Fyzická bezpečnost

Bezpečnost informací v ČR

Ing. Oldřich Luňáček, Ph.D.

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

Osnova

- Úvod
- Nakládání s informací
- Informační bezpečnost
- Základní pojmy (aktivum, hrozba, protiopatření)
- Analýza hrozeb

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

ÚVOD

Současná situace ve světě i v České republice (ČR) je zásadně ovlivněna rostoucí integrací států v nadnárodní organizace.

Oblasti života společnosti, které jsou zajišťovány různými složkami, jsou stále ve větší míře zabezpečovány pomocí integrovaných systémů, především s cílem zefektivnit činnost, eliminovat duplikace a minimalizovat nepokrytá místa.

Při řešení bezpečnosti se budeme zabývat jak hrozbami tak protiopatřeními				
Hrozby		Organizace	**Protiopatření**	
poruchy	přírodní kalamita		bezpečnost IS	organizační opatření
Internet	požár		bezpečnost práce	požární ochrana
epidemie	špionáž		řízení rizik	personální politika
konkurence	úrazy		audity	školení
zaměstnanci	selhání IS		politika	pojištění
legislativa	zásobování			
terorismus	kriminalita			

Nakládání s informací

- Vznik informace
- Uložení informace (papír či nosič informací)
- Poškození informace (úmyslné či neúmyslné)
- Zpracování informace
- Přenášení informace (dnes nejčastěji asi v komunikačních a informačních systémech)
- Ztráta informace
- Zničení informace (ochrana před útočníkem, nebo také následek útoku)

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

Podoba (výskyt) informace

- **Uložení informace**:
  tištěná či psaná na papíru,
  uložená na nosiči informací.

- **Výměna informací**:
  přenášena poštou či kurýrem,
  elektronický přenos.

- **Sdílení informací**
  předváděna vizuálně,
  slovně sdílená.

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

O jaké informace jde?

Utajované informace		Neutajované informace	
Přísně tajné	Chráněné dle zák. č. 412/2005 Sb.	**Neklasifikované veřejně přístupné informace**	Nepodléhají ochraně
Tajné	Chráněné dle zák. č. 412/2005 Sb.	**Skutečnosti na které se vztahuje povinnost mlčenlivosti**	Daně, trestní řízení apod.
Důvěrné	Chráněné dle zák. č. 412/2005 Sb.	**Osobní údaje**	Chráněné dle zák. č. 101/2000 Sb.
Vyhrazené	Chráněné dle zák. č. 412/2005 Sb.	**Zvláštní skutečnosti**	Chráněné dle zák. č. 240/2000 Sb.,

Informační bezpečnost

- Důvěrnost- informace pouze přístupná pouze osobám autorizovaným pro přístup k nim,
- Integrita- zabezpečení přesnosti a úplnosti přenášené informace a metod přenosů,
- Dostupnost- autorizovaní uživatelé mají zajištěn přístup k informacím kdykoliv potřebují.

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

Podíly na ztrátách informací

- 50-80 % management vlastní organizace
- 10-30% vlastní zaměstnanci
- 5-8% „vyšší moc“
- 0-8% útok zvenku

Důvody proč je nutný systém pro ochranu informací?

Dnešní doba je poznamenána spíše nadbytkem informací a proto je nutné optimalizovat činnost organizace při sběru, přenosu a ochraně dat.

Je zapotřebí zvýšit povědomí všech osob organizace o nutnosti ochrany informací,

Ochrana dat proti zcizení a zničení musí být jednou z priorit organizace.

Nakládání s informacemi musí být vždy v souladu s legislativními normami.

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

Současná situace

- Malá informovanost o rizicích a zranitelnostech
- Málo řídících a kontrolních mechanismů
- Riziko ztráty důvěryhodnosti

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

Faktory úspěchu

- Politika organizace
- Viditelná podpora a závazek vedení
- Efektivní sdílení bezpečnosti zaměstnanci a manažery
- Chápání požadavků na bezpečnost, analýzu rizik a zvládání rizik

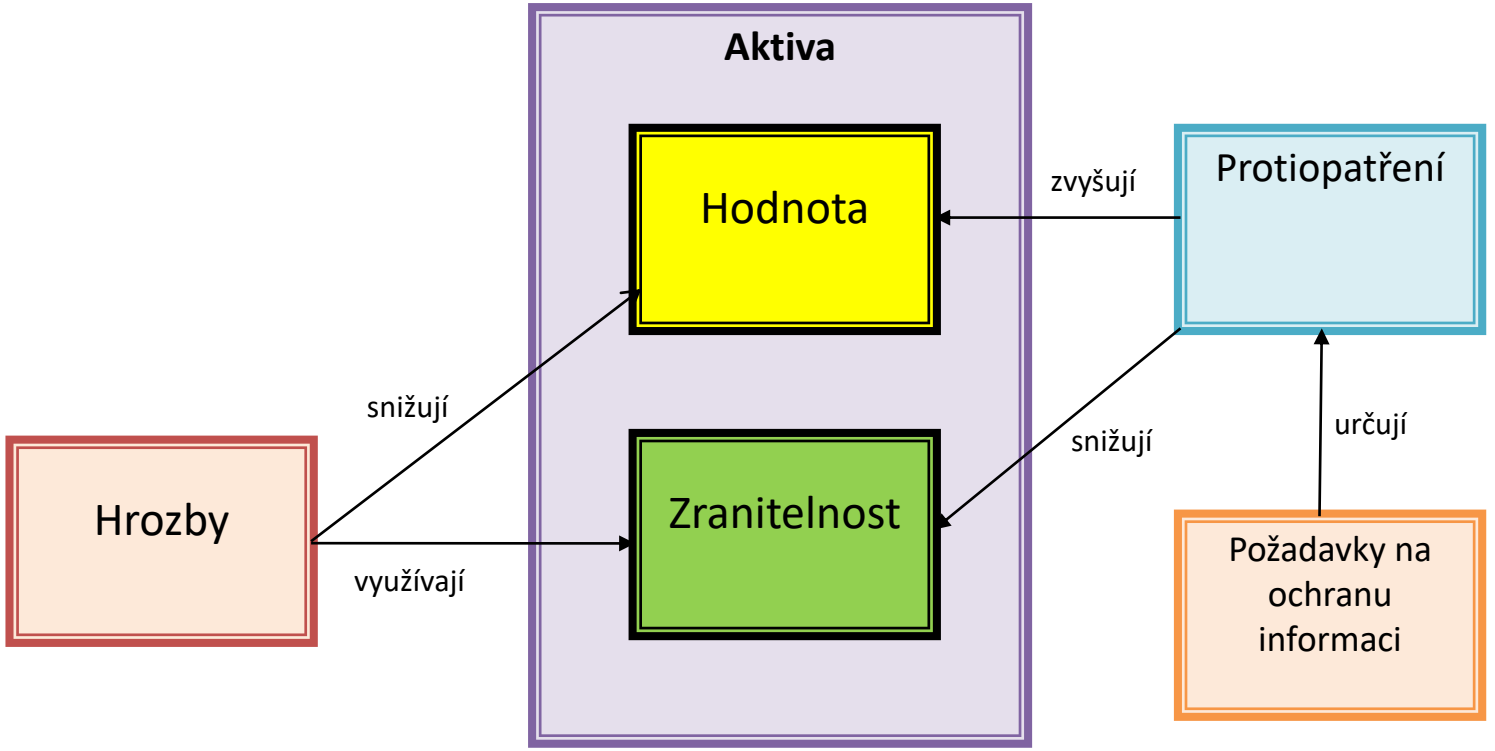
esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Faktory úspěchu

- Správná míra dokumentace
- Adekvátní míra výcviku a vzdělávání
- Vyvážený systém vyhodnocování bezpečnosti
- Zpětná vazba

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

Vztahy


Aktiva
Hodnota
Zranitelnost
Protiopatření
Hrozby
Požadavky na ochranu informaci
zvyšují
snižují
využívají
snižují
určují

Základní pojmy - aktivum

- je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.

- Aktiva se dělí 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.

Základní pojmy -zranitelnost

Je nedostatek analyzovaného aktiva (případně subjektu nebo jeho části), kterým může dojít k naplnění hrozby.

Je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem. Základní charakteristikou zranitelnosti je její úroveň.

Základní pojmy -zranitelnost

Úroveň zranitelnosti aktiva se hodnotí podle následujících faktorů:

- citlivost - náchylnost aktiva být poškozeno danou hrozbou;

- kritičnost - důležitost aktiva pro analyzovaný subjekt.

Základní pojmy – protiopatření

- Protiopatřením chápeme:

  postup,

  proces,

  procedura,

  technický prostředek nebo

  cokoliv, co je navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.

- Navrhují se s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.
- Je charakterizováno efektivitou a náklady.

Základní pojmy – protiopatření

- Navrhují se s cílem:

  předejít vzniku škody nebo

  usnadnit překlenutí následků vzniklé škody.

- Je charakterizováno:

  efektivitou a

  náklady.

Základní pojmy - riziko

Riziko je možnost že se hrozba naplní a dojde k poškození aktiva.

Riziko je potřeba eliminovat na co nejnižší míru kombinací různých opatření a metod.

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

Základní pojmy - riziko

Je nutné analyzovat možné nástroje a postupy, které by mohly pomoci řešit bezpečnost:

komplexně bez absence bezpečnostních děr,

vyváženě bez podceňovaných či přeceňovaných hrozeb či rizik,

hrozby a protiopatření **nebudou** posuzovány **izolovaně** každá zvlášť.

Základní pojmy - hrozba

- Hrozbou je:

  síla,

  událost,

  aktivita nebo

  osoba, která může způsobit škodu.

Základní pojmy - hrozba

- Může ji být např. požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy.

Hrozby	**Náhodné**	**Úmyslné**
Externí	Přírodního původu	Neoprávněný přístup
Interní	Technické selhání	Neoprávněné nakládání
	Lidská chyba	

Základní pojmy - hrozba

- Lze ji definovat jako úmyslně vyvolanou událost nebo náhodnou událost.
- Může mít negativní dopad na aktiva z hlediska jejich bezpečnostních aspektů.
- Aktiva jsou vystavena mnoha hrozbám a my jsme povinni hrozbám čelit.
- Pro stanovení efektivní a účinné ochrany je zapotřebí tyto hrozby identifikovat.

Hrozba

Hrozby se nejčastěji dělí podle úmyslu a podle zdroje:

Budeme-li dělit hrozby podle zdroje, dojdeme k následujícímu dělení:

- vnitřní hrozby - zdroj (příčina) hrozby se nachází uvnitř organizace;

- vnější hrozby - zdroj (příčina) hrozby se nachází mimo organizaci.

Hrozba

- Hrozba působí aktivně, pokud **dojde** ke změně stavu systému, díky narušením integrity a dostupnosti.

- Hrozba působí pasivně, když **nedochází** ke změně stavu systému, ale dochází k úniku informací.

Lze tedy konstatovat, že hrozba má:

- **Nositele**, mohou se jimi stát osoby a samovolné události. U osob rozeznáváme především zda působí zvenčí nebo zevnitř organizace.

- **Osoby útočící zvenčí provádí záměrné útoky** proti aktivům organizace.

- **U zaměstnanců organizace je pravděpodobnější neúmyslná činnost** než cílený útok.

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

Lze tedy konstatovat, že hrozba má

- **Objekt** hrozby, a tím jsou definovaná aktiva.
- **Mechanismus**, tím je způsob útoku na aktivum. Rozlišujeme, zda je proveden vlastními zaměstnanci či osobami zvenčí.
- Největším nebezpečím jsou hrozby od vlastních zaměstnanců organizace. V tomto případě je nutno podtrhnout skutečnost, že tyto osoby mají nejlepší podmínky k uskutečnění svých cílů.

Analýza hrozeb

- Je nezbytné znát hrozby, které mohou způsobit ztrátu aktiv abychom efektivně nastavili výkonný systém bezpečnosti.

- Použití nejvýhodnější analýzy hrozeb je důležité pro komplexní posouzení celé problematiky a stává se významným faktorem úspěchu.

- Oblast bezpečnosti utajovaných informací je velmi specifická a v této oblasti mohou existovat desítky hrozeb.

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

Lze tedy konstatovat, že hrozba má

- Nesmíme ale také opomenout neúmyslné hrozby od vlastních zaměstnanců

  Např. v případě neškoleného pracovníka.

- Hrozby přírodního původu lze efektivně eliminovat např. vhodným umístěním - před povodněmi či záplavami.

Identifikovat a analyzovat hrozby

- V současné době se používá **analýza hrozeb založená na tzv. stromu hrozeb.**

  je zobrazením systematického rozložení na dílčí části,

  Vznik této analýzy byl inspirován metodou analýzy poruch pomocí stromu (Fault Tree Analysis), která se od počátku 60. let minulého století začala používat pro vývoj systémů, kde jsou poruchy nepřijatelné (např. vesmírný program, přistání letadla, jaderné reaktory apod.).

  Strom poruch je grafový model poruch, jejichž důsledkem jsou definované nežádoucí události.

  Poruchami mohou být události, související s poruchami hardwarových prvků, lidských chyb, softwarových chyb nebo nějakých jiných souvisejících událostí, které mohou vést k nežádoucímu stavu.

Identifikovat a analyzovat hrozby

Strom poruch popisuje logické vzájemné vazby mezi základními událostmi (poruchami), které mohou vést k analyzované nežádoucí události.

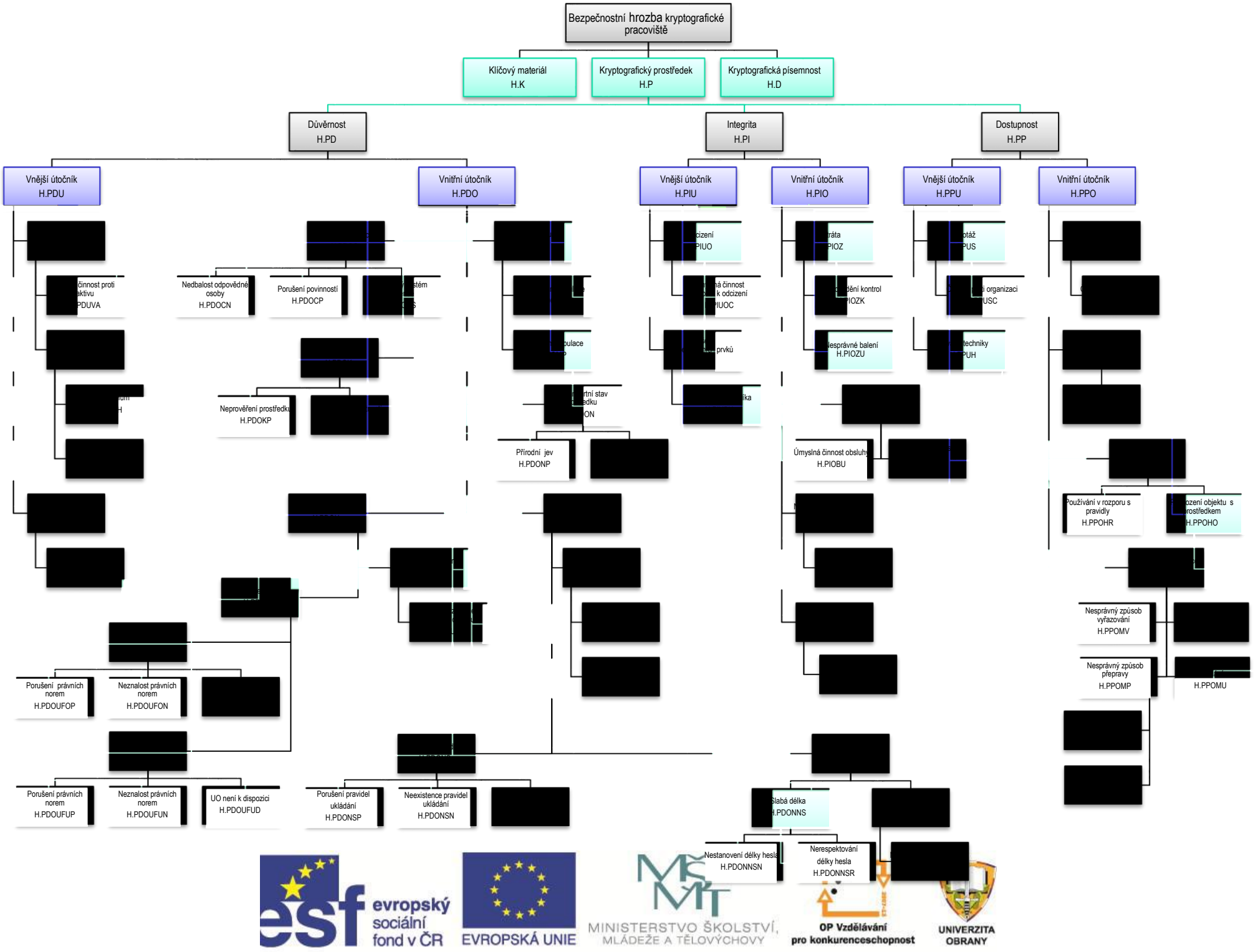
Hierarchické stromové uspořádání vyjádřené vzájemnými vazbami prvků zachycuje vztah nadřazenosti a podřízenosti prvků a vztah sounáležitosti podřízených prvků patřících k jednomu prvku nadřazenému.

Charakteristickým rysem analýzy pomocí stromu hrozeb je orientace na jedinou hrozbu. Pokud je systém rozsáhlejší, tak se vytváří několik stromů hrozeb pro každou jednotlivou hrozbu .

Tento způsob řešení však vede ke složitějšímu posuzování vlivu těch dílčích hrozeb, které se vyskytují ve více stromech.

Identifikovat a analyzovat hrozby

- Mnohem výhodnější je použití **analýzy hrozeb založené na grafu elementárních hrozeb.**
- Její podstatou je **analýza výchozích hrozeb a postupné dokreslování a zpřesňování hrozeb.**
- Cílem je nalezení **souboru navzájem nezávislých elementárních hrozeb**, ze kterých se obecnější hrozby popisují pomocí Booleovy logiky.
- Analýzou získané soustavy logických funkcí lze určit význam elementárních hrozeb, což umožňuje optimalizovat volbu bezpečnostních protiopatření.


Bezpečnostní hrozba kryptografické pracoviště
Klíčový materiál H.K
Kryptografický prostředek H.P
Kryptografická písemnost H.D
Důvěrnost H.PD
Integrita H.PI
Dostupnost H.PP
Vnější útočník H.PDU
Vnitřní útočník H.PDO
Vnější útočník H.PIU
Vnitřní útočník H.PIO
Vnější útočník H.PPU
Vnitřní útočník H.PPO
Nedbalost odpovědné osoby H.PDOCN
Porušení povinností H.PDOCP
Neprověření prostředku H.PDOKP
Přírodní jev H.PDONP
Úmyslná činnost obsluhy H.PIOBU
Nesprávné balení H.PIOZU
Používání v rozporu s pravidly H.PPOHR
Nesprávný způsob vyřazování H.PPOMV
Nesprávný způsob přepravy H.PPOMP
H.PPOMU
Porušení právních norem H.PDOUFOP
Neznalost právních norem H.PDOUFON
Porušení právních norem H.PDOUFUP
Neznalost právních norem H.PDOUFUN
UO není k dispozici H.PDOUFUD
Porušení pravidel ukládání H.PDONSP
Neexistence pravidel ukládání H.PDONSN
Slabá délka H.PDONNS
Nestanovení délky hesla H.PDONNSN
Nerespektování délky hesla H.PDONNSR
esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Je nutné zvážit zda:

- Všichni známe dokonale platnou legislativu.
- Každý perfektně své povinnosti zná a proto nemusíme vytvářet směrnice dokumentované postupy.
- Největší nepřítel je útočník zvenčí (nejlépe hacker).
- Cizí subjekt v našem prostoru je bezpečný.

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

Je nutné zvážit zda:

- Dodavatelé služeb nejsou rizikem.
- Používat univerzální klíče a přístupová hesla.
- Nevhodné prostory pro organizaci.
- Nevyhodnocování minulých incidentů.
- Nesledování nejnovějších trendů.

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

100% bezpečnost?

- Bezpečný systém je „takový který je vypnut, odpojen a uzamknut v nedobytném trezoru, umístěný v izolovaném betonovém v bunkru a je pod neustálým a velmi důkladným dozorem nadprůměrně vycvičených a nepodplatitelných stráží“.

100% bezpečnost?

- Vždy je nutné zvážit zda při aplikaci všech bezpečnostních opatření bude uživatel motivován takovýto systém používat.
- Aplikace bezpečnostních opatření musí splňovat svou funkci z hlediska ochrany ale taky musí být uživatelem akceptovány a používány

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

Literatura

Zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

POŽÁR, J.: Informační bezpečnost. Vydavatelství a nakladatelství Aleš Čeněk,s.r.o.. Plzeň 2005.

Dokument NATO C-M(2002)49 Security within NATO. 2002.

RODRYČOVÁ, J., STAŠA, P.: Bezpečnost informací jako podmínka prosperity firmy. Grada, Praha 2000.

Dobda, L.: Ochrana dat v IS

Burda, K. Threat analysis based on the graph of elementary threats. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

SCHNEIER, B. Attack Trees. Dr Dobb's Journal, Vol.24 (1999), No.12 (Dec.), s. 21-29

STEINER,F. Management rizik bezpečnosti informací[online].[cit. 2010-06-23]. Dostupné z WWW: < http://bpm-tema.blogspot.com/2007/11/management-rizik-bezpenosti-informac.html

Doporučená literatura

Vyhláška č. 432/2011 Sb., o zajištění KOUI.

Vyhláška č. **525/2005** Sb. o provádění **certifikace** při zabezpečování **KOUI**, ve znění vyhlášky č. **434/2011** Sb.

Vyhláška č. **405/2011** Sb., o **průmyslové bezpečnosti**

Vyhláška č. **363/2011** Sb., o **personální bezpečnosti** a o bezpečnostní způsobilosti

Vyhláška č. **528/2005** Sb., o **fyzické bezpečnosti a certifikaci technických prostředků**, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. **454/2011** Sb.

Vyhláška č. **529/2005 Sb**., o **administrativní bezpečnosti a o registrech utajovaných informací**, ve znění vyhlášky č. 55/2008 Sb. a vyhlášky č. **433/2011** Sb.

Doporučená literatura

RMO 16/2013 Ochrana určených neutajovaných informací v rezortu MO

RMO 14/2013 Ochrana utajovaných informací v resortu MO
RMO 33/2012 o personální bezpečnosti v rezortu MO

RMO 6/2010 ve znění RMO 14/2011 Zřízení rady pro kybernetickou bezpečnost

RMO 11/2010 ve znění RMO 42/2010 a RMO 17/2013 Spisový řád

RMO 18/2006 ve znění RMO 44/2010 a RMO 16/2012 Seznam zvlášť určených pracovišť

RMO 25/2007 Stanovení stupňů utajení

Doporučená Literatura

NV	85/2013	BIKS a EZ nakládajících s UI
NV	77/2013	Fyzická bezpečnost v rezortu MO
NV	20/2013	BIKS a EZ, které nakládají s určenými neutajovanými informacemi (UNI) v rezortu MO
NV	19/2013	Technické standardy pro přenosy dat prostřednictvím data linků
NV	18/2013	OUI poskytovaných podnikatelům
NV	60/2012	Administrativní bezpečnost
NV	12/2010	Spisová služba ve znění NV 61/2012
NV	111/2013	Zabezpečení kryptografické ochrany v rezortu MO