ISO/IEC 17799:2005
Information Security Management
Information Technology - Code of practice
for information security management

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1. Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 17799 byla připravena společnou technickou komisí ISO/IEC JTC 1 *Information technology*, subkomise SC 27, *IT Security techniques*.

Toto druhé vydání nahrazuje ISO/IEC 17799:2000, které tímto pozbývá platnosti.

Technická komise ISO/IEC JTC 1/SC 27 připravuje soubor mezinárodních norem věnovaných systému řízení bezpečnosti informací (ISMS). Soubor norem zahrnuje požadavky na systém řízení bezpečnosti informací, řízení rizik, metriky a měření výkonu a doporučení k implementaci. Soubor těchto norem bude vydán v sérii 27000. ISO/IEC 17799 by měla být do této nové řady začleněna v roce 2007 a to jako ISO/IEC 27002.

0 Úvod

1.1 Co je bezpečnost informací?

Informace jsou aktiva, která mají pro organizaci hodnotu. Je tedy nutné je vhodným způsobem chránit. Obzvláště se vzrůstající propojeností prostředí jednotlivých organizací je tato potřeba stále více aktuální. S rostoucí propojeností jsou informace vystaveny rostoucímu počtu různých hrozeb a zranitelností (viz také Směrnice OECD pro bezpečnost informačních systémů a sítí: směrem ke kultuře bezpečnosti 1).

Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, ukládány v elektronické podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci.

Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu činností organizace, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

Bezpečnosti informací lze dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, natrénovaných postupů, procedur, organizační struktury a programových a hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována, přezkoumávána a zlepšována proto, aby bylo dosaženo specifických bezpečnostních cílů organizace. Toto všechno by mělo být prováděno v soulady s ostatními řídícími procesy organizace.

1.2 Proč je nezbytná bezpečnost informací

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Vymezení, zavádění, podpora a zlepšování bezpečnosti informací může být zásadní pro udržení konkurenceschopnosti, peněžních toků (cash-flow), ziskovosti, právní shody a dobrého jména organizace.

Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáže, sabotáže, vandalizmu, požárů a povodní. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby (denial of service), jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Bezpečnost informací je důležitá z hlediska ochrany kritické infrastruktury a to jak v soukromém, tak ve státním sektoru. V obou sektorech je bezpečnost informací důležitá pro existenci některých služeb, například e-governmentu nebo e-komerce a zároveň kvůli vyhnutí se nebo snížení relevantních rizik. Propojení veřejných a privátních sítí i sdílení informačních zdrojů zvyšuje obtížnost řízení přístupu. Trend směřující k distribuovanému zpracování oslabil efektivnost centrální kontroly prováděnou specialisty.

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné. Bezpečnost, která může být dosažena technickými prostředky, je nedostačující a měla by být doplněna odpovídajícím řízením a postupy. Pro určení opatření, která je třeba přijmout, je nutné pečlivé plánování a rozbor každého detailu. Řízení bezpečnosti informací proto vyžaduje alespoň nějakou spoluúčast všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci majitelů organizace (akcionářů), dodavatelů, třetích stran, zákazníků a dalších externích subjektů. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

1.3 Jak stanovit bezpečnostní požadavky

Je nezbytné, aby organizace určila své bezpečnostní požadavky. K tomu existují tři hlavní zdroje.

1. Prvním zdrojem je hodnocení rizik, která organizaci hrozí, beroucí v potaz celkovou strategii a cíle organizace. V rámci hodnocení rizik se identifikují hrozby působící vůči aktivům, zranitelnosti, které mohou být hrozbami využity i pravděpodobnost jejich

výskytu, a provádí se odhad jejich potenciálního dopadu.
2. Druhým zdrojem jsou požadavky zákonů, podzákonných norem a smluvních ujednání, které organizace, její obchodní, smluvní partneři a poskytovatelé služeb musí splňovat.
3. Třetím zdrojem jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu své činnosti.

1.4 Hodnocení bezpečnostních rizik

Požadavky na bezpečnost jsou stanoveny za pomoci metodického hodnocení bezpečnostních rizik. Výdaje na bezpečnostní opatření by měly odpovídat ztrátám způsobeným narušením bezpečnosti.
Výsledky hodnocení rizik pomohou určit vedení organizace odpovídající kroky i priority pro řízení bezpečnostních rizik u informací a pro realizaci opatření určených k zamezení jejich výskytu. Hodnocení rizik by mělo být prováděno periodicky, aby bylo možné včas reagovat na jakékoliv změny v bezpečnostních požadavcích.
Více informací o hodnocení rizik je uvedeno v kapitole 4.1 „Hodnocení bezpečnostních rizik".

1.5 Výběr opatření

Jakmile jsou identifikovány bezpečnostní požadavky a rizika a bylo rozhodnuto jakým způsobem bude se zjištěnými riziky naloženo, měla by být vybrána a implementována opatření zajišťující snížení rizik na přijatelnou úroveň. Taková opatření mohou být vybrána z tohoto dokumentu nebo i z jiných souborů opatření. Pro pokrytí specifických potřeb mohou být vytvořena zcela nová opatření. Výběr konkrétních opatření je na rozhodnutí každé organizace. Rozhodnutí je založeno na kritériích určujících akceptaci nebo zvládání rizika a celkovém přístupu organizace k řízení rizik. Při výběru opatření by měla být zohledněna příslušná národní a mezinárodní legislativa a regulace.
Některá opatření v tomto dokumentu mohou být chápána jako základní doporučení pro řízení bezpečnosti informací a mohou být využita ve většině organizací. Detailněji jsou vysvětlena v části „Východiska bezpečnosti informací".
Další informace o výběru opatření a způsobech zvládání rizik jsou uvedeny v kapitole 4.2 „Zvládání bezpečnostních rizik".

1.6 Východiska bezpečnosti informací

Řada opatření může být považována za základní principy představující dobrá východiska pro implementaci bezpečnosti informací. Mohou vycházet ze základních legislativních požadavků nebo jsou obecně považována za nejlepších způsob řešení bezpečnosti informací.
Opatření, která by měla být pro organizaci podstatná z pohledu legislativy, jsou:
a) ochrana osobních údajů (viz 15.1.4);
b) ochrana důležité dokumentace organizace, jako například účetních záznamů (viz 15.1.3);
c) ochrana duševního vlastnictví (viz 15.1.2).
Opatření, považovaná za základ nejlepších praktik pro zajištění bezpečnosti informací, jsou:
a) dokument bezpečnostní politiky informací (viz 5.1.1);
b) přidělení odpovědností v oblasti bezpečnosti informací (viz 6.1.3);
c) vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti informací (viz 8.2.2);
d) bezchybné zpracování v aplikačních systémech (viz 12.2);
e) řízení technických zranitelností (viz 12.6);
f) řízení kontinuity činností organizace (viz 14);
g) zvládání bezpečnostních incidentů a kroky k nápravě (viz 13.2).
Tato opatření fungují ve většině organizací a prostředí.
Mělo by však být zdůrazněno, že ačkoliv všechna opatření v tomto dokumentu jsou důležitá, jejich význam by měl být určován ve světle specifických rizik, kterým organizace čelí. I když výše uvedené doporučení může být považováno za dobré východisko, nenahrazuje výběr opatření vycházející z hodnocení rizik.

1.7 Kritické faktory úspěchu

Jak ukazuje zkušenost, pro úspěšnou implementaci bezpečnosti informací v organizaci jsou často kritické následující faktory:
a) bezpečnostní politika, bezpečnostní cíle a činnosti, které respektují cíle činností organizace;
b) přístup k zavádění, udržování, monitorování a zlepšování bezpečnosti informací v souladu s kulturou organizace;
c) zřetelná podpora a angažovanost ze strany vedení organizace;
d) dobré pochopení bezpečnostních požadavků, hodnocení a řízení rizik;
e) účinný marketing bezpečnosti vůči vedení organizace, zaměstnancům a třetím stranám;
f) rozšíření směrnic a norem bezpečnostní politiky informací mezi všechny zaměstnance, vedení organizace a třetí strany;
g) zdroje na financování činností souvisejících s řízením bezpečnosti informací;
h) realizace odpovídajících školení, vzdělávání a programů zvyšování povědomí;
i) zavedení procesu zvládání bezpečnostních incidentů;
j) komplexní a vyvážený systém pro ohodnocení míry účinnosti řízení bezpečnosti informací a získávání návrhů ke zlepšení na základě zpětné vazby.

1.8 Vytváření vlastních směrnic

Tento soubor postupů může být chápán jako východisko pro vytváření specifických směrnic organizace. Ne všechna doporučení a opatření této sbírky postupů mohou být použitelná. Kromě toho mohou být nezbytná i další opatření, která nejsou v tomto dokumentu uvedena. V takovém případě je užitečné zanechat v nich odkaz na tuto normu a usnadnit tak ověření shody prováděné auditory a obchodními partnery.

1 Působnost

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení udržování a zlepšování systému řízení bezpečnosti informací v organizaci. Cíle, popsané

v normě, poskytují rady o obecně přijímaných cílech řízení bezpečnosti.
Cíle opatření a jednotlivá opatření obsažená v této mezinárodní normě by měla být implementována na základě požadavků zjištěných v rámci analýzy rizik. Norma může sloužit jako praktický průvodce při vývoji bezpečnostních standardů organizace, účinných řídících bezpečnostních postupů a také při budování důvěry mezi organizacemi.

2 Termíny a definice

Pro účely tohoto dokumentu jsou platné následující definice.

2.1

aktivum (asset)

cokoliv, co má pro organizaci nějakou hodnotu

[ISO/IEC 13335-1:2004]

2.2

opatření (control)

prostředek řízení rizik, zahrnuje politiky, směrnice, metodické pokyny, praktiky nebo organizační struktury, které mohou být povahy administrativní, technické, řídící nebo legislativní.

POZNÁMKA V anglickém originálu je termín „control" synonymem slovům „safeguard" (bezpečnostní opatření) a „counteremasure" (protiopatření). Dle kontextu je „control" překládáno jako opatření, bezpečnostní opatření, případně kontrola

2.3

metodický postup, doporučení, postup (guideline)

popis, který objasňuje co a jak má být uděláno, k dosažení cílů stanovených v jednotlivých politikách organizace

[ISO/IEC 13335-1:2004]

2.4

prostředky pro zpracování informací (information processing facilities)

jakýkoliv systém, služba nebo infrastruktura, zpracovávající informace anebo lokality, ve kterých jsou umístěny

2.5

bezpečnost informací (information security)

zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost a hodnověrnost

2.6

bezpečnostní událost (information security event)

bezpečnostní událost je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací

[ISO/IEC TR 18044:2004]

2.7

bezpečnostní incident (information security incident)

bezpečnostní incident je jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací

[ISO/IEC TR 18044:2004]

2.8

politika (policy)

celkový záměr a směr formálně vyjádřený vedením organizace

2.9

riziko (risk)

kombinace pravděpodobnosti, že dojde k nechtěné události a následků, které by z takové události mohly vzniknout

[ISO/IEC TR 18044:2004]

2.10

analýza rizik (risk analysis)

systematické používání informací k odhadu rizika a k určení jeho zdrojů

[ISO/IEC Guide 73:2002]

2.11

hodnocení rizik (risk assessment)

celkový proces analýzy a vyhodnocení rizik

[ISO/IEC Guide 73:2002]

2.12

vyhodnocení rizik (risk evaluation)

proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu

[ISO/IEC Guide 73:2002]

2.13

řízení rizik (risk management)

koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika

POZNÁMKA Řízení rizik zpravidla zahrnuje hodnocení rizik, zvládání rizik, akceptaci a seznámení s rizikem

[ISO/IEC Guide 73:2002]

2.14

zvládání rizik (risk treatment)

proces výběru a přijímání opatření pro změnu rizika

[ISO/IEC Guide 73:2002]

2.15

třetí strana (third party)

osoba, organizace nebo jiná seskupení, která jsou nezávislá na přímo zainteresovaných

stranách
[ISO/IEC Guide 2:1996]

2.16

hrozba (threat)

potenciální příčina nechtěného incidentu, která může vyústit v poškození systému nebo organizace
[ISO/IEC 13335-1:2004]

2.17

zranitelnost (vulnerability)

slabina aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami
[ISO/IEC 13335-1:2004]

3 Struktura normy

Norma obsahuje celkem 11 základních oddílů, které jsou dále rozděleny do 39 kategorií bezpečnosti. Mimo to jsou v kapitole 4 uvedeny základní informace o procesech hodnocení a zvládání rizik.

3.1 Oblasti bezpečnosti

Každý z oddílů obsahuje jednu nebo více kategorií bezpečnosti. Následující přehled uvádí seznam všech kapitol doplněný o počet kategorií bezpečnosti (počet je uveden v závorce za názvem kapitoly):

a) Bezpečnostní politika (1);
b) Organizace bezpečnosti (2);
c) Klasifikace a řízení aktiv (2);
d) Bezpečnost lidských zdrojů (3);
e) Fyzická bezpečnost a bezpečnost prostředí (2);
f) Řízení komunikací a řízení provozu (10);
g) Řízení přístupu (7);
h) Nákup, vývoj a údržba informačního systému (6);
i) Zvládání bezpečnostních incidentů (2);
j) Řízení kontinuity činností organizace (1);
k) Soulad s požadavky (3).

POZNÁMKA Pořadí jednotlivých oddílů bezpečnosti tak, jak jsou uvedeny v této normě, nijak neurčuje jejich důležitost. S ohledem na konkrétní okolnosti mohou být například všechny stejně důležité. Organizace by měla identifikovat pro ni aplikovatelné oddíly bezpečnosti, určit jejich důležitost a aplikovatelnost na konkrétní procesy.

3.2 Hlavní kategorie bezpečnosti

Každá z kategorií bezpečnosti obsahuje:

a) cíl opatření, určující čeho má být dosaženo;
b) jedno nebo více opatření, která lze použít k dosažení stanoveného cíle opatření.

Popis opatření je strukturován následovně:

Opatření

Přesná formulace konkrétního opatření, které vede k naplnění cíle opatření.

Doporučení k realizaci

Poskytuje podrobnější informace a doporučení na podporu implementace vybraných opatření, která vedou k dosažení cíle opatření. Ne všechna z těchto doporučení budou použitelná pro každou situaci, v takovýchto případech by měly být vybrány vhodnější postupy implementace opatření.

Další informace

Poskytuje další informace, které může být potřebné vzít do úvahy. Příkladem mohou být otázky legislativy a odkazy na další relevantní normy a předpisy.

4 Hodnocení a zvládání rizik

4.1 Hodnocení bezpečnostních rizik

V rámci hodnocení rizik by měla být identifikována a kvantifikována rizika, měla by být určena důležitost jednotlivých rizik s ohledem na kritéria pro jejich akceptaci a cíle organizace. Výstupem z hodnocení rizik by měla být doporučení a priority řízení jednotlivých rizik a priority implementace vybraných opatření na ochranu proti těmto rizikům. Celý proces hodnocení rizik a výběru vhodných opatření může být nutné opakovat pro různé části organizace nebo jednotlivé informační systémy.

Součástí hodnocení rizik by také měl být systematický přístup k odhadu velikosti rizika (analýza rizik) a proces porovnání odhadnutých rizik se stanovenými kritérii pro určení jejich důležitosti (vyhodnocení rizik).

Hodnocení rizik by mělo být prováděno v pravidelných intervalech, aby byly zjištěny změny v bezpečnostních požadavcích a změny z pohledu rizik, např. změny aktiv, hrozeb, zranitelností, dopadů, vyhodnocení rizik a také v případě, že nastanou významné organizační změny. Hodnocení rizik by mělo být prováděno metodicky tak, aby výsledky jednotlivých hodnocení byly srovnatelné a reprodukovatelné.

Rozsah hodnocení rizik by měl být jasně definován, hodnocení rizik v jednotlivých oblastech (části organizace, informační systémy) by měla být vzájemně propojena.

Rozsah hodnocení rizik může zahrnovat celou organizaci, část(i) organizace, vybraný informační systém, specifické prvky systému a nebo tam kde je to proveditelné, reálné a užitečné, služby. Příklady metodologií hodnocení rizik jsou uvedeny v normě ISO/IEC TR 13335-32.

4.2 Zvládání bezpečnostních rizik

Předtím než je rozhodnuto o způsobu zvládání rizika, měla by být stanovena kritéria, na základě kterých bude určováno, jestli je riziko pro organizaci akceptovatelné. Riziko může být akceptováno například z důvodu, že je nízké a nebo, že náklady spojené s jeho zvládáním jsou pro organizaci cenově nepříznivé. O takovýchto rozhodnutích by měly být vytvořeny záznamy.

Následně po provedeném hodnocení rizik musí být učiněno rozhodnutí jakým způsobem bude s identifikovanými riziky naloženo. Možné varianty zahrnují:
a) aplikace vhodných opatření na snížení velikosti rizika;
b) vědomá a objektivní akceptace rizika, za předpokladu, že je tak učiněno v souladu s bezpečnostní politikou organizace a kritérii pro akceptaci rizika;
c) vyhnutí se riziku zamezením činností, které jsou příčinou jeho vzniku;
d) přenos rizika na jiný subjekt (např. pojišťovny, dodavatele).
Jestliže bylo učiněno rozhodnutí o zvládáni rizika formou aplikace vhodných opatření, měl by být výběr těchto opatření proveden na základě požadavků identifikovaných v rámci hodnocení rizik.
Opatření by měla zaručit snížení rizika na přijatelnou úroveň, přičemž v úvahu by mělo být vzato následující:
a) požadavky a omezení národní a mezinárodní legislativy a předpisů;
b) cíle organizace;
c) provozní požadavky a omezení;
d) cena za implementaci a provozní náklady spojené s přijetím opatření na snížení rizika, dle požadavků a omezení organizace;
e) potřeba udržovat rovnováhu mezi investicemi spojenými s implementací a provozem opatření a případnými škodami způsobenými selháním bezpečnosti.
Opatření k implementaci mohou být vybírána z této normy nebo z jiných obdobných souborů opatření, případně mohou být navržena zcela nová opatření tak, aby co nejlépe odpovídala požadavkům organizace. Je důležité si uvědomit, že ne všechna opatření uvedená v této normě budou aplikovatelná pro každý informační systém, prostředí nebo organizaci. Jako příklad lze uvést opatření z kapitoly 10.1.3, které popisuje oddělení jednotlivých rolí jako způsob prevence proti podvodům a chybám. Zejména u malých organizací nemusí být toto opatření realizovatelné a pro dosažení stejného cíle bude nutné hledat jiná opatření. Jiným příkladem může být opatření z kapitoly 10.10, popisující monitorování přístupu k systému a sběr důkazů. Popsaná opatření, např. zaznamenávání událostí, mohou být v rozporu s platnou legislativou, jako je ochrana soukromí zákazníků nebo ochrana soukromí na pracovišti.
Opatření by měla být vybírána již ve fázi návrhu a specifikaci požadavků projektu nového systému. Opačný případ může mít za následek dodatečné zvýšení nákladů, méně účinná řešení a v nejhorším případě neschopnost dosáhnout požadované úrovně bezpečnosti.
Žádná sada opatření nemůže sama o sobě zajistit kompletní bezpečnost. Na podporu cílů organizace by měly proto být zavedeny řídící činnosti pro monitorování, vyhodnocování, zlepšování výkonnosti a účinnosti bezpečnostních opatření.

5 Bezpečnostní politika

5.1 Bezpečnostní politika informací

Cíl: Definovat směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.
Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci.

5.1.1 Dokument bezpečnostní politiky informací

Opatření
Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním třetím stranám.
Doporučení k realizaci
Dokument bezpečnostní politiky informací by měl obsahovat vyjádření podpory vedení organizace a měl by definovat zamýšlený přístup k budování bezpečnosti informací.
Dokument by měl obsahovat následující body:
a) definice bezpečnosti informací, její cíle, rozsah a její důležitost - mechanizmus umožňující sdílení informací (viz Úvod);
b) prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací;
c) stručný výklad bezpečnostních zásad, principů a norem a požadavky zvláštní důležitosti pro organizaci, například:
1. dodržování zákonných, regulatorních a smluvních požadavků;
2. požadavky na vzdělávání, školení a zvyšování povědomí v oblasti bezpečnosti;
3. zásady plánování kontinuity činností organizace;
4. důsledky porušení bezpečnostních zásad;
d) stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů;
e) odkazy na dokumentaci, která může bezpečnostní politiku podporovat, například na detailnější bezpečnostní politiky a postupy zaměřené na konkrétní informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat.
S dokumentem by měli být seznámeni uživatelé v rámci organizace, a to formou, která je relevantní, přístupná a pochopitelná všem potenciálním příjemcům.
Další informace
Bezpečnostní politika informací může být součástí (hierarchicky podřízena) dokumentu nejvyšší politiky organizace. V případech, kdy je bezpečnostní politika sdělována mimo organizaci, by měla být zajištěna ochrana citlivých informací před prozrazením. Další informace lze nalézt v normě ISO/IEC 13335-1:20043.

5.1.2 Přezkoumání a aktualizace bezpečnostní politiky informací

Opatření
Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti by bezpečnostní politika informací měla být přezkoumávána v plánovaných intervalech a vždy když nastane významná změna.

Doporučení k realizaci

Bezpečnostní politika informací by měla mít vlastníka (schváleného vedením organizace), odpovědného za její vytvoření, přezkoumání a aktualizaci. Součástí procesu přezkoumání by mělo být posouzení možností pro zlepšení bezpečnostní politiky informací. Měl by být posouzen stávající přístup organizace k řízení informační bezpečnosti jako reakce na změny v organizační či technické infrastruktuře, změny v legislativě a jiné okolnosti, mající vztah k činnostem organizace.

Při přezkoumání bezpečnostní politiky informací by měly být zohledněny závěry z přezkoumání provedeného vedením organizace. Měl by být vytvořen postup a plán pravidelného přezkoumání vedení organizace.

Vstupy pro přezkoumání vedením organizace by měly obsahovat:

a) zpětnou vazbu od zainteresovaných stran;

b) výsledky nezávislých přezkoumání (viz 6.1.8);

c) stav preventivních a nápravných činností (viz 6.1.8 a 15.2.1);

d) výsledky z předchozích přezkoumání vedením organizace;

e) výkonnost procesu a soulad s bezpečnostní politikou;

f) změny, které mohou mít vliv na přístup organizace k řízení bezpečnosti informací, včetně změn v organizační či technické infrastruktuře, dostupnosti zdrojů, změn smluvních, regulatorních a legislativních podmínek a jiné další okolnosti mající vztah k činnostem organizace;

g) trendy v oblasti hrozeb a zranitelností;

h) hlášení bezpečnostních incidentů (viz 13.1);

i) doporučení orgánů veřejné správy (viz 6.1.6).

Výstupy z přezkoumání prováděného vedením organizace by měly obsahovat jakákoliv rozhodnutí a činnosti mající vztah k následujícímu:

a) změnám a zlepšení přístupu organizace k řízení bezpečnosti informací a procesům organizace;

b) změnám cílů opatření a jednotlivých opatření;

c) změnám v přidělení zdrojů a odpovědností.

Měly by být udržovány záznamy o provedených přezkoumáních vedením organizace.

Mělo by být získáno od vedení organizace schválení aktualizované verze politiky.

6 Organizace bezpečnosti

6.1 Interní organizace

Cíl: Řídit bezpečnost informací v organizaci.

Měl by být vytvořen řídící rámec pro zahájení a řízení implementace bezpečnosti informací v organizaci.

Vedení organizace by mělo schválit politiku bezpečnosti informací, přiřadit role v oblasti bezpečnosti informací a koordinovat implementaci bezpečnosti v organizaci.

Jestliže je to nutné, pak by měl být v organizaci vytvořen specializovaný zdroj pro oblast bezpečnosti informací a měl by být dostupný pro celou organizaci. Aby bylo možné udržovat krok s posledními trendy v odvětví bezpečnosti informací, sledovat standardy, vybírat nejvhodnější metody a zajistit vhodné styčné body v případech bezpečnostních incidentů, měly by být uzavřeny smlouvy s externími odborníky v oboru bezpečnosti informací. Měl by být podporován multi-disciplinární přístup k bezpečnosti informací.

6.1.1 Závazek vedení

Opatření

Vedení organizace by mělo stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace. Mělo by demonstrovat svůj závazek a jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací.

Doporučení k realizaci

Vedení by mělo:

a) zajistit identifikaci cílů bezpečnosti, jejich soulad s požadavky organizace a integraci do relevantních procesů;

b) formulovat, přezkoumat a schválit bezpečnostní politiku informací;

c) přezkoumat účinnost implementace bezpečnostní politiky informací;

d) poskytnout jasný směr a viditelnou podporu bezpečnostním iniciativám;

e) zajistit dostatečné zdroje potřebné pro bezpečnost informací;

f) schválit přidělení jednotlivých rolí a odpovědností za bezpečnost informací v rámci organizace;

g) iniciovat plány a programy na zvyšování bezpečnostního povědomí;

h) zajistit, aby implementace bezpečnostních opatření byla koordinována v rámci celé organizace (viz 6.1.2).

Vedení organizace by mělo určit potřebnost konzultací od odborníka (interního nebo externího) na bezpečnost informací a přezkoumat a koordinovat výsledky konzultací v rámci organizace. V závislosti na velikosti organizace může být tato odpovědnost přesunuta na fórum pro řízení bezpečnosti informací nebo jiný řídící subjekt, jako například představenstvo.

Další informace

Další informace lze nalézt v normě ISO/IEC 13335-1:20044.

6.1.2 Koordinace bezpečnosti informací

Opatření

Činnosti v oblasti bezpečnosti informací by měly být koordinovány prostřednictvím zástupců různých útvarů z celé organizace.

Doporučení k realizaci

Koordinace bezpečnosti informací by měla zahrnovat součinnost zástupce vedení organizace, uživatelů, administrátorů, návrhářů aplikačních programů, auditorů, zaměstnanců oddělení bezpečnosti a odborníky na specifické oblasti, jako například pojištění, právní otázky, lidské zdroje, IT anebo řízení rizik.

Koordinace bezpečnosti by měla:
a) zajistit, aby aktivity v oblasti bezpečnosti informací byly prováděny v souladu s bezpečnostní politikou informací;
b) určit jakým způsobem bude naloženo se zjištěnými nesoulady;
c) schválit specifické metodologie a postupy v oblasti bezpečnosti informací, například hodnocení rizik, systém bezpečnostní klasifikace;
d) identifikovat významné změny v hrozbách a vystavení informací a prostředkům pro zpracování informací vůči těmto hrozbám;
e) zajistit podporu vzdělávání v oblasti bezpečnosti informací dotýkající se celé organizace, například školení a program zvyšování bezpečnostního povědomí;
f) vyhodnotit informace získané z procesu monitorování a přezkoumání bezpečnostních incidentů a doporučit vhodný způsob reakce na identifikované bezpečnostní incidenty.
Pokud organizace nevyužívá funkce fóra, vytvořeného ze zástupců jednotlivých útvarů, např. z důvodů velikosti organizace, měly by být veškeré výše popsané aktivity zajištěny jiným vhodným subjektem nebo určeným členem z vedení organizace.

6.1.3 Přidělení odpovědností v oblasti bezpečnosti informací

Opatření

Měly by být jednoznačně určeny odpovědnosti v oblasti bezpečnosti informací.

Doporučení k realizaci

Přidělení odpovědností v oblasti bezpečnosti informací by mělo být provedeno v souladu s bezpečnostní politikou informací (viz kapitola 4). Měly by být jednoznačně vymezeny odpovědnosti za ochranu jednotlivých aktiv a za realizaci určených bezpečnostních procesů. Tam, kde je to potřebné, by tyto odpovědnosti měly být doplněny o podrobnější interpretaci vztahující se ke specifickým místům, systémům nebo službám. Měly by být jasně definovány lokální odpovědnosti za ochranu aktiv a výkon bezpečnostních procesů, například plánování kontinuity činností organizace.
Jedinci s přidělenou odpovědností mohou jednotlivé činnosti v oblasti bezpečnosti delegovat. Nicméně v konečném důsledku zůstávají odpovědnými a měly by být schopni zaručit, že jakékoliv delegované činnosti byly vykonány správně.
Je nezbytné jasně vymezit oblasti odpovědnosti jednotlivých vedoucích; zvlášť by mělo být provedeno následující.
a) identifikování a jasné vymezení různých aktiv a bezpečnostních postupů spojených s každým jednotlivým systémem;
b) určení odpovědnosti relevantního subjektu za každé aktivum nebo bezpečnostní postup, detaily této odpovědnosti by měly být zdokumentovány (viz také 7.1.2);
c) jednoznačné vymezení a zdokumentování úrovně oprávnění jednotlivých subjektů.

Další informace

V mnoha organizacích bude jmenován vedoucí zaměstnanec5 odpovědný za bezpečnost informací, který nese veškerou odpovědnost za vývoj a implementaci bezpečnosti a který zajišťuje identifikaci opatření.
Avšak odpovědnost za financování a implementaci těchto opatření bude často zůstávat na vedoucích jednotlivých útvarů organizace. Jedním z obecně používaných postupů je jmenovat vlastníka pro každé informační aktivum. Ten se pak stane odpovědným za každodenní bezpečnost svěřeného aktiva.

6.1.4 Schvalovací proces pro prostředky zpracování informací

Opatření

Měl by být ustaven a zaveden postup schvalování (vedoucími zaměstnanci) nových prostředků pro zpracování informací.

Doporučení k realizaci

V úvahu by měla být vzata následující doporučení:
a) nová zařízení by měla být odsouhlasena jednotlivými vedoucími uživatelských útvarů organizace, kteří schválí jejich účel a použití. Schválení by také mělo být získáno od vedoucího zaměstnance odpovědného za bezpečnost provozu informačního systému, aby se zajistilo, že nebudou porušeny žádné relevantní bezpečnostní politiky a požadavky;
b) v nutných případech by mělo být zkontrolováno technické a programové vybavení, aby bylo zajištěno, že je kompatibilní s ostatními systémovými prvky;
c) použití soukromých prostředků zpracovávajících pracovní informace (např. notebooků, domácích PC nebo kapesních zařízení) by mělo být zvlášť schvalováno a měla by být přijata veškeré nutná opatření s tím spojená, protože použití těchto prostředků může znamenat vznik nových zranitelností.

6.1.5 Dohody o ochraně důvěrných informací

Opatření

Měly by být určeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.

Doporučení k realizaci

Dohody o ochraně důvěrnosti nebo o povinnosti zachovávat mlčenlivost by měli zajistit požadavek na ochranu důvěrné informace s využitím zákonem vymahatelných prostředků. Při určení požadavků na dohody o ochraně důvěrnosti nebo povinnost zachovávat mlčenlivost by mělo být bráno v úvahu:
a) určení informace, která má být chráněna (např. důvěrná informace);
b) očekávaná délka dohody, včetně upřesnění případů kdy požadavek na ochranu důvěrnosti trvá i po jejím vypršení;

c) upřesnění kroků následujících po ukončení dohody;
d) odpovědnosti a kroky, které signatáři dohody podniknou k zamezení neoprávněného prozrazení informací (např. dodržování principu „oprávněné potřeby znát" (need to know));
e) vlastnictví informací, obchodní tajemství a ochrana duševního vlastnictví a jakým způsobem to souvisí s ochranou důvěrných informací;
f) dovolené použití důvěrných informací a práva smluvních stran na jejich použití;
g) právo auditovat a monitorovat činnosti, které zahrnují důvěrné informace;
h) způsob oznámení a podání zprávy o neoprávněném prozrazení nebo porušení důvěrnosti informace;
i) podmínky za jakých mají být informace po ukončení dohody vráceny nebo zničeny;
j) kroky které budou podniknuty v případě, že dojde k porušení dohody.

V závislosti na bezpečnostních potřebách organizace mohou být dohody o ochraně důvěrných informací nebo povinnost zachovávat mlčenlivost doplněny o další potřebná ustanovení.

Dohody o ochraně důvěrných informací nebo povinnost zachovávat mlčenlivost by měly být v souladu s místními zákony a předpisy (viz také 15.1.1).

Požadavky obsažené v dohodách o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost by měly být v pravidelných intervalech, a v případě jakýchkoliv dalších změn ovlivňujících tyto požadavky, přezkoumávány.

Další informace

Dohody o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost slouží k ochraně informací organizace. Zavazují signatáře k odpovědnosti informace chránit, používat a zveřejňovat je pouze odpovědným a oprávněným způsobem.

V závislosti na konkrétní situaci mohou organizace volit různé formy dohod o ochraně důvěrných informací nebo o povinnosti zachovávat mlčenlivost.

6.1.6 Kontakt s orgány veřejné správy

Opatření

Měly by být udržovány přiměřené vztahy s orgány veřejné správy.

Doporučení k realizaci

Organizace by měly mít zavedeny postupy, které přesně určují za jakých podmínek a kým by měly být kontaktovány orgány veřejné správy (např. policie, hasiči, dozorčí orgány) a postupy včasného hlášení bezpečnostních incidentů v případech, kdy existuje podezření na porušení zákonů.

V některých případech mohou organizace, které jsou vystaveny útokům z internetu, využít služeb třetích stran (např. poskytovatelé internetového připojení nebo telekomunikační operátoři), k podniknutí nápravných opatření.

Další informace

Udržování dobrých vztahů s orgány veřejné zprávy může také patřit mezi požadavky na podporu zvládání bezpečnostních incidentů (viz 13.2) nebo procesů plánování kontinuity a obnovy činností po havárii (viz kapitola 14). Dobré kontakty na regulační orgány zase umožní organizaci předjímat připravované změny v zákonech a předpisech a dopředu se na ně připravit. Kontakty na další subjekty mohou zahrnovat komunální služby, pohotovostní služby, inspektoráty bezpečnosti práce, dále pak například hasiče (ve vztahu ke kontinuitě činností organizace), poskytovatele telekomunikačních služeb (ve vztahu ke směrování a dostupnosti kabeláže), dodavatele vody (pro potřeby chladících zařízení).

6.1.7 Kontakt se zájmovými skupinami

Opatření

Měly by být udržovány přiměřené vztahy se zájmovými skupinami nebo speciálními fóry na bezpečnost a profesními sdruženími.

Doporučení k realizaci

Členství ve specializovaných zájmových skupinách a diskusních fórech by mělo být zváženo z následujících důvodů:
a) rozšiřování znalostí o nejlepších praktikách a nejnovějších trendech v oblasti bezpečnosti informací;
b) ujištění se, že to jak je chápána bezpečnost informací v organizaci je dostatečné a odpovídá současným trendům;
c) obdržení včasného varování, získání doporučení a informací o bezpečnostních záplatách souvisejících s útoky a zranitelnostmi;
d) získání přístupu k doporučením a radám odborníků na bezpečnost informací;
e) sdílení a výměna informací o nejnovějších technologiích, produktech, hrozbách a zranitelnostech;
f) navázání vhodné spolupráce pří řešení bezpečnostních incidentů (viz také 13.2.1).

Další informace

Pro zlepšení spolupráce a koordinace při řešení záležitostí týkajících se bezpečnosti mohou být uzavřeny dohody o sdílení informací. Takovéto dohody by měly obsahovat požadavky na ochranu citlivých informací.

6.1.8 Nezávislá přezkoumání bezpečnosti informací

Opatření

Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cíle opatření, jednotlivá opatření, politiky, směrnice a postupy) by měly být v pravidelných intervalech (a nebo v případě jakékoliv významné změny ve vztahu k bezpečnosti) nezávisle přezkoumávány.

Doporučení k realizaci

Vedení organizace by mělo iniciovat nezávislá přezkoumání bezpečnosti informací. Nezávislá přezkoumání jsou důležitá pro zajištění toho, že přístup organizace k řízení bezpečnosti informací je vyhovující, přiměřený a dostatečně účinný. Součástí přezkoumání by mělo být zhodnocení možností pro zlepšení a změny v přístupu k bezpečnosti, včetně přezkoumání bezpečnostní politiky a cílů opatření.

Tato přezkoumání by měla být prováděna nezávislými subjekty, např. útvar interního auditu, nezávislý vedoucí zaměstnanec nebo třetí organizace specializující se na tuto činnost, přičemž potenciální kandidáti na tuto práci musí mít patřičné znalosti a zkušenosti.
Výsledky nezávislých přezkoumání by měly být zaznamenány a měly by s nimi být seznámeni vedoucí zaměstnanci, kteří přezkoumání iniciovali.
Pokud je v rámci nezávislého přezkoumání zjištěno, že přístup organizace k řízení bezpečnosti informací jeví nedostatky nebo nesoulad se směrem stanoveným v bezpečnostní politice informací (viz 5.1.1), měly by být ze strany vedoucích zaměstnanců zváženy kroky k nápravě.
Další informace
Nezávislé přezkoumání může být také zváženo u oblastí, které mají být pravidelně přezkoumávány vedoucími zaměstnanci (viz 15.2.1). Techniky přezkoumání mohou zahrnovat rozhovory s vedoucími zaměstnanci, kontrolu záznamů nebo přezkoumání bezpečnostních politik. ČSN EN ISO 19011, Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu, může také poskytnout další užitečné informace o tom jak provést nezávislé přezkoumání bezpečnosti, včetně ustavení a zavedení programu přezkoumání. V kapitole 15.3 jsou uvedena opatření týkající se nezávislých přezkoumání informačních systémů a použití nástrojů pro audit systému.

6.2 Externí subjekty

Cíl: Zachovat bezpečnost informací organizace a zařízení pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.
Bezpečnost informací a zařízení pro zpracování informací by neměla být snížena při zavedení produktů a služeb třetích stran.
Přístup externích subjektů k zařízení pro zpracování informací a k informacím by měl být kontrolován.
Tam, kde z činností organizace vyplývá potřeba přístupu externích subjektů, by mělo být provedeno hodnocení rizik plynoucích z tohoto přístupu tak, aby se zjistily důsledky z hlediska bezpečnosti a aby se definovaly požadavky na opatření. Opatření by měla být schválena a definována ve smlouvě se třetí stranou.

6.2.1 Identifikace rizik plynoucích z přístupu externích subjektů

Opatření
Předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací, by měla být identifikována rizika a implementována vhodná opatření na jejich pokrytí.
Doporučení k realizaci
Tam, kde existuje potřeba přístupu externích subjektů k informacím organizace a zařízení pro zpracování informací, by mělo být provedeno hodnocení rizik (viz také kapitola 4) tak, aby byly identifikovány požadavky na opatření. Při identifikace rizik spojených s přístupem externích subjektů by mělo být vzato v potaz následující:
a) identifikace zařízení pro zpracování informací ke kterým je potřebný přístup externích subjektů;
b) typ přístupu jaký bude mít externí subjekt k zařízení pro zpracování informací, např.:
1. fyzický přístup, např. přístup do kanceláří, do místností s počítači, do kartoték;
2. logický přístup, např. přístup k databázím organizace, do informačních systémů;
3. typ síťového spojení mezi organizací a externím subjektem, např. trvalé spojení, vzdálený přístup;
4. zda je přístup z prostor organizace a nebo mimo ně;
c) hodnota, citlivost a kritičnost příslušných informací pro organizaci;
d) opatření nutná k ochraně informací, ke kterým nemají mít externí subjekty přístup;
e) identifikace personálu na straně externích subjektů, který bude mít přístup k informacím;
f) způsob jakým je identifikována organizace nebo personál mající oprávnění k přístupu, jakým způsobem je toto oprávnění ověřeno a jak často znovu potvrzeno;
g) postupy a opatření používané externími subjekty při ukládání, komunikování, sdílení a výměně informací;
h) jaký může mít dopad nedostupnost informací a prostředků pro zpracování informací externím subjektem. Dopad jaký může mít zadání nebo obdržení nepřesných nebo klamných informací externím subjektem;
i) směrnice a postupy pro řešení bezpečnostních incidentů a potenciálních poškození, podmínky a okolnosti za jakých bude umožněn přístup externím subjektům v případě bezpečnostního incidentu;
j) zákonné, regulatorní a jiné relevantní smluvní požadavky ve vztahu k externím subjektům, které by měly být vzaty v potaz;
k) jaký to může mít vliv na zájmy akcionářů, podílníků a ostatních zájmových skupin.
Přístup třetích stran k informacím a k zařízením pro zpracování informací by neměl být umožněn do té doby, než jsou implementována přiměřená bezpečnostní opatření a podepsána dohoda, ve které se vymezí podmínky síťového propojení nebo přístupu třetí strany do prostor organizace a pracovní podmínky. Obecně, veškeré bezpečnostní požadavky plynoucí z možnosti přístupu třetí strany nebo interních opatření, musí být v souladu se smlouvou uzavřenou mezi třetí stranou a organizací (viz také 6.2.2 a 6.2.3).
Další informace
Informace mohou být ohroženy přístupem třetích stran s neadekvátním řízením bezpečnosti. Je nutné vědět, jaká opatření je nezbytné přijmout v souvislosti se zabezpečením přístupu třetích stran k zařízením pro zpracování informací. Například v případě potřeby zachování důvěrnosti informací může být uzavřena dohoda o zachování důvěrnosti.
Organizace mohou být vystaveny rizikům souvisejícím s interními procesy, řízením a komunikací při zajištění činností organizace formou outsourcingu nebo pokud se spolupráce

dotýká více externích subjektů.
Opatření uvedená v kapitolách 6.2.2 a 6.2.3 pokrývají různé typy externích subjektů a poskytovaných služeb, jako například:
a) poskytovatele služeb, jako jsou poskytovatelé informačních a síťových služeb, telefonní služby, služby podpory a údržby;
b) služby správy bezpečnosti;
c) zákazníky;
d) outsourcing zařízení a/nebo provozu, např. informačních systémů a technologií, služeb sběru dat, provozu call center;
e) konzultanty na řídící a obchodní činnosti a auditory;
f) vývojáře a dodavatele, např. informačních systémů a technologií;
g) úklid, zásobování, bezpečnostní ostraha a další externě zajišťované služby;
h) vykonání studentské praxe a jiné podobné krátkodobé akce.
Takovéto dohody mohou snížit rizika vyplývajících z přístupu externích subjektů.

6.2.2 Bezpečnostní požadavky pro přístup klientů

Opatření
Předtím, než je klientům umožněn přístup k informací a aktivům organizace, by měly být zjištěny veškeré požadavky na bezpečnost.
Doporučení k realizaci
Předtím než je umožněn přístup zákazníků k aktivům organizace by měly být zváženy následující požadavky pro zajištění bezpečnosti (v závislosti na typu a rozsahu přístupu nemusí být všechny aplikovatelné):
a) ochrana aktiv zahrnující:
1. postupy sloužící k ochraně aktiv organizace včetně informací a programového vybavení a řízení známých zranitelností;
2. postupy sloužící ke zjištění, zda nedošlo ke kompromitaci aktiv, například ztrátě nebo modifikaci dat;
3. integritu aktiv;
4. omezení kopírování a šíření informací;
b) popis každé služby nebo produktu, které jsou třetí straně zpřístupněny;
c) důvody, požadavky a výhody vyplývající z přístupu umožněného zákazníkům;
d) politika řízení přístupu zahrnující:
1. povolené metody přístupu a jeho kontrola, použití jedinečných identifikátorů, jako jsou uživatelské identifikátory a hesla;
2. autorizační proces pro přístup uživatele a jeho oprávnění;
3. prohlášení, že každý přístup který není explicitně povolen je zakázán;
4. proces zrušení přístupových práv nebo přerušení spojení mezi systémy;
e) systém hlášení, upozorňování a vyšetřování nepřesností informací (např. osobních údajů), bezpečnostních incidentů a případů prolomení bezpečnosti;
f) popis každé služby, která je třetí straně zpřístupněna;
g) cílová úroveň služby a neakceptovatelné úrovně služby;
h) právo monitorovat a zakázat aktivity uživatele;
i) konkrétní závazky a odpovědnosti na straně organizace a zákazníka;
j) odpovědnosti vyplývající z právních norem, například z legislativy na ochranu osobních údajů – zvláště v případech uzavírání smluv mezi stranami z různých států je nutné vzít v úvahu národní legislativu (viz také 15.1);
k) ochrana duševního vlastnictví a autorské právo (viz15.1.2) a ochrana jakékoliv týmové práce (viz také 6.1.5).
Další informace
Bezpečnostní požadavky pro zajištění přístupu zákazníků se mohou lišit v závislosti na informacích a zařízení pro zpracování informací ke kterým má zákazník přístup. Tyto požadavky mohou být naplněny v rámci dohod uzavřených se zákazníkem, ve kterých jsou identifikována veškerá rizika a požadavky na bezpečnost (viz také 6.1.5).
Dohody s externími subjekty mohou také zahrnovat další zúčastněné strany. Dohody umožňující přístup externích subjektů by měly zahrnovat dodatek, ve kterém budou ustanoveni další případní účastníci, kteří by měli přístup k aktivům organizace, a budou upraveny požadavky na tento přístup.

6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou

Opatření
Dohody, uzavřené s třetími stranami zahrnující přístup, zpracování, šíření nebo správu informací organizace nebo správu zařízení pro zpracování informací (případně dodávku produktů nebo služeb k zařízení pro zpracování informací), by měly pokrývat veškeré relevantní bezpečnostní požadavky.
Doporučení k realizaci
Dohody by měly zaručit, že mezi organizací a třetí stranou neexistuje nesoulad ve výkladu předmětu jejich plnění. Organizace by se tímto samy měly pojistit před zproštěním se odpovědnosti smluvních partnerů.
Doporučuje se zvážit zařazení následujících oblastí pro pokrytí všech identifikovaných požadavků na bezpečnost (viz 6.2.1):
a) bezpečnostní politika informací;
b) opatření pro zajištění ochrany aktiv, zahrnující:
1. postupy sloužící k ochraně aktiv organizace včetně informací a programového a technického vybavení;
2. jakákoliv opatření fyzické ochrany a mechanizmy, které zajišťují jejich plnění;
3. opatření k zajištění ochrany před škodlivým programovým vybavením (viz 10.4.1);

4. postup sloužící ke zjištění, zda nedošlo ke kompromitaci aktiv, například ztrátě nebo modifikaci informací, programového a technické vybavení;
5. opatření zajišťující vrácení či zničení informací/aktiv po ukončení smluvního vztahu nebo v jeho průběhu;
6. důvěrnost, integritu, dostupnost a další důležité vlastnosti aktiv;
7. omezení kopírování a šíření informací a dodržování dohod o ochraně důvěrných informací (viz 6.1.5);
c) školení uživatelů a správců v metodách, postupech a v bezpečnosti;
d) zajištění dostatečného povědomí uživatelů o bezpečnosti informací a jejich odpovědnostech;
e) tam, kde je to vhodné, podmínky přechodu personálu mezi smluvními stranami;
f) odpovědnost za instalaci a údržbu technického a programového vybavení;
g) jasná pravidla hlášení a schválený formát těchto hlášení;
h) jasný a specifikovaný proces řízení změn;
i) politiku řízení přístupu zahrnující:
1. důvody, požadavky a výhody, které činí přístup třetích stran nezbytným;
2. povolené metody přístupu, kontrola a použití jedinečných identifikátorů, jako jsou uživatelské identifikátory (ID) a hesla;
3. autorizační proces pro přístup uživatele a jeho oprávnění;
4. požadavky na vedení a dostupnost seznamu jednotlivců, kteří jsou vzhledem ke svým předdefinovaným právům a privilegiím oprávněni využívat nabízené služby;
5. prohlášení, že každý přístup který není explicitně povolen je zakázán;
6. proces zrušení přístupových práv nebo přerušení spojení mezi systémy;
j) systém hlášení, upozorňování a vyšetřování bezpečnostních incidentů a případů prolomení bezpečnosti, stejně tak jako porušení jakýchkoliv podmínek stanovených v dohodách;
k) popis každé služby, která je třetí straně zpřístupněna a popis každé zpřístupněné informace včetně bezpečnostní klasifikace (viz 7.2.1);
l) cílová úroveň služby a neakceptovatelné úrovně služby;
m) popis ověřitelných kritérií výkonnosti, způsob jejich sledování a hlášení;
n) právo monitorovat a zakázat jakékoliv aktivity uživatele mající vztah k aktivům organizace;
o) právo auditovat povinnosti stanovené v dohodách nebo mít právo nechat provést tyto audity třetí stranou a jmenovitě uvést legitimní práva auditorů;
p) ustavení procesu eskalace při řešení problému;
q) požadavky na kontinuitu služeb, včetně opatření pro zajištění dostupnosti a spolehlivosti, v souladu se stanovenými prioritami organizace;
r) konkrétní závazky a odpovědnosti na straně organizace a zákazníka;
s) odpovědnosti vyplývající z právních norem, například z legislativy na ochranu osobních údajů – zvláště v případech uzavírání smluv mezi stranami z různých států je nutné vzít v úvahu národní legislativu (viz také 15.1);
t) ochrana duševního vlastnictví a autorské právo (viz15.1.2) a ochrana jakékoliv týmové práce (viz také 6.1.5);
u) spolupráce třetích stran se subdodavateli a bezpečnostní opatření která musí subdodavatelé přijmout;
v) podmínky obnovení/ukončení dohod:
1. měl by být připraven náhradní plán pro případ, že se některá ze stran rozhodne ukončit spolupráci před řádným vypršením platné dohody;
2. vyjednání nových podmínek v případě, že dojde ke změně bezpečnostních požadavků organizace;
3. seznam aktiv, licencí, dohod nebo práv s nimi spojených.

Další informace

Dohody uzavírané mezí organizací a třetími stranami se mohou výrazně lišit. Měl by proto být kladen důraz na začlenění všech identifikovaných požadavků na bezpečnost. Tam kde je to potřebné, mohou být požadavky na opatření a postupy podrobněji rozvedeny v plánu řízení bezpečnosti.

Pokud je bezpečnost informací zajišťována formou outsourcingu, měly by uzavřené dohody upravovat způsob jakým bude třetí strana zajišťovat odpovídající úroveň bezpečnosti tak, jak bylo určeno v rámci hodnocení rizik. Dále způsob jakým bude udržována úroveň bezpečnosti a jak budou požadavky na bezpečnost upraveny v případě změn rizik.

Rozdíly v poskytování služeb formou outsourcingu a jinými typy spolupráce s třetími stranami jsou v otázkách právní závaznosti, plánování přechodných období a plánování pro případ narušení činností v průběhu přechodných období, plánování kontinuity činností a hloubkové prověrky (due diligence), sběru a správy informací o bezpečnostních incidentech. Je proto důležité aby organizace správně plánovala a řídila přechod k outsourcovaným službám a měla zavedeny postupy řízení změn a obnovy/ukončení dohod o outsourcingu.

7 Klasifikace a řízení aktiv

7.1 Odpovědnost za aktiva

Cíl: Udržovat přiměřenou ochranu aktiv organizace.

U všech důležitých informačních aktiv by měla být stanovena odpovědnost a určen jejich vlastník.

Pro všechna důležitá aktiva by měli být určeni vlastníci a měla by být stanovena jejich odpovědnost za udržování přiměřených bezpečnostních opatření. Odpovědnost za realizaci jednotlivých bezpečnostních opatření může být delegována, ale vlastní odpovědnost za ně by měla zůstat na vlastníkovi aktiva.

7.1.1 Evidence aktiv

Opatření

Měla by být identifikována všechna aktiva organizace, všechna důležitá aktiva by měla být evidována a seznam udržován aktuální.

Doporučení k realizaci

Organizace musí být schopna identifikovat svá aktiva a stanovit jejich relativní hodnotu a důležitost. Evidence by měla obsahovat informace potřebné pro případ obnovy po havárii. Měl by být uveden typ aktiva, jeho formát, umístění, informace o záloze, licenční informace a jeho hodnota pro organizaci. Seznam by neměl zbytečně duplikovat jiné, již existující seznamy. Pokud se tak stane, měla by být zajištěna shody uváděných informací.

Pro každé aktivum by měl být schválen a zaevidován jejich vlastník (viz 7.1.2) a bezpečnostní klasifikace (viz 7.2).

Evidence aktiv pomáhá zajistit udržování účinné bezpečnostní ochrany a může být vyžadována i k jiným účelům, jako je například bezpečnost a ochrana zdraví při práci, pojištění nebo potřeby finančního řízení (správy aktiv). Na základě důležitosti aktiva, jeho hodnoty pro organizaci a bezpečnostní klasifikaci, by měla být určena odpovídající úroveň jeho ochrany (více informací o tom jakým způsobem přiřadit aktivum hodnotu tak, aby to odpovídalo jejich důležitosti, lze nalézt v normě ISO/IEC TR 13335-36).

Další informace

Příkladem aktiv spojených s informačními systémy jsou:

a) informační aktiva: databáze a datové soubory, systémová dokumentace, uživatelské manuály, školicí materiály, provozní nebo podpůrné postupy, plány obnovy funkčnosti, dohody o zajištění záložního provozu, auditní záznamy, archivované informace;

b) aplikační programová aktiva: aplikační a systémové programové vybavení, vývojové nástroje a utility;

c) fyzická aktiva: počítačové vybavení (základní jednotky, monitory, notebooky, modemy), komunikační zařízení (směrovače, pobočkové ústředny, faxy, záznamníky), magnetická média (pásky a disky), další technická zařízení (napájecí zdroje, klimatizační zařízení), nábytek, prostory;

d) služby: počítačové a komunikační služby, další technické služby (topení, osvětlení, napájení, klimatizace);

e) lidé a jejich kvalifikace, dovednosti a zkušenosti;

f) nehmotná aktiva, jako například pověst a image organizace.

Evidence aktiv pomáhá zajistit udržování účinné ochrany a může být vyžadována i k jiným účelům, jako je například bezpečnost a ochrana zdraví při práci, pojištění nebo potřeby finančního řízení (správy aktiv). Proces vytvoření seznamu aktiv je nezbytným předpokladem pro řízení rizik (viz také kapitola 4).

7.1.2 Vlastnictví aktiv

Opatření

Veškeré informace a aktiva související se zařízením pro zpracování informací by měly mít určeného vlastníka7.

Doporučení k realizaci

Vlastník aktiva by měl být odpovědný za:

a) zajištění odpovídající klasifikace informací a aktiv souvisejících s prostředky pro zpracování informací;

b) přesné vymezení a pravidelné přezkoumání omezení přístupu a klasifikace aktiv, v souladu s platnou politikou řízení přístupu.

Vlastnictví může být přiděleno na:

a) proces;

b) přesně vymezený soubor činností;

c) aplikaci;

d) přesně vymezený soubor dat.

Další informace

Běžné úkoly (např. každodenní dohled nad aktivy) mohou být delegovány, odpovědnost však vždy zůstává na vlastníkovi aktiva.

Ve složitých informačních systémech může být výhodné seskupit aktiva, která dohromady zajišťují jednu konkrétní funkci (např. službu). V takovémto případě je vlastník služby odpovědný nejen za její správné fungování, ale také za všechna aktiva, která ji zajišťují.

7.1.3 Přípustné použití aktiv

Opatření

Měla by být ustavena, zdokumentována a do praxe zavedena pravidla pro přípustné použití informací a aktiv souvisejících se zařízením pro zpracování informací.

Doporučení k realizaci

Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli dodržovat pravidla pro přípustné použití informací a aktiv souvisejících se zařízením pro zpracování informací a to včetně:

a) pravidel pro použití elektronické pošty a internetu (viz 10.8);

b) doporučení pro použití mobilních zařízení, zejména mimo areál organizace (viz 11.7.1).

Odpovědní vedoucí by měli zveřejnit pravidla a doporučení pro použití aktiv. Zaměstnanci, smluvní strany a uživatelé třetích stran, kteří používají nebo mají přístup k aktivům organizace, by měli znát pravidla omezující použití informací, zdrojů, a aktiv souvisejících se zařízením pro zpracování informací. Měli by nést odpovědnost za použití jakýchkoli zdrojů pro zpracování informací.

7.2 Klasifikace informací

Cíl: Zajištění přiměřenosti ochrany informačních aktiv.

Informace by měly být klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany.

Informace mohou mít různý stupeň citlivosti a mohou být různě kritické, některé mohou

vyžadovat vyšší úroveň bezpečnosti nebo zvláštní způsob zacházení. Měl by existovat systém bezpečnostní klasifikace, který by určoval adekvátní stupeň ochrany a který by dával uživatelům informace o nutnosti zvláštního zacházení.

7.2.1 Doporučení pro klasifikaci

Opatření

Informace by měly být klasifikovány a to ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.

Doporoučení k realizaci

Klasifikace a odpovídající opatření pro ochranu informací by měly vycházet z potřeb a požadavků organizace na sdílení nebo omezení přístupu k informacím a dále by měly vycházet z dopadů, které vyplývají z nenaplnění těchto požadavků.

Pravidla klasifikace by měla zohledňovat skutečnost, že jednou provedená klasifikace není neměnná, ale že se může měnit podle předem určených pravidel (viz 11.1.1).

Odpovědnost za definici klasifikace jednotky informace (dokumentu, záznamu, souboru, diskety) a za periodické přezkoumávání této klasifikace by měla zůstat na autorovi nebo určeném vlastníku informace (viz 7.1.2). Při klasifikaci by nemělo být zapomenuto na efekt agregace, viz také kapitola 10.7.2.

Pozornost by měla být věnována počtu klasifikačních kategorií a výhodám plynoucím z jejich použití. Příliš komplexní struktury se mohou stát těžkopádné, neekonomické nebo nepraktické.

Pozornost by měla být věnována také interpretaci klasifikačního značení dokumentů z jiných organizací, které mohou mít jiné definice pro stejné nebo podobné značení.

Další informace

Úroveň ochrany informací může být také určena na základě požadavků na jejich důvěrnost, integritu, dostupnost a jakýchkoliv dalších požadavků.

Informace často po určité době přestávají být citlivé nebo kritické, například v případě jejich zveřejnění. S těmito skutečnostmi je nutné počítat, protože reklasifikace může přinést značné dodatečné administrativní náklady.

Pro zjednodušení procesu klasifikace mohou být jednotlivé dokumenty, u kterých existují stejné požadavky na bezpečnost, klasifikovány jako celek.

V zásadě klasifikace umožňuje rychle určit způsob zacházení s informacemi a způsob jejich ochrany.

7.2.2 Označování a nakládání s informacemi

Opatření

Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.

Doporučení k realizaci

Tyto postupy musí pokrývat informační aktiva ve fyzické i elektronické podobě.

Výstup ze systémů, obsahujících citlivé informace, by měl být (na výstupu) označen odpovídajícím klasifikačním návěštím. Značení by mělo odpovídat klasifikačním pravidlům ustanoveným podle 7.2.1. Toto platí zejména pro tiskové výstupy, výstupy na obrazovku, záznamová média (pásky, disky, CD, kazety), elektronické zprávy a přenosy souborů. Manipulační postupy by měly být definovány pro každou úroveň klasifikace tak, aby pokrývaly bezpečné zpracování informací, jejich uchování, přenos, deklasifikaci a likvidaci. Měly by být také definovány postupy pro sběr důkazů a zaznamenávání jakýchkoliv bezpečnostních událostí.

Dohody o sdílení dat, uzavřené mezi organizacemi, by měly obsahovat postupy identifikace klasifikovaných informací a způsob jakým mají být interpretována návěští, která používají jednotlivé organizace.

Další informace

Značení a bezpečné nakládání s klasifikovanými informacemi je klíčovým požadavkem pro sdílení informací. Nejvhodnější formou značení jsou „fyzická" návěští, avšak pro některá aktiva (například dokumenty v elektronické podobě) nelze použít „fyzický" způsob značení. Pro takový druh aktiv je třeba použít elektronické označovací prostředky. Oznámení o práci s klasifikovanou informací se může například zobrazit na monitoru nebo displeji. Tam kde není možné provést označení, mohou být použity jiné prostředky pro určení klasifikované informace, např. prostřednictvím procesu nebo meta-dat8.

8 Bezpečnost lidských zdrojů

8.1 Před vznikem pracovního vztahu9

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

Odpovědnosti za bezpečnost by měly být zohledněny v rámci přijímacího řízení, měly by být zahrnuty v pracovních smlouvách a popisech práce.

Potenciální uchazeči by měli být náležitě prověřeni, zejména v případě citlivých pracovních míst.

Všichni zaměstnanci, smluvní a třetí strany, využívající zařízení organizace pro zpracování informací, by měli podepsat dohodu odpovídající jejich rolím a povinnostem.

8.1.1 Role a odpovědnosti

Opatření

Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací by měly být stanoveny a zdokumentovány v souladu s bezpečnostní politikou organizace.

Doporučení k realizaci

Role a odpovědnosti v oblasti bezpečnosti informací by měly zahrnovat:

a) požadavek na realizaci a dodržování zásad v souladu s bezpečnostní politikou organizace (viz 5.1);

b) požadavek na ochranu aktiv před neautorizovaným přístupem, prozrazením, modifikací,

zničením nebo narušením;
c) požadavek na vykonávání určitých bezpečnostních postupů nebo činností;
d) požadavek na určení jednoznačné odpovědnosti za provedené činnosti;
e) požadavek hlásit bezpečnostní události nebo jiná bezpečnostní rizika.
V rámci přijímacího řízení by zájemcům o práci měly být jasně sděleny role a odpovědnosti spojené s místem o které se ucházejí.
Další informace
Popisy pracovních míst mohou být použity k doložení pracovních rolí a odpovědností v oblasti bezpečnosti informací. Role a odpovědnosti jedinců, kteří nejsou zaměstnanci organizace (například zaměstnanci třetích stran) by měly být jasně stanoveny a tito by měli být s nimi seznámeni.

8.1.2 Prověrka

Opatření
Všichni uchazeči o zaměstnání, smluvní a třetí strany by měly být prověřeni dle platných zákonů, předpisů a v souladu s etikou. Prověření by měla být prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti10 a potenciálních rizik. Doporučení k realizaci
Při prověřování by měl být brán zřetel na dodržení soukromí a ochranu osobních dat11 a související legislativu12.
Tam, kde je to povoleno, měly by být prověrky prováděny na základě:
a) dostupnosti dvou dostatečných referencí, například profesní a osobní;
b) kontroly životopisu uchazeče (s ohledem na úplnost a přesnost);
c) ověření proklamovaného vzdělání a odborné kvalifikace;
d) nezávislého ověření totožnosti (dalším dokladem, například cestovním pasem);
e) detailnějšího prověření, jako například výpisu z trestního rejstříku, finanční situace, atd..
Tam, kde práce, pracovní pozice vyžaduje přístup k prostředkům zpracovávajícím zejména citlivé informace (finanční nebo vysoce důvěrné), by organizace měla provést také detailnější prověrky spolehlivosti.
Měly by být stanoveny přesné postupy vymezující kritéria a omezení, např. kdo a jak je oprávněn prověrky provádět, kdy a jakým způsobem by měly prověrky probíhat.
Podobné prověrky by měly být provedeny také u externích pracovníků a pracovníků třetích stran. Tam, kde jsou smluvní strany zajišťovány agenturou, by smlouva s agenturou měla jasně specifikovat odpovědnost agentury za prověrky a také způsob, jakým agentura upozorní organizaci na skutečnost, že prověrka nebyla dokončena nebo že její výsledky vzbuzují podezření či pochybnosti. Obdobným způsobem by také dohody uzavřené se třetími stranami (viz také 6.2.3) měly jasně specifikovat veškeré odpovědnosti a povinnosti ve vztahu k prověrkám.
S informacemi o všech uchazečích (potenciální zaměstnanci, smluvní a třetí strany), které jsou získány v rámci prověrek by mělo být nakládáno v souladu s existujícími právními normami.
Pokud to zákon vyžaduje, měly by být uchazeči informováni o tom, že budou prověřováni.

8.1.3 Podmínky výkonu pracovní činnosti

Opatření
Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami by měly obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.
Doporučení k realizaci
Pracovní smlouvy by měly být v souladu s bezpečnostní politiku organizace a mimo to také upřesňovat a obsahovat následující:
a) všichni zaměstnanci, smluvní a třetí strany by měli, předtím než je jim umožněn přístup k citlivým informacím a zařízení pro zpracování informací, podepsat smlouvu o ochraně informací nebo o zachování mlčenlivosti;
b) práva a právní odpovědnost zaměstnanců, smluvních stran a ostatních uživatelů (například ve vztahu k autorskému zákonu nebo zákonu na ochranu osobních údajů);
c) odpovědnost za klasifikaci a správu aktiv spojených s informačním systémem a službami zaměstnavatele (viz také 7.2.1 a 10.7.3);
d) odpovědnosti zaměstnanců, smluvních a třetích stran pro nakládaní s informacemi obdrženými od jiných společností a zúčastněných stran;
e) odpovědnosti organizace při nakládání s osobními údaji, včetně těch údajů, které byly vytvořeny v průběhu pracovního poměru;
f) rozšíření odpovědností i mimo objekt organizace a mimo normální pracovní dobu (například v případě vzdálené práce z domova, viz také 9.2.5 a 11.7.1);
Neschopnost nadřízených dostatečně motivovat a řídit své podřízené může vést u zaměstnanců k pocitu, že jejich práce není dostatečně oceněná a důležitá, což může vyústit až v negativní dopad na organizaci.
Špatné vedení může například vést k zanedbání bezpečnosti a nebo ke zneužití aktiv organizace.

8.2.2 Povědomí, vzdělávání a školení v oblasti bezpečnosti informací

Opatření
Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran, by měli s ohledem na svoji pracovní náplň, projít odpovídajícím a pravidelně se opakujícím školením v oblasti bezpečnosti informací, bezpečnostní politiky a směrnicím organizace.
Doporučení k realizaci
Předtím, než je jim udělen přístup k aktivům nebo službám organizace, měli by se dotčení seznámit s bezpečnostní politikou, požadavky a očekáváními v oblasti bezpečnosti a absolvovat školení.
Součástí pravidelných školení by mělo být zvyšování povědomí o bezpečnostních požadavcích, právní odpovědnosti a organizačních opatřeních. Zaměstnanci by také měli absolvovat školení

zaměřené na správné použití prostředků pro zpracování informací, např. přihlašovací postupy, použití programových balíků a měli by získat informace o disciplinárním řízení (viz 8.2.3).

Další informace

Školení, vzdělávání a zvyšování bezpečnostního povědomí by mělo být uzpůsobeno roli, odpovědnostem a schopnostem dotčené osoby. Mělo by také zahrnovat informaci o známých hrozbách a postupech při hlášení bezpečnostních incidentů (viz také 13.1).

Cílem zvyšování bezpečnostního povědomí v rámci školení je naučit jednotlivce rozpoznávat bezpečnostní incidenty a problémy a reagovat na ně způsobem, který odpovídá jejich roli.

8.2.3 Disciplinární řízení

Opatření

Mělo by existovat formalizované disciplinární řízení vůči zaměstnancům, kteří se dopustili narušení bezpečnosti.

Doporučení k realizaci

Disciplinární řízení by nemělo být zahájeno bez předchozí ověření, že se opravdu jedná o narušení bezpečnosti (viz také 13.2.2).

Formální disciplinární řízení by mělo zajistit korektní a spravedlivé zacházení se zaměstnanci podezřelými z narušení bezpečnosti. Formální disciplinární řízení vedené proti narušiteli by mělo odpovídat povaze narušení a jeho dopadu na organizaci. Mělo by být vzato do úvahy zda se jedná o první nebo opakované narušení, zda byl narušitel dostatečně proškolen, dále by měly být vzaty do úvahy odpovídající legislativa, existující smlouvy a další relevantní okolnosti. V závažných případech by měl být narušitel okamžitě zbaven svých povinností, přístupových práv a výsad. Pokud je to nutné měl by být co nejrychleji a v doprovodu vyveden mimo prostory organizace.

Další informace

Disciplinární řízení by mělo působit jako odstrašující prostředek odrazující zaměstnance, pracovníky smluvních a třetích stran od porušení bezpečnostních politik, směrnic a od narušení bezpečnosti.

8.3 Ukončení nebo změna pracovního vztahu

Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

Měly by být určeny jednoznačné odpovědnosti za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, za odevzdání přiděleného vybavení a odejmutí přístupových práv.

Změna odpovědností a pracovního vztahu v rámci organizace by měla probíhat jako by se jednalo o odebrání odpovědností nebo ukončení pracovního vztahu, tedy tak, jak je popsáno v této kapitole. Při uzavření nového pracovního vztahu by se mělo postupovat tak, jak je popsáno v kapitole 8.1.

8.3.1 Odpovědnosti za ukončení pracovního vztahu

Opatření

Měly by být jasně definovány a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu.

Doporučení k realizaci

Ukončení pracovního vztahu by mělo respektovat stávající bezpečnostní požadavky a právní odpovědnosti, pokud je to vhodné, požadavky obsažené v dohodách o ochraně důvěrných informací (viz 6.1.5), podmínky obsažené v pracovních smlouvách (viz 8.1.3), které jsou platné i po skončení pracovního vztahu.

Odpovědnosti a povinnosti platné i po skončení pracovního vztahu by měly být obsaženy ve smlouvách uzavřených se zaměstnanci, smluvními a třetími stranami.

Případné změny odpovědností nebo pracovního vztahu by měly být řízeny stejným způsobem jako v případě jejich ukončení. Přidělení nových odpovědností nebo uzavření nového pracovního vztahu by měly probíhat způsobem popsaným v kapitole 8.1.

Další informace

Za proces a náležitosti spojené s ukončení pracovního vztahu je zpravidla odpovědné personální oddělení, které spolupracuje s nadřízeným pracovníka opouštějícího organizaci tak, aby byly dodrženy veškeré aspekty bezpečnosti a odpovídající postupy. V případě, že se jedná o ukončení pracovního vztahu se smluvní stranou, může být odpovědnost za ukončení pracovního vztahu na straně zprostředkovatelské agentury. V případě ostatních pracovníků (pracovníci třetích stran) je tato odpovědnost zpravidla na straně jejich domovské organizace. V některých případech může být nutné informovat zaměstnance, zákazníky, smluvní nebo třetí strany o provozních a personálních změnách.

8.3.2 Navrácení zapůjčených předmětů

Opatření

Při ukončení pracovního vztahu by měli zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené předměty, které jsou majetkem organizace.

Doporučení k realizaci

Celý proces ukončení pracovního vztahu by měl být formalizovaný a měl by zahrnovat navrácení poskytnutého programového vybavení, dokumentů a vybavení, které jsou majetkem organizace. Opomenuty by neměly být také další předměty, jako například mobilní výpočetní prostředky, kreditní karty, přístupové karty, programová dokumentace a informace uložené na elektronických mediích.

Mělo by být zajištěno zálohování a bezpečné smazání informací (viz také 10.7.1) uložených na zařízení, které bylo odkoupeno nebo je majetkem zaměstnance, smluvní nebo třetí strany.

V případech kdy zaměstnanci, smluvní nebo třetí strany mají znalosti, důležité z hlediska stávajícího provozu, mělo by být zajištěno jejich zadokumentování a předání organizaci.

8.3.3 Odebrání přístupových práv

Opatření

Při ukončení pracovního vztahu by měla být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna přístupová práva k informacím a prostředkům pro zpracováním informací.

Doporučení k realizaci

Při ukončení pracovního vztahu by měla být přezkoumána přístupová práva k aktivům spojeným s informačními systémy a službami. V rámci těchto přezkoumání by mělo být určeno zda je odejmutí přístupových práv nezbytné. Přístupová práva, která nebyla schválena jako součást nového pracovního vztahu by měla být odebrána. Odebrání nebo změna přístupových práv zahrnuje fyzický a logický přístup, klíče, identifikační karty, zařízení pro zpracování informací (viz také 11.2.4), předplatné a odstranění jakékoliv informace, která tyto pracovníky identifikuje jako stávající členy organizace. Při odchodu nebo změně pracovního nebo smluvního vztahu zaměstnance, smluvní nebo třetí strany by měla být změněna veškerá jim známá hesla k aktivním účtům.

Před ukončením nebo změnou pracovního vztahu, by měla být odebrána nebo omezena přístupová práva k informačním aktivům a prostředkům pro zpracování informací. Při rozhodování by měly být zváženy následující rizikové faktory:

a) zda se jedná o změnu nebo ukončení pracovního vztahu iniciovanou ze strany zaměstnance, smluvní nebo třetí strany nebo naopak o změnu iniciovanou ze strany organizace a jaké jsou pro to důvody;

b) stávající odpovědnosti zaměstnance, pracovníka smluvní nebo třetí strany;

c) hodnota aktiv ke kterým mají přístup.

Další informace

V některých případech mohou být přístupová práva sdílena mezi více uživateli, pracovníky smluvních nebo třetích stran, například skupinové ID. V těchto případech by měli být uživatelé opouštějící organizaci vyjmuti ze všech seznamů skupinových přístupových práv, a všem ostatním zaměstnancům a pracovníkům smluvních a třetích stran by mělo být zakázáno sdílet informace s odcházející osobou.

V případě, že je pracovní vztah ukončen ze strany organizace, existuje možnost, že se nespokojený zaměstnanec, pracovník smluvní nebo třetí strany, pokusí záměrně poškodit informace a nebo zařízení pro jejich zpracování. Osoba opouštějící organizaci na vlastní žádost se zase může pokusit shromáždit interní informace pro budoucí použití.

9 Fyzická bezpečnost a bezpečnost prostředí

9.1 Zabezpečené oblasti

Cíl: Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

Zařízení zpracovávající kritické nebo citlivé informace organizace, by měla být umístěny v zabezpečených zónách chráněných definovaným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Tato zařízení by měla být fyzicky chráněna proti neautorizovanému přístupu, poškození a narušení.

Jejich ochrana by měla odpovídat zjištěným rizikům.

9.1.1 Fyzický bezpečnostní perimetr

Opatření

Při ochraně prostor ve kterých se nachází informace nebo zařízení pro zpracování informací by měly být používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).

Doporučení k realizaci

Následující doporučení a opatření by měla být zvážena a podle vhodnosti implementována:

a) měl by být jasně definován bezpečnostní perimetr, umístění a úroveň každého bezpečnostního perimetru by mělo záviset na bezpečnostních požadavcích na aktiva, uvnitř perimetru, a na výsledku hodnocení rizik;

b) perimetr budovy nebo oblasti obsahující zařízení pro zpracování informací by měl být v řádném stavu (tj. neměla by v perimetru nebo v oblasti existovat slabá, lehce proniknutelná místa). Obvodové zdi objektu by měly mít pevnou konstrukci a vstupní dveře by měly být chráněny před neautorizovaným vstupem zabezpečeny kontrolními mechanizmy např. mřížemi, alarmy, zámky apod. Dveře a okna by měla být v případě nepřítomnosti uzavřeny. U oken, zejména pokud jsou v přízemí, by mělo být zváženo využití externích ochranných prvků;

c) pro kontrolu fyzického přístupu do objektu nebo budovy by mělo být využíváno recepce či jiných prostředků. Vstup by měl být umožněn pouze oprávněným osobám;

d) fyzické bariéry by měly, tam kde je to použitelné, být postaveny tak, aby chránily před neoprávněným vstupem a kontaminací;

e) požární dveře v bezpečnostním perimetru by měly být opatřeny elektronickým zabezpečovacím systémem (EZS) a měly by být monitorovány. Požární dveře (stejně tak i zdi) by měly splňovat požadovanou úroveň odolnosti, dle příslušných požadavků místních, národních a mezinárodních norem;

f) vnější dveře a dosažitelná okna by měly být chráněny vhodným detekčním systémem, který odpovídá místním, národním a mezinárodním normám a je pravidelně testován. Opuštěné prostory by měly být chráněny nepřetržitě, pod ochranou by měly být i další oblasti, například počítačové a komunikační místnosti;

g) zařízení pro zpracování informací spravované organizací by měla být fyzicky oddělena od prostředků třetích stran.

Další informace

Fyzické ochrany může být dosaženo prostřednictvím řady fyzických bariér kolem prostor organizace a kolem prostředků zpracovávajících informace. Znásobení počtu bariér dodává dodatečnou ochranu, selhání jedné bariéry pak neznamená okamžitou kompromitaci bezpečnosti. Zabezpečenou oblastí může být uzamykatelná kancelář nebo několik místností uvnitř fyzického bezpečnostního perimetru. Uvnitř bezpečnostního perimetru mohou být mezi oblastmi s rozdílnou

úrovní bezpečnosti dodatečné bariéry a perimetry zajišťující kontrolu fyzického přístupu. V budovách kde sídlí více organizací, by měla být zvážena dodatečná opatření pro zabezpečení fyzického přístupu.

9.1.2 Kontroly vstupu osob

Opatření

Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, měly by být tyto oblasti chráněny vhodným systémem kontrol vstupu.

Doporučení k realizaci

Měla by být zvážena následující opatření:

a) datum a čas příchodu a odchodu návštěvníků by měl být zaznamenán a návštěvníci by měly být pod stálým dohledem. Návštěvníci by měli získávat oprávnění přístupu jen ze specifického důvodu a měli by být seznámeni s předpisy o bezpečnostních požadavcích v oblasti a o nouzových postupech;

b) přístup do oblastí kde se zpracovávají nebo jsou uloženy citlivé informace by měl být kontrolován a umožněn pouze oprávněným osobám. Pro autorizaci a ověření všech přístupů by mělo být použito autentizace, například kartou a PIN. Auditní záznam o všech přístupech by měl být bezpečně uchováván;

c) po všech zaměstnancích, smluvních a třetích stranách a návštěvnících by mělo být požadováno používat nějakou formu viditelné identifikace V případě, že narazí na návštěvníka bez doprovodu a jakoukoliv jinou bez viditelného označení, měli by okamžitě kontaktovat zaměstnance ostrahy;

d) přístup do zabezpečených oblastí nebo k zařízením zpracovávajícím citlivé informace by měl být umožněn pomocnému servisnímu personálu třetích stran pouze tehdy, když to je nutné. Takový přístup by měl být schválen a monitorován;

a) přístupová práva do zabezpečených oblastí by měla být pravidelně přezkoumávána a aktualizována a v případě potřeby zrušena (viz 8.3.3).

9.1.3 Zabezpečení kanceláří, místností a zařízení

Opatření

Mělo by být navrženo a aplikováno fyzické zabezpečení kanceláří, místností a zařízení.

Doporučení k realizaci

Pro zabezpečení kanceláří, místností a zařízení by měla být zvážena následující doporučení:

a) v úvahu by měly být vzaty odpovídající předpisy a normy pro bezpečnost a ochranu zdraví při práci;

b) důležitá zařízení by měla být situována tak, aby nebyla veřejně přístupná;

c) tam kde je to použitelné, by měly budovy být nenápadné, aby co nejméně naznačovaly jejich účel, bez nápadného vnějšího nebo vnitřního značení indikujícího přítomnost prostředků pro zpracování informací;

d) adresáře a interní telefonní seznamy, na jejichž základě by mohlo být zjištěno umístění prostředků pro zpracování citlivých informací, by neměly být přímo přístupné veřejnosti.

9.1.4 Ochrana před hrozbami vnějšího prostředí

Opatření

Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami by měly být navrženy a aplikovány prvky fyzické ochrany.

Doporučení k realizaci

V úvahu by měly být vzaty i další bezpečnostní hrozby z okolí, například požár v sousední budově, vytopení vodou z jiné oblasti, výbuch na ulici.

Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami by měla být zvážena následující doporučení:

a) nebezpečné a hořlavé materiály by měly být uchovávány v dostatečné vzdálenosti od zabezpečených oblastí. Když to není nezbytné, v těchto oblastech by neměly být přechovávány velké zásoby provozního materiálů, například kancelářských potřeb;

b) záložní zařízení a zálohovací média by měla být umístěna v takové bezpečné vzdálenosti, aby se zabránilo jejich případnému zničení v případě havárie v hlavních prostorách;

c) mělo by být zajištěno a vhodně umístěno hasící zařízení.

9.1.5 Práce v zabezpečených oblastech

Opatření

Pro práci v zabezpečených oblastech by měly být navrženy a aplikovány prvky fyzické ochrany.

Doporučení k realizaci

V úvahu by měla být vzata následující opatření.

a) personál by měl mít znalosti o existenci zabezpečené oblasti a o činnostech v ní probíhajících na základě své oprávněné potřeby;

b) v zabezpečených oblastech by neměla být povolena práce bez dohledu, jak z důvodů bezpečnosti práce, tak proto, aby se předešlo možnosti škodlivých aktivit;

c) opuštěné zabezpečené oblasti by měly být fyzicky uzamčeny a pravidelně kontrolovány;

d) fotografické, zvukové, obrazové nebo jiné záznamové prostředky by neměly být používány bez schválení.

Opatření pro práci v zabezpečených oblastech zahrnují kontroly zaměstnanců, smluvních a třetích stran stejně tak i kontrolu veškerých jejich dalších aktivit.

9.1.6 Veřejný přístup, prostory pro nakládku a vykládku

Opatření

Prostory pro nakládku a vykládku a další místa, kudy se mohou neoprávněné osoby dostat do prostor organizace, by měla být kontrolována a pokud možno by měla být izolována od zařízení pro zpracování informací tak, aby se zabránilo neoprávněnému přístupu.

Doporučení k realizaci

V úvahu by měla být vzata následující opatření:

a) přístup do prostor pro nakládku a vykládku by měl být umožněn pouze osobám již známým a oprávněnému personálu;

b) prostory pro nakládku a vykládku by měly být navrženy tak, aby materiál mohl být vyložen, aniž by personál dodavatele měl přístup do jiných částí budovy;

c) v případě otevřených vnitřních dveří by měly být vnější dveře skladovacího prostoru zabezpečeny;

d) došlý materiál by měl být prozkoumán vzhledem k možnému ohrožení (viz 9.2.1 d)) předtím, než bude přemístěn ze skladovacího prostoru na místo použití;

e) došlý materiál by měl být, v souladu s postupy klasifikace a řízení aktiv, při převzetí zaevidován (viz 5.1);

f) tam kde je to možné by příchozí a odcházející zásilky měly být fyzicky odděleny.

9.2 Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození nebo kompromitaci aktiv a přerušení činnosti organizace.

Zařízení by měla být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů. Ochrana zařízení (včetně těch, která se používají mimo hlavní lokalitu) je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození. Pozornost by měla být věnována také jejich umístění a likvidaci. Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků, jako například dodávky elektrické energie a struktury kabelových rozvodů, mohou být požadována zvláštní opatření.

9.2.1 Umístění zařízení a jeho ochrana

Opatření

Zařízení by měla být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Doporučení k realizaci

V úvahu by měla být vzata následující opatření:

a) kde je to možné, zařízení by měla být umístěna tak, aby byl minimalizován nadbytečný přístup do pracovních prostor;

b) zařízení pro zpracování a ukládání citlivých dat by měla být umístěna tak, aby bylo sníženo riziko možného odezírání informací;

c) aktiva, která vyžadují zvláštní ochranu, by měla být izolována, aby se snížil rozsah požadované celkové ochrany;

d) pro minimalizaci rizik potenciálních hrozeb (např. krádež, oheň, výbušniny, kouř, voda, vibrace, prach, působení chemických látek, rušení elektrického napájení, elektromagnetické vyzařování a vandalismus) by měla být přijata odpovídající opatření;

e) organizace by měla zvážit svá pravidla týkající se jídla, pití a kouření v blízkosti zařízení zpracovávajících informace;

f) působení vnějšího prostředí (jako např. teplota a vlhkost), které by mohlo mít vliv na činnost zařízení pro zpracování informací, by mělo být monitorováno;

g) ve všech budovách by měla být nasazena ochrana proti blesku a ochrannými filtry proti blesku by měly být osazeny všechny vnější komunikační linky a elektrické vedení;

h) pro zařízení ve výrobním prostředí by mělo být zváženo používání zvláštních ochran, jako jsou například membránové klávesnice;

i) zařízení zpracovávající citlivé informace by mělo být chráněno, aby se zabránilo úniku citlivých informací prostřednictvím kompromitujícího (parazitního) elektromagnetického vyzařování.

9.2.2 Podpůrná zařízení

Opatření

Zařízení by mělo být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Doporučení k realizaci

Veškeré podpůrné služby, jako elektřina, dodávky vody, kanalizace, topení/ventilace a klimatizace by měly být přiměřené systému, který podporují. Pro snížení rizika špatného fungování nebo selhání by měly být podpůrné služby pravidelně kontrolovány a vhodným způsobem testovány. Mělo by být zajištěno vhodné elektrické napájení odpovídající specifikacím výrobce.

Pro elektrická zařízení zajišťující kritické operace organizace je doporučeno použití záložních zdrojů UPS13, umožňující korektní ukončení nebo pokračování v práci. Do plánů obnovy funkčnosti by měly být zapracovány činnosti prováděné v případě selhání UPS. UPS by měla být pravidelně kontrolována zda má odpovídající kapacitu a testována v souladu s doporučeními výrobce. Při nutnosti zpracovávání informací v případě déletrvajících výpadků proudu by mělo být zváženo použití záložního generátoru. Pro zajištění déletrvající činnosti generátoru by mělo být k dispozici odpovídající množství paliva. UPS a generátor by měly být pravidelně kontrolovány, aby se zajistilo, že mají dostatečnou kapacitu a měly by být také pravidelně testovány podle návodu výrobce. Mělo by být zváženo použití více zdrojů dodávek energie a nebo, v případě rozsáhlých lokalit, oddělené elektrické rozvodny.

V místnostech se zařízením v blízkosti nouzových východů, by měly být instalovány bezpečnostní (nouzové) vypínače pro rychlé vypnutí napájení v případě nebezpečí. Pro případ výpadku hlavního napájení by mělo být zajištěno nouzové osvětlení.

Dodávky vody by měly být stabilní a dostatečné pro zajištění klimatizace, pro zvlhčovače vzduchu a pro automatické hasící systémy (pokud jsou používány). Selhání dodávek vody může zapříčinit poškození zařízení nebo znemožní spuštění automatických hasících systémů . Měla by být zvážena možnost použití poplašných zařízení detekujících selhání podpůrných služeb.

Telekomunikační zařízení by mělo být k poskytovateli služby připojeno nejméně dvěma různými cestami, aby se zabránilo selhání hlasových služeb v případě, že dojde k výpadku na jedné z cest. Hlasové služby by měly odpovídat legislativním požadavkům krizové komunikace.

Další informace

Mezi možnosti jak dosáhnout kontinuity napájení patří znásobení přívodů dodávek energie, aby zařízení nebylo závislé na jednom zdroji.

9.2.3 Bezpečnost kabelových rozvodů

Opatření

Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat a podporu informačních služeb, by měly být chráněny před poškozením či odposlechem.

Doporučení k realizaci

Měla by být zvážena následující doporučení:

a) napájecí a telekomunikační linky připojené k prostředkům IT by měly tam, kde je to možné, vést pod zemí nebo by měly být chráněny jiným vhodným způsobem;

b) síťové kabelové rozvody by měly být chráněny před neoprávněným odposlechem nebo poškozením, například vedením v kolektoru anebo tím, že nebudou vedeny přes veřejné prostory;

c) napájecí kabely by měly být odděleny od komunikačních rozvodů, aby se zabránilo interferenci;

d) kabely a zařízení by měly být zřetelně označeny, aby se zabránilo možnosti záměny v případech provádění oprav poškozených kabelů;

e) pro snížení pravděpodobnosti vzniku chyb by měly být udržován seznam propojení;

f) u citlivých a kritických systémů by měla být další opatření:

1. instalace pancéřového potrubí a zamčených místností nebo skříní v kontrolních a ukončovacích místech;
2. použití alternativního směrování nebo alternativních přenosových cest poskytujících přiměřenou bezpečnost;
3. použití optických kabelů;
4. použití stínění kabelů na ochranu před elektromagnetickým vyzařováním;
5. zavedení technických kontrol a fyzických přezkoumání s následným odpojením neschválených zařízení připojených do rozvodů;
6. řízení přístupu k propojovacím panelům a k rozvodnám kabelů.

9.2.4 Údržba zařízení

Opatření

Zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Doporučení k realizaci

V úvahu by měla být vzata následující opatření:

a) zařízení by měla být udržována a provozována v souladu s doporučeními dodavatele;

b) opravy a servis zařízení by měl provádět pouze oprávněný personál;

c) o všech závadách nebo podezřelých chybách by měly být pořízeny záznamy, stejně tak o preventivních prohlídkách a opravách;

d) jak v případech údržby zařízení v rámci objektu, tak při jeho odeslání mimo objekt by měla být dodržena odpovídající opatření. V případech, kdy údržbu zařízení neprovádí prověřený personál, by z něj měly být odstraněny veškeré citlivé informace;

e) měly by být splněny všechny pojistné podmínky.

9.2.5 Bezpečnost zařízení mimo prostory organizace

Opatření

Zařízení používané mimo prostory organizace by mělo být zabezpečeno s přihlédnutím k různým rizikům vyplývajících z jejich použití mimo organizaci.

Doporučení k realizaci

Použití zařízení pro zpracování informací, bez ohledu na jejich vlastníka, mimo budovy organizace by mělo podléhat schválení vedením organizace.

Při práci mimo prostory organizace by měla být zvážena následující doporučení:

a) při cestách mimo organizaci by zařízení a média ve veřejných prostorách neměla být ponechána bez dozoru. Přenosný počítač by měl být přepravován jako příruční zavazadlo a v rámci možností ukrýván;

b) měly by se dodržovat pokyny výrobce týkající se ochrany zařízení, například zajištění ochrany proti působení silného magnetického pole;

c) pro práci doma by měla být určena vhodná opatření na základě hodnocení rizik, například uzamykatelné skříňky, pravidlo prázdného stolu, kontrola přístupu k počítači a zabezpečení spojení s kanceláří (viz také ISO/IEC 18028 Network Security);

d) zařízení používané mimo prostory organizace by mělo být pojištěno.

Bezpečnostní rizika, jako například poškození, krádež a odposlech, se mohou v různých lokalitách značně lišit a to by mělo být zváženo při výběru těch nejvhodnějších bezpečnostních opatření.

Další informace

Zařízení pro zpracování informací zahrnují všechny druhy osobních počítačů, organizérů, mobilních telefonů, čipových karet, dokumentů a ostatních zařízení, používaných pro práci doma nebo vynášených mimo normální pracovní umístění.

Více informací o dalších hlediscích ochrany přenosných zařízení lze najít v 11.7.1.

9.2.6 Bezpečná likvidace nebo opakované použití zařízení

Opatření

Všechna zařízení obsahující paměťová média by měla být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna nebo přepsána.

Doporučení k realizaci

U zařízení obsahujících citlivé informace by mělo být preferováno fyzické zničení nebo bezpečné smazání/přepsání dat za použití postupů znemožňujících jejich obnovu a to ještě před použitím běžné funkce mazání nebo formátování.

Další informace

Rozhodování o zničení, opravení nebo vyřazení poškozených zařízení obsahujících citlivá data by mělo být založeno na hodnocení rizik.

Informace organizace mohou být prozrazeny při nedbalé likvidaci nebo opakovaném použití zařízení (viz také 10.7.2).

9.2.7 Přemístění majetku

Opatření

Zařízení, informace nebo programové vybavení by bez schválení nemělo být přemisťováno.

Doporučení k realizaci

Měla by být zvážena následující doporučení:

a) zařízení, informace nebo programové vybavení by neměly být přemisťovány bez předchozího schválení;

b) měli by být určeni zaměstnanci, případně pracovníci smluvních a třetích stran, kteří mohou udílet povolení k přemístění aktiv organizace;

c) přemístění vybavení by mělo být časově omezeno a jeho včasné navrácení kontrolováno;

d) tam kde je to požadováno měly by být pořízeny záznamy o přemístění vybavení a jeho navrácení.

Další informace

Pro zjištění neschváleného přenášení majetku, nepovoleného vnášení nahrávacích zařízení, zbraní, atd., by měly být prováděny namátkové kontroly. Namátkové kontroly by měly být prováděny v souladu s odpovídajícími zákony a předpisy. Zaměstnanci by si měli být vědomi, že takové kontroly probíhají.

10 Řízení komunikací a řízení provozu

10.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz prostředků pro zpracování informací.

Měly by být stanoveny odpovědnosti a postupy pro řízení a správu prostředků zpracovávajících informace. Zahrnuje to vytváření vhodných provozních instrukcí a postupů.

V případě potřeby by měl být uplatněn princip oddělení funkcí, aby se snížilo riziko úmyslného zneužití systému nebo zneužití z nedbalosti.

10.1.1 Dokumentace provozních postupů

Opatření

Provozní postupy by měly být zdokumentovány a udržovány a měly by být dostupné všem uživatelům dle potřeby.

Doporučení k realizaci

Měly by být zdokumentovány postupy správy pro činnosti spojené s prostředky pro zpracování informací a komunikaci, jako například spuštění a zastavení systému, zálohování dat, údržba zařízení, zacházení s médii, správa počítačové místnosti, zacházení s korespondencí a bezpečnost práce.

Provozní postupy by měly obsahovat návod pro detailní výkon každé činnosti, včetně:

a) zpracování a zacházení s informacemi;

b) zálohování dat (viz 10.5);

c) časové návaznosti zpracování, včetně vzájemných souvislostí s jinými systémy, čas začátku první a dokončení poslední úlohy;

d) popis činnosti při výskytu chyb nebo jiných mimořádných stavů, které by mohly vzniknout při běhu úlohy, včetně omezení na používání systémových nástrojů (viz 11.5.4);

e) spojení na kontaktní osoby v případě neočekávaných systémových nebo technických potíží;

f) instrukce pro zacházení se speciálními výstupy, jako například se speciálním spotřebním materiálem, správa důvěrných výstupů, včetně instrukcí pro nakládání s chybnými výstupy z aplikací v případě jejich selhání (viz 10.7.2 a 10.7.3);

g) postupy při restartu systému a obnovovací postupy v případě selhání systému;

h) nakládání s auditními a systémovými záznamy (viz 10.10).

Provozní dokumentace a zdokumentované postupy systémových činností by měly být brány jako oficiální dokumentace a jejich změny by měly být odsouhlaseny vedoucími zaměstnanci. Pokud je to technicky proveditelné měla by být správa jednotlivých informačních systémů konzistentní (použití stejných postupů, nástrojů a služeb).

10.1.2 Řízení změn

Opatření

Změny ve vybavení a zařízení pro zpracování informací by měly být řízeny.

Doporučeni k realizaci

Provozní systémy a aplikační programové vybavení by měly podléhat přísnému řízení změn.

V úvahu by měla být zejména vzata následující opatření:

a) identifikace a zaznamenání důležitých změn;

b) plánování a testování změn;

c) zhodnocení potenciálních dopadů (včetně dopadů na bezpečnost) takových změn;

d) formální schvalovací postup pro navrhované změny;

e) seznámení všech osob, kterých se to dotýká, s detaily změn;

f) postupy určující odpovědnosti za přerušení změnového zásahu a obnovení provozu v případě jejich neúspěchu.

Pro zajištění dostatečné úrovně řízení změn zařízení, programového vybavení nebo postupů, by měly být stanoveny formální řídící postupy a odpovědnosti. O změnách programového vybavení

by měly být uchovávány veškeré relevantní informace, například v podobě auditních záznamů.

Další informace

Nedostatečná kontrola změn v prostředcích pro zpracování informací a systémech je běžnou příčinou bezpečnostních a systémových chyb. Změny provozního prostředí, zejména při přechodu z vývojového prostředí do ostrého provozu, mohou mít dopad na spolehlivost aplikací (viz také 12.5.1).

Změny provozních systémů by měly být prováděny pouze v nutných případech, například dojde-li k nárůstu rizika. Instalace nejnovějších verzí provozních systémů a aplikací by měla být předem dobře zvážena. Může zavést nové zranitelnosti a způsobit větší nestabilitu systému než předchozí verze, často je také spojena s dodatečným zaškolením personálu, s licenčními poplatky, poplatky za podporu a údržbu, nákupem nového hardwaru a dodatečnou administrací.

10.1.3 Oddělení povinností

Opatření

Pro snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv organizace by mělo být zváženo oddělení jednotlivých povinností a odpovědností.

Doporučení k realizaci

Princip oddělení povinností minimalizuje riziko úmyslného nebo nedbalostního zneužití systému. Pozornost by měla být věnována oblastem s nedělenou odpovědností jedince, který by mohl mít přístup k aktivům, mohl by je modifikovat nebo používat bez řádného oprávnění aniž by to bylo zjištěno. Vyvolání události by mělo být odděleno od jejího schválení. Při návrhu opatření by měla být zvážena možnost spolčení angažovaných jedinců.

V malých organizacích může být tato metoda řízení obtížně použitelná, ale tento princip by měl být aplikován tak, jak to je jen možné. Všude, kde je oddělení složité, by měla být zvážena jiná opatření, jako monitorování činností, auditní záznamy a dohled nadřízených zaměstnanců. Je důležité, aby bezpečnostní audit zůstal nezávislý.

10.1.4 Oddělení vývoje, testování a provozu

Opatření

Pro snížení rizika neoprávněného přístupu k provoznímu systému a nebo jeho změn by mělo být zváženo oddělení procesů vývoje, testování a provozu.

Doporučení k realizaci

Pro prevenci provozních problémů by měla být zvážena nezbytná úroveň oddělení provozního, testovacího a vývojového prostředí a zavedena vhodná opatření.

V úvahu by měla být vzata následující opatření:

a) měla by být stanovena a dokumentována pravidla pro převod programů z vývojového do provozního prostředí;

b) vývojové a provozní programové vybavení by mělo být provozováno na různých počítačích nebo v různých doménách či adresářích;

c) překladače, editory a jiné systémové utility by neměly být dosažitelné z provozních systémů, pokud to není nutné;

d) testovací prostředí by mělo co nejvíce simulovat provozní prostředí;

e) pro provozní a testovací systémy by měly být používány různé uživatelské profily. Nabídky by měly zobrazovat vhodné identifikační zprávy, aby se snížilo riziko chyby;

d) citlivá data by neměla být kopírována do testovacích systémů (viz 12.4.2).

Další informace

Vývoj a testování mohou způsobit vážné problémy, například nechtěnou modifikaci souborů, prostředí nebo způsobení systémové chyby. Je proto potřebné mít známé a stabilní prostředí, které zaručí smysluplnost testování a rozpozná nevhodný přístup vývojářů.

Tam, kde má vývojový a testovací personál přístup k provoznímu systému, může být schopen vnést do něj neschválený a netestovaný kód nebo změnit provozní data. V některých systémech by tato možnost mohla být zneužita k podvodu nebo k zavedení netestovaného nebo škodlivého kódu. Takový kód může způsobit vážné provozní problémy.

Vývojáři a personál provádějící testování mohou také představovat hrozbu pro důvěrnost provozních dat. Vývojové a testovací práce, v případě že sdílejí stejné výpočetní prostředí, mohou umožnit i nechtěné změny programů a informací. Oddělení vývojových, testovacích a provozních zařízení je proto žádoucí pro snížení rizika nechtěných změn nebo neautorizovaného přístupu k provozním programům a obchodním datům (viz také 12.4.2).

10.2 Řízení dodávek třetích stran

Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávky služeb ve shodě s uzavřenými dohodami.

Pro zajištění toho, že služby dodávané třetími stranami jsou v souladu s dohodnutými požadavky, by organizace měla kontrolovat realizaci dohod, monitorovat míru souladu jejich dodržování a v případě potřeby zajistit nápravu.

10.2.1 Dodávky služeb

Opatření

Zajistit, aby úroveň služeb týkajících se bezpečnosti informací poskytovaných třetí stranou byla v souladu se smluvními podmínkami.

Doporučení k realizaci

Součástí služeb poskytovaných třetí stranou by měla být realizace dohodnutých bezpečnostní opatření, vymezení služeb a jejich správy. V případech, kdy jsou služby zajištěny formou outsourcingu, by organizace měla naplánovat nezbytný přenos (informací, zařízení pro zpracování informací a čehokoliv co vyžaduje přesun), a zajistit bezpečnost po celou dobu přenosu.

Organizace by měla zajistit, aby třetí strana měla dostatečné kapacity a měla navržené a otestované plány pro zajištění kontinuity, a dohodnuté úrovně, poskytovaných služeb v případě jejich selhání nebo v případě krizové události (viz 14.1).

10.2.2 Monitorování a přezkoumávání služeb třetích stran

Opatření

Služby, zprávy a záznamy poskytované třetí stranou by měly být monitorovány a pravidelně přezkoumávány, audity by měly být opakovány v pravidelných intervalech.

Doporučení k realizaci

Monitorování a přezkoumávání služeb poskytovaných třetími stranami, by mělo zajistit, že je dodržována bezpečnost informací a dohodnuté podmínky, a že vzniklé bezpečnostní incidenty a nastalé problémy jsou řešeny odpovídajícím způsobem. Toto by také mělo zahrnovat kontrolu dodržování smluvních podmínek a ostatních činností ve vazbě na smluvní vztah:

a) monitorování úrovně poskytovaných služeb na dohodnuté úrovni;

b) přezkoumávání hlášení o službách poskytovaných třetí stranou a uspořádání pravidelných informativních schůzek;

c) poskytnutí informací o bezpečnostních incidentech a přezkoumání poskytnutých informací jak třetí stranou, tak organizací, podle toho jak je stanoveno v dohodách, metodických pokynech a směrnicích;

d) přezkoumání auditních záznamů týkajících přístupů k systému a činností prováděných v systému, záznamů o bezpečnostních událostech, provozních problémech, selháních, chybách a přerušeních poskytovaných služeb;

e) řešení a zvládání nastalých problémů.

Organizace by měla určit osobu nebo ustavit servisní tým pracovníků odpovědných za nastavení a udržování vztahů se třetí stranou. Dále by měla organizace zajistit, že třetí strana určí odpovědnosti pro kontrolu souladu a prosazování požadavků stanovených v dohodách.

K dispozici by měl být personál s dostatečnými technickými dovednostmi a zdroje pro monitorování požadavků stanovených v dohodách (viz 6.2.3), zejména pak dodržování požadavků na bezpečnost informací. V případě, že je zjištěn jakýkoliv nesoulad v poskytovaných službách, by měla být sjednána náprava.

Organizace by měla zajistit dostatečnou kontrolu a transparentnost všech aspektů bezpečnosti týkajících se citlivých a kritických informací nebo zařízení pro zpracování informací, ke kterým je přistupováno, jsou zpracovávány a nebo jsou spravovány třetí stranou. Organizace by měla zajistit dohled nad činnostmi souvisejícími s bezpečností, jako je např. řízení změn, identifikace zranitelností, proces zaznamenávání a reakce na bezpečností incidenty.

Další informace

V případě, že jsou služby zajištěny formou outsourcingu nese organizace konečnou odpovědnost za zpracovávané informace.

10.2.3 Řízení změn služeb poskytovaných třetími stranami

Opatření

Změny v poskytování služeb, včetně udržování a zlepšování existujících bezpečnostních politik, směrnic a bezpečnostních opatření, by měly být řízeny s ohledem na kritičnost systémů a procesů organizace, které jsou součástí opakovaného hodnocení rizik.

Doporučení k realizaci

Proces řízení změn služeb poskytovaných třetí stranou by měl reflektovat:

a) nutné změny provedené organizací za účelem:

1. vylepšení aktuálně nabízených služeb;
2. vývoje nových aplikací a systémů;
3. změny a aktualizace stávajících politik a směrnic;
4. realizace nových opatření pro zvládání bezpečnostní incidentů a opatření na zvýšení bezpečnosti;

b) nutné změny služeb poskytovaných třetích stranou za účelem:

1. změny a vylepšení sítí;
2. použití nových technologií;
3. zavedení nových produktů nebo nových verzí/aktualizací programů;
4. změny fyzického umístění servisních zařízení;
5. změny dodavatelů.

10.3 Plánování a přejímání informačních systémů

Cíl: Minimalizovat riziko selhání informačních systémů.

Pro zajištění odpovídající kapacity a zdrojů a výkonu informačního systému je nutné provést odpovídající přípravu a plánování.

Aby se snížilo riziko přetížení systému, měl by být vytvářen odhad budoucích kapacitních požadavků.

Před schválením nových systémů a před jejich uvedením do provozu by k nim měly být stanoveny, písemně zdokumentovány a otestovány provozní požadavky.

10.3.1 Řízení kapacit

Opatření

Pro zajištění požadovaného výkonu informačního systému, s ohledem na budoucí kapacitní požadavky, by mělo být monitorováno, nastaveno a projektováno využití zdrojů.

Doporučení k realizaci

Pro každou stávající a plánovanou činnost by měly být identifikovány kapacitní požadavky. Pro zajištění a tam, kde je to nezbytné pro zlepšení dostupnosti a efektivity systému, by mělo být aplikováno monitorování a zlepšování výkonu systému. Měla by být zavedena opatření umožňující včasnou detekci vzniklých problémů. Součástí provozních a systémových doporučení by měl být i požadavek na plánování budoucí spotřeby kapacit na současný a uvažovaný směr vývoje ve zpracování informací v organizaci.

Zvláštní pozornost by měla být věnována zdrojům, které vyžadují delší dobu pro realizaci dodávky nebo obnášejí vysoké náklady. Vedoucí pracovníci by měli sledovat trendy jejich použití, zejména pak v relaci k aplikacím organizace a nástrojům pro správu systému.

Tyto informace by měly být použity pro identifikaci a prevenci kritických míst, které by mohly způsobovat ohrožení bezpečnosti nebo uživatelských služeb, a pro naplánování vhodných

opatření k nápravě.

10.3.2 Přejímání systémů

Opatření

Měla by být určena kritéria pro přejímání nových informačních systémů, jejich aktualizaci a zavádění nových verzí a vhodný způsob testování systému v průběhu vývoje a před zavedením do ostrého provozu.

Doporučení k realizaci

Vedoucí zaměstnanci by měli zajistit, aby požadavky a kritéria pro přejímání nových počítačových systémů byly jednoznačně definovány, schváleny, zdokumentovány a testovány. Přechod na nové systémy, instalace aktualizací a zavádění nových verzí by měl být formálně schválen. Předtím než je provedeno formální schválení mělo by zváženo následující:

a) požadavky na výpočetní a paměťový výkon;

b) postupy pro zotavení se z chyb a restartů systému, a havarijní plány;

c) příprava a testování rutinních provozních postupů, které by představovaly normu;

d) schválená sada nasazených bezpečnostních opatření;

e) účinné manuální operace;

f) plán kontinuity činností organizace (viz 14.1);

g) potvrzení, že instalace nového systému nebude mít nepříznivý vliv na existující systémy, zejména v době špičky zatížení, jako je například konec měsíce;

h) potvrzení, že byly zváženy dopady nového systému na celkovou bezpečnost organizace;

i) školení v obsluze a použití nového systému;

j) snadnost použití může pozitivně ovlivnit výkon uživatelů a zabránit zbytečným chybám.

Na všech vývojových stupních nových důležitých programů rozvoje by měl být konzultován provozní personál a uživatelé, aby byla zajištěna provozní účinnost navrhovaného systému, a také by se měly provést příslušné testy, aby se potvrdilo, že systém plně vyhovuje všem přejímacím kritériím.

Další informace

Součástí přejímání nových systémů může také být proces formální certifikace a akreditace ověřující naplnění bezpečnostních požadavků.

10.4 Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programů a dat.

Pro prevenci a detekování škodlivých programů a nepovolených mobilních kódů jsou vyžadována patřičná opatření.

Programy a zařízení pro zpracování informací jsou zranitelné škodlivými programy, jako jsou například počítačové viry, síťoví červi, trojští koně a logické bomby. Uživatelé by měli být upozorňováni na nebezpečí neschválených a škodlivých programů. Vedoucí zaměstnanci by měli tam, kde je to vhodné, aplikovat zvláštní opatření pro jejich předcházení a detekování a zavést postupy odstranění škodlivých programů a kontroly mobilních kódů.

10.4.1 Opatření na ochranu proti škodlivým programům

Opatření

Na ochranu proti škodlivým programům a nepovoleným mobilním kódům by měla být implementována opatření na jejich detekci, prevenci a nápravu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.

Doporučení k realizaci

Ochrana proti škodlivým programům by měla být založena na detekci škodlivých programů, opravných programů, na bezpečnostním povědomí, dále na vhodném přístupu k systému a na opatřeních zajišťujících řízení změn.

V úvahu by měla být vzata následující opatření:

a) ustavení formálních pravidel požadujících dodržování licenčních podmínek a zákaz používání neschváleného programového vybavení (viz 15.1.2);

b) ustavení formálních pravidel zajišťujících ochranu proti rizikům vyplývajícím ze získávání programů z externích sítí nebo z jiných médií a určujících, jaká ochranná opatření by měla být přijata;

c) zavedení pravidelné kontroly programů a datového obsahu systémů kritických pro vnitropodnikové procesy. Měla by být formálně prošetřována přítomnost libovolných neschválených souborů nebo neodsouhlasených úprav ;

d) instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií, buď jako preventivní prostředek využívaný ad-hoc způsobem, nebo pravidelně. Prováděné kontroly by měly zahrnovat:

1. ověření všech souborů na elektronických nebo optických médiích nejistého a neověřeného původu nebo souborů získaných prostřednictvím neautorizovaných sítí před jejich použitím na přítomnost škodlivých programů;

2. testování všech příloh elektronické pošty a stažených dat na přítomnost škodlivých programů před jejich použitím. Tato kontrola může být prováděna na různých místech, například na poštovním serveru, na pracovních stanicích nebo při vstupu do sítě organizace;

3. kontrola obsahu webových stránek na přítomnost škodlivého kódu;

e) určení řídících postupů a povinnosti při práci s antivirovou ochranou v systémech, školení uživatelů, hlášení a nápravy virových útoků (viz 13.1 a 13.2);

f) příprava odpovídajících plánů kontinuity činností organizace pro zotavení se z virových útoků, včetně kompletního zálohování a obnovy potřebných dat a programů (viz kapitola 14);

g) zavedení pravidelného sběru nových informací (odběr časopisů, hledání na internetu) o nových škodlivých kódech;

h) zavedení postupů zajišťujících platnost informací o virech a správnost i informační

hodnotu varovných signálů. Vedoucí zaměstnanci by měli zajistit, aby pro odlišení reálných virů od falešných byly použity kvalifikované zdroje informací, tj. časopisy s dobrým renomé, spolehlivé internetové zdroje a dodavatelé antivirových programů. Zaměstnanci by měli znát problém falešných virů, měli by vědět, co dělat, když zprávu o takovém viru obdrží nebo objeví.

Další informace

Pro zvýšení účinnosti ochrany před škodlivými programy je vhodné použít více různých antivirových programů.

Pro zajištění odpovídající ochrany lze antivirové programy nastavit tak, aby automaticky probíhala aktualizace definičních souborů a skenovacího enginu. Antivirové programy by měly být nainstalovány na každé pracovní stanici.

Pozornost by měla být zvýšena vždy když je prováděna údržba systému nebo řešena krizová událost, v rámci kterých mohou být obejita běžná ochranná opatření.

10.4.2 Opatření na ochranu proti mobilním kódům

Opatření

Použití povolených mobilních kódů by mělo být nastaveno v souladu s bezpečnostní politikou, mělo by být zabráněno spuštění nepovolených mobilních kódů.

Doporučení k realizaci

Měla by být zvážena následující opatření na ochranu proti neoprávněnému spuštění mobilních kódů:

a) spouštění mobilních kódů v logicky odděleném prostředí;

b) zamezení spouštění všech mobilních kódů;

c) zamezení příjmu mobilních kódů;

d) zapnutí dostupných technických opatřeních na jednotlivých systémech zajišťujících správu mobilních kódů;

e) kontrola všech prostředků využívajících mobilní kódy;

f) použití kryptografických opatření pro ověření původu mobilního kódu.

Další informace

Mobilní kód je programový kód, který se přenáší z jednoho počítače na druhý a poté se automaticky spustí a vykoná specifickou funkci za minimální nebo žádné součinnosti s uživatelem. Mobilní kódy jsou součástí řady middleware služeb (např. zajišťujících propojení jednotlivých aplikací).

Kromě ověření toho, že neobsahuje škodlivý kód, je kontrola mobilních kódů důležitá z důvodu vyhnutí se neoprávněnému použití nebo narušení systému, sítě nebo aplikačních zdrojů a jiným narušením bezpečnosti.

10.5 Zálohování

Cíl: Udržovat integritu a dostupnost informací a zařízení pro jejich zpracování.

Měly by být vytvořeny rutinní postupy realizující schválenou politiku zálohování a strategii (viz 14.1) pro vytváření záložních kopií dat a testování jejich včasného obnovení.

10.5.1 Zálohování informací

Opatření

Záložní kopie důležitých informací a programového vybavení organizace by měly být pořizovány a testovány v pravidelných intervalech.

Doporučení k realizaci

Pro zajištění obnovy všech důležitých informací a programového vybavení organizace v případě katastrofy nebo selhání médií (nosičů dat) by mělo být zajištěno adekvátní zálohovací zařízení.

V úvahu by měla být vzata následující opatření:

a) mělo by být stanoveno minimální nutné množství vytvářených záloh;

b) měly by být vytvořeny přesné a úplné záznamy o záložních kopiích s popsanými postupy obnovy;

c) rozsah vytvářených záloh (např. kompletní nebo přírůstkové zálohy) a frekvence s jakou jsou vytvářeny by měla odpovídat požadavkům organizace na dostupnost informací, požadavkům na bezpečnost informací a jejich kritičnosti z hlediska kontinuity činností organizace;

d) zálohy by měly být uloženy na bezpečném místě, v dostatečné vzdálenosti od sídla organizace, aby v případě havárie nebyly poškozeny nebo zničeny;

e) záložním informacím by měla být věnována přiměřená úroveň fyzické a vnější ochrany (viz kapitola 9), odpovídající normám v hlavním sídle. Opatření používaná pro média v hlavním sídle by měla být rozšířena i na místo s uloženými záložními kopiemi;

f) záložní média by měla být pravidelně testována, aby bylo zajištěno, že se na ně lze v nutném případě spolehnout;

g) obnovovací postupy by měly být pravidelně prověřovány a testovány, aby se potvrdilo, že jsou účinné a že mohou být provedeny v čase vymezeném provozním obnovovacím postupům;

h) v případech, kdy je požadováno zajištění důvěrnosti zálohovaných informací, by mělo být použito šifrování.

Postupy zálohování jednotlivých systémů by měly být pravidelně testovány, aby vyhovovaly požadavkům plánů kontinuity činností organizace (viz kapitola 11). U kritických systémů by zálohování mělo zahrnovat veškeré systémové informace, aplikace a data potřebná pro kompletní obnovu systému v případě havárie.

Měla by být určena doba archivace důležitých informací organizace a také jakékoliv požadavky na archivní kopie, které by měly být trvale uchovávány (viz 15.1.3).

Další informace

Celý proces vytváření záloh může být zautomatizován, takováto řešení však musí být před spuštěním důkladně otestována. Po uvedení do provozu musí být sytém automatického vytváření záloh pravidelně testován.

10.6 Správa sítě

Cíl: Zajistit ochranu informací v počítačových sítích a ochranu jejich infrastruktury.
Pozornost vyžaduje správa bezpečnosti počítačových sítí, které mohou přesahovat hranice organizace.
Pro zabezpečení citlivých dat přenášených veřejnými sítěmi mohou být požadována dodatečná opatření.

10.6.1 Síťová opatření

Opatření

Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečnosti informací při přenosu by počítačové sítě měly být vhodným způsobem spravovány a kontrolovány.

Doporučení k realizaci

Správci sítí by měli realizovat opatření pro zajištění bezpečnosti dat v sítích a ochrany souvisejících služeb před neoprávněným přístupem.
Zejména by měla být vzata v úvahu následující opatření:
a) tam, kde je to vhodné, by měla být odpovědnost za provoz sítě oddělena od odpovědnosti za provoz počítačů (viz 10.1.3);
b) měly by být stanoveny odpovědnosti a postupy pro správu vzdálených zařízení, včetně zařízení v prostorách uživatelů;
c) měla by být zavedena zvláštní opatření, která by zajišťovala důvěrnost a integritu dat přenášených veřejnými nebo bezdrátovými sítěmi a ochranu připojených systémů a aplikací (viz 11.4 a 12.3). Pro zajištění dostupnosti síťových služeb a připojených počítačů mohou být vyžadována zvláštní opatření;
d) měly by být vytvořeny a zavedeny vhodné postupy zaznamenávání a monitorování událostí souvisejících s bezpečností;
e) činnosti související se správou počítačů a sítí by měly být důkladně koordinovány, a to jak z hlediska optimalizace služeb pro organizaci, tak pro zajištění jejich konzistence v rámci celé infrastruktury zajišťující zpracování informací.

Další informace

Další informace k bezpečnosti sítí viz norma ISO/IEC 1802814.

10.6.2 Bezpečnost síťových služeb

Opatření

Měly by být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu.

Doporučení k realizaci

Způsobilost poskytovatele síťových služeb bezpečně zajistit správu dohodnutých síťových služeb by měla být prověřena a průběžně monitorována, mělo by být odsouhlaseno právo provádět audit.
Měla by být identifikována bezpečnostní nastavení spojená s konkrétními službami, jako jsou bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na jejich správu. Organizace by měla zajistit implementaci těchto opatření poskytovatelem síťových služeb.

Další informace

Síťové služby zahrnují poskytnutí připojení, služby privátních sítí, sítí s přidanou hodnotou a správu bezpečnostních řešení jako jsou například bezpečnostní brány (firewall) a systémy pro detekci průniku. Tyto služby mohou zahrnovat obyčejné přidělení neřízené šířky pásma (kapacity) pro připojení až po komplexní řešení s přidanou hodnotou.
Bezpečnostní prvky síťových služeb mohou zahrnovat:
a) technologie použité pro zajištění bezpečnosti síťových služeb, jako např. autentizace, šifrování a kontroly síťových spojení;
b) technické parametry požadované pro zajištění bezpečného připojení k síťovým službám síťových připojení v souladu s platnými pravidly;
c) postupy omezující přístup k síťovým službám nebo k aplikacím.

10.7 Bezpečnost při zacházení s médii

Cíl: Předcházet neoprávněnému prozrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.
Média by měla být kontrolována a fyzicky zabezpečena.
Měly by být stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií (např. pásky, disky), vstupních/výstupních dat a systémové dokumentace před neoprávněným prozrazením, modifikací, odstraněním nebo poškozením.

10.7.1 Správa vyměnitelných počítačových médií

Opatření

Měly by být vytvořeny postupy pro správu vyměnitelných počítačových médií.

Doporučení k realizaci

Pro správu vyměnitelných médií by měla být zvážena následující doporučení:
a) pokud již nejsou znovupoužitelná média potřebná, měl by být předtím, než jsou odstraněna z organizace, vymazán jejich obsah;
b) v nutných případech by měla být požadována autorizace pro odstranění médií z organizace a měl by se o tom vést záznam pro potřeby auditu;
c) ukládat všechna média v bezpečném prostředí v souladu se specifikacemi výrobce;
d) informace, u kterých požadavek na dostupnost přesahuje životnost médií (dle specifikací výrobce) na kterých jsou uloženy, by měly být přemístěny, aby se zabránilo jejich případné ztrátě;
e) zaregistrování všech vyměnitelných médií pro snížení pravděpodobnosti jejich ztráty;
f) použití vyměnitelných mechanik by mělo být povoleno jen v odůvodněných případech.

Všechny postupy a úrovně oprávnění by měly být jednoznačně zdokumentovány.

Další informace

Vyměnitelná média zahrnují pásky, disky, flashdisky, přenositelné harddisky, CD, DVD a tiskové výstupy.

10.7.2 Likvidace médií

Opatření

Jestliže jsou média dále provozně neupotřebitelná, měla by být bezpečně a spolehlivě zlikvidována.

Doporučení k realizaci

Při nedbalé likvidaci médií by se mohla citlivá data dostat do cizích rukou. Pro minimalizaci tohoto rizika by měly být vytvořeny formální postupy bezpečné likvidace médií. Postupy pro bezpečnou likvidaci by měly odpovídat citlivosti informací.

Zejména by měla být vzata následující opatření:

a) média, obsahující citlivé informace, by měla být bezpečně zlikvidována, například spálením nebo skartováním nebo smazáním dat před jejich opětovným použitím jiným způsobem v rámci organizace;

b) měly by být vytvořeny postupy pro identifikaci médií, které vyžadují bezpečnou likvidaci;

c) může být jednodušší stanovit pravidla bezpečného sběru a likvidace pro všechna média, než se snažit vyčlenit ta s citlivými daty;

d) řada organizací nabízí sběr a likvidaci papíru, zařízení a médií. Při výběru vhodného smluvního partnera je nutné dávat zejména pozor na to, aby dodržoval odpovídající opatření a měl zkušenosti;

e) likvidace citlivých médií by měla být, podle možností, zaznamenávána pro potřeby následného auditu.

Při nahromadění většího množství médií k likvidaci by měl být zvážen efekt agregace, kdy se velké množství neklasifikovaných informací stává citlivějším než malé množství klasifikovaných informací.

Další informace

Citlivé informace mohou být prozrazeny při nedbalé likvidaci médií (další informace o likvidaci zařízení viz také 9.2.6).

10.7.3 Postupy pro manipulaci s informacemi

Opatření

Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.

Doporučení k realizaci

Tato pravidla by měla zajistit manipulaci s informacemi, jejich zpracování, ukládání a sdílení v souladu s jejich klasifikací (viz 7.2).

V úvahu by měla být vzata následující doporučení:

a) manipulace se všemi médii a jejich označování by mělo odpovídat jejich klasifikaci;

b) omezení přístupu pro zabránění vstupu neoprávněným osobám;

c) zachovávání záznamu o oprávněných příjemcích dat;

d) ověření kompletnosti vstupních dat, zda bylo zpracování řádně ukončeno a bylo provedeno odsouhlasení výsledků;

e) ochrana tiskových dat, čekajících na výstup, na úrovni odpovídající jejich citlivosti;

f) ukládání médií způsobem odpovídajícím specifikacím výrobce;

g) udržování nutnosti distribuce dat na minimální úrovni;

h) zřetelné označování všech kopií dat pro všechny autorizované příjemce;

i) kontrola rozdělovníku a seznamu autorizovaných příjemců v pravidelných intervalech.

Další informace

Výše uvedené postupy jsou použitelné v dokumentech, počítačových systémech, sítích, přenosných počítačích, mobilní sdělovací technice, poště, hlasové poště, hlasové komunikaci obecně, v multimédiích, v poštovním styku, při použití faxů a při používání dalších citlivých médií, například čistých bankovních šeků a faktur.

10.7.4 Bezpečnost systémové dokumentace

Opatření

Systémová dokumentace by měla být chráněna proti neoprávněnému přístupu.

Doporučení k realizaci

Pro ochranu systémové dokumentace před neoprávněným přístupem by mělo být zváženo následující:

a) systémová dokumentace by měla být bezpečně uložena;

b) seznam oprávněných osob pro přístup k systémové dokumentaci by měl být omezen na minimum a měl by být autorizován vlastníkem aplikace;

c) systémová dokumentace, která je uložena na veřejné síti nebo je jejím prostřednictvím poskytována, by měla být odpovídajícím způsobem chráněna.

Další informace

Systémová dokumentace může obsahovat řadu citlivých informací, například popisy aplikačních procesů, procedur, datových struktur, autorizačních procesů.

10.8 Výměny informací

Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.

Výměna informací a programů mezi organizacemi by měla být založena na formální politice, prováděna v souladu s platnými dohodami a měla by být ve shodě s platnou legislativou (viz kapitola 15).

Měly by být stanoveny postupy a normy pro ochranu informací a jejich nosičů při přepravě.

10.8.1 Postupy při výměně informací a programů

Opatření

Měly by být ustaveny a do praxe zavedeny formální postupy, politiky a opatření na ochranu informací při jejich výměně pro všechny typy používaných komunikačních zařízení.

Doporučení k realizaci

Při vytváření postupů a zavádění opatření pro výměnu informací by mělo být zváženo následující:

a) postupy určené na ochranu informací před jejich zachycením, odposlouchávám, zkopírováním, modifikací, špatným směrováním a zničením;

b) postupy detekce a ochrany před škodlivými kódy, které mohou být přenášeny elektronickou poštou (viz také 10.4:1);

c) postupy na ochranu citlivých informací přenášených v přílohách elektronické pošty;

d) politika a směrnice upravující použití zařízení pro elektronickou komunikaci (viz 7.1.3);

e) postupy pro použití bezdrátové komunikace s ohledem na související specifická rizika;

f) odpovědnost zaměstnanců, smluvních a třetích stran za to, že nezkompromitují organizaci, například odesláním hanlivých zpráv, použitím elektronické pošty k obtěžování či neautorizovaným nákupům, atd.;

g) použití kryptografických technik pro zajištění důvěrnosti, integrity a autentičnosti přenášených informací (viz 12.3);

h) vytvoření pravidel pro uchování a likvidace veškeré obchodní korespondence, včetně elektronické pošty v souladu s místní legislativou a předpisy;

i) nenechávat citlivé a kritické informace volně ležet v tiskárnách, kopírkách a faxech, kde mohou být přístupné neautorizovaným osobám;

j) zavedení opatření a omezení souvisejících s přesměrováním elektronické komunikace, např. automatické přeposílání elektronické pošty na externí emailovou adresu;

k) připomínání zaměstnancům, že mají dodržovat adekvátní opatrnost, například neprobírat citlivé informace, které by mohly být při telefonování zaslechnuty či odposlechnuty:

1. osobami v bezprostřední blízkosti, zejména při použití mobilního telefonu;

2. instalovaným odposlechem nebo jinou formou elektronického odposlouchávání umožněného fyzickým přístupem k telefonnímu přístroji nebo telefonní lince nebo použitím prohledávacích přijímačů při použití analogových mobilních nebo bezdrátových telefonů;

3. dalšími osobami na druhé straně telefonu;

l) nenechávat zprávy na záznamníku, protože tyto zprávy mohou být přehrány neautorizovanou osobou, uloženy do veřejné sítě nebo uloženy jako výsledek chybného telefonátu;

m) upozorňování zaměstnanců na problémy spojené s použitím faxů, zejména:

1. neautorizovaný přístup k vnitřním pamětem pro uchování faxových zpráv s cílem jejich opětovného vyvolání;

2. úmyslné nebo náhodné přeprogramování faxu tak, aby posílal zprávy na specifická čísla;

3. posílání dokumentů a zpráv na špatné místo z důvodu překlepu v čísle nebo použitím špatného čísla z paměti přístroje;

n) upozorňování zaměstnanců na to, aby při registraci programového vybavení nezadávali své osobní údaje (např. emailová adresa), které pak mohou být použity neoprávněným způsobem;

o) upozorňování zaměstnanců na to, že moderní faxová zařízení a kopírky používají vyrovnávací paměť, ve které je uložen obsah tištěných stránek, pro případ, že v zásobníku dojde papír nebo nastane chyba při přenosu dat.

Zaměstnanci by dále měli být upozorněni na to, aby nevedli důvěrnou konverzaci na veřejnosti, v otevřené kanceláři a na místech, kde jsou tenké zdi.

Zařízení použitá pro výměnu informací by měla splňovat požadavky relevantní legislativy (viz kapitola 15).

Další informace

Výměna informací může probíhat s použitím celé řady různých typů komunikačních zařízení, zahrnujících elektronickou poštu, hlasová zařízení, fax a video.

Výměna programů může probíhat za použití různých počítačových médií, stáhnutím programů z internetu a nebo jejich nákupem od oficiálního prodejce.

Měly by být zváženy provozní a bezpečnostní dopady v souvislosti s elektronickou výměnou dat (EDI), elektronickým obchodem a elektronickou poštou a společně s požadavky na bezpečnostní opatření.

Informace mohou být ohroženy díky nedostatku bezpečnostního povědomí, neznalosti pravidel a postupů používání odpovídající techniky, například zaslechnutí obsahu hovoru vedeného pomocí mobilního telefonu na veřejných místech, zaslechnutí obsahu zprávy na telefonním záznamníku nebo fax zaslaný omylem nesprávné osobě.

Aktivity organizace mohou být přerušeny a informace ohroženy při chybách komunikačních prostředků, jejich přetížení nebo rušení (viz 10.3 a kapitola 14). Informace mohou být také ohroženy v případě, že jsou tyto prostředky přístupné neoprávněným uživatelům (viz kapitola 11).

10.8.2 Dohody o výměně informací a programů

Opatření

Výměna informací a programů by měla být založena na dohodách uzavřených mezi organizací a externími subjekty.

Doporučení k realizaci

V dohodách o výměně informací a programů by měly být zváženy následující bezpečnostní hlediska:

a) odpovědnosti vedoucích zaměstnanců týkající se kontroly a potvrzení oznámení

o přenosu, odeslání a přijetí;
b) postupy pro oznámení odesílateli (přenos, odeslání a přijetí);
c) postupy pro zajištění nepopiratelnosti doručení;
d) minimální technické normy pro balení a přepravu;
e) dohody o uložení zdrojových kódů programů a informací u nezávislé třetí strany;
f) pravidla pro identifikaci kurýra;
g) odpovědnosti a povinnosti v bezpečnostního incidentu, například v případě ztráty dat;
h) použití schváleného systému označování citlivých a kritických informací, zaručujícího okamžité pochopení smyslu označení a toho, že informace je odpovídajícím způsobem chráněna;
i) vlastnictví dat a programového vybavení a odpovědnosti za ochranu osobních údajů, dodržování autorských práv a další podobné otázky (viz 15.1.2 a 15.1.4);
j) technické normy pro nahrávání a čtení informací a programů;
k) jakákoliv zvláštní opatření pro ochranu citlivých předmětů, jako jsou například šifrovací klíče (viz 12.3).

Měly by být vytvořeny a do praxe zavedeny politiky, směrnice a standardy na ochranu informací a médií při přepravě (viz také 10.8.3) a měly by být odkazovány v uzavřených dohodách. Bezpečnostní část těchto dohod by měla odrážet citlivost všech vyměňovaných informací organizace.

Další informace

Výměna informací a programů (elektronická i manuální) mezi organizacemi by měla být založena na dohodách, z nichž některé mohou mít podobu formálních smluv nebo mohou být součástí podmínek pracovního vztahu. Postup výměny citlivých informací by měl být pro všechny zúčastněné organizace a uzavřené dohody nastaven stejně.

10.8.3 Bezpečnost médií při přepravě

Opatření

Média obsahující informace by měla být během přepravy mimo organizaci chráněna proti neoprávněného přístupu, zneužití nebo narušení.

Doporučení k realizaci

Aby byla zajištěna ochrana počítačových médií během jejich přepravy mezi lokalitami, měla by být aplikována následující opatření:
a) použití spolehlivé dopravy nebo spolehlivých kurýrů;
b) seznam oprávněných kurýrů by mělo schválit vedení organizace;
c) obal by měl být dostatečný, aby chránil obsah před jakýmkoliv fyzickým poškozením, které by mohlo vzniknout během přepravy, a měl by být v souladu se specifikacemi výrobce. Například ochrana proti vlivům okolí jako jsou horko, vlhko nebo elektromagnetické pole, které mohou snížit účinnost obnovy uložených informací;
d) v případě potřeby by měla být přijata zvláštní opatření pro ochranu citlivých informací před neoprávněným prozrazením nebo modifikací. Například:
1. používání uzamykatelné přepravní skříňky;
2. osobní doručování;
3. balení odolné proti vniknutí (které umožňuje odhalit jakýkoliv pokus o získání přístupu);
4. ve výjimečných případech rozdělení zásilky do více dílčích zásilek a odeslání různými cestami.

Další informace

Informace mohou být během přepravy zranitelné ze strany neoprávněného přístupu, zneužití nebo narušení, například při zasílání médií poštou nebo kurýrem.

10.8.4 Elektronické zasílání zpráv

Opatření

Elektronicky přenášené informace by měly být vhodným způsobem chráněny.

Doporučení k realizaci

Při návrhu opatření na ochranu elektronické komunikace by mělo být zváženo následující:
a) ochrana informací proti neoprávněnému přístupu, modifikaci nebo odmítnutí služby;
b) zajištění správného přenosu a adresování zpráv;
c) celková spolehlivost a dostupnost služeb;
d) zákonné požadavky, například požadavky na elektronický podpis;
e) získání souhlasu používat externí veřejné služby jako je například okamžité odesílání zpráv (instant messaging) nebo sdílení souborů;
f) silnější úroveň kontroly oprávněnosti vzdálených přístupů uživatelů.

Další informace

Elektronické komunikace jako elektronická pošta (email), elektronická výměna dat (EDI) a okamžitý odesílatel zpráv (instant messenger) jsou důležitou součástí obchodní komunikace. Elektronická komunikace je vystavena jinému okruhu bezpečnostních rizik než tradiční výměna informací v papírové podobě.

10.8.5 Podnikové informační systémy

Opatření

Na ochranu informací v propojených podnikových informačních systémech by měla být vytvořena a do praxe zavedena politika a odpovídající směrnice.

Doporučení k realizaci

Pozornost, věnovaná bezpečnosti a dopadům na provozní činnosti vyplývající z propojení systémů, by měla zahrnovat:
a) známé zranitelnosti administrativních a účetních systémů tam, kde jsou informace sdíleny mezi jednotlivými částmi organizace;
b) zranitelnost informací v podnikových komunikačních systémech, například zaznamenávání telefonních nebo konferenčních hovorů, důvěrnost hovorů, uchovávání faxů, otevírání pošty, distribuce pošty;

c) politika a vhodná opatření pro správu sdílených informací;
d) vyjmutí citlivých informací a dokumentů podléhajících utajení v případě, že systém nemá odpovídající úroveň ochrany (viz 5.2);
e) omezení přístupu k časovým plánům vybraných osob, například těch, které pracují na citlivých projektech;
f) skupiny zaměstnanců a smluvních nebo obchodních partnerů, které mohou systém používat, a lokality, z nichž je povolen přístup k systému (viz 6.2 a 6.3);
g) omezení určitých zařízení pro vybrané kategorie uživatelů;
h) identifikaci statutu uživatele, například seznamy zaměstnanců organizace a smluvních partnerů v adresáři využívaném dalšími uživateli;
i) zálohování informací uložených v systému a uchovávání záloh (viz 10.5.1);
j) požadavky na náhradní provoz a prostředky pro jeho zajištění (viz 14).

Další informace

Elektronické kancelářské systémy poskytují příležitosti pro rychlejší šíření a sdílení informací organizace za použití kombinace dokumentů, počítačů, přenosných počítačů, mobilní komunikace, pošty, hlasové pošty, hlasové komunikace obecně, multimédií, poštovních služeb a faxů.

10.9 Služby elektronického obchodu

Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.

Měly by být zváženy bezpečnostní dopady a požadavky na opatření spojené s použitím služeb podporujících elektronický obchod, včetně on-line transakcí. Pozornost by měla být věnována ochraně integrity a dostupnosti elektronicky publikovaných informací na veřejně přístupných systémech.

10.9.1 Elektronický obchod

Opatření

Informace přenášené ve veřejných sítích v rámci elektronického obchodování by měly být chráněny před podvodnými aktivitami, před zpochybňováním smluv, prozrazením či modifikací.

Doporučení k realizaci

Úvahy o bezpečnosti elektronického obchodu by měly zahrnovat následující:
a) úroveň důvěry v proklamovanou identitu (např. formou autentizace) druhé strany, kterou každá ze stran (zákazník a obchodník) požaduje;
b) proces autorizace pro nastavení cen, vydávání nebo podepisování důležité obchodní dokumentace;
c) zajištění toho, aby obchodní partneři byli dostatečně informováni o svých oprávněních;
d) stanovení a naplnění požadavků na důvěrnost, integritu a průkaznost odeslání a přijetí klíčových dokumentů a na nepopíratelnost odpovědnosti za smlouvy, např. v rámci výběrových řízení a smluvních procesů;
e) úroveň vyžadované důvěry v integritu zveřejněných ceníků;
f) důvěrnost jakýchkoliv citlivých dat a informací;
g) důvěrnost a integrita informací představujících objednávku, informací o plátci a adresátovi a potvrzení příjmu;
h) odpovídající stupeň kontroly pro ověření informací o platbě od zákazníka;
i) výběr nejvhodnějšího způsobu platby zamezujícího podvodu;
j) úroveň ochrany vyžadované pro zaručení důvěrnosti a integrity informací objednávky;
k) prevence proti ztrátě nebo duplikaci transakcí;
l) odpovědnost za podvodné transakce;
m) požadavky na pojištění.

Mnohé z předcházejícího může vyřešit použití kryptografických technik, popsaných v 12.3, při zvážení souladu se zákonnými požadavky (viz 15.1, a zvlášť 15.1.6 pro kryptografickou legislativu).

Dohody o elektronickém obchodování mezi obchodními partnery by měly být podepřeny písemnou smlouvou, v níž se obě strany zavazují k dohodnutým obchodním podmínkám, včetně detailů autorizace (viz předcházející b)). Mohou být potřebné i další dohody s poskytovateli informačních a síťových služeb.

Veřejné obchodní systémy by měly publikovat své obchodní podmínky pro zákazníky.

Pozornost by měla být věnována odolnosti proti útokům na hostitelský systém používaný pro elektronický obchod a bezpečnostním dopadům síťových propojení, nutných pro jeho implementaci (viz 11.4.6).

Další informace

Elektronický obchod je zranitelný ze strany velkého počtu síťových hrozeb, což může mít za následek výskyt podvodných aktivit, námitky vůči podmínkám smluv a prozrazení či modifikaci informací.

Pro účely elektronického obchodu může být využito řady autentizačních metod, např. používání veřejných šifrovacích klíčů a digitálních podpisů (viz také 12.3) na snížení rizika. Pro tyto účely může být využito služeb důvěryhodných třetích stran.

10.9.2 On-line transakce

Opatření

Měla by být zajištěna ochrana informací přenášených při on-line transakcích tak, aby byl zajištěn úplný přenos informací a zamezilo se špatnému směrování, neoprávněné změně zpráv, neoprávněnému prozrazení, neoprávněné duplikaci nebo opakování zpráv.

Doporučení k realizaci

Pro zabezpečení on-line transakcí by mělo být zváženo následující:
a) použití elektronického podpisu všemi účastníky transakce;
b) všechny aspekty související s transakcí, zajištění toho, že:
1. jsou prověřena platnost oprávnění všech zúčastněných stran;
2. transakce bude důvěrná;

3. bude chráněno soukromí všech zúčastněných stran;
c) šifrování komunikace mezi zúčastněnými stranami;
d) zabezpečení protokolů použitých pro komunikaci;
e) zajištění toho, aby úložiště detailních informací o transakcích nebylo veřejně přístupné, např. v intranetu organizace. Informace by neměly být uchovávány tak, aby byly volně přístupné z internetu;
f) tam kde je použito služeb důvěryhodné autority (např. pro účely vystavení a udržování digitálních podpisů a/nebo certifikátů) je bezpečnost součástí celého procesu správy certifikátu/podpisu.
Další informace
Rozsah přijatých opatření by měl být úměrný velikosti rizik spojených s každým typem on-line transakce.
Provedené transakce by měly odpovídat zákonům, pravidlům a omezením podle jurisdikce, ve které je transakce zahájena, skrze kterou probíhá a kde je ukončena a nebo informace o ní uloženy.
Existuje řada různých transakcí, které mohou být prováděny online, např. finanční transakce.

10.9.3 Veřejně přístupné informace

Opatření
Informace publikované na veřejně přístupných systémech by měly být chráněny proti neoprávněné modifikaci.
Doporučení k realizaci
Programy, data a jiné informace zpřístupňované na veřejně dostupných systémech a vyžadující vysoký stupeň integrity by měly být chráněny adekvátními mechanizmy, jako například digitálním podpisem (viz 12.3). Veřejně přístupné systémy by měly být, předtím než jsou na ně umístěny informace, testovány na slabiny a možná selhání.
Pro zveřejnění informací by měly existovat formální schvalovací procesy. Veškeré vstupy poskytnuté zvenčí by měly být prověřeny a projít schválením.
Elektronické publikační prostředky a systémy, zejména ty, které umožňují zpětnou vazbu a přímý vstup informací, by měly být pečlivě kontrolovány, aby:
a) získávání informací bylo plně v souladu s legislativou (viz 15.1.4);
b) vstup a zpracování informací v systému proběhlo úplně a korektně a v daném časovém rámci;
c) citlivé informace byly v průběhu sběru, zpracování a ukládání ochráněny;
d) přístup k veřejně přístupným prostředkům neumožnil nechtěný přístup i k dalším sítím, které jsou k těmto prostředkům připojeny.
Další informace
Informace na veřejně přístupných systémech, například informace na webových serverech přístupné prostřednictvím Internetu, by měly odpovídat zákonům, pravidlům a omezením podle jurisdikce, ve které je systém umístěn nebo kde je realizován obchod. Neoprávněná modifikace publikovaných informací může vážně poškodit dobrou pověst organizace.

10.10 Monitorování

Cíl: Detekovat neoprávněné zpracování informací.
Systémy by měly být monitorovány a bezpečnostní události zaznamenávány. Pro zajištění včasné identifikace problémů informačních systémů by měl být používán operátorský deník a záznamy předchozích selhání.
Veškeré aktivity související s monitorováním a zaznamenáváním událostí by měly být v souladu s relevantními zákonnými požadavky.
Monitorování systému umožňuje kontrolování účinnosti přijatých opatření a ověření souladu s modelem politiky řízení přístupu.

10.10.1 Zaznamenávání událostí

Opatření
Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, by měly být pořizovány a uchovány po stanovené období tak, aby byly se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu.
Doporučení k realizaci
Auditní záznamy by měly také obsahovat:
a) identifikátory uživatelů (uživatelská ID);
b) datum, čas a podrobnosti klíčových událostí, např. přihlášení a odhlášení;
c) identifikátor terminálu nebo místa, pokud je to možné;
d) záznam o úspěšných a odmítnutých pokusech o přístup k systému;
e) záznam o úspěšných a odmítnutých pokusech o přístup k datům a jiným zdrojům;
f) změny konfigurace systému;
g) použití oprávnění;
h) použití systémových nástrojů a aplikací;
i) soubory, ke kterým bylo přistupováno a typ přístupu;
j) sítě, ke kterým bylo přistupováno a použité protokoly;
k) alarmy vyvolané systémy pro kontrolu přístupy;
l) aktivaci a deaktivaci ochranných systémů, jako jsou antivirové systémy a systémy pro detekci průniku.
Další informace
Auditní záznamy mohou obsahovat důvěrné osobní údaje. Měla by být přijata vhodná opatřená na jejich ochranu (viz také 15.1.4). Pokud je to možné, neměli by systémoví administrátoři mít oprávnění mazat záznamy a nebo deaktivovat vytváření záznamů o své vlastní činnosti (viz 10.1.3).

10.10.2 Monitorování používání systému

Opatření

Měla by být stanovena pravidla pro monitorování použití zařízení pro zpracování informací, výsledky těchto monitorování by měly být pravidelně přezkoumávány.

Doporučení k realizaci

Požadovaná úroveň monitorování jednotlivých prostředků by měla být stanovena na základě hodnocení rizik. Veškeré aktivity související s monitorováním událostí by měly být v souladu s relevantními zákonnými požadavky.

Oblasti, které by se měly vzít v úvahu, jsou následující:

a) neautorizovaný přístup, včetně informací jako:

1. uživatelské ID;
2. datum a čas klíčových událostí;
3. druh událostí;
4. soubory, ke kterým bylo přistupováno;
5. použité programy/nástroje;

b) všechny privilegované operace, jako:

1. použití privilegovaných účtů, např. účtu supervisora, administrátora;
2. spuštění a ukončení systému;
3. připojení a odpojení vstupně/výstupních zařízení;

c) pokusy o neoprávněný přístup, jako:

1. neúspěšné nebo odmítnuté aktivity uživatelů;
2. neúspěšné nebo odmítnuté pokusy o přístup k datům nebo jiným zdrojům;
3. narušení přístupové politiky a upozornění od síťových bran a firewallů;
4. varování speciálních systémů pro detekci průniků;

d) systémová varování nebo chyby, jako:

1. zprávy nebo varování z konzole;
2. výjimky v systémových záznamech;
3. alarmy správy sítě;
4. alarmy spuštěné systémy pro kontrolu přístupu;

e) změny nebo pokusy o změnu bezpečnostních opatření nastavení bezpečnosti systému.

Výstupy monitorování by měly být pravidelně kontrolovány. Frekvence kontrol by měla záviset na zjištěných rizicích. Měly by být zváženy následující rizikové faktory:

a) kritičnost aplikačních procesů;

b) hodnota, citlivost nebo kritičnost ovlivněných informací;

c) minulé zkušenosti s průnikem do systému a jeho zneužitím a frekvence s jakou jsou zneužívány existující zranitelnosti systému;

d) stupeň propojení systémů (zejména veřejné sítě);

e) deaktivace zařízení pro zaznamenávání událostí.

10.10.3 Ochrana vytvořených záznamů

Opatření

Zařízení pro zaznamenávání informací a vytvořené záznamy by měly být vhodným způsobem chráněny proti neoprávněnému přístupu a zfalšování.

Doporučení k realizaci

Opatření by se měla zaměřovat na ochranu proti neautorizovaným změnám a provozním problémům, včetně:

a) úpravy zaznamenávaných druhů zpráv;

b) editování nebo mazání záznamů;

c) nedostatečné kapacity médií pro záznamy a následné nezaznamenávání nebo přepisování předchozích událostí.

Další informace

Systémové záznamy často obsahují velké množství informací, z nichž většina nesouvisí s bezpečnostním monitorováním. Při identifikaci důležitých událostí pro účely sledování bezpečnosti by měla být zvážena možnost automatického kopírování vhodných typů zpráv do druhého protokolu a/nebo použití vhodných systémových programů nebo nástrojů auditu k vyšetřování souborů.

Systémové záznamy musí být dostatečně chráněny, protože data, která mohou být modifikována nebo vymazána mohou vytvořit falešný pocit bezpečí.

10.10.4 Administrátorský a operátorský deník

Opatření

Aktivity správce systému a systémového operátora by měly být zaznamenávány.

Doporučení k realizaci

Záznamy by měly obsahovat:

a) čas kdy došlo k události (úspěšné i neúspěšné pokusy);

b) podrobnosti o události (např. seznam použitých souborů) nebo o chybách (např. jaké chyby se objevily a jakým způsobem byly odstraněny);

c) jaký účet byl použit, který správce nebo operátor ho použil;

d) dotčené procesy.

Administrátorský a operátorský deník by měly být v pravidelných intervalech přezkoumávány.

Další informace

Pro monitorování systémových a síťových aktivit správců je možné použít externě spravovaný systém pro detekci průniku.

10.10.5 Záznam selhání

Opatření

Měly by být zaznamenány a analyzovány chyby a provedena opatření k nápravě.

Doporučení k realizaci

Hlášení uživatelů o problémech systému pro zpracování nebo výměnu informací by měla být zaznamenána. Měla by existovat jasná pravidla pro zacházení s nahlášenými chybami,

zahrnující:
a) přezkoumání záznamů chyb k zajištění jejich uspokojivého řešení;
b) přezkoumání opatření k nápravě, zajišťujících, aby bezpečnostní opatření nebyly zneužity a prováděné činnosti byly schváleny.
Mělo by být zajištěno zaznamenávání selhání (porucha), pokud to systém umožňuje.
Další informace
Zaznamenávání selhání (poruch) a chyb může ovlivnit výkon systému. Zaznamenávání selhání a chyb by mělo být umožněno pouze kompetentním personálu, rozsah zaznamenávání byl měl být pro každý jednotlivý systém nastaven na základě hodnocení rizik.

10.10.6 Synchronizace času

Opatření
Hodiny všech důležitých systémů pro zpracování informací by měly být v rámci organizace nebo domény synchronizovány se schváleným zdrojem přesného času.
Doporučení k realizaci
V případě, že počítačová nebo komunikační zařízení používají hodiny s reálným časem, měly by být nastaveny na smluvený standard, například greenwichský nebo místní čas. Protože některé hodiny se předcházejí nebo zpožďují, měly by existovat postupy, které kontrolují a korigují všechny významnější změny.
Z hlediska správného určení reálného vzniku časové značky je důležitá správná interpretace formátu datum/čas. V úvahu by také měla být vzata místní specifika (např. letní čas).
Další informace
Správné nastavení počítačových hodin je důležité pro zajištění přesnosti auditních záznamů, které mohou být potřebné pro vyšetřování nebo jako důkaz při soudních či disciplinárních řízeních. Nepřesné auditní záznamy mohou takové vyšetřování brzdit nebo mohou narušit důvěryhodnost takového důkazu. Pro nastavení přesného času primárního serveru může být například využit GPS signál nebo radiový signál z atomových hodin. Pro automatickou synchronizaci času všech ostatních klientů s primárním serverem lze použít protokol NTP (Network Time Protocol).

11 Řízení přístupu

11.1 Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.
Přístup k informacím, zařízením pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků.
V úvahu by se měla brát pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

11.1.1 Politika řízení přístupu

Opatření
Měla by být vytvořena, dokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.
Doporučení k realizaci
Přístupová pravidla a oprávnění by měla být jasně stanovena pro každého uživatele nebo skupinu uživatelů v seznamu pravidel přístupu. Pravidla by měla pokrývat jak logický, tak fyzický přístup (viz kapitola 9), oba typy přístupů by měly být řešeny současně. Uživatelům a poskytovatelům služeb by mělo být předáno jasné vyjádření o provozních požadavcích, jež naplňuje řízení přístupu.
Politika řízení přístupu by měla brát v úvahu následující hlediska:
a) bezpečnostní požadavky jednotlivých aplikací organizace;
b) identifikace všech informací ve vztahu k jednotlivým aplikacím a rizika, kterým jsou informace vystaveny
c) pravidla pro šíření informací a pravidla schvalování, tj. princip oprávněné potřeby znát, bezpečnostní úrovně a klasifikaci informací (viz 7.2);
d) konzistence přístupových pravidel a klasifikace informací pro různé systémy a sítě;
e) odpovídající legislativa a ostatní smluvní závazky ve vztahu k ochraně přístupu k datům nebo službám (viz kapitola 15.1);
f) standardní přístupové profily uživatelů pro běžné kategorie činností;
g) řízení přístupových pravidel v distribuovaném a síťovém prostředí rozeznávajícím všechny možné typy připojení;
h) oddělení jednotlivých rolí pro řízení přístupu, např. vyřizování požadavků na přístup, schvalování přístupu, správa přístupů;
i) požadavky na formální schválení žádostí o přístup (viz 11.2.1);
j) požadavky na pravidelné přezkoumání přístupových práv (viz 11.2.4);
k) odebrání přístupových práv (viz 8.3.3).
Další informace
Při stanovování pravidel řízení přístupu by měla být zvážena následující hlediska:
a) rozlišení mezi pravidly, která musí být v platnosti vždy, a těmi, která jsou nepovinná nebo podmíněná;
b) stanovit pravidla na základě principu „Všechno, co není výslovně povoleno, je zakázáno“, ne na základě měkčího pravidla „Všechno, co není výslovně zakázáno, je povoleno“;
c) změny ve značení informací (viz 7.2), které jsou vyvolány automaticky zařízeními pro zpracování informací, a změny, které jsou vyvolány z rozhodnutí uživatele;
d) změny uživatelských oprávnění, které jsou vyvolány automaticky zařízením pro zpracování informací, a ty, které jsou vyvolány administrátorem;
e) pravidla, která vyžadují schválení administrátorem nebo jinou pověřenou osobou, a ta, která toto nevyžadují.
Pravidla pro řízení přístupu by měla být podporována zavedením formálních postupů a jasně určených odpovědností (viz například 6.1.3, 11.3, 11.4.1, 11.6).

11.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.

Měly by existovat formální postupy pro přidělování uživatelských práv k informačním systémům a službám.

Postupy by měly pokrývat všechny fáze životního cyklu přístupu uživatele, od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele, který přístup k informačním systémům a službám již dále nepotřebuje. V případě nutnosti by měla být věnována zvláštní pozornost potřebě řídit přidělování privilegovaných přístupových oprávnění, která umožňují uživatelům překonat kontroly v systému.

11.2.1 Registrace uživatele

Opatření

Měl by existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.

Doporučení k realizaci

Postup pro registraci a uživatele a jejího zrušení by měl zahrnovat:

a) použití unikátního uživatelského identifikátoru (ID), aby bylo možné propojit uživatele s jím provedenými akcemi, a zajistit tak jejich odpovědnost. Použití skupinového ID by mělo být povoleno pouze tam, kde to je nezbytné pro určitou práci, použití by mělo být chváleno a dokumentováno;

b) kontrolu toho, že uživatel má oprávnění používat informační systém nebo služby od vlastníka systému. Vhodný může být také zvláštní souhlas s přístupovými právy od nadřízených uživatele;

c) kontrolu toho, že úroveň přiděleného přístupu odpovídá záměrům organizace (viz 11.1) a je shodná s bezpečnostní politikou organizace, například není v rozporu s principem oddělení povinností (viz 10.1.3);

d) předání dokumentu vymezujícího přístupová práva jednotlivým uživatelům;

e) požadavek na uživatele, aby podepsali prohlášení, že rozumí podmínkám přístupu;

f) zajištění toho, aby poskytovatelé služeb neumožnili přístup, dokud nebude proces autorizace dokončen;

g) udržování formálního záznamu o všech registrovaných osobách oprávněných využívat službu;

h) ihned odebrat přístupová práva uživatelům, kteří změnili pracovní místo nebo opustili organizaci;

i) pravidelně kontrolovat a odstranit již dále nepotřebné ID uživatelů a jejich účty (11.2.4);

j) zajistit, aby již nepotřebné ID uživatelů nebyly přiděleny jiným uživatelům.

Další informace

Mělo by být zváženo zavedení přístupových rolí uživatelů dle konkrétních požadavků organizace, které by zahrnovalo vždy několik přístupových práv do typických uživatelských profilů. Požadavky na přístup a přezkoumání jejich oprávněnosti (viz 11.2.4) se lépe zpracovávají na úrovni uživatelských rolí než pro jednotlivá přístupová práva.

Mělo by být zváženo začlenění klauzule specifikující sankce za pokus o neautorizovaný přístup zaměstnanců nebo servisního personálu do jejich pracovních smluv a servisních kontraktů (viz také 6.1.5, 8.1.3 a 8.2.3).

11.2.2 Řízení privilegovaného přístupu

Opatření

Přidělování a používání privilegií by mělo být omezeno a řízeno.

Doporučení k realizaci

Ve víceuživatelských systémech, u nichž je nutná ochrana proti neautorizovanému přístupu, by mělo být přidělování privilegovaných oprávnění řízeno prostřednictvím formálního autorizačního procesu. Měly by být zváženy následující kroky:

a) měla by být popsána privilegia spojená s každým prvkem systému (například s operačním nebo databázovým systémem a všemi aplikacemi) a kategorie zaměstnanců, kterým by měla být přidělena;

b) privilegia by měla být přidělována jednotlivcům na základě jejich oprávněné potřeby pro použití a případ od případu a v souladu s politikou řízení přístupu (viz 11.1.1), například požadavek na minimalizaci jejich provozní role určené podle potřeby;

c) měl by být dodržován proces autorizace a zachováván záznam všech přidělených privilegií. Privilegia by neměla být přidělena, dokud není proces autorizace dokončen;

d) měl by být podporován vývoj a používání takových systémových rutin, které by omezovaly nutnost přidělovat privilegia uživatelům;

e) měl by být podporován vývoj a používání takových programů, které by vyžadovaly oprávnění ke svému spuštění;

f) privilegia by měla být přidělena jiným uživatelským ID než těm, které jsou používány pro běžnou práci.

Další informace

Nepatřičné použití systémových privilegií (určité funkce nebo prostředky, dávající uživateli možnost překonat systémové nebo aplikační kontroly) je často hlavním spolupůsobícím faktorem selhání systémů.

11.2.3 Správa uživatelských hesel

Opatření

Přidělování hesel by mělo být řízeno formálním procesem.

Doporučení k realizaci

Proces by měl vyhovovat následujícím požadavkům:

a) vyžadovat od uživatelů podpis prohlášení, že se zavazují k držení svých hesel v tajnosti a k zachování hesel pracovní skupiny pouze mezi jejími členy (to může být začleněno

v pracovních podmínkách, viz 8.1.3);
b) zajistit, aby v případě, že si uživatelé sami mění své heslo (viz 11.3.1), dostali na počátku bezpečné jednorázové heslo, které jsou nuceni ihned po přihlášení změnit;
c) zavést postupy jednoznačné identifikace uživatelů předtím než jim je poskytnuto nové, náhradní a nebo dočasné heslo;
d) dočasně přidělená hesla by měla být jedinečná a neměla by být lehce uhodnutelná;
e) uživatelé by měli potvrdit přijetí hesel;
f) hesla by nikdy neměla být v počítači uložena v nechráněné podobě;
g) dodavateli přednastavená hesla by měly být ihned po instalaci systému nebo aplikačního programového vybavení změněna;
Další informace
Hesla jsou běžným prostředkem pro ověření identity uživatele předtím, než je mu umožněn přístup do systému nebo ke službě s ohledem na jeho oprávnění. Pokud je to vhodné, mělo by být zváženo použití i jiných technologií autentizace a identifikace uživatele, jako je biometrie, například ověření otisku prstu, podpisu a použití technických prostředků, například čipových karet.

11.2.4 Přezkoumání přístupových práv uživatelů

Opatření
Vedení organizace by mělo v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.
Doporučení k realizaci
Přezkoumání přístupových práv uživatelů by mělo zaručovat, že:
a) přístupová práva uživatelů jsou přezkoumávána v pravidelných intervalech (doporučuje se interval 6 měsíců) a po každé změně, jako například povýšení, přeložení na nižší pozici nebo ukončení pracovního poměru (viz 11.2.1);
b) při přeřazení na jinou pracovní pozici v rámci organizace by měla být stávající přístupová práva přezkoumána;
c) autorizace speciálních privilegovaných oprávnění (viz 11.2.2) jsou přezkoumávána v kratších intervalech, doporučuje se interval 3 měsíců;
d) přidělená privilegovaná oprávnění by měla být přezkoumávána v pravidelných intervalech, aby bylo zajištěno, že nedošlo k získání neoprávněného privilegia;
e) změny u privilegovaných účtů by měly být zaznamenány pro potřeby pravidelných přezkoumání.
Další informace
Pro udržení účinného řízení přístupu k datům a informačním službám by mělo vedení organizace v pravidelných intervalech provádět kontrolu přístupových práv uživatelů.

11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a prostředků pro zpracování informací.
Pro účinné zabezpečení je nezbytná spolupráce oprávněných uživatelů.
Uživatelé by si měli být vědomi odpovědnosti za dodržování účinných opatření kontroly přístupu, zejména s ohledem na používání hesel, a bezpečnosti jim přidělených prostředků.
Pro snížení rizika neoprávněného přístupu (nebo poškození) k dokumentům, médiím a prostředkům pro zpracování informací, by měla být zavedena zásada prázdného stolu a prázdné obrazovky monitoru.

11.3.1 Používání hesel

Opatření
Při výběru a používání hesel by mělo být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy.
Doporučení k realizaci
Všichni uživatelé by měli být obeznámeni s tím, že:
a) hesla se udržují v tajnosti;
b) hesla nesmí být zaznamenána (např. na papíře, v souborech nebo v přenosných zařízeních), s výjimkou jejich bezpečného uložení a když byl způsob jejich uložení schválen;
c) hesla se musí změnit v případě jakéhokoliv náznaku možného kompromitování systému nebo hesla;
d) heslo by mělo být kvalitní, mělo by mít minimální délku šest znaků, a to tak, aby:
1.bylo dobře zapamatovatelné;
2. nebylo založeno na informacích vztahujících se k osobě, které by mohl kdokoliv další lehce uhodnout nebo získat, například jména, telefonní čísla, data narození apod.;
3. nebylo zranitelné při použití slovníkových útoků (nemělo by se skládat ze slov vyskytujících se ve slovnících);
4. neobsahovalo po sobě jdoucí stejné znaky a neobsahovalo pouze číselné nebo pouze písmenné skupiny.
e) musí měnit hesla v pravidelných intervalech nebo na základě počtu přihlášení (hesla pro privilegovaný přístup by se měla měnit častěji než normální hesla) a vyhýbat se opakovanému použití nebo opakování starých hesel;
f) musí změnit dočasná hesla při prvním přihlášení;
g) nebudou zahrnovat hesla do žádného automatizovaného přihlašovacího procesu, například uložení do makra nebo funkční klávesy;
h) nebudou sdílet osobní uživatelská hesla;
i) nebudou používat stejná hesla pro soukromé a pracovní účely.
Jestliže uživatelé potřebují, aby měli přístup k více službám nebo platformám, a musí udržovat více hesel, může jim být doporučeno používat jedno silné heslo (viz d) pro všechny služby u

kterých si jsou jisti, že poskytují rozumnou úroveň zabezpečení uložených hesel.
Další informace
Zvláštní péče by také měla být věnována help desku, který řeší ztracená a zapomenutá hesla a může se také stát cílem útoku.

11.3.2 Neobsluhovaná uživatelská zařízení

Opatření
Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaných zařízení.
Doporučení k realizaci
Všichni uživatelé by si měli být vědomi bezpečnostních požadavků a postupů pro zabezpečení neobsluhovaného zařízení, stejně jako své odpovědnosti za provádění takovéto ochrany.
Uživatelům by mělo být doporučeno:
a) při ukončení práce ukončit aktivní relace nebo je zajistit vhodným mechanizmem, například spořičem obrazovky s heslem;
b) odhlásit se v případě ukončení relace od sálových počítačů, serverů a kancelářských PC (tj. nevypínat pouze monitor počítače nebo terminál);
c) pokud se nepoužívají, zabezpečit PC nebo terminály pomocí uzamčení klávesnice nebo ekvivalentní kontroly, například přístupovým heslem (viz 11.3.3).
Další informace
Zařízení instalovaná v uživatelských prostorech, například pracovní stanice nebo souborový server, mohou vyžadovat zvláštní ochranu před neoprávněným přístupem, když jsou delší dobu bez obsluhy.

11.3.3 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření
Měla by být přijata zásada prázdného stolu ve vztahu k dokumentům a vyměnitelným médiím a zásada prázdné obrazovky monitoru u prostředků pro zpracování informací.
Doporučení k realizaci
Zásada prázdného stolu a prázdné obrazovky monitoru by měla brát v potaz klasifikaci informací (viz 7.2), zákonné a smluvní požadavky (viz 15.1), rizika a kulturní aspekty organizace. V úvahu by měla být vzata následující Opatření
a) citlivé nebo kritické informace organizace, např. papírové dokumenty a počítačová média by měly být v případě, že se nepoužívají, a zejména když je kancelář prázdná, uzamčeny (ideálně v protipožárním sejfu nebo v uzamykatelných skříňkách nebo v jiném bezpečném druhu nábytku);
b) přihlášené osobní počítače, počítačové terminály by neměly být ponechávány bez dozoru, a v případě, že se nepoužívají, by měly být chráněny klíčem, heslem nebo jinými opatřeními;
c) body shromažďující došlou a odeslanou korespondenci, stejně tak jako faxové přístroje bez dohledu by měly být chráněny;
d) kopírky a další reprodukční zařízení (např. skenery, digitální kamery) by měly být v mimopracovní době uzamčeny (nebo jiným způsobem chráněny před neoprávněným použitím);
e) dokumenty obsahující citlivé nebo klasifikované informace by měly být po vytištění okamžitě odebírány z tiskárny.
Další informace
Zásada prázdného stolu a prázdné obrazovky monitoru snižuje riziko neoprávněného přístupu, ztráty a poškození informací během nebo mimo běžnou pracovní dobu. Sejfy nebo jiné podobné typy zařízení mohou být také využity k bezpečnému uložení informací a jejich ochraně proti katastrofám, jakými mohou být například požár, zemětřesení, povodeň nebo výbuch. Mělo by být zváženo použití tiskáren u kterých dojde k vytištění úlohy teprve po identifikaci kartou nebo PIN kódem na terminálu (uživatel musí stát u tiskárny).

11.4 Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám.
Přístup k interním i externím síťovým službám by měl být řízen.
Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb. K tomu je potřeba:
a) vhodné rozhraní sítě organizace se sítěmi jiných organizací nebo veřejnými sítěmi;
b) odpovídající autentizační mechanizmus pro uživatele a zařízení;
c) řízení přístupu uživatelů k informačním službám.

11.4.1 Politika užívání síťových služeb

Opatření
Uživatelé by měli mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.
Doporučení k realizaci
Politika formulovaná ve vztahu k sítím a síťovým službám by měla pokrývat:
a) sítě a síťové služby, ke kterým je povolen přístup;
b) autorizační postupy určující kdo je oprávněn přistupovat k jakým sítím a síťovým službám;
c) řídící kontrolní mechanizmy a postupy určené k ochraně přístupu k síťovým připojením a službám;
d) možnosti pro přístup k síti nebo síťovým službám (např. podmínky za kterých je povoleno telefonní připojení k internetové službě nebo vzdáleného systému)
Politika užívání síťových služeb by měla být v souladu s politikou řízení přístupu (viz 11.1).
Další informace
Neoprávněné nebo nezabezpečené připojení k síťovým službám může mít vliv na celou organizaci. Toto opatření je důležité zejména u síťových připojení k citlivým nebo kritickým aplikacím organizace či pro uživatele připojující se z vysoce rizikových lokalit, například veřejné

nebo vnější oblasti nespadající do působnosti bezpečnostních opatření organizace.

11.4.2 Autentizace uživatele externího připojení

Opatření

Přístup vzdálených uživatelů měl být autentizován.

Doporučení k realizaci

Autentizace vzdálených uživatelů může být zajištěna například použitím kryptografických technik, autentizačních předmětů (hardware token) nebo protokolem typu výzva/odpověď (challenge/response). Implementaci takovýchto technik například využívají virtuální privátní sítě (VPN sítě). Pro kontrolu identity zdroje komunikace může být také použito vyhrazené soukromé linky nebo prostředků pro ověření síťové adresy uživatele.

Ochranu proti neautorizovanému a nechtěnému připojení k prostředkům pro zpracování informací organizace mohou zajistit opatření zajišťující zpětné volání, například použití modemů pro zpětné volání (dial-back). Tento druh opatření se používá pro autentizaci uživatele, pokoušejícího se o připojení do sítě organizace ze vzdálené lokality. Při použití těchto opatření, by organizace neměla používat síťové služby, které zahrnují přesměrování hovoru a v případě, že je používá, by měla být funkce přesměrování zakázána, aby se zabránilo vytvoření slabin, které obsahuje. Je také důležité, aby proces zpětného volání obsahoval na straně organizace kontrolu ukončení původního spojení. V opačném případě může vzdálený uživatel zůstat na lince a předstírat, že verifikace zpětným voláním byla provedena. Postupy a opatření zajišťující zpětné volání by měly být otestovány, aby neumožňovaly tento způsob zneužití.

Autentizace uzlů může být i alternativním prostředkem autentizace skupin vzdálených uživatelů, kteří jsou připojeni k bezpečným sdíleným počítačovým prostředkům. Kryptografické techniky, např. založené na certifikátech fyzických počítačů, lze použít pro autentizaci uzlů. Toto je jen jeden z příkladů řešení VPN sítí.

Pro bezpečný přístup k bezdrátovým sítím by měly být implementovány dodatečné techniky autentizace. Je to z důvodu vyššího rizika narušení komunikace nebo vložení falešné zprávy než je tomu u sítí klasických.

Další informace

Externí připojení, například přístup komutovanou linkou, představuje určitý potenciál pro neoprávněný přístup k informacím organizace. Existují různé typy autentizačních metod, některé z nich poskytují větší úroveň ochrany než jiné, například metody založené na použití kryptografických technik mohou zajistit silnou autentizaci. Je důležité, aby navržený stupeň požadované ochrany, který slouží jako základ pro výběr vhodné autentizační metody, vycházel z hodnocení rizik.

Možnost automatického připojení ke vzdáleným počítačům může představovat cestu vedoucí k získání neoprávněného přístupu k aplikacím organizace. Vzdálená připojení k počítačovým systémům by tedy měla být autentizována. To je zvláště důležité v případě připojení přes otevřenou síť, která je mimo působnost správy bezpečnosti organizace.

11.4.3 Identifikace zařízení v sítích

Opatření

Pro autentizaci připojení z vybraných lokalit a přenosných zařízení by se měla zvážit automatická identifikace zařízení.

Doporučení k realizaci

Automatická identifikace zařízení je způsob, který může být použit, jestliže je důležité, aby byla komunikace iniciována pouze z určité lokality nebo zařízení. Zabudovaný nebo připojený identifikátor zařízení může být používán pro indikaci povolení zahájit nebo přijímat určité transakce. Indikátory by měly jasně ukazovat ke které síti se může zařízení připojit, je to pro případy kdy existuje více sítí vyžadujících různou úroveň zabezpečení. V některých případech může být nutné, pro zajištění bezpečnosti identifikátoru zařízení, zvážit jeho fyzickou ochranu.

Další informace

Automatická identifikace zařízení může být doplněna o další techniky autentizace uživatelů těchto zařízení (viz 11.4.2). Identifikace zařízení může být dodatečně použita spolu s autentizací uživatelů.

11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Opatření

Fyzický i logický přístup k diagnostickým a konfiguračním portům by měl být bezpečně řízen.

Doporučení k realizaci

Přiměřeným bezpečnostním mechanizmem ochrany diagnostických a konfiguračních portů může být například uzamčení klávesnice a použití dalších mechanizmů zamezujících fyzickému přístupu k portům. Příkladem těchto podpůrných bezpečnostních mechanizmů může být povolení přístupu k diagnostickým a konfiguračním portům výhradně na základě dohody mezi správcem služby a personálem zajišťujícím podporu technického a programového vybavení, které vyžaduje přístup.

Porty, služby a obdobná zařízení instalovaná na počítačích nebo síťových zařízeních, pokud nejsou pro organizace potřebné, by měly být zakázány nebo odstraněny.

Další informace

Mnoho počítačových, síťových a komunikačních systémů obsahuje prostředky pro vzdálenou konfiguraci a diagnostický přístup, které využívá podpůrný personál pro údržbu systému. Pokud jsou nechráněny, představují diagnostické porty prostředek k neoprávněnému přístupu.

11.4.5 Princip oddělení v sítích

Opatření

Skupiny informačních služeb, uživatelů a informačních systémů by měly být v sítích odděleny.

Doporučení k realizaci

Jedna z metod správy bezpečnosti velkých sítí je rozdělení sítí do separátních logických domén, tj. vnitřních síťových domén organizace a externích síťových domén, kde každá z nich je chráněna definovaným bezpečnostním perimetrem. V rámci logických domén mohou být pro další

bezpečné oddělení síťových prostředí (např. veřejně přístupné systémy, vnitřní sítě a kritická aktiva) uplatněny silnější skupiny opatření. Domény by měly být vymezeny na základě různých bezpečnostních požadavků a výsledků analýzy rizik.
Tento bezpečnostní perimetr může být vytvořen instalací bezpečnostní brány mezi sítě, které mají být propojeny, aby přístup a tok informací mezi dvěma doménami byl pod kontrolou. Tato brána by měla být nakonfigurována tak, aby filtrovala komunikaci mezi těmito doménami (viz 11.4.6 a 11.4.7) a blokovala neautorizovaný přístup v souladu se zásadami řízení přístupu organizace (viz 11.1). Příkladem tohoto typu brány je firewall. Jinou metodou oddělení logických domén je vytvoření virtuálních privátních sítí pro různé skupiny uživatelů v rámci organizace. Sítě mohou být také odděleny s využitím funkčnosti síťových zařízení, např. přepínáním protokolu IP. Oddělené domény mohou být vytvořeny na základě řízení toku dat s využitím možností směrování a přepínání, jako například nastavení ACL15.
Kritéria pro separaci sítí by měla být založena na systému řízení přístupu a požadavcích na přístup (viz 10.1), s přihlédnutím k relativní ceně a výkonovým důsledkům zavedení vhodného síťového směrování nebo bran (viz 11.4.6 a 11.4.7).
Oddělení v sítích by mělo být založeno na klasifikaci ukládaných a zpracovávaných informací, úrovni důvěry a typu činností, kterými se organizace zabývá tak, aby byl v případě narušení služeb minimalizován celkový dopad na organizaci.
Mělo by být zváženo oddělení bezdrátových sítí od interních a privátních sítí. V případech kdy není přesně vymezen perimetr bezdrátové sítě by mělo být provedeno hodnocení rizik a identifikována vhodná opatření (např. silná autentizace, kryptografické metody a výběr kmitočtu) zajišťující oddělení sítí.
Další informace
Sítě se stále více rozšiřují za tradiční hranice organizace. Z důvodů vytváření partnerství může být zapotřebí propojení nebo sdílení prostředků pro zpracování a výměnu informací. Takové rozšíření může zvyšovat riziko neoprávněného přístupu k existujícím informačním systémům, které využívají síť, přičemž u některých z těchto systémů může být vyžadována ochrana před jinými uživateli sítě vzhledem k jejich citlivosti nebo kritičnosti.

11.4.6 Řízení síťových spojení

Opatření
U sdílených sítí, zejména těch, které přesahují hranice organizace, by měly být omezeny možnosti připojení uživatelů. Omezení by měla být v souladu s politikou řízení přístupu a s požadavky aplikací (viz 11.1).
Doporučení k realizaci
Oprávnění pro přístup uživatelů k síti by měla být udržována aktuální a v souladu s politikou řízení přístupu (viz 11.1).
Připojení uživatelů může být omezeno prostřednictvím síťových bran, které filtrují síťový provoz podle předdefinovaných tabulek nebo pravidel. Příklady aplikací, na které by měla být nasazena omezení, jsou:
a) odesílání zpráv, např. elektronická pošta;
b) přenos souborů;
c) interaktivní přístup;
d) přístup k aplikacím.
Mělo by být zváženo omezení přístupu k síti na určitou denní dobou nebo datum.
Další informace
Zavedení opatření omezujících možnosti připojení uživatelů mohou být stanoveny v politice řízení přístupu pro sdílené sítě, zejména těch, které přesahují hranice organizace.

11.4.7 Řízení směrování sítě

Opatření
Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, by mělo být zavedeno řízení směrování sítě. Access Control List
Doporučení k realizaci
Řízení směrování by mělo být založeno na ověření zdrojové a cílové adresy.
Pokud jsou využívány zástupné (proxy) servery a/nebo překlad síťových adres, mohou být k ověření zdrojové a cílové adresy využity bezpečnostní brány umístěné na interních a externích kontrolních síťových bodech. Realizátoři tohoto opatření by měli znát sílu všech nasazených mechanizmů. Požadavky pro řízení směrování sítě by měly vycházet z politiky řízení přístupu (viz 11.1).
Další informace
U sdílených sítí, zvláště přesahují-li hranice organizace, může být vyžadována implementace dodatečných omezení směrování. Tato opatření jsou zejména běžná pro sítě sdílené s uživateli třetích stran.

11.5 Řízení přístupu k operačnímu systému

Cíl: Předcházet neautorizovanému přístupu k operačním systémům.
Pro omezení přístupu k prostředkům počítače by měly být použity bezpečnostní prostředky na úrovni operačního systému.Tyto prostředky by měly být schopné:
a) autentizace oprávněných uživatelů v souladu se stanovenou politikou řízení přístupu;
b) zaznamenávat úspěšné a neúspěšné pokusy o autentizaci;
c) zaznamenávat využití systémových privilegií;
d) spouštět varování při porušení systémových bezpečnostních politik;
e) poskytovat vhodné prostředky pro autentizaci;
f) v případě potřeby omezit dobu připojení uživatele.

11.5.1 Bezpečné postupy přihlášení

Opatření
Přístup k operačnímu systému by měl být řízen postupy bezpečného přihlášení.
Doporučení k realizaci

Postup přihlášení k operačnímu systému by měl být řešen tak, aby byla minimalizována příležitost neoprávněného přístupu. Přihlašovací postup by tedy měl prozrazovat minimum informací o systému, aby neposkytoval zbytečnou podporu neoprávněnému uživateli. Dobrý přihlašovací postup by měl:

a) nezobrazovat identifikátory systému nebo aplikace, dokud není přihlašovací proces dokončen;

b) zobrazovat obecné varování, že počítač smí používat pouze oprávnění uživatelé;

c) neposkytovat nápovědu během přihlašovacího postupu, která by pomohla neoprávněnému uživateli;

d) zkontrolovat platnost přihlašovacích informací jen v případě, že jsou vstupní data kompletní. Pokud se vyskytne chyba, systém by neměl indikovat, která část dat je správná, nebo chybná;

e) omezit počet povolených neúspěšných přihlašovacích pokusů (doporučují se tři pokusy) a zároveň zvážit:

1. zaznamenání neúspěšných pokusů;
2. povolení dalšího pokusu o přihlášení až za určitou dobu nebo odmítnutí dalších pokusů bez dalšího specifického potvrzení;
3. odpojení všech spojení na data;
4. zasílání varovných zpráv do systémové konzole (správci sítě) v případě, že je překročen maximální počet pokusů o přihlášení;
5. nastavení maximálního počtu pokusů o opětovné zadání hesla, společně s jeho minimální délkou, podle toho jakou má systém pro organizaci hodnotu;

f) omezit minimální a maximální dobu povolenou pro přihlášení. Pokud je překročena, systém by měl přihlašovací postup ukončit;

g) při dokončení úspěšného přihlášení zobrazit následující informace:

1. datum a čas předchozího úspěšného přihlášení;
2. podrobnosti o všech neúspěšných pokusech o přihlášení od posledního úspěšného přihlášení;

h) nezobrazovat heslo při jeho zadávání a nebo jej maskovat použitím zástupných symbolů;

i) neposílat hesla přes sít v čitelné (nezašifrované) textové podobě.

Další informace

Hesla, která jsou při pokusu o přihlášení odesílána v nešifrované podobě, mohou být snadno odchycena za použití programů monitorujících síťový provoz (tzv. sniffers).

11.5.2 Identifikace a autentizace uživatelů

Opatření

Všichni uživatelé by měli mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), měl by být také zvolen vhodný způsob autentizace k ověření jejich identity.

Doporučení k realizaci

Toto opatření by se mělo vztahovat na všechny typy uživatelé (včetně podpůrného technického personálu, jako jsou operátoři, administrátoři sítě, systémoví programátoři a databázoví administrátoři).

Uživatelská ID by měla umožňovat pozdějšího vysledování odpovědnosti konkrétních osob za činnosti v systému. Běžné aktivity uživatelů by neměly být prováděny z privilegovaných účtů. Ve výjimečných případech, kde to představuje jednoznačný přínos pro organizaci, se může používat sdílený uživatelský identifikátor pro skupiny uživatelů nebo pro určitou činnost. Tyto případy by měly být písemně schváleny vedoucím zaměstnancem. Pro udržení odpovědnosti mohou být nutná další dodatečná opatření.

Použití generických anebo obecných ID by mělo být povoleno pouze v případech, kdy není potřeba sledovat aktivity konkrétních uživatelů (např. když je k objektům povolen přístup pouze pro čtení) a nebo v případech kdy jsou zavedena jiná opatření (např. heslo pro automaticky generované ID je vždy přiřazeno pouze jednomu konkrétnímu uživateli a je o tom vytvořen záznam).

Tam kde je vyžadována silná autentizace a ověření identity by jako alternativy k heslům mělo být zváženo použití kryptografických prostředků, paměťových nebo čipových karet a nebo biometrických autentizačních technologií.

Další informace

Pro zajištění identifikace a autentizace se velmi často používají hesla (viz také 11.3.1 a 11.5.3), jejich princip spočívá v tajemství, které zná pouze uživatel. Stejného výsledku může být dosaženo pomocí kryptografických prostředků a autentizačních protokolů. Stupeň použité identifikace a autentizace by měl odpovídat citlivosti chráněných informací.

Pro I&A mohou být také použity předměty, které jsou vlastnictvím uživatelů, jako například paměťové nebo čipové karty. Pro autentizaci identity osoby mohou být použity také biometrické autentizační technologie, využívající unikátní osobní charakteristiky nebo rysy. Kombinace bezpečného propojení technologií a mechanizmů přináší kvalitnější autentizaci.

11.5.3 Systém správy hesel

Opatření

Systém správy hesel by měl být interaktivní a měl by zajišťovat použití kvalitních hesel.

Doporučení k realizaci

Systém správy hesel by měl:

a) prosazovat používání individuálních hesel a uživatelských ID pro udržení odpovědnosti;

b) umožnit uživatelům volit a měnit si své vlastní heslo a zahrnout do systému postup pro potvrzení hesla, který by zamezoval možným překlepům;

c) prosazovat výběr kvalitních hesel (viz 11.3.1);

d) prosazovat obměnu hesel (viz 11.3.1);

e) donutit uživatele změnit si dočasně přidělené heslo při prvním přihlášení (viz 11.2.3);

f) udržovat záznam předchozích uživatelských hesel a zabránit uživatelům znovu je použít;
g) při zadávání hesla nezobrazovat heslo na obrazovce;
h) ukládat soubory hesel odděleně od dat aplikace;
i) ukládat a přenášet hesla v chráněné podobě (např. v zašifrovaná nebo hashovaná);
Další informace
Hesla jsou jedním ze základních prostředků pro ověřování oprávnění uživatelů přistupovat k počítačovým službám.
Některé aplikace vyžadují, aby byla uživatelská hesla přidělena nezávislou autoritou; v takovýchto případech nejsou výše uvedené body b), d) a e) aplikovatelné. Ve většině případů jsou hesla volena a spravována uživateli. Doporučení týkající se používání hesel jsou uvedena v kapitole 11.3.1.

11.5.4 Použití systémových nástrojů

Opatření
Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly by mělo být omezeno a přísně kontrolováno.
Doporučení k realizaci
Měla by být zvážena následující opatření:
a) pro systémové nástroje používat postupy identifikace, autentizace a autorizace;
b) oddělení systémových nástrojů od aplikačních programů;
c) omezení použití systémových nástrojů pouze pro minimální možný počet důvěryhodných oprávněných uživatelů (viz také 11.2.2);
d) autorizace pro případ náhodného použití systémových nástrojů;
e) omezení dostupnosti systémových nástrojů, například jen na dobu provedení schválených změn;
f) záznam o každém použití systémových nástrojů;
g) definování a dokumentování autorizačních úrovní pro systémové nástroje;
h) odstranění všech nepotřebných programových nástrojů a systémových programů;
i) zamezení přístupu k systémovým nástrojům pro uživatele, kteří mají přístup k aplikacím v systémech, kde je vyžadováno oddělení povinností.
Další informace
Většina instalací počítačů obsahuje jeden nebo více systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly.

11.5.5 Časové omezení relace

Opatření
Neaktivní relace by měly se po stanovené době nečinnosti ukončit.
Doporučení k realizaci
Časový mechanizmus by měl po definované době nečinnosti smazat obsah obrazovky a pokud možno později zavřít jak aplikace, tak ukončit síťové relace. Časová prodleva před ukončením relace by měla odrážet bezpečnostní rizika vyplývající z prostor, klasifikace informací, používaných aplikací a uživatelů, kteří zařízení využívají.
U některých systémů může být realizována omezená forma časového ukončení relace, která smaže obrazovku a zabrání neautorizovanému přístupu, ale nezavírá aplikace nebo síťové relace.
Další informace
Implementace tohoto opatření je zejména důležitá ve vysoce rizikových oblastech, například ve veřejných nebo externích prostorech, které jsou mimo působnost bezpečnostní správy organizace, aby se zabránilo přístupu neoprávněných osob.

11.5.6 Časové omezení spojení

Opatření
U vysoce rizikových aplikací by pro zajištění dodatečné bezpečnosti mělo být zváženo použití omezení doby spojení.
Doporučení k realizaci
Toto opatření by se mělo zvážit u citlivých počítačových aplikací, zejména těch, které jsou využívány uživateli ve vysoce rizikových lokalitách, například ve veřejných nebo externích prostorech mimo působnost bezpečnostní správy organizace. Příklady těchto omezení jsou:
a) použití předdefinovaného časového intervalu, například pro dávkové přenosy souborů nebo pravidelné interaktivní relace krátkého trvání;
b) omezení doby spojení na běžnou pracovní dobu, pokud neexistují požadavky na práci přesčas nebo na vícesměnný provoz;
c) opakovaná autentizace po určitých časových intervalech.
Další informace
Vymezení doby, po kterou je povoleno připojení k počítačovým službám, omezuje příležitost pro neoprávněný přístup. Časová omezení připojení také zamezují uživatelům ponechávat relace otevřené a vyhnout se tak opětovné autentizaci.

11.6 Řízení přístupu k aplikacím a informacím

Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.
Pro omezení přístupu k aplikačním systémům by měly být použity bezpečnostní prostředky. Logický přístup k programům a informacím by měl být omezen na oprávněné uživatele. Aplikační systémy by měly:
a) kontrolovat přístup uživatelů k datům a funkcím aplikačního systému v souladu s definovanou politikou řízení přístupu;
b) poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům, které mohou obejít systémové a aplikační kontrolní mechanizmy;
c) nenarušit bezpečnost jiných systémů, se kterými jsou sdíleny informační zdroje;

11.6.1 Omezení přístupu k informacím

Opatření
Uživatelé aplikačních systémů, včetně pracovníků podpory, by měli mít přístup k informacím

a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu.

Doporučení k realizaci

Omezení přístupu by mělo být založeno na požadavcích na jednotlivé aplikace a musí být v souladu s celkovou politikou přístupu k informacím organizace (viz 11.1).

Na podporu politiky přístupu by se mělo vzít v úvahu využití následujících opatření:

a) zajištění řízení přístupu k funkcím aplikačního systému prostřednictvím nabídek;

b) omezení přístupových oprávnění uživatelů, například na čtení, zápis, mazání, vykonání/spuštění;

c) omezení přístupových práv ze strany dalších aplikací;

d) zajištění toho, že výstupy z aplikačního systému, který nakládá s citlivými informacemi, obsahují relevantní informace, že tyto jsou posílány pouze oprávněným terminálům nebo do oprávněných lokalit, včetně pravidelné kontroly výstupů, aby nebyly publikovány nadbytečné údaje.

11.6.2 Oddělení citlivých systémů

Opatření

Citlivé aplikační systémy by měly mít oddělené (izolované) počítačové prostředí.

Doporučení k realizaci

Pro citlivé aplikační systémy by mělo být zváženo následující:

a) citlivost aplikačního systému by měla být explicitně určena a zdokumentována vlastníkem aplikace (viz 7.1.2);

b) v případě provozování citlivé aplikace ve sdíleném prostředí by měly být aplikační systémy, se kterými budou sdíleny zdroje, určeny a odsouhlaseny vlastníkem citlivé aplikace.

Další informace

Některé aplikační systémy jsou vzhledem k možným ztrátám tak citlivé, že vyžadují zvláštní zacházení.

Citlivost může určovat, zda by měl být aplikační systém:

a) provozován pouze na vyhrazeném počítači nebo;

b) sdílet zdroje pouze s důvěryhodnými aplikačními systémy.

Izolace citlivých aplikačních systémů může být zajištěna cestou jejich fyzického a nebo logického oddělení (viz také 11.4.5).

11.7 Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití zařízení pro práci na dálku.

Požadovaná ochrana by měla odpovídat rizikovosti těchto specifických způsobů práce. Při použití mobilních výpočetních prostředků by mělo být zváženo riziko práce v nechráněném prostředí a měla by být zajištěna vhodná ochrana. V případě práce na dálku by měla být zavedena ochrana na místě výkonu práce a měly by být zajištěny vhodné podmínky pro tento způsob práce.

11.7.1 Mobilní výpočetní zařízení a sdělovací technika

Opatření

Měla by být ustavena formální pravidla a přijata opatření na ochranu proti rizikům použití mobilních výpočetních a komunikačních prostředků.

Doporučení k realizaci

Při použití mobilních výpočetních prostředků, například notebooků, palmtopů, laptopů a mobilních telefonů, by měla být věnována zvláštní pozornost tomu, aby nebyly prozrazeny informace organizace. Měla by být přijata taková formální pravidla, které by brala v úvahu riziko práce s mobilním výpočetním zařízením, zejména v nezabezpečeném prostředí.

Tato pravidla by měla zahrnovat například požadavky na fyzickou ochranu, kontrolu přístupu, kryptografické techniky, zálohování a antivirovou ochranu. Tato pravidla by rovněž měla zahrnovat požadavky a doporučení pro připojování mobilních výpočetních zařízení k sítím a návod k použití těchto prostředků na veřejných místech.

Pozornost by měla být věnována použití mobilních výpočetních zařízení na veřejných místech, v zasedacích místnostech a jiných nechráněných místech mimo prostor organizace. Měla by být k dispozici ochrana proti neautorizovanému přístupu a prozrazení informací uložených a zpracovávaných těmito prostředky, například použitím kryptografických technik (viz 12.3).

Při použití těchto zařízení na veřejných místech by se uživatelé měli vyhnout riziku odpozorování neautorizovanými osobami. Měly by být použity prostředky proti škodlivým programům a tyto prostředky by měly být aktualizovány (viz 10.4).

V pravidelných intervalech by měly být vytvářeny zálohy všech kritických informací organizace. Mělo by být k dispozici zařízení schopné provádět rychlé a jednoduché zálohování informací. Zálohy by měly být odpovídajícím způsobem chráněny proti krádeži nebo ztrátě informací.

Při použití mobilních výpočetních zařízení připojených k sítím by měla být zajištěna vhodná ochrana. Vzdálený přístup k informacím organizace prostřednictvím veřejných sítí by měl být umožněn pouze po úspěšné identifikaci a autentizaci, a to s nasazením vhodných mechanizmů řízení přístupu (viz 11.4).

Mobilní výpočetní prostředky by měly být také chráněny proti zcizení, zejména pokud zůstávají například v autech nebo jiných dopravních prostředcích, hotelových pokojích, konferenčních centrech a zasedacích místnostech. Pro případ krádeže nebo ztráty mobilních výpočetních zařízení by měly být ustaveny přesné postupy beroucí v potaz právní požadavky, požadavky na pojištění a další bezpečnostní požadavky organizace. Zařízení, obsahující důležité, citlivé nebo kritické informace organizace, by nemělo zůstávat bez dohledu a mělo by být pokud možno fyzicky zabezpečeno nebo by jeho funkce měly být zajištěny speciálním uzamčením. Více informací o fyzické ochraně mobilních zařízení lze nalézt v 9.2.5.

Aby bylo dosaženo povědomí o dalších rizicích tohoto způsobu práce a opatřeních, která by měla být zavedena, měla by být pro personál, používající mobilní zařízení, organizována školení.

Další informace

Bezdrátová připojení jsou podobná ostatním typům síťových připojení, existuje však několik důležitých rozdílů, které je třeba mít na paměti při výběru vhodných opatření. Typickými rozdíly jsou:

a) některé bezdrátové bezpečnostní protokoly mají známé slabiny;

b) vytvoření záloh informací uložených na mobilních výpočetních prostředcích nemusí vždy proběhnout tak, jak bylo naplánováno. Důvodem může být omezená šířka přenosového pásma a/nebo bylo vytvoření zálohy naplánováno na dobu, kdy nebylo zařízení připojeno k síti.

11.7.2 Práce na dálku

Opatření

Organizace by měla vytvořit a do praxe zavést zásady, operativní plány a postupy pro práci na dálku.

Doporučení k realizaci

Organizace by měla schválit aktivity práce na dálku pouze tehdy, jestliže jsou splněny odpovídající bezpečnostní požadavky a jsou zavedena opatření, jež jsou v souladu s bezpečnostní politikou organizace.

Na vzdáleném pracovišti by měla existovat vhodná ochrana například proti zcizení zařízení a informací, neautorizovanému vyzrazení informací, neautorizovanému vzdálenému přístupu k vnitřním systémům organizace nebo zneužití prostředků. Je důležité, aby práce na dálku byla schvalována a kontrolována vedoucími zaměstnanci a aby byly zavedeny vhodné podmínky pro tento způsob práce.

Mělo by být zváženo následující:

a) existence fyzické bezpečnosti pracoviště a práce na dálku včetně fyzického zabezpečení budovy a místního prostředí;

b) navrhované prostředí práce na dálku;

c) požadavky na komunikační bezpečnost, zahrnující potřeby vzdáleného přístupu k interním systémům organizace, citlivost informací, ke kterým je přistupováno a které jsou přenášeny komunikačními linkami, i citlivost interního systému;

d) hrozba neautorizovaného přístupu k informacím nebo zdrojům ze strany ostatních lidí užívajících místnosti, například rodina a přátelé

e) používání domácích sítí a požadavky nebo omezení na konfiguraci bezdrátových síťových služeb;

f) politika a procedury pro zamezení sporů ohledně práv v intelektuálnímu vlastnictví vytvořeného na zařízení v soukromém vlastnictví;

g) přístup k vybavení v soukromém vlastnictví, který může být omezen zákonem (např. z důvodů kontroly zabezpečení nebo v rámci vyšetřování);

h) licenční podmínky na provoz programového vybavení, které mohou stanovovat odpovědnost organizace za licence klientských aplikací také na pracovních stanicích, které jsou soukromým majetkem zaměstnanců, smluvních nebo třetích stran;

i) požadavky na antivirovou ochranu a firewall.

Kontroly a podmínky, které by měly být zváženy, zahrnují:

a) zajištění vhodného zařízení a skladovacího vybavení pro práci na dálku tam, kde není povoleno používat prostředky v soukromém vlastnictví, které nejsou pod kontrolou organizace;

b) určení povoleného druhu práce, pracovní doby, klasifikace informací, které mohou být drženy, a klasifikace interních systémů a služeb, ke kterým bude mít daná osoba při práci na dálku přístup;

c) zajištění vhodného komunikačního zařízení včetně metod pro bezpečný vzdálený přístup;

d) fyzickou bezpečnost;

e) pravidla a doporučení pro přístup k zařízení a informacím ze strany rodiny a návštěv;

f) zajištění technické a programové podpory a údržby;

g) zajištění pojištění;

h) zálohovací postupy a postupy zajištění kontinuity činností organizace;

i) audit a monitorování bezpečnosti;

j) zrušení oprávnění, přístupových práv a vrácení vybavení při ukončení práce na dálku.

Další informace

Při práci na dálku umožňují komunikační technologie personálu pracovat vzdáleně z určeného místa mimo organizaci.

12 Nákup, vývoj a údržba informačního systému

12.1 Bezpečnostní požadavky systémů

Cíl: Zajistit, aby se bezpečnost stala neodlučitelnou součástí informačních systémů.

To zahrnuje provozní systémy, infrastrukturu, interní aplikace organizace, zakoupené produkty, služby a uživatelsky vyvinuté aplikace. Návrh a implementace informačního systému na podporu procesů organizace může být z hlediska bezpečnosti kritický. Bezpečnostní požadavky by měly být stanoveny a odsouhlaseny ještě před zahájením vývoje informačního systému. Všechny bezpečnostní požadavky by měly být v projektu stanoveny již ve fázi definice požadavků a měly by být zdůvodněny, odsouhlaseny a dokumentovány jako součást vývoje informačního systému.

12.1.1 Analýza a specifikace bezpečnostních požadavků

Opatření

Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů by měly obsahovat také požadavky na bezpečnostní opatření.

Doporučení k realizaci

Tato specifikace by měla vzít v úvahu začlenění automatizovaných kontrol do systému, ale

i potřebu doplňujících manuálních kontrol. Stejně by se mělo postupovat i při testování, vytvořených nebo zakoupených, programových balíků aplikací organizace.
Bezpečnostní požadavky a opatření by měly odrážet hodnotu informačních aktiv pro organizaci (viz 7.2) a možnou škodu, která by mohla být výsledkem nedostatečné bezpečnosti nebo jejího selhání.
Požadavky na bezpečnost informačních systémů a procesy implementace bezpečnosti by měly být začleněny do projektu informačního systému již v jeho počáteční fázi. Opatření, která jsou začleněna ve fázi návrhu, lze implementovat a udržovat výrazně levněji než ty, které jsou začleňovány v průběhu nebo po implementaci.
U zakoupených produktů by měl nejprve následovat formální proces testování a zavedení do provozu. Ve smlouvách s dodavateli by měly být specifikovány požadavky na bezpečnost. U produktů jejichž bezpečnostní funkce nesplňují specifikované požadavky na bezpečnost by ještě před jejich nákupem mělo být zváženo přijetí opatření na pokrytí nově zavedeného rizika. Pokud s sebou dodatečné změna funkčnosti produktů přináší také nové riziko, měla by tato funkčnost být buďto zrušena, a nebo by měl být přezkoumán její potenciální přínos a přijetí dodatečných opatření.
Další informace
Vedení organizace se může, po důkladném zvážení (například z důvodů nižších nákladů), rozhodnout používat nezávisle certifikované a ohodnocené produkty. Podrobnější informace o požadavcích na kritéria, podle kterých je hodnocena bezpečnost IT produktů, lze nalézt v normě ISO/IEC 1540816 a dalších normách.
Norma ISO/IEC 13335-317 poskytuje návod jak správně určit požadavky na bezpečnostní opatření v rámci procesu řízení rizik.

12.2 Správné zpracování v aplikacích

Cíl: Předcházet chybám, ztrátě, modifikaci nebo zneužití uživatelských dat v aplikacích.
Pro zajištění bezchybného zpracování by do aplikačních systémů, včetně těch, které jsou vytvořeny uživatelsky, měly být zahrnuty vhodné kontroly. Měly by zahrnovat potvrzení platnosti vstupních dat, interního zpracování a výstupních dat.
Přijetí dodatečných kontrol by mělo být zváženo u systémů, které zpracovávají nebo mají vliv na zpracování citlivých, cenných nebo kritických informací.

12.2.1 Kontrola vstupních dat

Opatření
Vstupní data aplikací by měla být kontrolována z hlediska správnosti a adekvátnosti.
Doporučení k realizaci
Kontrolovány by měly být transakční vstupy, vlastní data (např. jména a adresy, úvěrové limity, zákaznická referenční čísla) a číselníky (např. prodejní ceny, kurzové převodní tabulky, daňové sazby).
V úvahu by měla být vzata následující opatření:
a) zdvojený vstup nebo jiná vstupní kontrola, jako například specifikace rozsahu nebo definovaná pole dat, pro detekování následujících chyb:
1. hodnoty mimo rozsah;
2. neplatné znaky v datových polích;
3. chybějící nebo nekompletní údaje;
4. překročení horního a dolního vymezení rozsahu dat;
5. neoprávněná nebo nekonzistentní kontrolní data;
b) pravidelná kontrola obsahu klíčových polí nebo datových souborů pro potvrzení jejich platnosti a integrity;
c) kontrola papírových vstupních dokumentů za účelem zjištění jakýchkoliv neoprávněných změn ve vstupních datech (všechny změny vstupních dokumentů by měly být schváleny);
d) postupy při reakci na zjištěné chyby validace;
e) postupy pro testování hodnověrnosti vstupních dat;
f) stanovení odpovědností všeho personálu, který se účastní procesu vstupu dat;
g) vytvoření záznamu o činnostech, které jsou součástí procesu vstupu dat (viz 10.10.1).
Další informace
Pro snížení rizika chyb a zabránění běžným útokům, včetně přetečení zásobníku a podstrčení kódu, by měla být zvážena implementace automatických kontrol a verifikace dat.

12.2.2 Kontrola vnitřního zpracování

Opatření
Pro detekci jakéhokoliv poškození nebo modifikace informací vzniklého chybami při zpracování nebo úmyslnými zásahy, by mělo být zváženo začlenění kontroly platnosti dat.
Doporučení k realizaci
Návrh aplikací by měl zajistit implementaci těchto omezení tak, aby se minimalizovalo riziko chyb při zpracování vedoucí ke ztrátě integrity. Za zvážení stojí následující specifické oblasti:
a) použití funkcí vstupu, modifikace a mazání za účelem provedení změn v datech;
b) postupy, které brání spuštění programům ve špatném pořadí nebo zabraňují jejich spuštění po předchozím selhání zpracování (viz také 10.1.1);
c) použití vhodných programů na zotavení se z chyb a pro zajištění správného zpracování dat;
d) použití ochrany proti útokům způsobujícím přetečení bufferu.
Měl by být připraven kontrolní seznam, veškeré činnosti dokumentovány a výsledky bezpečně uchovány. Příklady kontrol, které mohou být začleněny, jsou následující:
a) relační nebo dávková kontrola pro porovnání bilancí datových souborů po transakčních aktualizacích;
b) bilanční (balancing) kontroly pro ověření celkové hodnoty otevíraných dat oproti celkové hodnotě předtím uzavřených dat, zejména:

1. kontrola mezi jednotlivými úlohami (run-to-run);
2. celková hodnota provedená aktualizacemi souboru;
3. kontrola mezi jednotlivými programy (program-to-program);
c) verifikace vstupních dat generovaných systémem (viz 12.2.1);
d) prověrka integrity dat nebo programů zasílaných či nahrávaných mezi centrálním počítačem a vzdálenou stanicí;
e) výpočet celkového kontrolního součtu (hash) záznamů a souborů;
f) ověření, zda jsou programy spouštěny ve správný čas;
g) prověrka, zda jsou programy spouštěny ve správném pořadí a jsou zastaveny v případě chyby a zda je další zpracování pozastaveno až do odstranění problému;
h) vytváření záznamů o činnostech v průběhu zpracování (viz 10.10.1).

Další informace

Správně vložená data mohou být poškozena chybami technického vybavení, při zpracování nebo úmyslnými zásahy. Požadované kontroly platnosti dat budou záviset na podstatě aplikací a dopadu možného poškození dat na chod organizace.

12.2.3 Integrita zprávy

Opatření

U jednotlivých aplikací by měly být stanoveny bezpečnostní požadavky na zajištění autentizace a integrity zpráv, dle potřeby určena, a zavedena vhodná opatření.

Doporučení k realizaci

Pro stanovení nutnosti zajištění integrity zpráv a určení její nejvhodnější metody by se mělo provést hodnocení rizik.

Další informace

Jako vhodný prostředek pro implementaci autentizace zpráv mohou být použity kryptografické metody (viz 12.3).

12.2.4 Kontrola výstupních dat

Opatření

Pro zajištění toho, že zpracování uložených informací je bezchybné a odpovídající dané situaci, by mělo být provedeno ověření platnosti výstupních dat.

Doporučení k realizaci

Výstupní kontrola platnosti dat může zahrnovat:
a) prověrku hodnověrnosti, tedy ověření přijatelnosti výstupních dat;
b) porovnávací kontrolní součet zajišťující, že byla zpracována všechna data;
c) poskytnutí dostatku informací pro čtenáře nebo následný proces zpracování, pro stanovení správnosti, kompletnosti, přesnosti a klasifikace informací;
d) postupy pro reakce na výstupní testy platnosti dat;
e) definice odpovědností všeho personálu účastnícího se výstupního procesu
f) vytvoření záznamu všech činností v rámci procesu ověření platnosti výstupních dat.

Další informace

Systémy jsou zpravidla postaveny na předpokladu, že po provedení kontroly platnosti, verifikace a testování jsou výstupní data správná. Ne vždy je však tento předpoklad správný, i otestované systémy mohou za určitých okolností produkovat neplatná data.

12.3 Kryptografická opatření

Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků. Měla by být vytvořena pravidla pro použití kryptografických opatření. K podpoře používání kryptografických technik by měl v organizaci existovat systém jejich správy.

12.3.1 Politika pro použití kryptografických opatření

Opatření

Měla by být vytvořena a zavedena pravidla pro používání kryptografických opatření na ochranu informací.

Doporučení k realizaci

Při vytváření pravidel by mělo být zváženo následující:
a) manažerský přístup k zavedení kryptografických opatření v celé organizaci, včetně základních principů, podle kterých by měly být informace chráněny (viz 5.1.1);
b) na základě výsledků hodnocení rizik by měla být stanovena požadovaná úroveň ochrany a to s ohledem na typ, sílu a kvalitu požadovaného šifrovacího algoritmu;
c) použití šifrování na ochranu citlivých informací při přenosu na mobilních nebo vyměnitelných počítačových médiích a zařízení a nebo komunikačními linkami;
d) přístup ke správě klíčů, včetně metod řešení ochrany šifrovacích klíčů, obnovení šifrovaných informací v případě ztráty, vyzrazení nebo poškození klíčů;
e) úlohy a odpovědnosti, například kdo je odpovědný za:
1. implementaci pravidel;
2. správu klíčů včetně jejich generování (viz 12.3.2);
f) normy, které budou přijaty, aby implementace opatření v celé organizaci byla účinná (pro které procesy budou použita která řešení)
g) dopad, jaký má šifrování informací na prováděné kontroly obsahu (např. detekce virů).

Při implementaci pravidel použití kryptografie v organizaci by měl být brán zřetel na předpisy a místní omezení, která mohou platit při použití kryptografických technik v různých částech světa a pro přenos šifrovaných informací za hranice státu (viz také 15.1.6).

Kryptografická opatření mohou být použita k dosažení různých bezpečnostních cílů, např.:
a) důvěrnosti: použití šifrování na ochranu uložených nebo přenášených citlivých nebo kritických informací;
b) integrity/autentičnosti: použití digitálních podpisů nebo na ochranu autentičnosti a integrity uložených nebo přenášených citlivých a kritických informací;
c) nepopiratelnosti: použití kryptografických technik k získání důkazu o tom, zda událost nebo činnost nastala.

Další informace

Rozhodnutí, zda je vhodné použití kryptografického řešení, by mělo být součástí širšího procesu hodnocení rizik a výběru opatření. Toto hodnocení pak může být použito při určení vhodnosti kryptografických opatření, aplikaci konkrétních opatření a dále účelu či procesů organizace, pro které mají být využity.

Organizace by měla vytvořit pravidla pro používání kryptografických opatření na ochranu svých informací. Tato pravidla jsou potřebná, aby bylo možno maximalizovat výhody a minimalizovat rizika z použití kryptografických metod a také pro vyvarování se nevhodného nebo nesprávného použití. Při použití digitálních podpisů by měl být brán zřetel na všechny relevantní právní úpravy, které stanovují podmínky vážící se k právní závaznosti digitálních podpisů (viz 15.1).

Při určení odpovídající úrovně ochrany, výběru vhodných produktů, které zajistí odpovídající ochranu a implementaci bezpečného systému správy klíčů, by mělo být dáno na doporučení specialistů (viz také 12.3.2).

Technická komise ISO/IEC JTC SC27 vytvořila řadu norem týkajících se kryptografických technik. Další informace lze také nalézt ve standardu IEEE P136318 a směrnici OECD19.

12.3.2 Správa klíčů

Opatření

Na podporu používání kryptografických technik v organizaci by měl existovat systém jejich správy.

Doporučení k realizaci

Všechny klíče by měly být chráněny před modifikací a zničením. Tajné a soukromé klíče je třeba chránit proti neautorizovanému prozrazení. Pro zabezpečení prostředků určených ke generování, ukládání a archivaci klíčů by měly být použity prostředky fyzické ochrany.

Systém správy klíčů by měl být založen na schváleném souboru norem, postupů a bezpečných metod pro:

a) generování klíčů pro různé kryptografické metody a aplikace;
b) generování a získávání certifikátů veřejných klíčů;
c) distribuci klíčů určeným uživatelům včetně způsobu jejich aktivace po předání;
d) ukládání klíčů včetně toho, jak autorizovaní uživatelé získávají ke klíčům přístup;
e) změny nebo aktualizace klíčů včetně pravidel určujících, kdy by měly být klíče měněny a jakým způsobem;
f) zacházení s prozrazenými klíči;
g) revokace klíčů včetně toho, jak mají být klíče staženy z oběhu nebo deaktivovány, například v případě prozrazení nebo při odchodu uživatele z organizace (v tomto případě by klíče měly být rovněž archivovány);
h) obnovení ztracených nebo poškozených klíčů jako součást řízení kontinuity činností organizace, například pro obnovení šifrovaných informací;
i) archivaci klíčů, například pro informace archivované nebo zálohované;
j) ničení klíčů;
k) zaznamenávání a audit aktivit majících souvislost se správou klíčů.

Pro snížení pravděpodobnosti vyzrazení klíčů by tyto měly mít určenu dobu aktivace a deaktivace, aby jejich použití bylo časově omezeno. Délka platnosti klíče by měla být závislá na okolnostech, ve kterých se kryptografická opatření používají, a na předpokládaných rizicích.

Současně s bezpečnou správou tajných a privátních klíčů by měla být zvážena i ochrana veřejných klíčů. Autentizace veřejných klíčů se zpravidla řeší certifikáty veřejných klíčů, které jsou vydávány certifikační autoritou. Ta by měla být uznávanou organizací a pro zajištění požadovaného stupně důvěryhodnosti by měla mít zavedena vhodná opatření a postupy.

Obsah dohod o úrovni služeb nebo smluv s externím poskytovatelem kryptografických služeb, například s certifikační autoritou, by měl pokrývat právní závaznost, spolehlivost a dobu odezvy zajišťovaných služeb (viz 6.2.3).

Další informace

K účinnému použití kryptografických technik je správa kryptografických klíčů nezbytná. Další informace poskytuje norma ISO/IEC 1177020.

Kryptografické techniky jsou následující:

a) systém tajných klíčů, kdy dvě nebo více stran sdílí stejný klíč, který je použit jak k šifrování, tak k dešifrování informací. Tento klíč musí být udržován v tajnosti, protože kdokoliv, kdo má přístup k tomuto klíči, by mohl dešifrovat všechny informace, které byly zašifrované tímto klíčem nebo by mohl zavést neautorizované informace;
b) systém veřejných klíčů, kde každý uživatel má pár klíčů. Veřejný klíč (který může být přístupný každému) a soukromý klíč (který musí být držen v tajnosti). Systém veřejných klíčů může být použit pro šifrování i pro vytváření digitálních podpisů (viz také normy ISO/IEC 979621 a ISO/IEC 1488822).

Existuje hrozba, že někdo padělá digitální podpis výměnou veřejného klíče uživatele za svůj veřejný klíč. Tento problém se řeší zejména certifikáty veřejných klíčů.

Na ochranu šifrovacích klíčů mohou být také použity kryptografické techniky. Mělo by být zváženo vytvoření postupů pro vyřizování zákonných požadavků na přístup ke kryptografickým klíčům, například šifrované informace může být zapotřebí zpřístupnit v nešifrované podobě v případě, že by měly sloužit jako důkaz v soudním sporu.

12.4 Bezpečnost systémových souborů

Cíl: Zajistit bezpečnost systémových souborů

Přístup k systémovým souborům a zdrojovým kódům programů by měl být řízen, projekty IT a podpůrné činnosti by měly být prováděny bezpečným způsobem. Měla by být přijata opatření zabraňující prozrazení citlivých informací v testovacím prostředí.

12.4.1 Správa provozního programového vybavení

Opatření

Měly by být zavedeny postupy kontroly instalace programového vybavení na provozních

systémech.
Doporučení k realizaci
Pro snížení rizika poškození provozních systémů by měla být zvážena následující opatření:
a) aktualizace, provozního programového vybavení, aplikací a knihoven programů by měly být prováděny pouze oprávněným správcem na základě schválení vedením (viz 10.4.3);
b) pokud je to možné, měly by provozní systémy obsahovat pouze spustitelný kód. Provozní systémy by neměly obsahovat vývojový kód nebo kompilátory ;
c) spustitelný kód by neměl být implementován do provozního systému dříve, než je k dispozici doklad o úspěšném testování a převzetí uživatelem a než jsou aktualizovány odpovídající zdrojové knihovny. Testy by měly být prováděny na oddělených systémech (viz také 10.1.4) a měly by zahrnovat ověření použitelnosti, bezpečnosti, vlivu na ostatní systémy a optimálnosti pro uživatele;
d) měl by být používán systém kontroly konfigurace pro udržování přehledu o instalovaném programovém vybavení a systémové dokumentaci;
e) měla by být připravena strategie umožňující návrat, po implementaci změn, do původního stavu;
f) měly by být udržovány auditní záznamy všech aktualizací provozních programových knihoven;
g) pro případ nouze by měly být uchovány předcházející verze programového vybavení;
h) staré verze programového vybavení by měly být archivovány spolu se všemi požadovanými informacemi a parametry, postupy, konfiguracemi a podpůrnými programy po celou dobu uchování dat v archivu.
Dodavatelsky pořízené programové vybavení použité v provozních systémech by mělo být udržováno způsobem, který podporuje dodavatel. Na některé starší verze programového vybavení může dodavatel přestat poskytovat podporu. Organizace by měla zvážit rizika spojená s provozem nepodporovaného programového vybavení.
Každé rozhodnutí o povýšení verze by mělo brát v úvahu její bezpečnost, tj. její nové bezpečnostní vlastnosti nebo počet, a závažnost bezpečnostních problémů s ní spojených.
V případě, že existují opravné dávky (záplaty) pro programové vybavení, které mohou pomoci odstranit nebo redukovat bezpečnostní slabiny, měly by být použity (viz také 12.6.1).
Fyzický nebo logický přístup by měl být umožněn dodavatelům pouze tehdy, pokud je to třeba ze servisních důvodů a pokud to bylo schváleno vedením. Aktivity dodavatelů by měly být monitorovány.
Počítačové programové vybavení může záviset na externě dodávaných programech a modulech.Ty by měly být monitorovány a kontrolovány, aby se zabránilo neoprávněným změnám, které by mohly být příčinou vzniku bezpečnostních slabin.
Další informace
Provozní systémy by měly být aktualizovány pouze v případech, kdy existuje takový požadavek, například pokud stávající verze operačního systému již nestačí aktuálním požadavkům organizace. Aktualizace by neměly probíhat jen proto, že je k dispozici nová verze operačního systému. Nové verze operačních systémů mohou být méně bezpečné, méně stabilní a méně prověřené než stávající systém.

12.4.2 Ochrana systémových testovacích údajů

Opatření
Testovací data by měla být pečlivě vybrána, chráněna a kontrolována.
Doporučení k realizaci
Pro účely testování je vhodné se vyhnout použití provozních databází obsahujících osobní nebo jinak citlivé údaje. Pokud se tato data použijí, je zapotřebí před tím provést jejich anonymizaci.
Pro ochranu provozních dat použitých pro testovací účely by měla být použita následující
Opatření
a) postupy řízení přístupu, které se používají v provozních aplikačních systémech, by měly být použity i při testování aplikačních systémů;
b) každé kopírování provozních informací do testovacího aplikačního systému by mělo být samostatně schváleno;
c) provozní informace by měly být okamžitě po ukončení testů z testovacího aplikačního systému smazány.
d) kopírování provozních informací by mělo být zaznamenáno do auditních záznamů.
Další informace
Systémové a přejímací testování obvykle vyžaduje značné množství testovacích dat, která by měla být co možná nejvíce podobná datům provozním.

12.4.3 Řízení přístupu ke knihovně zdrojových kódů

Opatření
Přístup ke knihovně zdrojových kódů by měl být omezen.
Doporučení k realizaci
Aby se minimalizovalo možné poškození počítačových programů (zavedení neschválených funkčních prvků a provedení nechtěných změn), měly by se uplatnit přísné kontroly na přístup ke knihovnám zdrojových kódů programu a souvisejících položek (jako jsou návrh, popisy, plány přezkoušení a plány ověření platnosti. U zdrojových kódů programů toho lze dosáhnout vytvořením kontrolovaného centrálního úložiště, nejlépe v knihovnách zdrojových kódů. Pro řízení přístupu do těchto knihoven je možné zvážit následující doporučení (viz také 11) snižující pravděpodobnost poškození počítačových programů:
a) kde je to možné, neměly by být knihovny zdrojových kódů uloženy v provozních systémech;
b) zdrojové kódy programů a knihovny zdrojových kódů by měly být spravovány v souladu se zavedenými postupy;
c) pracovníci podpory IT by neměli mít neomezený přístup ke knihovnám zdrojových kódů;

d) aktualizace zdrojových knihoven programů a souvisejících položek a předávání zdrojových programů programátorům by mělo být prováděno pouze na základě řádného schválení;
e) výpisy z programu by měly být uloženy na bezpečném místě (viz 10.7.4);
f) všechny přístupy ke knihovnám zdrojových kódů by měly být zaznamenány do auditního záznamu;
g) udržování a kopírování knihoven zdrojového kódu programu by mělo být předmětem přísných postupů změnového řízení (viz 12.5.1).

Další informace

Zdrojový kód programu je kód napsaný programátorem a následně zkompilovaný (sestavený) do spustitelného kódu. Některé programovací jazyky formálně nerozlišují mezi zdrojovým kódem a spustitelným kódem, protože se spustitelný kód vytváří až při požadavku na spuštění. Normy ISO 1000723 a ISO/IEC 1220724 poskytují další informace ohledně řízení jakosti a životního cyklu programového vybavení.

12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost programů a informací aplikačních systémů.

Projektové a podpůrné prostředí by mělo být pod přísnou kontrolou.

Vedoucí a správci, kteří jsou odpovědní za aplikační systémy, by měli mít také odpovědnost za bezpečnost projektového a podpůrného prostředí. Měli by zajistit, že všechny plánované změny systému budou podrobeny kontrole, aby nenarušily bezpečnost systému nebo provozního prostředí.

12.5.1 Postupy řízení změn

Opatření

Měly by být zavedeny formální postupy řízení změn.

Doporučení k realizaci

Pro minimalizaci poškození informačních systémů by měly být prosazovány a dokumentovány formální postupy pro řízení změn. Postupy zavádění nových a významné změny u stávajících systémů by měly být formálně řízeny a dokumentovány včetně technických specifikací, měly by podléhat testování a kontrole kvality. Měly by také zajišťovat, aby bezpečnostní a kontrolní postupy nebyly narušeny, aby programátoři měli přístup pouze k těm částem systému, které potřebují ke své práci, aby všechny změny byly potvrzeny formální dohodou a odsouhlasením. Vždy, když je to vhodné, by měly být aplikační a provozní postupy řízení změn propojeny (viz také 8.1.2). Tento proces by měl zahrnovat:
a) udržování záznamu schválených stupňů oprávnění;
b) zajištění toho, že požadavek na změny byl vznesen oprávněnými uživateli;
c) přezkoumaní opatření a integrity postupů proto, aby v případě změn nemohlo dojít k jejich kompromitaci;
d) určení veškerého programového vybavení, informací, databázových entit a technického vybavení, které vyžadují doplnění nebo změny;
e) formální schválení podrobných návrhů před zahájením práce;
f) zajištění toho, aby změny byly před provedením akceptovány oprávněnými uživateli;
g) zajištění toho, aby systémová dokumentace byla aktualizována při ukončení každé změny a stará dokumentace byla archivována nebo zničena;
h) udržování kontroly verzí u všech aktualizací programového vybavení;
i) udržování auditního záznamu všech požadavků na změny;
j) zajištění toho, aby v případě nutnosti byly provedeny změny v provozní dokumentaci (viz 10.1.1) a uživatelských postupech;
k) zajištění toho, aby změny byly prováděny včas a nebyl narušen daný proces organizace.

Další informace

Změna aplikačního programového vybavení může ovlivnit stávající provozní prostředí. Mezi dobré praktiky patří testování nových programů v prostředí, které je odděleno od vývojového a provozního prostředí (viz také 10.1.4). To umožňuje získání kontroly nad novými programy a zajišťuje další ochranu provozních informací použitých pro testovací účely. Takto by se měly také nejprve aplikovat záplaty, opravné balíčky a další aktualizace. U kritických systémů by, z důvodů možného selhání, neměly být nastaveny automatické aktualizace (viz 12.6).

12.5.2 Technické přezkoumání aplikací po změnách operačního systému

Opatření

V případě změny operačního systému by měly být přezkoumány a otestovány kritické aplikace, aby bylo zajištěno, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.

Doporučení k realizaci

Tento proces by měl zahrnovat:
a) přezkoumání opatření a procesů zabezpečujících integritu v aplikacích, aby bylo zajištěno, že nejsou narušeny změnami operačního systému;
b) zajištění toho, aby roční plán podpory a rozpočet na ni pokrýval přezkoumání a testování systému vyvolané změnami operačního systému;
c) zajištění toho, aby změny operačního systému byly včas oznámeny tak, aby mohla být provedena náležitá přezkoumání před jejich realizací;
d) zajištění toho, aby příslušné změny byly zaneseny do plánů kontinuity činností organizace (viz 14).

Měla by být určena konkrétní odpovědnost za sledování zranitelností a dodavateli nově vydaných záplat a oprav (viz 12.6).

12.5.3 Omezení změn programových balíků

Opatření

Modifikace programových balíků by měly být omezeny pouze na nezbytné změny, veškeré prováděné změny musí být řízeny.

Doporučení k realizaci

Dodavatelsky pořízené programové balíky by měly být používány beze změn. V případech, kdy je opravdu nutné modifikovat sady programového vybavení, by se měly vzít v úvahu následující body:
a) možné riziko narušení vestavěných kontrol a procesů zajišťujících integritu;
b) zda by měl být získán souhlas dodavatele;
c) možnost získání požadovaných změn od dodavatele formou standardní aktualizace programu;
d) důsledky toho, že se organizace stane z důvodu provedení změn odpovědnou za budoucí udržování programů.
Pokud jsou změny nezbytné, pak by se originální programové vybavení mělo uchovat a změny by měly být provedeny na jednoznačně označené kopii. Pro zajištění toho, že jsou vždy instalovány nejnovější a schválené záplaty a aktualizace by měl být zaveden řízený proces aktualizace aplikačního programového vybavení. Všechny změny by měly být plně zdokumentovány, aby se mohly znovu použít u budoucích verzí programového vybavení.
Pokud je to vyžadováno, měly by provedené změny být nezávisle otestovány a potvrzeny.

12.5.4 Únik informací

Opatření

Mělo by být zabráněno úniku informací.

Doporučení k realizaci

Pro snížení pravděpodobnosti rizika úniku informací (např. využitím skrytých kanálů) by měly být vzaty v úvahu následující doporučeni:
a) skenování odchozích médií a komunikací jestli neobsahují skryté informace;
b) provádět maskování, časté změny chování a komunikování systému, ke snížení pravděpodobnosti odhalení informací;
c) využití systémů a aplikačního programového vybavení s ověřenou vysokou mírou integrity, například produktů splňujících kritéria bezpečného vývoje (viz ISO/IEC 1540825);
d) pravidelné monitorování systému a činností zaměstnanců, pokud je to v souladu s příslušnou legislativou a předpisy;
e) monitorování využití zdrojů v počítačových systémech.

Další informace

Skryté kanály jsou cesty, jejichž cílem není zprostředkovávat tok informací, mohou se však v sítích nebo systémech vyskytovat. Například manipulace (změna hodnot) bitů v datových paketech komunikačních protokolů může být využita jako skrytá metoda signalizace.
Stoprocentní ochrana proti skrytým kanálům je obtížná, ne-li nemožná. Tyto kanály jsou však často využity trojskými koni (viz 10.4.1), proto přijetí opatření na ochranu proti trojským koňům může výrazně snížit riziko zneužití skrytých kanálů.
Ochrana před neautorizovaným přístupem k síti (viz 11.4) spolu s politikou a postupy odrazujícími personál od zneužití síťových služeb (viz 15.1.5)

12.5.5 Programové vybavení vyvíjené externím dodavatelem

Opatření

Vývoj programového vybavení externím dodavatelem by měl být organizací dohlížen a monitorován.

Doporučení k realizaci

Když je vyvíjeno programové vybavení externím dodavatelem, měly by být zváženy následující body:
a) licenční ujednání, vlastnictví kódu a práv duševního vlastnictví (viz 15.1.2);
b) osvědčení kvality a správnosti provedených prací;
c) uložení zdrojového kódu u nezávislé třetí strany pro případ problémů externího dodavatele;
d) právo přístupu k vývoji pro audit kvality a správnosti provedené práce;
e) smluvní podmínky na kvalitu a zabezpečení kódu;
f) testování na odhalení trojských koní a škodlivých kódů před instalací.

12.6 Řízení technických zranitelností

Cíl: Snížit rizika vyplývající ze zneužití veřejně publikovaných technických zranitelností.
Řízení (správa) technických zranitelností by mělo být zavedeno efektivním, systematickým a opakovatelným způsobem, s využitím metrik pro ověření její účinnosti. Toto by mělo zahrnovat všechny operační systémy a použité programové vybavení.

12.6.1 Řízení, správa a kontrola technických zranitelností

Opatření

Mělo by být zajištěno včasné získání informace o existenci technické zranitelnosti v provozovaném informačním systému, vyhodnocena úroveň ohrožení organizace vůči této zranitelnosti a přijata příslušná opatření na pokrytí souvisejících rizik.

Doporučení k realizaci

Aktuální a kompletní evidence aktiv (viz. 7.1) je nezbytným předpokladem pro účinné řízení technických zranitelností. Informace potřebné pro podporu řízení technických zranitelností zahrnují dodavatele programového vybavení (pro operační systémy i aplikace), číslo verze, aktuální stav nasazení (např. který SW je instalován na jakých počítačových systémech) a osoby odpovědné za dané programové vybavení.
Měly by být prováděny přiměřené a včasné kroky pro nalezení potenciálních technických zranitelností. Pro vytvoření účinného procesu řízení (správy) technických zranitelností by měla být realizována následující doporučení :
a) organizace by měla definovat a vytvořit role a odpovědnosti související s řízením technických zranitelností, které by měly zahrnovat sledování zranitelností, hodnocení rizik zranitelností, záplatování (instalace opravných balíčků), sledování a evidenci aktiv a další potřebné koordinační odpovědnosti;

b) měly by být nalezeny a evidovány informační zdroje pro identifikaci odpovídajících technických zranitelností používaného programového vybavení a další technologie (v závislosti na evidenci aktiv viz. 7.1.1); tyto informační zdroje by měl být aktualizovány v závislosti na změnách v evidenci nebo v případě nálezu nových a užitečných zdrojů;
c) měl by být definován časový harmonogram pro sled činností reagujících na hlášení o zjištěných potencionálních technických zranitelnostech;
d) jakmile je zjištěna potencionální technická zranitelnost měla by organizace ohodnotit související rizika a provést nápravná opatření; taková opatření mohou zahrnovat záplatování (instalaci opravných balíčků) nebo případně další aktivity;
e) v závislosti na tom, jak naléhavě musí být technická zranitelnost řešena, musí být vybrána následná akce s přihlédnutím na postupy řízení změn (viz. 12.5.1) nebo v závislosti na postupu pro zvládání bezpečnostních incidentů (viz. 13.2);
f) jestliže je dostupná záplata (opravný programový balíček), mělo by být ohodnoceno riziko spojené s její instalací (mělo by být porovnáno riziko související s neošetřenou zranitelností s rizikem instalace opravné záplaty);
g) záplaty (opravné programové balíčky) by měly být otestovány a vyhodnoceny před jejich instalací, aby se ověřila jejich účinnost a existence nežádoucích vedlejších efektů; pokud záplaty (opravné programové balíčky) nejsou dostupné, měla by být zváženy další opatření, jako například:
1. vypnutí (znepřístupnění) služeb nebo vlastností (funkcí, parametrů, práv) umožňujících využitelnost zranitelnosti;
2. přizpůsobení nebo přidání opatření pro omezení přístupových práv (např. firewallu) na hranici sítě (viz. 11.4.5);
3. zvýšení monitorování pro detekci nebo ochranu před samotnými útoky;
4. zvýšení informovanosti o dané zranitelnosti;
h) uchovat záznamy o všech provedených procedurách;
i) proces řízení technických zranitelností by měl být pravidelně sledován a vyhodnocován aby byla zajištěna jeho účinnost a efektivita;
j) systémy s vysokým rizikem by měly být řešeny nejdříve.

Další informace

Správná funkčnost procesu řízení (správy) technických zranitelností je kritická pro mnoho organizací a proto by měla být pravidelně sledována. Pro identifikaci všech potencionálních technických zranitelností, souvisejících s použitými technologiemi je nezbytná přesná evidence. Řízení technických zranitelností může být vnímáno jako součást procesu řízení změn a jako takové může využít jeho vlastností a postupů (viz. 10.1.2 a 12.5.1).

Na dodavatele je často vyvíjen významný tlak, aby uvolňovali záplaty (opravné programové balíčky) pro své produkty co nejdříve. Proto se stává, že některé záplaty (opravné programové balíčky) neřeší správně problém a mohou obsahovat nežádoucí vedlejší efekty. V některých případech se může také stát, že odinstalování záplaty poté co byla nainstalována nelze bez problémů provést.

Pokud není možné záplaty (opravné programové balíčky) náležitě otestovat (například z nedostatku zdrojů), je nutno zvážit odložení jejich instalace do doby, kdy budou známy a vyhodnoceny zkušenosti ostatních uživatelů s jejich instalací.

13 Zvládání bezpečnostních incidentů

13.1 Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

Měly by být ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a slabiny by měli zaměstnanci ihned hlásit na určené místo.

13.1.1 Hlášení bezpečnostních událostí

Opatření

Bezpečnostní události by měly být hlášeny příslušnými řídícími cestami tak rychle, jak je to jen možné.

Doporučení k realizaci

Pro hlášení bezpečnostní události by měl být vytvořen formalizovaný postup, včetně postupu reakce na incidenty a jejich eskalace (zvýšení stupně důležitosti), definující činnosti, které by měly být po přijetí hlášení provedeny. Pro hlášení bezpečnostních událostí by mělo být zřízeno kontaktní místo.

Kontaktní místo by mělo být známo všem zaměstnancům organizace, mělo by být vždy k dispozici a mělo by vždy zajistit přiměřenou a včasnou reakci.

Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli být seznámeni s povinností hlásit bezpečnostní události tak rychle, jak je to jen možné. Měli by také znát postupy a kontaktní místo pro hlášení bezpečnostních událostí. Postupy hlášení by měly zahrnovat:
a) vytvoření procesu zajišťujícího přiměřenou zpětnou vazbu, aby ten, kdo nahlásí incident, byl informován o výsledcích vyšetřování incidentu a jeho uzavření;
b) formuláře podporující proces hlášení bezpečnostních událostí a zároveň zajišťující, že hlášení bude splňovat veškeré nezbytné kroky (napomáhající osobě, která incident hlásí, provést všechny nezbytné kroky);
c) nastavení správného chování v případě bezpečnostní události, např.
1. okamžité zaznamenání všech důležitých detailů (např. typ nesouladu nebo narušení, chybné fungování, hlášky na obrazovce, podivné chování);
2. za žádných okolností neprověřovat bezpečnostní události, ale okamžitě je hlásit na určené místo;

d) odkaz na zavedená formalizovaná pravidla pro disciplinární řízení se zaměstnanci, smluvními stranami nebo uživateli třetích stran, kteří způsobili narušení bezpečnosti.

V místech s vysokým rizikem by pro uživatele, kteří by se mohli stát cílem donucování, měla být zvážena možnost vyvolání poplachu pod nátlakem26. Postupy reakce na poplach vyvolaný pod nátlakem by měly reflektovat rizikovost nastalé situace.

Další informace

Některé příklady bezpečnostních událostí a incidentů jsou:

a) ztráta služby, zařízení nebo vybavení;

b) chybné fungování nebo přetížení systému;

c) lidské chyby;

d) nesoulad s politikami nebo směrnicemi;

e) porušení opatření fyzické bezpečnosti;

f) nekontrolované změny systému;

g) chybné fungování technického a programového vybavení;

h) porušení přístupu.

Tyto incidenty mohou být, při dodržením důvěrnosti, použity při školeních uživatelů jako příklady toho, co se může stát, jak na to reagovat a jak takovým bezpečnostním incidentům v budoucnu předcházet (viz také 8.2.2). Pro správnou identifikaci bezpečnostní události je nezbytné co možná nejdříve po výskytu události zajistit důkazy (viz 13.2.3).

Jakékoliv chybné a nebo jiné neobvyklé chování systému může být příznakem pokusu o narušení nebo útoku na bezpečnost a mělo by tedy vždy být hlášeno jako bezpečnostní událost.

Detailnější informace o hlášení bezpečnostních událostí a zvládání bezpečnostních incidentů podává norma ISO/IEC TR 18044.

13.1.2 Hlášení bezpečnostních slabin

Opatření

Všichni zaměstnanci, smluvní strany a další nespecifikovaní uživatelé informačního systému a služeb by měli být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.

Doporučení k realizaci

Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli tyto skutečnosti hlásit svým nadřízeným nebo přímo poskytovateli služeb a to tak rychle, jak je to jen možné, aby se zamezilo vzniku bezpečnostního incidentu. Postup hlášení by měl být jednoduchý, přístupný a kdykoliv dostupný. Uživatelé by měli být informováni o tom, že nesmí za žádných okolností podezřelé slabiny prověřovat.

Další informace

Zaměstnancům, smluvním stranám a uživatelům třetích stran by mělo být doporučeno, aby se nepokoušeli podezřelé slabiny sami prověřovat. Testování bezpečnostních slabin může být interpretováno jako potenciální zneužití systému. Mimo to může testování slabin také způsobit narušení informačního sytému nebo služby a vyústit až v podniknutí příslušných právních kroků proti osobě, která testování provedla.

13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

Pro účinné zvládání bezpečnostních útoků a slabin by měly být stanoveny odpovědnosti a zavedeny formalizované postupy umožňující okamžitou reakci. Měl by být nastaven proces neustálého zlepšování reakce, monitorování, vyhodnocování a celkového zvládání bezpečnostních incidentů.

Pro zajištění souladu s právními požadavky by v případech, kdy je to vyžadováno, měly být shromážděny důkazy.

13.2.1 Odpovědnosti a postupy

Opatření

Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty by měly být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.

Doporučení k realizaci

Kromě hlášení bezpečnostních událostí a slabin (viz 13.1) by pro detekci bezpečnostních incidentů mělo být praktikováno monitorování systému, sledování varovných signálů a zranitelností (10.10.2).

V úvahu by měla být vzata následující doporučení:

a) Postupy by měly pokrývat všechny možné typy bezpečnostních incidentů, včetně:

1) selhání systému a ztráty služby;

2) škodlivého kódu (viz 10.4.1);

3) odepření poskytnutí služby;

4) chyby, které jsou důsledkem nekompletních nebo nepřesných vstupních dat;

5) porušení důvěrnosti a integrity;

6) zneužití informačních systémů.

b) Vedle běžných plánů kontinuity (viz 14.1.3) by postupy měly také zahrnovat (viz 13.2.2.):

1) analýzu a identifikaci příčiny incidentu;

2) kontrolu incidentu;

3) plánování a implementaci opravných prostředků, aby se zabránilo opakováni incidentu;

4) komunikaci s těmi, kteří byli ovlivněni incidentem nebo kteří se podílejí na zotavení se z něj;

5) hlášení určenému subjektu.

c) Soubor auditních záznamů a podobné důkazy je vhodné zajistit (viz 13.2.3) a adekvátním způsobem zabezpečit, aby bylo možno:

1) analyzovat vnitřní problémy;
2) použít je jako forenzních důkazu v souvislosti s možným porušením smlouvy nebo porušením regulatorních požadavků nebo pro případ občansko-právního či trestněprávního řízení podle odpovídající legislativy pro zneužití počítačů nebo podle zákona o ochraně osobních údajů;
3) použít je při jednání o náhradě škody s dodavateli programového vybavení a služeb.

d) Činnosti při opravách selhání systému a zotavení se z narušení bezpečnosti by měly být pečlivě a formálně kontrolovány. Postupy by měly zajišťovat, aby:
1) přístup do systému a k datům byl umožněn pouze na základě jednoznačné identifikace a autorizace pracovníků (viz také 6.2 pro přístup třetích stran);
2) všechny činnosti při mimořádné události byly detailně dokumentovány;
3) činnosti při mimořádné události byly hlášeny vedení organizace a systematicky kontrolovány;
4) integrita systémů organizace a opatření byla potvrzena s minimálním prodlením.

Postupy zvládání bezpečnostních incidentů by měly být odsouhlaseny vedením a mělo by být zajištěno, aby zodpovědné osoby byly obeznámeny s nastavenými prioritami pro zvládání bezpečnostních incidentů.

Další informace

Bezpečnostní incidenty mohou svým dopadem překročit hranice organizace či dokonce státu. Pro správnou reakci na tyto incidenty je třeba sladit odezvu a umožnit výměnu informaci o těchto incidentech s externě spolupracujícími organizacemi podle aktuální potřeby.

13.2.2 Ponaučení z bezpečnostních incidentů

Opatření

Měly by existovat mechanizmy, které by umožňovaly kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů.

Doporučení k realizaci

Informace získané při vyhodnocení bezpečnostních incidentů by měly být využity pro identifikaci opakujících se incidentů nebo incidentů s velkými následky.

Další informace

Závěry z vyhodnocení bezpečnostních incidentů mohou také signalizovat potřebu využití dodatečných nebo důkladnějších opatření, která by omezila frekvenci, škody a náklady jejich budoucích výskytů. Kromě toho by měly být vzaty v úvahu při revizi bezpečnostní politiky (viz 5.1.2).

13.2.3 Shromaždování důkazů

Opatření

V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (dle práva občanského nebo trestního) vůči osobě a nebo organizaci, by měly být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat.

Doporučení k realizaci

Měly by být vytvořeny a do praxe zavedeny interní směrnice pro sběr a předkládání důkazů pro podporu interního disciplinárního řízení.

Obecně tato pravidla zahrnují:
a) přípustnost důkazu: zda může či nemůže být důkaz použit u soudu;
b) důkazní síla: kvalita a kompletnost důkazu;

Organizace by měly pro dosažení přípustnosti důkazů zajistit, že jejich informační systémy odpovídají publikovaným normám nebo praktickým doporučením pro vytvoření přípustných důkazů.

Váha předloženého důkazního materiálu by měla odpovídat všem platným požadavkům. Aby měly předkládané důkazy požadovanou váhu, musí být doložena kvalita a kompletnost postupů zajišťující korektnost a konzistenci jejich sběru, ukládání a zpracování. Obecně lze těchto přísně definovaných postupů dosáhnout při splnění následujících podmínek:
a) pro papírové dokumenty: originál je uchováván bezpečně a je pořizován záznam o tom, kdo jej nalezl, kde byl nalezen, kdy byl nalezen, kdo dosvědčí jeho nález. Případné šetření by mělo potvrdit, že originály nebyly falšovány;
b) pro informace na počítačových médiích: pro zajištění dostupnosti by měly být pořízeny kopie nebo obrazy (dle aktuálních požadavků) všech výměnných médií, informací na pevných discích nebo v paměti počítače. Měl by být uchovány logy o všech činnostech v průběhu kopírování a proces by měl být svědecky doložitelný. Jedna kopie médií a protokolu (nejlépe přímo originály) by měly být bezpečně uchovány.

Jakákoliv forenzní zkoumání by měla být prováděna zásadně na kopiích důkazního materiálu. Vždy by měla být zajištěna integrita důkazního materiálu. Kopírování důkazního materiálu by mělo být prováděno pod dohledem důvěryhodného svědka. Měly by být vytvořeny záznamy o tom, kdy a kde byla kopie vytvořena, kdo kopírování prováděl a jaké nástroje a programy byly pro vytvoření kopií použity.

Další informace

Když je bezpečnostní událost poprvé zjištěna, nemusí být ještě zřejmé, jestli povede k soudnímu sporu. Existuje proto nebezpečí, že potřebné důkazy budou náhodně a nebo záměrně zničeny ještě před tím, než se projeví závažnost tohoto incidentu. Je proto vhodné při každém záměru učinit právní kroky, kontaktovat včas právníka nebo policii a nechat si poradit o nezbytných důkazech.

Sběr důkazního materiálu může přesáhnout hranice organizace a/nebo jurisdikce. V takovýchto případech by mělo být zajištěno, aby byla organizace oprávněna požadovaný důkazní materiál sbírat. Pro zvýšení šancí na přijetí důkazního materiálu soudem, by měly být do úvahy vzaty požadavky příslušné soudní jurisdikce, u které bude případ projednáván.

14 Řízení kontinuity činností organizace

14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Cíl: Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit jejich včasnou obnovu.

Pro minimalizaci následků a zotavení se ze ztráty informačních aktiv (které může být např. výsledkem přírodních pohrom, nehod, chyb zařízení a úmyslného jednání) na přijatelnou úroveň, za pomoci preventivních a zotavovacích opatření, by měl být zaveden proces řízení kontinuity činností organizace. Tento proces by měl identifikovat kritické činnosti organizace a začlenit požadavky řízení bezpečnosti informací s ohledem na požadavky provozní, personální, materiální, dopravní a požadavků na zařízení.

Důsledky pohrom, bezpečnostních chyb a ztráty/dostupnosti služeb by měly být identifikovány v rámci analýzy dopadů. Pro zajištění toho, aby mohly být obnoveny klíčové činnost organizace v požadovaných lhůtách, je vhodné připravit a implementovat plány kontinuity. Bezpečnost informací by se měla stát nedílnou součástí procesu řízení kontinuity činností a dalších řídících procesů v rámci organizace.

Řízení kontinuity činností organizace by mělo zahrnovat opatření k identifikaci a minimalizaci rizik, omezovat důsledky škodlivých incidentů a zajistit včasnou dostupnost informací potřebných pro obnovení nezbytných činností.

14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace

Opatření

V rámci organizace by měl existovat řízený proces pro rozvoj a udržování kontinuity činností organizace.

Doporučení k realizaci

Proces by měl v sobě zahrnovat následující klíčové prvky řízení kontinuity činností organizace:

c) pochopení rizik, kterým organizace čelí z hlediska jejich pravděpodobnosti a dopadu, včetně identifikace a stanovení priority kritických procesů organizace (viz 14.1.2);

d) identifikace všech aktiv, které jsou součástí kritických procesů organizace (viz 7.1.1);

e) pochopení dopadů, které může přerušení mít na činnosti organizace (je důležité, aby byla nalezena taková řešení, která pokryjí malé, stejně tak jako velké incidenty ohrožující životaschopnost organizace), a stanovení cílů v oblasti zařízení pro zpracování informací;

f) zvážení možnosti uzavření pojistky, která může tvořit součást celého procesu zajištění kontinuity činností a řízené provozních rizik;

g) identifikace a zvážení implementace dodatečných preventivních a nápravných opatření;

h) identifikace dostatečných finančních, organizačních, technických a okolních zdrojů na pokrytí identifikovaných požadavků na bezpečnost informací;

i) zajištění bezpečnosti personálu, ochrany majetku organizace a ochrany zařízení na zpracování informací;

j) formulace a dokumentace plánů kontinuity činností, pokrývajících požadavky na bezpečnost informací a v souladu s odsouhlasenou strategií řízení kontinuity činností organizace (viz 14.1.3);

k) zavedení pravidelného testování a aktualizace plánů a postupů (viz 14.1.5);

l) zajištění, aby řízení kontinuity činností organizace bylo součástí procesů a struktury organizace. Odpovědnost za proces koordinace řízení kontinuity by měla být v rámci organizace stanovena na odpovídající úrovni (viz 6.1.1).

14.1.2 Kontinuita činností organizace a hodnocení rizik

Opatření

Měly by být identifikovány možné příčiny přerušení činností organizace, včetně jejich pravděpodobnosti, velikosti dopadu a možných následků na bezpečnost informací.

Doporučení k realizaci

Kontinuita činností organizace z pohledu bezpečnosti informací, by měla být založena na identifikaci událostí (nebo sledu událostí), které mohou být příčinou přerušení procesů, např. chyba zařízení, povodeň, požár. Poté by mělo následovat hodnocení rizik, k určení pravděpodobnosti a velikosti dopadu těchto druhů přerušení jak z hlediska rozsahu škod, tak doby jejich obnovení.

Hodnocení rizik by mělo být prováděno za plného zapojení vlastníků zdrojů a vlastníků procesů organizace. Toto hodnocení by mělo zahrnout všechny procesy v organizaci a mělo by obsahovat výsledky týkající se bezpečnosti informací, nemělo by být omezeno pouze na zařízení pro zpracování informací. K získání celkového pohledu na požadavky kontinuity činností organizace je důležité dát dohromady jednotlivé aspekty rizika.

V závislosti na výsledcích hodnocení rizik by měla být vytvořena strategie stanovující celkový přístup k problému kontinuity činností organizace. Takto vytvořená strategie by měla být schválena vedením organizace a měl by být vytvořen a schválen plán její implementace.

14.1.3 Vytváření a implementace plánů kontinuity

Opatření

Pro udržení nebo obnovení provozních činností organizace po přerušení nebo selhání kritických procesů a pro zajištění dostupnosti informací v požadovaném čase a na požadovanou úroveň by měly být vytvořeny plány.

Doporučení k realizaci

V procesu plánování kontinuity činností organizace by mělo být zváženo:

a) určení a odsouhlasení všech odpovědností a postupů obnovy činností;

b) stanovení přijatelné úrovně pro ztrátu služeb nebo informací;

c) zavedení nouzových postupů tak, aby bylo možné dokončit zotavení a obnovu činností v požadovaných lhůtách. Zvláštní pozornost je třeba věnovat ohodnocení vnitřních

a vnějších závislostí organizace a existujícím smlouvám;
d) provozní postupy až do obnovení činností;
e) dokumentace odsouhlasených procedur a postupů;
f) vhodné proškolení personálu o odsouhlasených havarijních procedurách a postupech, včetně krizového řízení;
g) testování a aktualizace plánů.
Proces plánování by se měl soustředit na požadované cíle, např. obnovení specifických služeb zákazníkům v přijatelném časovém horizontu. Měly by být zváženy všechny služby a zdroje, kterých by se to mohlo týkat, včetně personálu, zdrojů nepředstavujících zařízení pro zpracování informací, jakož i možnosti nouzového zajištění náhradních prostředků pro zpracovávání informací. Zajištění náhradních prostředků může být řešeno formou dohody o reciproční výpomoci a nebo uzavřením komerční smlouvy.
Plány kontinuity činností organizace by měly pokrývat zjištěné zranitelnosti a proto také mohou obsahovat citlivé informace, které je potřebné vhodným způsobem chránit. Kopie plánu by tedy měly být ukládány na dostatečně vzdálených místech (záložní lokalita), aby nebyly zničeny v případě havárie v hlavní lokalitě. Vedení organizace by mělo zajistit pravidelnou aktualizaci plánů kontinuity a zajistit, aby úroveň jejich ochrany byla stejná jako v hlavní lokalitě. Veškeré další materiály potřebné pro spuštění činností obnovy dle plánů by měly být také dostupné v záložní lokalitě.
Úroveň zavedených bezpečnostních opatření v záložních lokalitách by měla být ekvivalentní úrovni bezpečnosti v hlavní lokalitě.
Další informace
Plány a činnosti krizového řízení nemusí být nutně shodné s činnostmi a plány řízení kontinuity, tj. krize může být zvládnuta běžnými řídícími postupy.

14.1.4 Systém plánování kontinuity činností organizace

Opatření
Pro zajištění konzistentnosti plánů a pro určení priorit testování a údržby by měl být k dispozici jednotný systém plánů kontinuity činností organizace.
Doporučení k realizaci
Každý plán by měl popisovat přístup k zajištění kontinuity činností organizace, např. zajištění dostupnosti a bezpečnosti informací a informačních systémů. Každý plán kontinuity by měl jasně specifikovat podmínky své aktivace, stejně jako osoby s odpovědností za vykonávání každého bodu plánu. Při vzniku nových požadavků by havarijní postupy, jako např. evakuační plány nebo jakékoliv existující dohody o zajištění náhradního provozu, měly být adekvátním způsobem doplněny. Revize postupů by měla být začleněna do programu řízení změn v organizaci, aby bylo zajištěno, že problematika kontinuity činností je vždy náležitě zajištěna.
Každý plán by měl mít stanoveného vlastníka. Havarijní postupy, plány manuálního náhradního provozu a plány na znovuobnovení činnosti by měly být v odpovědnosti vlastníků daných prostředků nebo vlastníků procesů organizace. Prostředky pro zajištění náhradních technických služeb, jako jsou zařízení pro zpracování a výměnu informací, jsou obvykle v odpovědnosti poskytovatelů servisních služeb.
Systém plánování kontinuity činností organizace by měl pokrývat identifikované požadavky na bezpečnost informací a měl by brát v úvahu následující:
a) podmínky aktivace plánů, které popisují návod jak postupovat (např. jak vyhodnotit situaci, kdo to provede atd.) než dojde k samotné aktivaci každého z plánů;
b) havarijní postupy, popisující činnosti, které by měly být provedeny po vzniku incidentu ohrožujícího činnosti organizace nebo lidské životy. Měly by zahrnovat části věnované vztahům s veřejností a efektivní spolupráci s odpovídajícími veřejnými institucemi, např. policií, hasiči a představiteli místní správy;
c) postupy obnovy popisující činnosti pro přesun důležitých aktivit organizace a dalších podpůrných služeb na náhradní dočasné místo a zajišťující obnovení činnosti organizace v požadované době;
d) dočasné provozní postupy až do doby obnovení činnosti;
e) postupy popisující způsob opětovného uvedení organizace do normálního provozu;
f) harmonogram údržby, určující jak a kdy bude plán testován, a proces aktualizace plánu;
g) vzdělávací aktivity a aktivity k zlepšení povědomí, zaměřené na pochopení procesů plánování kontinuity a pro zajištění jejich efektivního průběhu;
h) individuální odpovědnosti popisující kdo odpovídá za kterou složku plánu. Mohou být podle potřeby stanoveny alternativy;
i) kritická aktiva a zdroje potřebné pro zajištění havarijních postupů, náhradních provozů a postupů obnovení činnosti.

14.1.5 Testování, udržování a přezkoumání plánů kontinuity

Opatření
Plány kontinuity činností by měly být pravidelně testovány a aktualizovány, aby se zajistila jejich aktuálnost a efektivnost.
Doporučení k realizaci
Testy plánů kontinuity by měly zajistit, že všichni členové týmu obnovy i ostatní dotčení pracovníci mají plány v povědomí a jsou si vědomi svých odpovědností a rolí v případě aktivace plánu.
Harmonogram testů plánů kontinuity by měl stanovovat, jak a kdy by měl být každý prvek plánu testován. Jednotlivé komponenty plánu by měly být testovány v pravidelných intervalech.
Pro ověření, že plány budou fungovat i v reálném situaci, by měly být použity různé testovací techniky, které by měly zahrnovat:
a) ověření různých scénářů u stolu (přezkoumání a kritické rozebrání obsahu a realizovatelnosti plánu);
b) simulace (zejména pro nácvik rolí krizového řízení a činností následně po incidentu);

c) technické testy obnovy (prověření zda mohou být informační systémy efektivně obnoveny);
d) testy obnovení v náhradní lokalitě (paralelní provoz procesů organizace v záložní lokalitě);
e) testy externě zajišťovaných zařízení a služeb (prověření, že externě poskytované služby a produkty splňují smluvní závazky);
f) testy úplného přerušení (testování toho, že se organizace, personál, zařízení, prostředky a procesy mohou s přerušeními vypořádat).
Tyto techniky testování mohou být použity v libovolné organizaci s přihlédnutím k povaze specifických plánů obnovy. Výsledky testů by měly být zaznamenány a zjištěné nedostatky odstraněny.
Měla by být stanovena odpovědnost za provádění pravidelných revizí každého plánu kontinuity. Po změně podmínek v organizaci, které se ještě neodrazily v plánech kontinuity, by měla proběhnout odpovídající aktualizace těchto plánů. Tento formální změnový proces by měl prostřednictvím pravidelných kontrol celého plánu zajistit, že jsou aktualizované plány distribuovány a prosazovány.
Příklady situací, které si mohou vynutit aktualizaci plánů, zahrnují nákup nového zařízení nebo modernizaci provozního systému a změny:
a) ve složení personálu;
b) v adresách nebo telefonních číslech;
c) v celkové strategii organizace;
d) lokality, zařízení a zdrojů;
e) v legislativě;
f) smluvních partnerů, dodavatelů a klíčových zákazníků;
g) v procesech nebo v jejich vytvoření/zrušení;
h) rizicích (provozních a ekonomických).

15 Soulad s požadavky

15.1 Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.
Návrh, provoz a používání informačních systémů může být předmětem zákonných, podzákonných nebo smluvních bezpečnostních požadavků.
Specifické požadavky vyplývající ze zákona by měly být konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky. Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle jednotlivých zemí.

15.1.1 Určení relevantní legislativy

Opatření
Pro každý informační systém by měly být jednoznačně definovány, zdokumentovány a udržovány aktuální veškeré relevantní zákonné, podzákonné a smluvní požadavky a způsob jakým je organizace dodržuje.
Doporučení k realizaci
K těmto požadavkům by měla být stanovena a zdokumentována odpovídající specifická opatření a osobní odpovědnosti za prosazení jejich dodržování.

15.1.2 Zákony na ochranu duševního vlastnictví

Opatření
Pro zajištění souladu se zákonnými, podzákonnými a smluvními požadavky při použití předmětů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví by měly být zavedeny vhodné postupy.
Doporučení k realizaci
Na ochranu předmětů podléhajících zákonu na ochranu duševního vlastnictví by měla být zvážena následující doporučení:
a) vydání pravidel dodržování autorských práv, která přesně vymezují zákonné použití programových a informačních produktů;
b) získávání programové vybavení pouze od známých a ověřených dodavatelů;
c) udržování povědomí o pravidlech dodržování autorských práv a zdůrazňování disciplinárního řízení při jejich porušení;
d) udržování odpovídajícího registru aktiv a určení všech aktiv podléhajících zákonu na ochranu duševního vlastnictví;
e) vedení dokladů a důkazů vlastnictví licencí, instalačních disket, manuálů apod.;
f) zavedení vhodných opatření k tomu, aby nebyl překročen maximální počet uživatelských přístupů k programům;
g) vytvoření kontrolních mechanizmů, zajišťujících instalaci pouze schválených a licencovaných programových produktů;
h) vytvoření pravidel zajišťujících dodržování odpovídajících licenčních podmínek;
i) vytvoření pravidel pro rušení nebo převod licenčních práv;
j) používání vhodných auditních nástrojů;
k) dodržování požadavků a podmínek u programů a informací získaných z veřejných sítí;
l) zákaz vytváření duplikátů27, převádění do jiných formátů nebo extrahování komerčních záznamů (filmy, audio) pokud to není autorským právem povoleno;
m) zákaz kopírování celých nebo částí knih, článků, zpráv a dalších dokumentů, u kterých to není autorským právem povoleno.
Doporučení k realizaci
Zákony na ochranu duševního vlastnictví zahrnují autorské právo na programové vybavení a dokumenty, zákon o ochraně průmyslového vzoru, obchodních značek, patentů a licencí na zdrojové kódy.
Zákonem chráněné programové produkty jsou zpravidla dodávány na základě licenčních

ujednání, která například limitují jejich použití pouze na určené počítače a/nebo mohou omezovat jejich kopírování pouze na vytvoření záložních kopií. Personál by měl být seznámen s požadavky ochrany duševního vlastnictví vztahující se na programového vybavení vyvinutého organizací.

Zákonné, podzákonné a smluvní povinnosti mohou omezovat kopírování vlastnických materiálů. Zejména mohou požadovat, aby organizace používala pouze materiály organizací vyvinuté, k nimž má organizace licenci nebo které byly organizaci poskytnuty jejich autorem. Porušení autorských práv může vést k žalobě nebo k zahájení trestního stíhání.

15.1.3 Ochrana záznamů organizace

Opatření

Důležité záznamy organizace by měly být chráněny proti ztrátě, zničení a padělání a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.

Doporučení k realizaci

Záznamy by měly být kategorizovány podle druhů, např. účetní, databázové, transakční, a auditní záznamy, provozní postupy, každý s informacemi o době uchování a druhu záznamového média, např. papír, mikrofiše, magnetický nebo optický záznam. Všechny kryptografické klíče k zašifrovaným archivům, použité šifrovací programy a digitální podpisy (viz 12.3), by měly být bezpečně uchovány a v případě potřeby poskytnuty oprávněným osobám.

Pozornost by měla být věnována možnosti zhoršování stavu médií použitých pro uchování dokladů. Skladovací a manipulační postupy by měly být v souladu s doporučeními výrobce. Pro účely dlouhodobého skladování by mělo být zváženo použití papíru a mikrofišů.

Pokud jsou pro uchování používána elektronická média, měly by k nim být doplněny postupy pro přístup k datům (jak z hlediska čitelnosti médií, tak z hlediska formátu) v průběhu celé doby uchování, aby se zabránilo možným ztrátám způsobeným budoucími technologickými změnami. Archivní systémy by měly být vybrány tak, aby umožňovaly získat data v přijatelném časovém horizontu a v akceptovatelném datovém formátu, v závislosti na konkrétním požadavku.

Systém uchování a manipulace by měl zajistit jasnou identifikaci záznamů a dobu jejich uchování vyplývající ze zákonných či podzákonných norem. Po uplynutí této doby by měl systém umožnit odpovídající likvidaci záznamů, které již pro organizaci nejsou potřebné.

Pro splnění těchto povinností by měla organizace provést následující kroky:

a) měly by být vydány směrnice týkající se ukládání, uchovávání, zpracovávání a likvidace záznamů a informací;

b) měl by být vytvořen harmonogram uchovávání, který by identifikoval důležité typy dokladů a dobu jejich uchování;

c) měl by být udržován soupis zdrojů klíčových informací;

d) měla by být realizována vhodná opatření na ochranu důležitých dokladů a informací proti ztrátě, zničení a falzifikaci.

Další informace

U některých dokumentů může být požadováno, aby byly bezpečně uchovávány pro splnění zákonných či podzákonných norem a pro podporu důležitých činností organizace. Příkladem těchto dokladů jsou takové doklady, které mohou být použity jako důkaz toho, že organizace vyvíjí činnost v souladu se zákonnými a podzákonnými normami, nebo pro zajištění odpovídající ochrany proti potenciálním občansko-právním či trestně-právním žalobám a nebo k potvrzení finančního stavu organizace určenému vlastníkům, partnerům a auditorům. Doba uchování a obsah uchovávaných informací mohou být stanoveny zákonem nebo předpisem.

Další informace o tom jak spravovat záznamy organizace lze nalézt v normě ISO 15489-128.

15.1.4 Ochrana osobních údajů a soukromí

Opatření

Ochrana osobních údajů a soukromí by měla být zajištěna v souladu s odpovídající legislativou, předpisy, a pokud je to relevantní, se smlouvami.

Doporučení k realizaci

Organizace by měla vytvořit a do praxe zavést pravidla na ochranu osobních údajů a soukromí. S pravidly by měly být seznámeny všechny osoby, které se nějakým způsobem podílejí na zpracování osobních údajů.

Soulad s těmito pravidly a legislativou na ochranu osobních údajů29 vyžaduje odpovídající řídící struktury a kontrolu. Často toho lze nejlépe dosáhnout určením odpovědné osoby, např. manažera ochrany osobních údajů, který by měl poskytovat doporučení vedoucím pracovníkům, uživatelům a servisním organizacím o tom, jaká je jejich individuální odpovědnost a jaké specifické postupy by měli dodržovat. Odpovědnost za manipulaci s osobními údaji a prosazení povědomí o principech ochrany osobních dat stanovených odpovídající legislativou leží na vlastníkovi dat. Na ochranu osobních údajů by měly být zavedeny vhodná technická a organizační opatření.

Další informace

V mnoha zemích existuje legislativa zavádějící opatření pro sběr, zpracování a přenos osobních dat (obecně informace o žijících osobách, které mohou být podle těchto dat identifikovány). V závislosti na příslušné národní legislativě, tato opatření mohou ukládat povinnosti tomu, kdo tyto osobní informace sbírá, zpracovává a poskytuje, a mohou omezovat přenos těchto dat za hranice země.

15.1.5 Prevence zneužití zařízení pro zpracování informací

Opatření

Mělo by být zakázáno používat zařízení pro zpracování informací jiným než autorizovaným způsobem.

Doporučení k realizaci

Používání zařízení pro zpracování informací by mělo být autorizováno vedoucími zaměstnanci. Jakékoliv použití těchto prostředků pro jiné organizace nebo neoprávněné účely bez schválení vedoucími zaměstnanci (viz 6.1.4) by mělo být považováno za zneužití těchto prostředků. Pokud

je taková činnost zjištěna díky monitorování nebo jiným prostředkům, měly by informace o ní být předány konkrétnímu vedoucímu zaměstnanci odpovědnému za zahájení disciplinárního řízení.
Před zavedením monitorovacích postupů by měla být zajištěna právní konzultace.
Všichni uživatelé byli obeznámeni s přesným rozsahem svého přístupu a s existencí systému zaznamenávajícího neautorizované chování. Toho může být dosaženo například udělením písemné autorizace, jejíž kopie je podepsána uživatelem a bezpečně uchována organizací. Zaměstnancům organizace, smluvním stranám a uživatelů třetích stran by mělo být oznámeno, že není povolen žádný přístup s výjimkou toho, který je autorizován.
Při přihlášení by měla být na monitoru počítače zpráva, že prostředek pro zpracování informací je vlastněn organizací a neautorizovaný přístup není povolen. Uživatel musí zprávu na monitoru potvrdit a pro pokračování v přihlášení reagovat odpovídajícím způsobem (viz 11.5.1).
Další informace
Zařízení pro zpracování informací jsou primárně nebo výhradně určena pro účely organizace, která je vlastní.
Nástroje pro detekci narušení, kontroly obsahu a další monitorovací nástroje mohou pomoci při prevenci a detekci zneužití zařízení pro zpracování informací.
Mnoho zemí má nebo připravuje legislativu na ochranu proti zneužití počítačů. Použití počítače pro neoprávněné účely může být považováno za trestný čin.
Legálnost použití monitoringu používání prostředků se v jednotlivých zemích liší a může být vyžadováno předchozí upozornění zaměstnanců na takové monitorování či získání jejich souhlasu. Při přihlášení do veřejně přístupných systémů (např. veřejné servery) by se při přihlášení měla zobrazit hláška o tom, že podléhají monitorování.

15.1.6 Regulace kryptografických opatření

Opatření
Kryptografická opatření by měla být používána v souladu s příslušnými úmluvami, zákony a předpisy.
Doporučení k realizaci
Pro dosažení souladu s příslušnými úmluvami, zákony a předpisy by mělo být zváženo následující:
a) omezení importu a exportu počítačového technického a programového vybavení určeného k realizaci kryptografických funkcí;
b) omezení importu a exportu počítačového technického a programového vybavení navrženého tak, aby mohl být doplněn kryptografickými funkcemi;
c) omezení použití šifrování;
d) povinné či nepovinné metody přístupu státu k informacím zašifrovaným za pomoci technického či programového vybavení pro zajištění důvěrnosti jejich obsahu.
Pro zajištění souladu s místními právními úpravami by měla být vyhledána právní pomoc. Právní pomoc by měla být také vyhledána v případě přenosu šifrovaných informací nebo kryptografických prostředků do zahraničí.

15.2 Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.
Bezpečnost informačních systémů by měla být pravidelně přezkoumávána.
Tato přezkoumání by měla být prováděna proti příslušným bezpečnostním politikám. Jednotlivé technické platformy a informační systémy by měly být auditovány, zda odpovídají relevantním bezpečnostním normám a opatřením.

15.2.1 Shoda s bezpečnostními politikami a normami

Opatření
Vedoucí zaměstnanci by měli zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami.
Doporučení k realizaci
Vedoucí zaměstnanci by měli pravidelně provádět přezkoumání souladu všech oblastí v rozsahu jejich odpovědností, aby bylo zajištěno, že jsou v souladu s bezpečnostní politikou a normami a ostatními požadavky na bezpečnost.
V přídě, že je při přezkoumání zjištěn nesoulad, měli by vedoucí zaměstnanci:
a) určit příčiny nesouladu;
b) vyhodnotit potřebu přijetí opatření k nápravě;
c) určit a implementovat nápravná opatření;
d) přezkoumat přijatá nápravná opatření.
Závěry z přezkoumání a přijatá nápravná opatření by měly být zaznamenány a záznamy uchovány. Vedoucí zaměstnanci by měli s výsledky přezkoumání seznámit osoby provádějící v organizaci nezávislá přezkoumání bezpečnosti (viz 6.1.8).
Další informace
Operativní monitorování použití systému je popsáno v 10.10.

15.2.2 Kontrola technické shody

Opatření
Informační systémy by měly být pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy.
Doporučení k realizaci
Kontrola technické shody může být prováděna manuálně (v případě potřeby s využitím vhodných programových nástrojů), zkušeným systémovým inženýrem nebo pomocí automatizovaného programového vybavení, které vytváří technickou zprávu pro následné vyhodnocení technickým odborníkem.
K penetračním testům a analýze zranitelností by se mělo přistupovat obezřetně, protože takovéto aktivity mohou vést k ohrožení bezpečnosti systému. Tyto testy by měly být plánovány, dokumentovány a měly by být opakovatelné.
Kontroly technické shody by měly být prováděny pouze kvalifikovanými, oprávněnými zaměstnanci nebo pod jejich dohledem.

Další informace

Kontrola technické shody zahrnuje přezkoumání provozního systému, aby bylo zajištěno, že technická a programová opatření jsou správně implementována. Tento typ kontroly souladu vyžaduje asistenci technického odborníka.

Kontrola shody obsahuje také například penetrační testy a analýzu zranitelností, které mohou být prováděny nezávislými experty sjednanými speciálně pro tento účel. Takovéto kontroly mohou být užitečné pro detekci zranitelností systému a pro prověření toho, jak účinná jsou opatření proti v prevenci neautorizovaného přístupu při existenci těchto zranitelností. Penetrační testování a analýzy zranitelností poskytují informaci o aktuálním stavu systému. Informace je omezena na ty části systému30, na kterých bylo penetrační testování prováděno. Penetrační testy a analýzy zranitelností nenahrazují analýzu rizik.

15.3 Hlediska auditu informačních systémů

Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do informačních systémů.

Měla by existovat opatření pro zajištění bezpečnosti provozního systému a nástrojů auditu v průběhu vlastního auditu.

Ochrana nástrojů auditu je nutná, aby byla zajištěna jejich integrita a předešlo se jejich zneužití.

15.3.1 Opatření k auditu informačních systémů

Opatření

Požadavky auditu a činnosti zahrnující kontrolu provozních systémů by měly být pečlivě naplánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace.

Doporučení k realizaci

Při auditu by měly být dodržovány následující doporučení:

a) požadavky auditu by měly být schváleny na příslušné úrovni vedení organizace;

b) rozsah kontrol by měl být schválen a kontrolován;

c) přístup k programům a datům by měl být omezen pouze na čtení;

d) další, jiný typ přístupu než pouze pro čtení by měl být povolen jen na samostatných kopiích souborů systému. Kopie souborů by po ukončení auditu měly být smazány a nebo, pokud je to vyžadováno, řádným způsobem chráněny;

e) zdroje k provádění kontrol by měly být explicitně identifikovány a měly by být dostupné;

f) požadavky na speciální nebo dodatečné zpracování by měly být identifikovány a odsouhlaseny;

g) veškerý přístup by měl být monitorován, evidován a měl by o něm být vytvořen referenční záznam; u kritických systémů by mělo být zváženo použití záznamů s časovou známkou;

h) všechny postupy, požadavky a odpovědnosti by měly být dokumentovány;

i) osoba/-y provádějící audit by měla být nezávislá na činnostech, jejichž audit provádí.

15.3.2 Ochrana nástrojů pro audit informačních systémů

Opatření

Přístup k nástrojům určeným pro audit informačních systémů by měl být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.

Doporučení k realizaci

Nástroje určené pro audit systému, aplikační programové vybavení nebo datové soubory, by měly být odděleny od vývojových a provozních systémů a neměly by být uchovávány na magnetických páskách nebo v uživatelských oblastech, pokud není zajištěna přiměřená úroveň jejich ochrany.

Další informace

V případech, kdy se auditu účastní zástupci třetích stran existuje riziko zneužití nástrojů pro audit systému a informací, ke kterým mají přístup. Mělo by být zváženo přijetí opatření (například okamžitá změna hesel prozrazených auditorovi) na pokrytí těchto rizik a následků, dalším příkladem mohou být opatření uvedená v kapitole 6.2.1 (hodnocení rizik) a 9.1.2 (omezení fyzického přístupu).

Index

A

R

Ř

S