Bezpečnost informací v ČR

Osnova

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

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				
Hrozby		**Aktiva organizace informace**	**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)

Podoba (výskyt) informace

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

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

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

Kromě toho ve svém okolí se budeme určitě zabývat :

- Data jsou souborem:
  - faktů,
  - měření a
  - statistik,
  - sama o sobě nemají vypovídací schopnost, protože nejsou nijak zpracována, neobsahují žádná porovnání s ostatními údaji a není možno podle jednotlivých dat rozhodovat.

Ve svém okolí se budeme určitě zabývat :

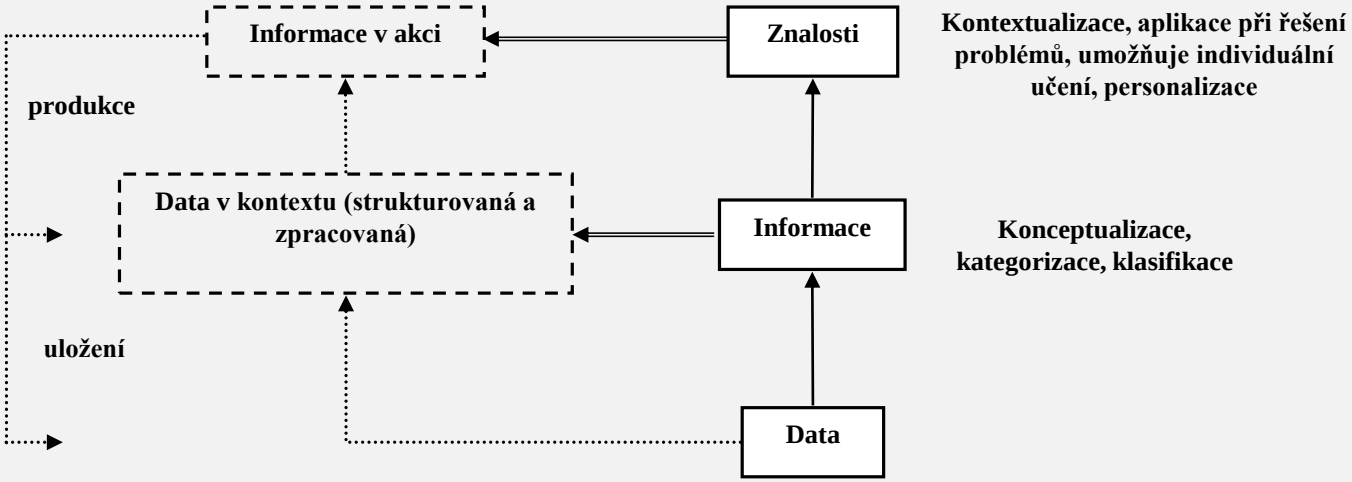
- Informace představují uspořádaná nebo zpracovaná data, u nichž je kontrolována jejich aktuálnost a přesnost. Data obsažená v informaci jsou porovnávána, uspořádávána a hodnocena.

Ve svém okolí se budeme určitě zabývat :

- **Znalosti** jsou kromě dat a informací také i zkušenosti a porozumění.
- **Znalosti:**
  - je možno také charakterizovat jako správná řešení problémů,
  - obsahují informace sdělované v určitém kontextu, významné a použitelné v dané situaci,
  - je možné přímo použít k řešení problému,
  - jejich významná vlastnost je jejich použitelnost

Znalostní pyramida

1. **data**: fakta, obrázky, zvuky (+ interpretace + význam =)
2. **informace**: formátovaná, filtrovaná a sumarizovaná data (+ akce + aplikace =)
3. **znalosti**: instinkty, ideje, pravidla a procedury, které vedou akce a rozhodnutí



Znalosti

- **Tacitní znalosti** - jde o skryté znalosti jednotlivce, někdy také označované jako nevyslovené a nevyslovitelné, které vznikají při učení. Jsou rozptýlené, nestrukturované a obtížně se vyjadřují slovy.
  - Bývají vysoce **osobní** a obtížně se formalizují.
  - Mají charakter spíše **subjektivní, kognitivní** (poznávací) a empirický (zkušenostní).
  - Jsou to **empirické znalosti** založené na předtuše, instinktu a osobní prozíravosti.
  - Skryté znalosti představují rezervoár zkušeností, náhledů, expertíz, know-how, obchodních tajemství a zvláštních dovedností, který se vytvářel v průběhu učení podporovaného vhodnou organizační strukturou.

Znalosti

- **Explicitní znalosti** jde o znalosti spíše **objektivního**, racionálního a technického charakteru:
  - plány,
  - procedury,
  - software, dokumenty apod.
    - Jejich forma umožňuje distribuci bez nutnosti osobního kontaktu.
    - Snadno se kodifikují a předávají ostatním.
- Výše uvedené rozdělení nemůže být beze zbytku uplatněno na všechny znalosti, protože mnoho z nich má vlastnosti obou.
- Navíc v rámci svého životního cyklu se znalosti rozvíjejí a mění z tacitních na explicitní a z explicitních na tacitní.

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. **GDPR 25.5.2018**
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.

Podíly na ztrátách informací

- 50-80 % management vlastní organizace (nesprávné rozhodnutí)
- 10-30% vlastní zaměstnanci (úmyslná nebo neúmyslná činnost)
- 5-8% „vyšší moc“ (záplavy, úder blesku apod.)
- 0-8% útok zvenku (útočník)

Důvody proč je nutný systém pro ochranu informací?

- Nakládání s informacemi musí být vždy v souladu s legislativními normami (zákony).
- Dnešní doba je poznamenána spíše nadbytkem informací a proto je nutné optimalizovat činnost organizace při sběru, přenosu a ochraně dat.
- Nejvíce používáme KIS pro nakládání s informacemi.
- I proto je zapotřebí zvýšit povědomí všech osob organizace o nutnosti ochrany informací,
- Ochrana dat proti zcizení a zničení musí být jednou z priorit organizace.

Současná situace

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

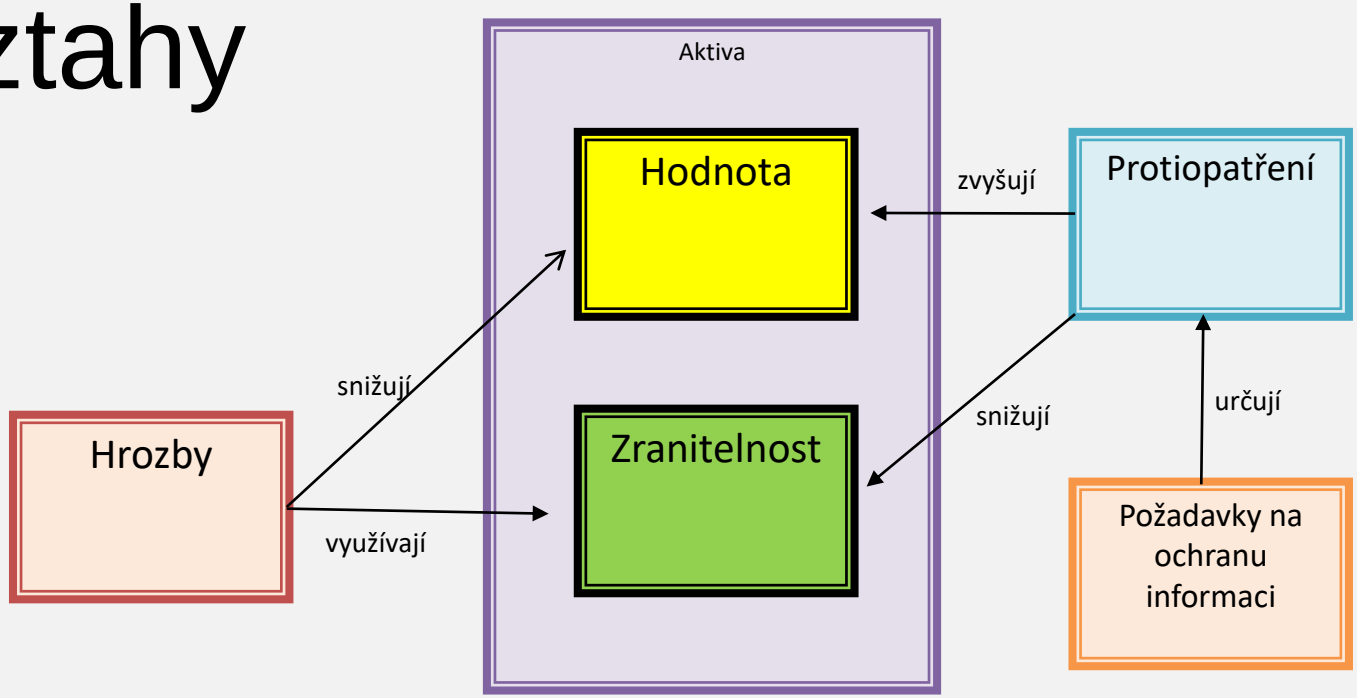
Faktory úspěchu

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

Faktory úspěchu

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

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), a 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.

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.

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

Základní pojmy - hrozba

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.

Podle úmyslu můžeme provést rozdělení:

- náhodné hrozby - jedná se o hrozby, které byly způsobeny zcela náhodně;
- úmyslné hrozby - jedná se o hrozby, které byly naplánovány.

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.

Hrozba

- Pro definovaná aktiva můžeme definovat hrozby, označené:
  - podle objektu hrozby,
  - bezpečnostního aspektu,
  - nositele hrozby,
  - a dále např. mechanismu naplnění hrozby.

Hrozba

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.

Lze tedy konstatovat, že:

- **Pravděpodobnost cíleného útoku** je vyšší u vnějšího útočníka.
- Samovolné události jsou náhodnými událostmi, které jsou zapříčiněny např.:
  - zemětřesením,
  - úderem blesku,
  - povodněmi,
  - sesuvy půdy či například
  - zkraty v elektroinstalaci.

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.

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.

Je nutno vzít do úvahy:

- 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.

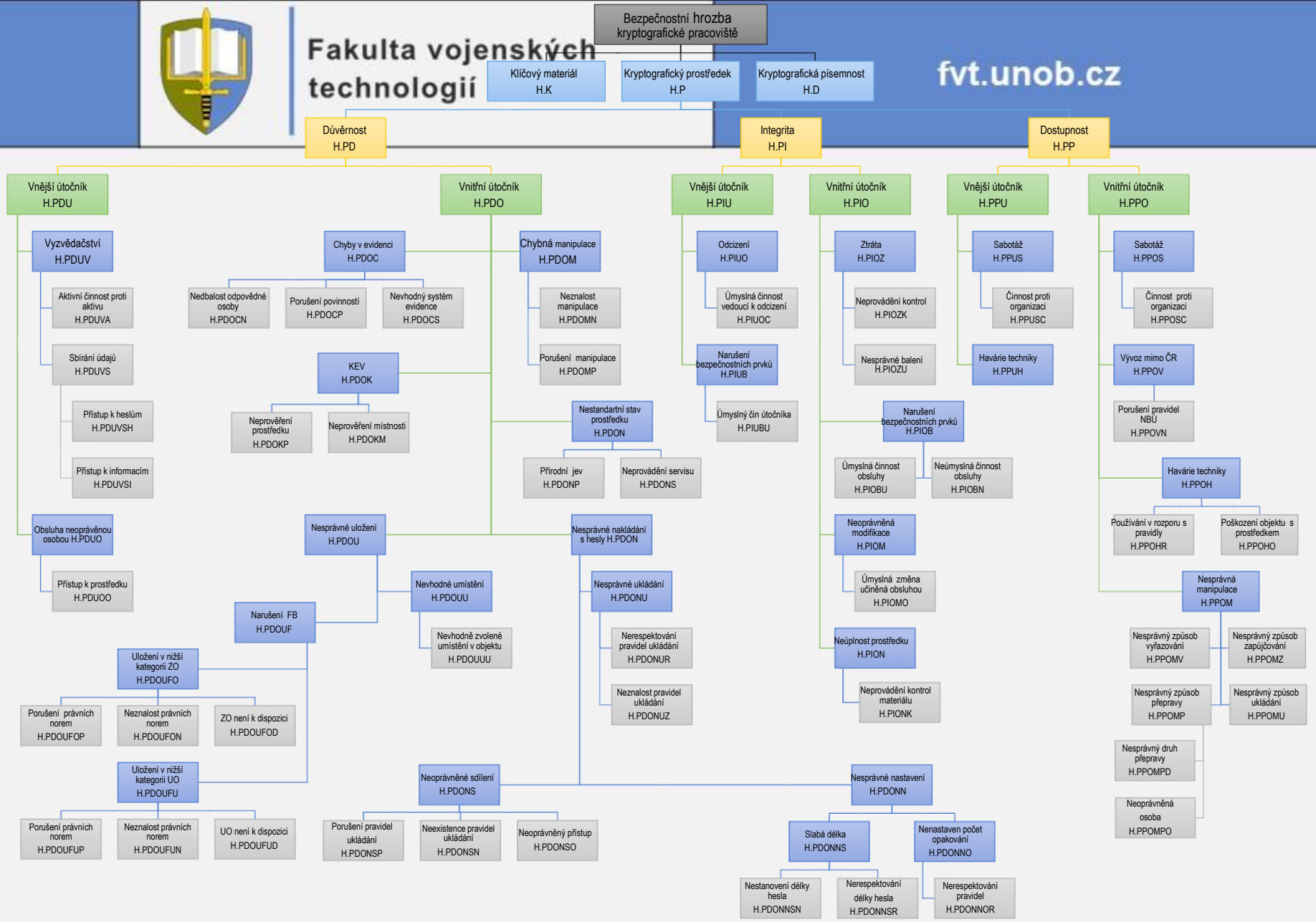
- Hierarchické stromové uspořádání vyjádřené vzájemnými vazbami prvků zachycuje vztah nadřazenosti a podřízenosti prvků a vztah sounáležitosti podřízených prvků patřících k jednomu prvku nadřazenému.

- 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
Vyzvědačství H.PDUV
Aktivní činnost proti aktivu H.PDUVA
Sbírání údajů H.PDUVS
Přístup k heslům H.PDUVSH
Přístup k informacím H.PDUVSI
Obsluha neoprávněnou osobou H.PDUO
Přístup k prostředku H.PDUOO
Chyby v evidenci H.PDOC
Nedbalost odpovědné osoby H.PDOCN
Porušení povinností H.PDOCP
Nevhodný systém evidence H.PDOCS
KEV H.PDOK
Neprověření prostředku H.PDOKP
Neprověření místnosti H.PDOKM
Nesprávné uložení H.PDOU
Nevhodné umístění H.PDOUU
Nevhodně zvolené umístění v objektu H.PDOUUU
Narušení FB H.PDOUF
Uložení v nižší kategorii ZO H.PDOUFO
Porušení právních norem H.PDOUFOP
Neznalost právních norem H.PDOUFON
ZO není k dispozici H.PDOUFOD
Uložení v nižší kategorii UO H.PDOUFU
Porušení právních norem H.PDOUFUP
Neznalost právních norem H.PDOUFUN
UO není k dispozici H.PDOUFUD
Chybná manipulace H.PDOM
Neznalost manipulace H.PDOMN
Porušení manipulace H.PDOMP
Nestandartní stav prostředku H.PDON
Přírodní jev H.PDONP
Neprovádění servisu H.PDONS
Nesprávné nakládání s hesly H.PDON
Nesprávné ukládání H.PDONU
Nerespektování pravidel ukládání H.PDONUR
Neznalost pravidel ukládání H.PDONUZ
Neoprávněné sdílení H.PDONS
Porušení pravidel ukládání H.PDONSP
Neexistence pravidel ukládání H.PDONSN
Neoprávněný přístup H.PDONSO
Odcizení H.PIUO
Úmyslná činnost vedoucí k odcizení H.PIUOC
Narušení bezpečnostních prvků H.PIUB
Úmyslný čin útočníka H.PIUBU
Ztráta H.PIOZ
Neprovádění kontrol H.PIOZK
Nesprávné balení H.PIOZU
Narušení bezpečnostních prvků H.PIOB
Úmyslná činnost obsluhy H.PIOBU
Neúmyslná činnost obsluhy H.PIOBN
Neoprávněná modifikace H.PIOM
Úmyslná změna učiněná obsluhou H.PIOMO
Neúplnost prostředku H.PION
Neprovádění kontrol materiálu H.PIONK
Nesprávné nastavení H.PDONN
Slabá délka H.PDONNS
Nestanovení délky hesla H.PDONNSN
Nenastaven počet opakování H.PDONNO
Nerespektování délky hesla H.PDONNSR
Nerespektování pravidel H.PDONNOR
Sabotáž H.PPUS
Činnost proti organizaci H.PPUSC
Havárie techniky H.PPUH
Sabotáž H.PPOS
Činnost proti organizaci H.PPOSC
Vývoz mimo ČR H.PPOV
Porušení pravidel NBÚ H.PPOVN
Havárie techniky H.PPOH
Používání v rozporu s pravidly H.PPOHR
Poškození objektu s prostředkem H.PPOHO
Nesprávná manipulace H.PPOM
Nesprávný způsob vyřazování H.PPOMV
Nesprávný způsob zapůjčování H.PPOMZ
Nesprávný způsob přepravy H.PPOMP
Nesprávný způsob ukládání H.PPOMU
Nesprávný druh přepravy H.PPOMPD
Neoprávněná osoba H.PPOMPO

Je nutné zvážit zda:

- všichni známe dokonale platnou legislativu,
- každý zná perfektně své povinnosti a proto nemusíme vytvářet směrnice dokumentované postupy,
- největším nepřítelem je útočník zvenčí (nejlépe hacker)?
- cizí subjekt v našem prostoru je bezpečný,

Je nutné zvážit zda:

- nejsou dodavatelé služeb rizikem,
- používat univerzální klíče a přístupová hesla,
- nepoužíváme nevhodné prostory,
- opravdu vyhodnocujeme incidenty,
- sledujeme nejnovější trendy.

100% bezpečnost?

- Bezpečný systém je takový, který je:
  - vypnut,
  - odpojen od vnějšího prostředí,
  - uzamknut v nedobytné místnosti,
  - chráněn v nedobytném a odolném bunkru,
  - pod dohledem nadprůměrně vycvičených a neúplatných strážců.

  - Budeme skutečně takový systém používat????

100% bezpečnost?

- Vždy je nutné zvážit zda při aplikaci všech bezpečnostních opatření bude uživatel motivován a ochoten tento systém používat.

- Aplikace bezpečnostních opatření musí splňovat svou funkci z hlediska ochrany ale taky musí být uživatelem akceptovány a používány.

Otázky do samostudia

- Jaké znaky by mělo mít řízení informací v organizaci?
- Analyzuje informace ve svém okolí
  - jaké druhy informací, jakým způsobem se k Vám dostaly, pravdivost/nepravdivost, pro koho jsou určeny, apod.

Literatura

- DVOŘÁK, Jan. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář. Praha: Wolters Kluwer, 2018. Komentáře Wolters Kluwer. ISBN 978-80-7598-016-8.
- RODRYČOVÁ, J., STAŠA, P.: Bezpečnost informací jako podmínka prosperity firmy. Grada, Praha 2000.
- 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.
- HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.

Literatura

- Vyhláška č. 432/2011 Sb., o zajištění KOUI (ve znění 417/2013)
- 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 (ve znění 416/2013)
- Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti (ve znění 415/2013))
- 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.)
- Rozkazy a normativní výnosy resortu Ministerstva obrany