MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 8
SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ - ŘÍZENÍ PŘÍSTUPU

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

1. Požadavky na řízení přístupu.
2. Politika řízení přístupu.
3. Řízení přístupu uživatelů.
4. Odpovědnosti uživatelů.
5. Řízení přístupu k síti.
6. Řízení přístupu k operačnímu systému.
7. Řízení přístupu k aplikacím a informacím.
8. Mobilní výpočetní zařízení a práce na dálku.
9. 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. Požadavky na řízení přístupu

Cílem je řídit přístup k informacím.

Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků.

Měla by být zohledněna pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

Politika řízení přístupu

Politika řízení přístupu by měla být **vytvořena**, **zdokumentována** a v závislosti na aktuálních bezpečnostních požadavcích **přezkoumávána**.

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**, 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

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;
c) pravidla pro šíření informací a pravidla schvalování;
d) konzistence přístupových pravidel a klasifikace informací pro různé systémy a sítě;
e) odpovídající legislativa a ostatní smluvní závazky;
f) standardní přístupové profily uživatelů pro běžné kategorie činností;
g) řízení pravidel přístupu v distribuovaném a síťovém prostředí;
h) oddělení jednotlivých rolí pro řízení přístupu;
i) požadavky na formální schválení žádostí o přístup;
j) požadavky na pravidelné přezkoumávání přístupových práv;
k) odebrání přístupových práv

2. Řízení přístupu uživatelů

Cílem je 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.

Registrace uživatele

Postup pro registraci uživatele a jejího zrušení by měl zahrnovat:

a) použití unikátního uživatelského identifikátoru (ID);
b) uživatel má oprávnění používat informační systém nebo služby od vlastníka systému;
c) úroveň přiděleného přístupu odpovídá záměrům organizace a že je shodná s bezpečnostní politikou organizace;
d) předání dokumentu vymezujícího přístupová práva uživatelům;
e) požadavek na uživatele, aby podepsali prohlášení;
f) udržování formálního záznamu o všech registrovaných osobách;
g) ihned odebrat přístupová práva uživatelům, kteří změnili pracovní místo nebo opustili organizaci;
h) pravidelně kontrolovat a odstranit již dále nepotřebné ID uživatelů;
i) nepotřebné ID uživatelů nepřidělovat jiným uživatelům.

Řízení privilegovaného přístupu

Ve víceuživatelských systémech by mělo být přidělování privilegovaných oprávnění řízeno prostřednictvím formálního autorizačního procesu. Měly by být zváženy následující kroky:

a) popsána privilegia spojená s každým prvkem systému a kategorie zaměstnanců, kterým by měla být přidělena;

b) privilegia by měla být přidělována jednotlivcům na základě jejich oprávněné potřeby a v souladu s politikou řízení přístupu;

c) měl by být dodržován proces autorizace a zachováván záznam všech přidělených privilegií;

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 nevyžadují oprávnění ke svému spuštění;

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

Správa uživatelských hesel

Přidělování hesel by mělo být řízeno formálním procesem a měl by vyhovovat následujícím požadavkům:

a) vyžadovat od uživatelů podpis prohlášení, že se zavazují udržovat přidělená hesla v tajnosti;

b) zajistit, aby v případě, že si uživatelé sami mění své heslo, dostali na počátku bezpečné jednorázové heslo;

c) zavést postupy jednoznačné identifikace uživatelů předtím, než jim je poskytnuto nové, náhradní nebo dočasné heslo;

d) dočasná hesla by měla být uživatelům sdělena bezpečným způsobem;

e) dočasně přidělená hesla by měla být jedinečná a neměla by být lehce uhodnutelná;

f) hesla by nikdy neměla být v počítači uložena v nechráněné podobě;

g) dodavateli přednastavená hesla by měla být ihned po instalaci systému nebo aplikačního programového vybavení změněna.

Přezkoumání přístupových práv uživatelů

Přezkoumání přístupových práv uživatelů by mělo zaručovat, že:

a) přístupová práva uživatelů jsou přezkoumávána v pravidelných intervalech (například interval 6 měsíců) a po každé změně;

b) při přeřazení na jinou pracovní pozici v rámci organizace by měla být stávající přístupová práva přezkoumána;

c) autorizace speciálních privilegovaných oprávnění 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.

3. Odpovědnosti uživatelů

Cílem je předcházet neoprávněnému uživatelskému přístupu, vyzrazení 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 řízení 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.

Používání hesel

Při výběru a používání hesel by mělo být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy:

a) hesla se udržují v tajnosti;
b) hesla nesmí být zaznamenána, 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 dostatečnou délku;
e) musí měnit hesla v pravidelných intervalech a vyhýbat se opakovanému použití nebo opakování původních hesel;
f) musí změnit dočasná hesla při prvním přihlášení;
g) nebudou sdílet osobní uživatelská hesla;
h) nebudou používat stejná hesla pro soukromé a pracovní účely.

Neobsluhovaná uživatelská zařízení

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 počítačů, serverů a kancelářských;

c) pokud se nepoužívají, zabezpečit PC nebo terminály pomocí uzamčení klávesnice nebo ekvivalentní kontroly, například přístupovým heslem.

Zásada prázdného stolu a prázdné obrazovky monitoru

V úvahu by měla být vzata následující opatření:

a) citlivé nebo kritické informace by měly být v případě, že se nepoužívají, a zejména když je kancelář prázdná, uzamčeny;

b) přihlášené osobní počítače, počítačové terminály, by neměly být ponechávány bez dozoru a měly by být chráněny klíčem, heslem nebo jinými opatřeními;

c) kopírky a další reprodukční zařízení by měly být v mimopracovní době uzamčeny;

d) dokumenty obsahující citlivé nebo klasifikované informace by měly být po vytištění okamžitě odebírány z tiskárny.

4. Řízení přístupu k síti

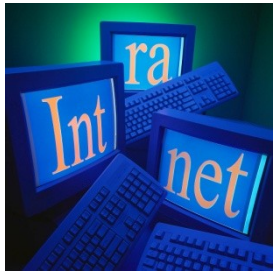
Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb.

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.



4. Řízení přístupu k síti

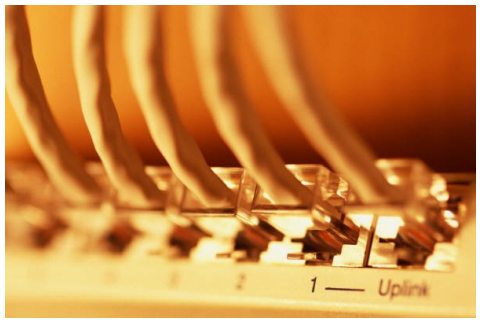
Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb.

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.



Politika užívání síťových služeb

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.

Politika užívání síťových služeb by měla být v souladu s politikou řízení přístupu .

Autentizace uživatele pro externí připojení

Autentizace vzdálených uživatelů může být zajištěna například použitím:

- kryptografických technik,
- autentizačních předmětů,
- protokolem typu výzva/odpověď.

Implementaci takovýchto technik například využívají virtuální privátní sítě (VPN).

Existují různé typy autentizačních metod.

Princip oddělení v sítích

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

Jedna z metod správy bezpečnosti velkých sítí je rozdělení sítí do separátních logických domén.

Sítě mohou být také odděleny s využitím funkčnosti síťových zařízení.

Mělo by se zvážit oddělení bezdrátových sítí od interních a privátních sítí.

Řízení síťových spojení

U sdílených sítí, zejména těch, které přesahují hranice organizace, by měly být omezeny možnosti připojení uživatelů.

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 se zvážit omezení přístupu k síti na určitou denní dobu nebo datum.

5. Řízení přístupu k operačnímu systému

Předcházet neautorizovanému přístupu k operačním systémům.

Pro omezení přístupu k operačním systémům pro oprávněné uživatele by měly být použity bezpečnostní prostředky:

- Bezpečné postupy přihlášení.
- Identifikace a autentizace uživatelů.
- Systém správy hesel.
- Použiti systémových nástrojů.
- Časové omezení.

Bezpečné postupy přihlášení

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

Příklad přihlašovacího postupu:

- nezobrazovat identifikátory systému nebo aplikace;
- zobrazovat obecné varování, že počítač smí používat pouze oprávnění uživatelé;
- neposkytovat nápovědu během přihlašovacího postupu;
- zkontrolovat platnost přihlašovacích informací;
- omezit počet povolených neúspěšných přihlašovacích pokusů;
- omezit minimální a maximální dobu povolenou pro přihlášení;
- nezobrazovat heslo při jeho zadávání anebo jej maskovat použitím zástupných symbolů;
- neposílat hesla přes síť v čitelné (nezašifrované) textové podobě.

Identifikace a autentizace uživatelů

Všichni uživatelé by měli mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID).

Uživatelská ID by měla umožňovat pozdější vysledování odpovědnosti konkrétních osob za činnosti v systému.

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

Systém správy hesel

Systém správy hesel by měl:

- prosazovat používání individuálních hesel a uživatelských ID pro zachování odpovědnosti;
- umožnit uživatelům volit a měnit si své vlastní heslo;
- prosazovat výběr kvalitních hesel;
- prosazovat obměnu hesel;
- donutit uživatele změnit si dočasně přidělené heslo při prvním přihlášení;
- udržovat záznam předchozích uživatelských hesel a zabránit uživatelům znovu je použít;
- při zadávání hesla nezobrazovat heslo na obrazovce;
- ukládat soubory hesel odděleně od dat aplikace;
- ukládat a přenášet hesla v chráněné podobě.

Časová omezení

Časové omezení relace

Neaktivní relace by se měly po stanovené době nečinnosti ukončit.

Implementace tohoto opatření je zejména důležitá ve vysoce rizikových oblastech.

Časové omezení spojení

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.

6. Řízení přístupu k aplikacím a informacím

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:

- kontrolovat přístup uživatelů k datům a funkcím;
- poskytovat ochranu před neoprávněným přístupem ke všem nástrojům a systémovým programům;
- nenarušit bezpečnost jiných systémů.

7. Mobilní výpočetní zařízení a práce na dálku

Zajistit bezpečnost informací při použití mobilní výpočetní techniky a 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.

Mobilní výpočetní zařízení

Při použití mobilních výpočetních prostředků, například notebooků, palmtopů, laptopů a mobilních telefonů, by měla být věnována zvláštní pozornost tomu, aby nebyly vyzrazeny informace organizace.

Měla by být přijata taková formální pravidla, která by zohledňovala riziko používání mobilního výpočetního zařízení, zejména v nezabezpečeném prostředí.

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

Práce na dálku

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

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.

ZÁVĚR

Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků.

Měla by být zohledněna pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

Dotazy?

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

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ