MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 7
SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – ŘÍZENÍ KOMUNIKACÍ A ŘÍZENÍ PROVOZU

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

esf evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost | UNIVERZITA OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

- ✓Provozní postupy a odpovědnosti
- ✓Řízení dodávek služeb třetích stran
- ✓Plánování a přejímání informačních systémů
- ✓Ochrana proti škodlivým programům a mobilním kódům
- ✓Zálohování
- ✓Správa bezpečnosti sítě
- ✓Bezpečnost při zacházení s médii
- ✓Výměna informací
- ✓Služby elektronického obchodu
- ✓Monitorování
- ✓Závěr

Literatura

ČSN ISO/IEC 27000 Datum vydání : 1.5.2010

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Datum vydání : 1.10.2006

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

1. Provozní postupy a odpovědnosti

Cílem je 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.

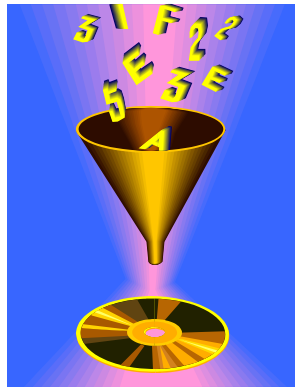
- **Dokumentace provozních postupů**
- **Řízení změn**
- **Oddělení povinností**
- **Oddělení vývoje, testování a provozu**

Dokumentace provozních postupů

Provozní postupy by měly obsahovat návod k podrobnému provedení každé činnosti, včetně:

- zpracování a zacházení s informacemi;
- zálohování dat;
- časové návaznosti zpracování;
- popis činnosti při výskytu chyb nebo jiných mimořádných stavů;
- spojení na kontaktní osoby v případě neočekávaných systémových nebo technických potíží;
- instrukce pro zacházení se speciálními výstupy;
- postupy při restartu systému a obnovovací postupy v případě selhání systému;
- zpracování záznamů z auditu a systémových záznamů.

Řízení změn



V úvahu by měla být zejména vzata následující opatření:

- identifikace a zaznamenání důležitých změn;
- plánování a testování změn;
- zhodnocení potenciálních dopadů takových změn;
- formální schvalovací postup pro navrhované změny;
- seznámení všech osob s podrobnostmi o změnách;
- postupy určující odpovědnosti za přerušení změnového zásahu a obnovení provozu v případě jejich neúspěchu.

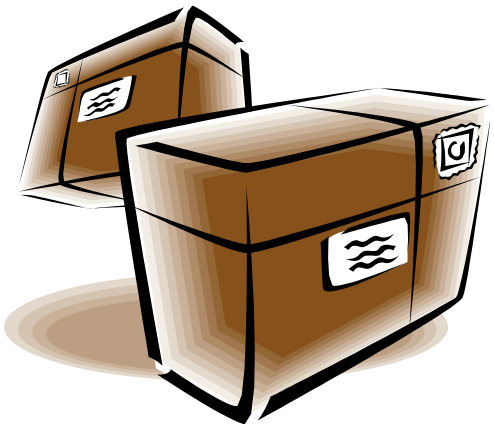
Nedostatečná kontrola změn v prostředcích pro zpracování informací a systémech je běžnou příčinou bezpečnostních a systémových chyb!!!

Oddělení povinností

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

Princip oddělení povinností minimalizuje riziko úmyslného nebo nedbalostního zneužití systému.

V malých organizacích může být tato metoda řízení obtížně použitelná, přesto by měl být tento princip v rámci možností aplikován.



Oddělení vývoje, testování a provozu

Vývoj a testování mohou způsobit vážné problémy, například nechtěnou modifikaci souborů, prostředí nebo způsobení systémové chyby.

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;

f) citlivá data by neměla být kopírována do testovacích systémů.

2. Řízení dodávek služeb třetích stran

Cílem je zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávaní služeb ve shodě s uzavřenými dohodami.

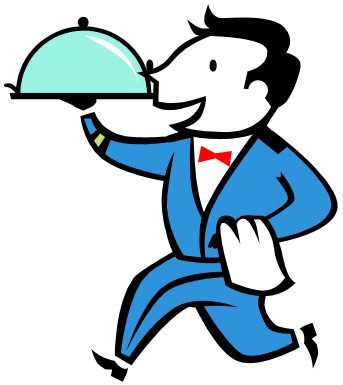
Pro zajištění toho, že služby dodávané třetími stranami jsou v souladu s dohodnutými požadavky, by organizace měla kontrolovat realizaci dohod, monitorovat míru souladu jejich dodržování a v případě potřeby zajistit nápravu.

- **Dodávky služeb**
- **Monitorování a přezkoumávání služeb třetích stran**
- **Řízení změn služeb poskytovaných třetími stranami**

Dodávky služeb

Cílem je zajistit, aby bezpečnostní opatření, definice a úroveň poskytovaných služeb, byly třetí stranou implementovány, provozovány a udržovány ve shodě s uzavřenými dohodami.

Součástí služeb poskytovaných třetí stranou by měla být realizace dohodnutých bezpečnostních opatření, vymezení služeb a jejich správy.



Monitorování a přezkoumávání služeb třetích stran

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:

a) monitorování úrovně poskytovaných služeb na dohodnuté úrovni;

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

c) poskytnutí informací o bezpečnostních incidentech a přezkoumání poskytnutých informací jak třetí stranou, tak organizací;

d) přezkoumání auditních záznamů týkajících se 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.

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

Řízení změn služeb poskytovaných třetími stranami

Proces řízení změn služeb poskytovaných třetí stranou by měl zohlednit:

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 postupů;

4)realizace nových opatření pro zvládání bezpečnostních 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)zavedení nových vývojových nástrojů a prostředí;

5)změny fyzického umístění servisních zařízení;

6)změny dodavatelů.

3. Plánování a přejímání informačních systémů

Cílem je minimalizovat riziko selhání informačních systémů.

Pro zajištění odpovídající kapacity, 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 dokumentovány a otestovány provozní požadavky.

- **Řízení kapacit**
- **Přejímání systémů**

Řízení kapacit

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

Pro každou stávající a plánovanou činnost by měly být identifikovány kapacitní požadavky.

Zvláštní pozornost by měla být věnována zdrojům, které vyžadují delší dobu pro realizaci dodávky nebo obnášejí vysoké náklady.

Přejímání systémů

Přechod na nové systémy, instalace aktualizací a zavádění nových verzí, by měl být formálně schválen.

Předtím, než je provedeno formální schválení, by mělo být 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;

g) potvrzení, že instalace nového systému nebude mít nepříznivý vliv na existující systémy;

h) školení v obsluze a použití nového systému.

4. Ochrana proti škodlivým programům a mobilním kódům

Cílem je chránit integritu programového vybavení a dat.

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

Programy a prostředky 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.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Opatření na ochranu proti škodlivým programům

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 například následující opatření:

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

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;

d)instalace a pravidelná aktualizace antivirových detekčních a opravných programů pro kontrolu počítačů a médií.

Opatření na ochranu proti mobilním kódům

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

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 opatření na jednotlivých systémech zajišťujících správu mobilních kódů;

e) kontrola všech prostředků využívajících mobilní kódy;

f) použití kryptografických opatření pro ověření původu mobilního kódu.

5. Zálohování

Cílem je udržovat integritu a dostupnost informací a prostředků pro jejich zpracování.

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

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

Zálohování informací

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 a frekvence s jakou jsou vytvářeny;

d)zálohy by měly být uloženy na bezpečném místě;

e)záložním informacím by měla být věnována přiměřená úroveň fyzické a vnější ochrany;

f)záložní média by měla být pravidelně testována;

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 důležité zajištění důvěrnosti zálohovaných informací, by mělo být použito šifrování.

6. Správa bezpečnosti sítě

Cílem je zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury.

Pozornost vyžaduje správa bezpečnosti počítačových sítí, které mohou přesahovat hranice organizace. Pro zabezpečení citlivých dat přenášených veřejnými sítěmi mohou být požadována dodatečná opatření.

Síťová opatření

Bezpečnost síťových služeb

Síťová 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.

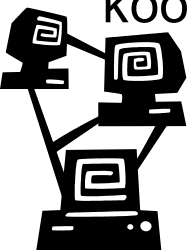
Opatření:

a)tam, kde je to vhodné, by měla být odpovědnost za provoz sítě oddělena od odpovědnosti za provoz počítačů;

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.

d)činnosti související se správou počítačů a sítí by měly být důkladně koordinovány.



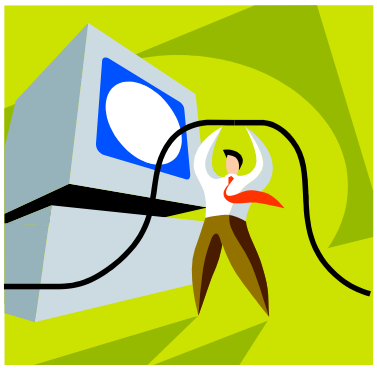
Bezpečnost síťových služeb

Bezpečnostní prvky síťových služeb mohou zahrnovat:

a)technologie použité pro zajištění bezpečnosti síťových služeb, 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.



7. Bezpečnost při zacházení s médii

Cílem je předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiva přerušení činností organizace.

Média by měla být kontrolována a fyzicky zabezpečena.

Měly by být stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií, vstupních /výstupních dat a systémové dokumentace před neoprávněným vyzrazením, modifikací, odstraněním nebo poškozením.

Správa výměnných počítačových médií

Pro správu vyměnitelných médií by měla být zvážena následující doporučení:

a)pokud již nejsou opakovaně použitelná 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 (podle 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 mechanik pro vyměnitelná média by mělo být povoleno jen v odůvodněných případech. Všechny postupy a úrovně oprávnění by měly být jednoznačně dokumentovány.

Likvidace médií

Zejména by měla být vzata v úvahu 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 média 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 médií obsahujících citlivé informace by měla být, podle možností, zaznamenávána pro potřeby následného auditu.

Postupy pro manipulaci s informacemi

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;

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.

Bezpečnost systémové dokumentace

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.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

8. Výměna informací

Cílem je 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.

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

9. Služby elektronického obchodu

Cílem je 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.

Elektronický obchod

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

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

Pro účely elektronického obchodu může být využito řady autentizačních metod.

On-line transakce

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

Pro zabezpečení on-line transakcí by mělo být zváženo následující:
a)použití elektronického podpisu všemi účastníky transakce;
b)všechny aspekty související s transakcí;
c)šifrování komunikace mezi zúčastněnými stranami;
d)zabezpečení protokolů použitých pro komunikaci;
e)zajištění toho, aby úložiště detailních informací o transakcích nebylo veřejně přístupné. Informace by neměly být uchovávány tak, aby byly volně přístupné z internetu;
f)tam kde je použito služeb důvěryhodné autority je bezpečnost součástí celého procesu správy certifikátu/podpisu.

Veřejně přístupné informace

Informace publikované na veřejně přístupných systémech by měly být chráněny proti neoprávněné modifikaci.

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. Monitorování

Cílem je 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.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Pořizování auditních záznamů

Auditní záznamy by měly hlavně obsahovat:

a) identifikátory uživatelů (uživatelská ID);

b) datum, čas a podrobnosti klíčových událostí, např. přihlášení a odhlášení;

c) záznam o úspěšných a odmítnutých pokusech o přístup k systému, k datům a jiným zdrojům;

d) změny konfigurace systému;

e) použití oprávnění;

f) použití systémových nástrojů a aplikací;

g) soubory, ke kterým bylo přistupováno, a typ přístupu;

h) sítě, ke kterým bylo přistupováno, a použité protokoly;

i) alarmy vyvolané systémy pro kontrolu přístupu;

j) aktivaci a deaktivaci ochranných systémů, jako jsou antivirové systémy a systémy pro detekci průniku.

Monitorování používání systému

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

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

a) neautorizovaný přístup,
b) všechny privilegované operace,
c) pokusy o neoprávněný přístup,
d) systémová varování nebo chyby,
e) změny nebo pokusy o změnu bezpečnostních opatření nastavení bezpečnosti systému.

Ochrana vytvořených záznamů

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

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

a) úpravy zaznamenávaných druhů zpráv;

b) editování nebo vymazání záznamů;

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

Systémové záznamy musí být dostatečně chráněny.

Administrátorský a operátorský deník

Aktivity správce systému a systémového operátora by měly být zaznamenávány.

Záznamy by měly obsahovat:

a) čas, kdy došlo k události;

b) podrobnosti o události nebo o chybách;

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

d) dotčené procesy.

Záznam selhání

Mělo by být zajištěno zaznamenávání selhání (poruch), pokud to systém umožňuje.

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 nebyla zneužita a prováděné činnosti byly schváleny.

Zaznamenávání selhání (poruch) a chyb může ovlivnit výkon systému.

Synchronizace hodin

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.

Správné nastavení počítačových hodin je důležité pro zajištění přesnosti auditních záznamů, které mohou být potřebné pro vyšetřování nebo jako důkaz při soudních či disciplinárních procesech.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ