MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 8
ŘÍZENÍ AKTIV KYBERNETICKÉ BEZPEČNOSTI

Ing. Oldřich LUŇÁČEK, Ph.D.
Univerzita obrany, Fakulta VT
Katedra 209
E-mail.: oldrich.lunacek@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

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.

OBSAH

- Základní pojmy
- Odpovědnost za aktiva
- Klasifikace informací

Základní pojmy

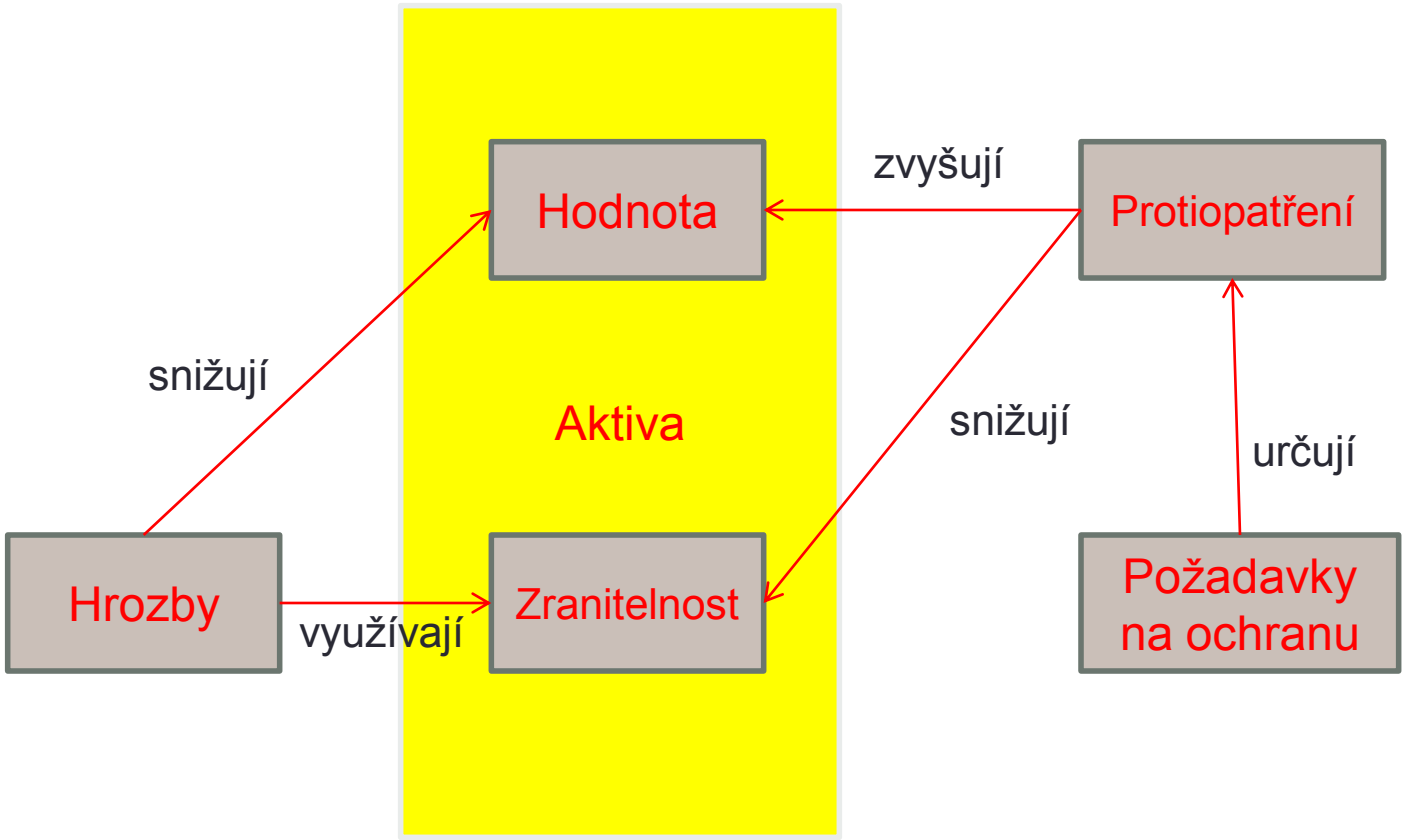
- **Aktivum** je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby a dělíme je na:
  - **hmotná** (například nemovitosti, cenné papíry, peníze apod.)
  - **nehmotná** (například informace, prestiž organizace, morálka pracovníků, kvalita personálu apod.).
- Aktivem ale může být sám subjekt, neboť hrozba může působit na celou jeho existenci.
- **Hrozba** je **síla, událost, aktivita nebo osoba**, která může **způsobit škodu**. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy.
- **Zranitelnost je nedostatek analyzovaného aktiva** (případně subjektu nebo jeho části), kterým může dojít k naplnění hrozby. Zranitelnost je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle následujících faktorů:
  - **citlivost** - náchylnost aktiva být poškozeno danou hrozbou;
  - **kritičnost** - důležitost aktiva pro analyzovaný subjekt.

Základní pojmy

- **Protiopatření je**
  - **postup,**
  - **proces,**
  - **procedura,**
  - **technický prostředek** nebo cokoliv, co je navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.
- Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.
- Protiopatření je charakterizováno efektivitou a náklady.

- **Bezpečnostní aspekty**:
  - Důvěrnost - k základním prvkům bezpečnosti mají přístup pouze oprávněné subjekty.
  - Autentičnost (integrita) - aktiva smí být modifikována pouze oprávněnými subjekty.
  - Dostupnost - musí být zajištěna dostupnost aktiv oprávněným subjektům.

Základní pojmy



Základní pojmy

- **bezpečnostní událost** (*information security event*)
- **bezpečnostní incident** (*information security incident*)
- **zbytkové riziko** *(residual risk)*
- **riziko** (*risk*)
- **akceptace rizika** *(risk acceptance)*
- **analýza rizik** (*risk analysis*)

Základní pojmy

- **hodnocení rizik** (*risk assessment*)
- **vyvarování se rizik** *(risk avoidance)*
- **seznámení s rizikem** *(risk communication)*
- **regulace rizik** *(risk control)*
- **měřítka rizik** *(risk criteria)*
- **hrozba** (*threat*)
- **zranitelnost** (*vulnerability*)

Identifikace aktiv

- Aktivum je něco, co má hodnotu nebo je jinak užitečné pro organizaci, provozní činnosti organizace a jejich kontinuitu.
- Řádná správa aktiv a odpovědnost za ně je pro organizaci zásadní a měla by být hlavním úkolem na všech úrovních řízení.
- Je nutné jasně identifikovat a přiměřeně ocenit důležitá aktiva a zhotovit a udržovat evidenci aktiv.
- Seskupení podobných nebo příbuzných aktiv do souborů (skupin), snižuje míru úsilí potřebného k procesu hodnocení rizik.

Identifikace aktiv

- Odpovědnost za aktiva pomáhá udržovat přiměřenou bezpečnost informací.
- Každé jednotlivé aktivum nebo skupina aktiv musí mít jednoznačně určeného vlastníka a odpovědnost za provádění bezpečnostních opatření by měla být připsána právě vlastníkovi.
- Odpovědnost za zavádění bezpečnostních opatření je možné přenést, ale odpovědnost za aktiva by měla zůstat vlastníkovi aktiv.

Identifikace aktiv

- Vlastník aktiv by měl odpovídat za:
  - stanovení vhodné bezpečnostní klasifikace a přístupových práv k aktivu,
  - učinit a zdokumentovat tato rozhodnutí a provést příslušná bezpečnostní opatření.
- Vlastník také odpovídá za pravidelné přezkoumání přístupových práv a bezpečnostní klasifikace.

Identifikace aktiv

- Kromě toho je užitečné:
  - ustavit,
  - dokumentovat a
  - zavést do praxe pravidla pro přípustné použití aktiv, která popisují povolené a zakázané akce při každodenním používání aktiv.
- Osoby používající aktiva by měly znát a dodržovat tato pravidla, protože správné zacházení s aktivy je součástí jejich odpovědnosti.

Identifikace aktiv

Identifikace aktiv

- Jedním z nejcennějších a nejdůležitějších druhů aktiv jsou informace, které musí být chráněny bez ohledu na jejich formu, obsažené například:
  - v databázích a datových souborech,
  - systémové dokumentaci,
  - smlouvách,
  - uživatelských příručkách,
  - školících materiálech,
  - provozních nebo pomocných postupech,
  - metodických pokynech,
  - dokumentech obsahujících důležité obchodní výsledky, plánech kontinuity nebo
  - smlouvách o záložním provozu.
- K tomu je třeba přidat další aktiva, která se používají k ukládání nebo zpracování informací, nebo mají dopad na bezpečnost informačních aktiv. Tato další aktiva zahrnují následující:

Identifikace aktiv

- *Procesy a služby:*
  - včetně procesů organizace,
  - činností vztahujících se ke konkrétním aplikacím,
  - výpočetní a komunikační služby a
  - další technické služby přispívající ke zpracování informací (vytápění, osvětlení, dodávky elektrického proudu, klimatizace);
- *Programové vybavení:*
  - včetně aplikačního a systémového programového vybavení,
  - vývojových nástrojů a
  - utilit

Identifikace aktiv

- *Fyzické položky včetně :*
  - včetně počítačového vybavení a komunikačních zařízení,
  - médií (papír, pásky a disky) a
  - dalšího technického vybavení (zdroje elektrické energie, klimatizační jednotky),
  - nábytku a
  - prostředků používaných ke zpracování informací;
- *Lidé včetně:*
  - zaměstnanců,
  - zákazníků,
  - předplatitelů a všech dalších osob v ISMS, které jsou zapojeny do ukládání a zpracování informací.

Hodnocení aktiv

- Hlavními prvky hodnocení rizik jsou:
  - identifikace a
  - ohodnocení aktiv podle potřeb organizace.
- Je nezbytné ohodnotit důležitost aktiv pro organizaci a jejich možný vliv na různé podnikatelské příležitosti.
- Jednou z možností jak vyjádřit hodnotu aktiva je popsat, jaký dopad by měly nechtěné incidenty, např. neoprávněné vyzrazení, modifikace, nedostupnost a/nebo ztráta, na aktivum a s ním spojené zájmy organizace, které by byly přímo či nepřímo poškozené.
- Vlastníci a uživatelé aktiv nejlépe znají jejich důležitost, proto by měli poskytnout směrodatné vstupní údaje pro hodnocení aktiv, především jak mohou aktiva ovlivnit obchodní/provozní postupy a cíle činností organizace.

Hodnocení aktiv

- U každého aktiva je třeba zjistit možný dopad na:
  - důvěrnost,
  - integritu,
  - dostupnost nebo jakoukoliv jinou jeho podstatnou vlastnost, pokud je aktivum poškozeno.
- Informace a další příslušná aktiva by se měla klasifikovat v souladu se stanovenou hodnotou a významem aktiva a právními požadavky nebo požadavky organizace.
- Klasifikace naznačuje míru potřeby, priority a předpokládaný stupeň ochrany při nakládání s informacemi.
- Stanovení klasifikace je odpovědností vlastníka aktiva ,stejně jako její pravidelné přezkoumání, které zajistí, že klasifikace odpovídá skutečnému stavu.

Odpovědnost za aktiva

- Organizace musí nastavit a udržovat přiměřenou ochranu aktiv organizace
- U důležitých informačních aktiv musí být stanovena :
  - Odpovědnost – může být delegována, vlastní odpovědnost má vlastník
  - Vlastník- má odpovědnost za udržování přiměřených bezpečnostních opatření

Odpovědnost za aktiva

- Evidence aktiv
  - Každé aktivum má schváleného vlastníka
  - Vlastník aktiva je zaevidován organizací
  - Zaevidována je i bezpečnostní klasifikace vlastníka
  - Důležitosti aktiva musí odpovídat úroveň ochrany.

Odpovědnost za aktiva

- Evidence aktiv
- Příklady aktiv spojených s informačními systémy:
  - Informační aktiva
  - Aplikační programová aktiva
  - Fyzická aktiva
  - Služby
  - Lidé
  - Nehmotná aktiva

Odpovědnost za aktiva

- Vlastnictví aktiv
  - Informace a aktiva mají mít svého vlastníka
  - Vlastník má svou odpovědnost:
    - Zajištění odpovídající klasifikace informací a aktiv souvisejících s prostředky pro zpracování informací.
    - Přesné vymezení a pravidelné k přezkoumání omezení přístupu a klasifikace aktiv, v souladu s politikou řízení přístupu.

Odpovědnost za aktiva

- Přípustné požití aktiv
  - Pravidla zavedena do praxe musí být:
    - určena,
    - dokumentována,
  - pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.

Odpovědnost za aktiva

- Přípustné použití aktiv
  - Pravidla pro přípustné použití informací a aktiv souvisejících s prostředky zpracování informací musí dodržovat:
    - všichni zaměstnanci,
    - smluvní strany,
    - uživatelé třetích stran.

Klasifikace informací

- Informace musí mít odpovídající stupeň ochrany
- Při klasifikaci musí být naznačena jejich:
  - potřebnost,
  - důležitost,
  - stupeň ochrany.

Klasifikace informací

Doporučení pro klasifikaci

- Informace by měly být klasifikovány s ohledem na:
  - hodnotu,
  - právní požadavky.
  - citlivost,
  - kritičnost.

Klasifikace informací

Doporučení pro klasifikaci

- Úroveň ochrany informace může být určena na základě požadavku na:
  - důvěrnost.
  - dostupnost,
  - intergitu.

Klasifikace informací

Označování a zacházení s informacemi

- Pro označování a zacházení s informacemi musí být vytvořeny a zavedeny postupy
- Tyto postupy jsou v souladu s klasifikačním schématem organizace
- Postupy zahrnují informační aktiva v:
  - fyzické,
  - elektronické podobě.

Klasifikace informací

Označování a zacházení s informacemi

- Výstup ze systémů obsahujících citlivé informace by měl být označen odpovídajícím klasifikačním návěštím:
  - tiskové výstupy,
  - výstupy na obrazovku,
  - záznamová média
  - elektronické zprávy,
  - přenosy souborů.

Klasifikace informací

Označování a zacházení s informacemi:

- Označování a bezpečné nakládání s klasifikovanými informacemi je klíčový požadavek pro sdílení informací.
- Nejvhodnější forma označení „fyzické návěští“.

Dotazy?

Ing. Oldřich LUŇÁČEK, Ph.D.
Univerzita obrany, Fakulta VT
Katedra 209
E-mail.: oldrich.lunacek@unob.cz