2 Změny v síťové infrastruktuře

Veškeré změny v síťovém modelu musí být schváleny Manažerem KB. Před realizací takových změn musí být síťovými administrátory sestaven havarijní plán pro případ neúspěšného ukončení nebo musí být nová infrastruktura budována paralelně se stávající.

Změnou v síťovém modelu se rozumí:

- změna oproti pravidlům a požadavkům stanoveným touto přílohou BPI MD, nebo zvláštním předpisem stanovujícím požadavky na provoz v demilitarizovaných zónách,
- modifikace propojení nebo struktury jednotlivých síťových segmentů či vytvoření nových,
- změna v IP plánu,
- změny statických „routovacích“ pravidel a „routovacích“ tabulek,
- změny, které by mohly mít dopady na funkčnost bezpečnostních prvků, např.:
  - změny ve struktuře evidencí síťových prvků a prostupů mezi síťovými segmenty či sítěmi,
  - změny v konfiguraci IDS zařízení v síťových prvcích,
  - libovolné změny v konfiguraci segmentů sítě, které slouží pro přenos dat mezi bezpečnostními systémy.
- zavádění nových technologií,
- a další, které administrátoři síťové infrastruktury budou považovat za zásadní.

1.3 Bezpečnost bezdrátových sítí

Instalaci zařízení pro poskytování služeb bezdrátové sítě mohou provádět pouze k tomu pověření pracovníci provozních útvarů se souhlasem administrátorů síťové infrastruktury.

Administrátoři jsou povinni nastavit zařízení umožňujících bezdrátový přístup do sítě MD tak, aby byly naplněny minimálně tyto požadavky:

- zařízení nesmí umožňovat anonymní přístup,
- pro autentizaci zařízení k bezdrátové síti musí být použit minimálně jeden z těchto mechanismů:
  - uživatelský certifikát vydaný interní CA – Certifikační autorita MD – nebo jinou důvěryhodnou certifikační autoritou schválenou manažerem KB,
  - 802.1x mechanismus s centrálním autentizačním prvkem,
- pro ochranu komunikace musí být použito minimálně WPA2,
- musejí být vytvářeny auditní záznamy o připojených zařízeních obsahující minimálně datum a čas připojení/odpojení zařízení, jeho MAC adresu a IP adresu.

Zařízení, která nesplňují výše uvedené požadavky, nesmějí být do interní sítě MD připojena. Provoz takových zařízení je možný pouze v případě, že umožňují přístup (jsou propojena) pouze přímo do Internetu.

Manažer KB nebo jím pověřený zaměstnanec je oprávněn provádět detekci a testy bezdrátových sítí v okolí provozních prostor MD.

1.4 Internetová gateway pro uživatele

Uživatelé (zaměstnanci MD i externisté) mohou přistupovat k Internetu pouze přes centrální přístupovou“ gateway“/“proxy“ server. Administrátoři této „gateway“ jsou povinni:

- nastavit prostupy pouze pro povolené protokoly na povolených portech,
- umožnit komunikaci s a přes tuto „gateway“ pouze z interní sítě MD.

Povolené protokoly a porty pro komunikaci uživatelů do Internetu jsou:

- http (80),
- https (443),
- ftp (20, 21),
- další pouze na základě výjimky, schválené Manažerem KB.

Administrátoři této „gateway“ jsou povinni na ni zajistit logování přístupu uživatelů k Internetu a jeho využívání. Události musí být logovány minimálně v rozsahu:

- zdrojová IP adresa,
- přihlašovací jméno (např. z Active Directory MD) nebo jiné jednoznačné určení uživatele,
- datum a čas,
- požadované „url“.

Tyto logy musí být ve všech kopiích klasifikovány přinejmenším bezpečnostním klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU“. Administrátoři jsou povinni tyto logy uchovávat minimálně po dobu jednoho roku a na vyžádání je poskytnout Manažerovi KB.

Kapitola 2 MOBILNÍ VÝPOČETNÍ NEBO KOMUNIKAČNÍ ZAŘÍZENÍ A PRÁCE NA DÁLKU

Veškeré klientské přístupy musí být konfigurovány tak, aby neumožnily spojení zařízením, která nesplní definovanou bezpečnostní politiku pro přístup. Tato politika musí obsahovat minimálně:

- definici autentizačních mechanismů (silná autentizace, vícefaktorová autentizace),
- definici šifrovacích algoritmů,
- definici technologií pro VPN spojení,
- zákaz jakýchkoliv dalších síťových připojení na klientském zařízení.

Administrátoři klientských zařízení používaných pro vzdálený přístup k síti MD je musí konfigurovat tak, aby vyhověly výše uvedené politice.

Pro „site-to-site“ přístupy musí být definována bezpečnostní politika, která musí obsahovat minimálně:

- definici autentizačních mechanismů – důvěryhodný certifikát nebo bezpečně vyměněný „pre-shared“ klíč (délka alespoň 20 znaků, použití velkých a malých písmen, číslic a speciálních znaků),
- definici šifrovacích algoritmů,
- definici technologií pro VPN spojení.

Za definici těchto politik zodpovídají administrátoři serverových zařízení pro vzdálený přístup. Všechny tyto politiky (a jejich změny či aktualizace) musí být před aplikací schváleny Manažerem KB.

Vzdálené přístupy externích subjektů musí být schváleny Manažerem KB.

2.1 Práce na dálku

Povinnosti zaměstnanců při práci s mobilními prostředky výpočetní techniky se řídí ustanovením BPI MD.

K síti MD mohou vzdáleně přistupovat různé skupiny – zaměstnanci, dodavatelé, externí spolupracovníci a další. Pro tyto přístupy musí být vytvořeny oddělené body přístupu minimálně pro tyto skupiny:

- klientský přístup pro zaměstnance MD,
- klientský přístup pro externisty,
- přístup pro dodavatele, kteří na MD pracují na implementaci systémů („site-to-site“),

- přístup pro dodavatele, kteří na MD provádějí externí správu zařízení („site-to-site“).

Veškeré „site-to-site“ VPN mohou dodavatelům zpřístupňovat pouze nezbytně nutnou část infrastruktury.

ČÁST VIII. AKVIZICE, VÝVOJ A ÚDRŽBA SYSTÉMŮ

Kapitola 1 BEZPEČNOSTNÍ POŽADAVKY

Bezpečnostní požadavky systémů musí splňovat veškeré zákonné požadavky na informace v těchto systémech zpracovávané a dále musí splňovat požadavky stanovené touto přílohu BPI MD.
Aplikace nesmí pracovat s informacemi, které nejsou pro její fungování potřebné. Po síti (interní i veřejné) mohou být přenášena pouze data, ke kterým má uživatel či aplikace na základě svých oprávnění přístup; jiné informace nesmějí být přenášeny ani skrytě.

1.1 Analýza a specifikace požadavků

Základní bezpečnostní požadavky musejí být součástí prvotní analýzy připravovaného software i jeho jednotlivých komponent. V závislosti na plánovaném použití software a jeho architektuře mohou být Manažerem KB stanoveny další požadavky vyplývající z analýzy rizik.

Při formulaci požadavků a výběru řešení musí být zohledněny zejména tyto skutečnosti:

- naplnění zákonných požadavků a požadavků, uvedených v BPI MD a v jejích přílohách,
- kapacity provozních útvarů a útvarů provádějících akceptační (provozní i bezpečnostní) testy,
- dřívější bezpečnostní a provozní incidenty,
- další požadavky Manažera KB a výsledky analýzy rizik,
- naplnění dalších předem stanovených výběrových (provozních, bezpečnostních, uživatelských a podobně) kritérií.

1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Aplikační služby provozované ve veřejných datových sítích musí dále splňovat:

- všechny servery musí pro ověření (své) identity a šifrování při komunikaci s klienty používat certifikáty schválené MD,
- komunikace se servery partnerů musí být zajištěna šifrováním a autentizace serverů certifikáty,
- veškerá komunikace (včetně autentizace uživatelů) musí být šifrována dle požadavků této přílohy BPI MD (tj. aplikace nedělají ani „redirect“ z HTTP na HTTPS, spojení může být navázáno pouze na HTTPS),
- na front-end serverech nesmí být trvale uchovávána data a nesmí obsahovat databáze uživatelů,
- veškeré přístupy uživatelů musí být logovány podle požadavků této přílohy BPI MD,
- servery musí být od veřejných sítí odděleny FW, může být povolena pouze definovaná komunikace,
- serverům provozujícím různé služby zákazníkům nesmí být kromě nezbytné aplikační výměny dat umožněna vzájemná komunikace.

1.3 Ochrana transakcí aplikačních služeb

Ochrana transakcí aplikačních služeb musí splňovat minimálně tyto požadavky:

- aplikace/systém musí splnit všechny požadavky stanovené touto přílohou BPI MD,

- pro veškeré transakce musí být použito potvrzení elektronickým podpisem (na straně koncových uživatelů může být nahrazen OTP a/nebo druhým autentizačním faktorem),
- veškerá komunikace mezi všemi komponentami systému musí být šifrována pomocí certifikátů (komunikace s koncovým uživatelem může být šifrována ad hoc),
- musí být definován seznam schválených důvěryhodných certifikačních autorit, certifikáty jiných CA nesmějí být akceptovány,
- administrátoři aplikace/systému jsou povinni zkontrolovat dodržování certifikační politiky (minimálně obnova „root" certifikátu, pravidelnost vydávání CRL, povolený způsob využití certifikátů) každé schválené CA před provedením konfigurace, která umožní akceptaci certifikátů vydaných danou autoritou; tuto kontrolu musí administrátoři opakovat minimálně jednou za šest měsíců a o jejím provedení musí učinit záznam do provozní dokumentace,
- certifikáty protistrany musí být ověřeny (podpis certifikátem vydávající CA, kontrola CRL),
- konfigurace kryptografických prostředků aplikací je možná bez zásahu do aplikace pouhou změnou konfigurace, tj. není nutné programování,
- na „frontendových" serverech nesmějí být trvale uchovávány žádné uživatelské ani transakční údaje,
- přístup uživatelů/partnerů k datům smí být umožněn pouze přes aplikaci na frontendovém serveru,
- transakční data musí být uložena šifrovaně, administrátorům nesmí být k těmto údajům umožněn přístup,
- veškeré použité šifrovací algoritmy a délky klíčů musí splňovat požadavky této přílohy BPI MD.

Kapitola 2 BEZPEČNOST V PROCESECH VÝVOJE A PODPORY

Při vývoji SW musí být dodrženy minimálně tyto podmínky:

- vyvíjené aplikace/systémy musí umožnit naplnění všech ustanovení touto přílohu BPI MD (zejména řízení přístupu, politika hesel, logování, ochrana komunikace, zálohování),
- bezpečnostní model a další bezpečnostní požadavky musí být definovány před zahájením prací na vývoji aplikace/systému,
- při vývoji aplikací/systému musí být dodrženy metodiky pro bezpečný vývoj a provoz a správu IT systémů nebo jejich relevantní části (např. ITIL – Information Security Infrastructure Library, OWASP – Open Web Application Security Project, PCI DSS – The Payment Card Industry Data Security Standard,...) a doporučení výrobců vývojových nástrojů, existují-li,
- vývojové prostředí musí být odděleno od provozního i testovacího, přístup do vývojového prostředí mohou mít pouze pověření pracovníci,
- pro vývoj podobě jako pro testování nesmějí být použita ostrá data,
- zdrojové kódy aplikací ve správě/vlastnictví MD musí být klasifikovány přinejmenším klasifikačním stupněm „PRO VNITŘNÍ POTŘEBU" (a podle této klasifikace s nimi musí být nakládáno),
- u aplikací/systémů dodávaných na klíč musí být smluvně zajištěno, že zdrojové kódy budou majetkem MD,
- aplikace musí pracovat pod vlastním účtem, který nemá superuživatelská oprávnění,
- musí být uplatněna zásada minimální manipulace s daty (aplikace nebo její funkční části nepracují s daty a nepřistupují k datům, která nejsou pro vykonávanou činnost potřeba) a minimálních přístupových práv (aplikace nebo její funkční části mají pouze taková oprávnění, která potřebují pro vykonávanou činnost),

Je-li vývoj realizován externě, musí dodavatel předem potvrdit dodržení ustanovení této kapitoly.

Kapitola 3 DATA PRO TESTOVÁNÍ

Testování nesmí probíhat nad ostrými daty. Pro potřeby testování musí být vytvořena vlastní data, která obsahem neodpovídají produkčním datům (při zajištění dostatečné vypovídající hodnoty testování).

ČÁST IX. ŘÍZENÍ INCIDENTŮ BEZPEČNOSTI INFORMACÍ

Kapitola 1 ODPOVĚDNOST A POSTUPY

Povinnosti uživatelů i administrátorů a příslušné postupy pro zvládání bezpečnostních incidentů jsou podrobně popsány v Příloze č. 11.

Vlastníci informačních aktiv a správci systémů jsou povinni činit taková opatření, aby nedocházelo ke vzniku bezpečnostních incidentů.

Administrátoři jsou zejména povinni dbát na předcházení bezpečnostním incidentům (jsou povinni zajistit zejména nepřetržité automatizované vyhodnocování bezpečnostních událostí) a neprodleně reagovat v případě, že bezpečnostní incident nastane.

Bezpečnostními incidenty se rozumí stav systému, služby nebo sítě, ukazující na možné porušení bezpečnosti informací (obecně nebo vyplývající z bezpečnostní dokumentace) nebo selhání bezpečnostních opatření.

Kapitola 2 PODÁVÁNÍ ZPRÁV O INCIDENTECH BEZPEČNOSTI INFORMACÍ

Hlášení bezpečnostních incidentů se provádí dle ustanovení v Příloze č. 11.
Administrátoři systémů, kterých se nalezený bezpečnostní incident dotýká, jsou dále povinni:

- bezodkladně zasáhnout přiměřeným způsobem tak, aby znemožnili pokračování zjištěného nežádoucího stavu,
- zajistit veškeré dostupné auditní záznamy pro případ jejich potřeby při vyšetřování bezpečnostního incidentu či přípravě a realizaci nápravných opatření. Tyto záznamy jsou administrátoři na vyžádání povinni předat pracovníkům v oblasti bezpečnosti,
- řešit (případně navrhnout řešení) následky bezpečnostního incidentu,
- provést kontrolu všech systémů, které by mohly být incidentem zasaženy, resp. informovat administrátory těchto systémů,
- najít a odstranit příčiny vzniku bezpečnostního incidentu, resp. požadovat nápravu u příslušných útvarů MD nebo dodavatelů. Není-li náprava možná je administrátor povinen informovat Manažera KB a svého nadřízeného a spolupracovat při návrhu a implementaci alternativního řešení.

Kapitola 3 PODÁVÁNÍ ZPRÁV O ZRANITELNOSTECH BEZPEČNOSTI INFORMACÍ

Zranitelnost je nedostatek, který umožňuje uplatnění hrozby, resp. překonat stávající bezpečnostní opatření, např. využívat IS MD v rozporu s přidělenými přístupovými právy.

Všichni zaměstnanci jsou povinni informovat o zjištění zranitelnosti a nahlásit ji v rámci Incident Managementu jako možné riziko.

Administrátoři systémů, kterých se nalezená zranitelnost dotýká, jsou dále povinni:

- informovat o zranitelnosti administrátory dalších systémů, které mohou být podobně postiženy, nadřízeného zaměstnance a Manažera KB,
- zdokumentovat nalezenou zranitelnost a navrhnout řešení na její eliminaci. Navržené řešení musí být před implementací schváleno Manažera KB,
- provést potřebné zásahy na dotčeném systému,
- v případě, že slabina byla nalezena na systému podporovaném, resp. spravovaném jeho výrobcem či dodavatelem (interním i externím), informovat jej o bezpečnostní zranitelnosti a požadovat nápravu. Není-li náprava možná je administrátor povinen informovat Manažera KB a svého nadřízeného a spolupracovat při návrhu a implementaci alternativního řešení resp. kompenzačního opatření.

K posouzení a rozhodnutí o událostech bezpečnosti informací je oprávněn Manažer KB.

Kapitola 4 ODEZVA NA INCIDENTY BEZPEČNOSTI INFORMACÍ

Při stanovení bezpečnostních požadavků jsou odpovědné osoby povinny zohledňovat skutečnosti, které byly v minulosti rozhodné pro vznik bezpečnostního incidentu.

Způsob řešení bezpečnostního incidentu je administrátor povinen zaznamenat do systémové dokumentace a případně i do havarijních plánů (doporučeno odkazem na dokumentaci). Záznam musí obsahovat identifikaci "kořenové příčiny" incidentu, tedy bod, kde incident opravdu vznikl, nikoliv pouze bod, kde se incident projevil.

Znalosti získané z analýz a řešení bezpečnostních incidentů jsou povinni zaměstnanci zohlednit v návrzích při zavádění produktů a služeb v rámci MD tak aby se snížila pravděpodobnost nebo dopady následných incidentů.

Kapitola 5 SHROMAŽĎOVÁNÍ DŮKAZŮ

V rámci šetření bezpečnostních incidentů jsou administrátoři povinni:

- předat/zpřístupnit pracovníkům v oblasti bezpečnosti, pověřeným šetřením incidentů veškeré vyžádané dostupné logy ze systémů ve své správě (záznamy podléhající zvláštnímu režimu mohou administrátoři předat pouze v souladu s pravidly, danými platnými právními předpisy),
- předat/zpřístupnit pracovníkům v oblasti bezpečnosti pověřeným šetřením incidentů veškerou vyžádanou provozní dokumentaci systémů ve své správě,
- na vyžádání nastavit detailnější logování dle požadavků pracovníků v oblasti bezpečnosti pověřených šetřením incidentů, pokud to negativně neovlivní provoz systému,
- předat pracovníkům v oblasti bezpečnosti pověřeným šetřením incidentů veškeré další požadované dostupné informace o konfiguraci a provozu systémů ve své správě.

ČÁST X. ŘÍZENÍ KONTINUITY ČINNOST

Požadavky na řízení kontinuity činností a plány obnovy blíže specifikují přílohy č. 9 a 10 BPI MD.

ČÁST XI. SOULAD S POŽADAVKY

Administrátoři systémů a zařízení jsou povinni dodržovat obecně závazné právní předpisy.

Administrátoři MD jsou povinni dodržovat pravidla a bezpečnostní opatření definovaná interní bezpečnostní dokumentací MD.