# MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

## TÉMA Č. 1
## SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – AKVIZICE, VÝVOJ A ÚDRŽBA IS

Ing. Petr HRŮZA, Ph.D.
Univerzita obrany
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)


INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

# OBSAH

- Základní pojmy
- Bezpečnostní požadavky informačních systémů
- Správné zpracování v aplikacích
- Kryptografická opatření
- Bezpečnost systémových souborů
- Bezpečnost procesů vývoje a podpory
- Řízení technických zranitelností
- 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.

# ZÁKLADNÍ POJMY

- Aktivum
- Riziko
- Hrozba
- Zranitelnost
- Informační systém

# Analýza a specifikace bezpečnostních požadavků

- Informační systémy se staly neoddělitelnou částí života společnosti.
- Hovoříme o **informační a znalostní** společnosti.
- Bezpečnost je neoddělitelnou součástí informačních systémů.

# Bezpečnostní požadavky informačních systémů

- Bezpečnost musí být řešena v následujících oblastech:
  - provozní systémy;
  - infrastruktura;
  - interní aplikace organizace;
  - zakoupené produkty;
  - služby;
  - uživatelsky vyvinuté aplikace.

# Bezpečnostní požadavky informačních systémů

**Analýza a specifikace bezpečnostních požadavků**

- Nastavení bezpečnostních požadavků a opatření by mělo odrážet hodnotu informačních aktiv pro samotnou organizaci.
- Analýza a aplikace bezpečnostních požadavků
  - Při budování či rozšiřování informačních systémů je nutné definovat také bezpečnostní požadavky.
  - Je vhodné vzít do úvahy začlenění kontrol do systému:
    - automatizované;
    - manuální.
  - Je zapotřebí testovat i zakoupené či vytvořené programové balíky.
- Vedení organizace může používat nezávisle certifikované a ohodnocené produkty po důkladném zvážení.

# Správné zpracování v aplikacích

Cílem je předcházet:

- chybám;
- ztrátě;
- neoprávněné modifikaci;
- zneužití informací.

Vhodné je začlenit kontroly do aplikačních systémů, které by měly zahrnovat potvrzení platnosti:

- vstupních dat;
- interního zpracování;
- výstupních dat.

# Správné zpracování v aplikacích

Vstupní data by měla být kontrolována z hlediska (validace vstupních dat):

- správnosti;
- adekvátnosti.

Můžeme uvažovat o použití následujících opatření:

- Zdvojený vstup nebo jiná kontrola např. specifikace rozsahu nebo definovaná pote dat pro detekování chyb.
- Pravidelná kontrola obsahu klíčových polí nebo datových souborů pro potvrzení jejich platnosti a integrity.
- Kontrola papírových vstupních dokumentů za účelem zjištění jakýchkoliv neoprávněných změn ve vstupních datech.
- Postupy při reakci na zjištěné chyby validace.
- Postupy pro testování věrohodnosti vstupních dat.
- Stanovení odpovědnosti všech zaměstnanců, účastnících se procesu vstupu dat.
- Vytvoření záznamu o činnostech , které jsou součástí procesu vstupu dat.

# Správné zpracování v aplikacích

## Kontrola vnitřního zpracování

- Pro detekci poškození informací při zpracování nebo úmyslnými zásahy by měly být začleněny kontroly validace dat do aplikace.
- Aplikace jež by měly zajistit minimalizaci rizika chyb při zpracování z hlediska integrity :
  - Použití funkcí vstupu, modifikace a mazání za účelem provedení změn v datech.
  - Postupy, které brání spouštění programů v nesprávném pořadí nebo zabraňují jejich spuštění po předchozím selhání.
  - Použití vhodných programů na zotavení se z chyb a pro zajištění správného zpracování dat.
  - Použití ochrany proti útoků přetečení bufferu.

# Správné zpracování v aplikacích

Integrita zpráv:

- Měly být stanoveny požadavky na zajištění integrity a autentizace zpráv.
- Nejvhodnější z hlediska zajištění integrity je provedení hodnocení rizik.
- Kryptografické metody jako vhodný prostředek pro autentizaci zpráv.

# Správné zpracování v aplikacích

## Validace výstupních dat

- Pro zajištění, že zpracování uložených informací je bezchybné a odpovídající, je nutné ověřit platnost výstupních dat.
- Výstupní kontrola může zahrnovat:
  - Prověrku věrohodnosti - ověření přijatelnosti výstupních dat.
  - Porovnávací kontrolní součet zajišťující , že byla zpracována všechny data.
  - Postupy reakce na výstupní testy planosti dat.
  - Určení odpovědnosti všech zaměstnanců, kteří jsou zainteresováni na vstupním procesu.
  - Vytvoření záznamu všech činností v rámci procesu ověření platnosti výstupních dat.

# Správné zpracování v aplikacích

Kryptografická opatření:

- Pomocí kryptografických prostředků bude organizace chránit **důvěrnost, autentičnost a integritu** informací.
- Je zapotřebí realizovat a zavést politiku pro používání kryptografických opatření s důrazem na ochranu informací.
- Na podporu používání kryptografických technik v organizaci by měl existovat systém jejich správy.

# Správné zpracování v aplikacích

Kryptografická opatření:

- Organizace by měla mít systém správy klíčů
- Všechny klíče by měly být chráněny před modifikací a zničením.
- Tajné a soukromé klíče  je nutno chránit proti vyzrazení.
- Prostředky fyzické ochrany by měly být použity pro zabezpečení prostředků určených k generování, ukládání a archivaci klíčů.

# Správné zpracování v aplikacích

Kryptografická opatření:

- Je nutno také zvážit ochranu veřejných klíčů.
- Autentizace veřejných klíčů se zpravidla řeší certifikáty veřejných klíčů, které jsou vydávány certifikační autoritou.
- Systém tajných klíčů.
- Systém veřejných klíčů.

# Bezpečnost systémových souborů

- Cílem je zajistit bezpečnost systémových souborů.
- Přístup k systémovým souborům a zdrojovým kódům programů by měl být řízen.
- Projekty a podpůrné činnosti by měly být prováděny bezpečným způsobem.
- Je vhodné přijmout opatření zabraňující vyzrazení citlivých informací v testovacím prostředí.

# Bezpečnost systémových souborů

Správa provozního programového vybavení

- Je nutno zavést postupy pro kontrolu instalace programového vybavení na provozních systémech.
- Můžeme uvažovat o realizaci opatření ke snížení rizika poškození provozních systémů:
  - Oprávněný správce provádí aktualizace provozního programového vybavení, aplikací knihoven.
  - Provozní systémy by měly obsahovat jen spustitelný kód.
  - Spustitelná od by neměl být implementován do provozního systému dřív než je doklad o úspěšném testování a převzetí uživatelem a jsou aktualizovány všechny zdrojové knihovny.
  - Systém kontroly konfigurace by měl být spuštěn pro přehled o instalovaném programovém vybavení a systémové dokumentaci.
  - Měla by být připravena strategie umožňující návrat do původního stavu.
  - Měly by být udržovány auditní záznamy všech aktualizací provozních programových knihoven.
  - Pro případ nouze by měly být uschovány předcházející verze programového vybavení.
  - Neaktuální verze programového vybavení by měly být archivovány spolu s požadovanými informacemi a parametry, konfiguracemi a podpůrnými programy po celou uchování dat v archivu.

# Bezpečnost systémových souborů

## Ochrana dat pro testování systému

- Data pro testování by měla být pečlivě:
  - vybrána;
  - chráněná;
  - kontrolovaná.
- Nevhodné je používat databáze s osobními či citlivými údaji.
- Pro ochranu provozních dat pro testování by měla být použita:
  - Postupy řízení přístupu, které se používají v aplikačních systémech.
  - Každé kopírování provozních informací do testovacího aplikačního systému by mělo být samostatně schváleno.
  - Provozní informace by měly být okamžitě po ukončení testů odstraněny.
  - Kopírování provozních informací by mělo být zaznamenáno do auditních záznamů.

# Bezpečnost systémových souborů

Řízení přístupu ke knihovně zdrojových kódů:

- Přístup ke knihovně zdrojových kódů by měl být omezen.
- Pro řízení přístupu do knihoven je možné zvážit následující doporučení snižující pravděpodobnost poškození počítačových programů:
  - Kde je to možné neukládat knihovny zdrojových kódů v provozních systémech.
  - Zdrojové kódy programů a knihovny zdrojových kódů by měly být spravovány v souladu se zavedenými postupy.
  - IT pracovníci by neměli mít neomezený přístup ke knihovnám zdrojových kódů.
  - Aktualizace knihoven programů a souvisejících položek a předávání zdrojových programů programátorům by mylo být prováděno po řádném schválení.
  - Výpisy z programu by měly být uloženy na bezpečném místě.
  - Všechny přístupy ke zdrojovým kódům my měly být zaznamenány do auditního záznamu.
  - Udržování a kopírování knihoven kódu programu by mělo být předmětem postupů změnového řízení.

# Bezpečnost procesů vývoje a podpory

- Je nezbytné udržovat bezpečnost programového vybavení a informací aplikačních systémů.
- Projektové a podpůrné prostředí pod přísnou kontrolou:
  - Vedoucí a správci odpovědní za aplikační systémy by měli mít odpovědnost za bezpečnost projektového a podpůrného prostředí
  - Tyto osoby zajistí podrobení se kontrole všech plánovaných změn s cílem nenarušit bezpečnost systému nebo provozního prostředí.

# Bezpečnost procesů vývoje a podpory

Postupy řízení změn:

- Zavedení formálních postupů řízení změn.
- Zavedení postupů je vhodné pro minimalizaci změn.
- Nutno je prosazovat a dokumentovat.
- Nové a významné změny je nutno testovat a provést kontrolu kvality programátoři mají přístup jen tam kde potřebují – pracují.
- Nutnost propojení aplikačních a provozních postupů řízení změn.

# Bezpečnost procesů vývoje a podpory

## Postupy řízení změn

- Propojení aplikačních a provozních postupů zahrnuje:
  - Udržování záznamu schválených stupňů oprávnění.
  - Zajištění vznešení požadavku oprávněným uživatelem.
  - Přezkoumání opatření a integrity postupů proto, aby v případě změn nedošlo ke kompromitaci.
  - Určení veškerého programového vybavení, informací, databázových entit a technického vybavení, které vyžaduje doplnění změny.
  - Formální schválení podrobných návrhů před zahájením práce.
  - Změny před prováděním akceptovány oprávněnými uživateli.
  - Systémová dokumentace aktualizovaná při ukončení každé změny a neaktuální dokumentace je archivována nebo zničena.
  - Udržování kontroly verzí u všech aktualizací programového vybavení.
  - V případě nutnosti jsou provedeny změny v provozní dokumentaci a uživatelských postupech jsou prováděny včas a není narušen proces organizace.

# Bezpečnost procesů vývoje a podpory

- Technická přezkoumání aplikací po změnách operačního systému:
  - Nutnost přezkoumat a otestovat kritické aplikace v případě změn v operačním systému.
  - Nutno zjistit zda nemají negativní dopad na provoz či bezpečnost organizace.
  - Konkrétní odpovědnost za sledování zranitelnosti.

# Bezpečnost procesů vývoje a podpory

- Omezení změn programových balíků:
  - Modifikace programových balíků by měly být omezeny na nezbytné změny a změny které musí být řízeny.
  - Všechny změny dokumentovat.
  - Pokud je to vyžadováno, změny by měly být nezávisle otestovány a potvrzeny.

# Bezpečnost procesů vývoje a podpory

- Únik informací:
  - Organizace by měla učinit veškerá dostupná opatření aby zabránila úniku informací.
  - Pozornost věnovat úniku informací cestou skrytých kanálů.
  - 100% ochrana **neexistuje**!!!

# Bezpečnost procesů vývoje a podpory

- Programové vybavení vyvíjené externím dodavatelem
  - Organizace by měla dohlížet a monitorovat vývoj programového vybavení externím dodavatelem.
  - Je zapotřebí zvážit:
    - Licenční ujednání, duševní vlastnictví a vlastnictví kódu.
    - Osvědčení kvality a správnosti provedených prací.
    - Uložení zdrojového kódu a nezávislé 3. strany pro případ problémů dodavatele.
    - Právo k přístupu k vývoji pro audit kvality a správnosti provedené práce.
    - Smluvní podmínky na kvalitu a zabezpečení kódu.
    - Testování na odhalení trojských koní a škodlivých kódů před instalací.

# Řízení technických zranitelností

- Snahou organizace je snížit rizika vyplývající z využívání zveřejněných technických zkušeností.
- Toto řízení by mělo být zavedeno:
  - efektivním;
  - systematickým;
  - opakovatelným způsobem;
  - s využitím metrik pro ověření účinnosti.
- Zahrnuje všechny operační systémy a programové vybavení.

# Řízení technických zranitelností

- Organizace by měla zajistit:
  - získání informací o existenci technických zranitelností v provozovaném informačním systému;
  - vyhodnotit úroveň ohrožení organizace vůči zjištěným zranitelnostem;
  - přijetí příslušných opatření na pokrytí rizik.
- Aktuální a kompletní evidence je předpoklad účinného řízení technických zranitelností.
- Informace pro toto řízení zahrnují i dodavatele programového vybavení, číslo verze, aktuální stav nasazení, odpovědné osoby za programové vybavení.
- Cílem je provádění včasných a přiměřených kroků pro nalezení technických zranitelností.

# Dotazy?

Ing. Petr HRŮZA, Ph.D.
Univerzita obrany
E-mail.: petr.hruza@unob.cz