Analýza bezpečnosti organizace

Obsah

- Bezpečnostní analýza
- Analýza hrozeb
- Návrh bezpečnostní analýzy

BEZPEČNOSTNÍ ANALÝZA

- Analýza bezpečnosti organizace je zaměřena na vytvoření komplexních bezpečnostních protiopatření vedoucích k celistvé ochraně aktiv organizace.

- Pro samotné provedení analýzy použijeme obecné schéma bezpečnostní analýzy, které je upraveno pro řešení bezpečnosti organizace.

- Analýza bezpečnosti organizace je prováděna v 6 posloupných krocích.

BEZPEČNOSTNÍ ANALÝZA - POSTUP provedení

1. Určení bezpečnostní správy organizace
2. Stanovení rozsahu analýzy
3. Identifikace aktiv
   - lidské zdroje
   - procesy
   - informace
   - majetek
4. Identifikace hrozeb
5. Identifikace a ocenění zranitelnosti
6. Návrh protiopatření
   - procedurální
   - technické

BA 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.

BA základní pojmy

- **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.

BA základní pojmy

- **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.

BA 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.

BA 1.krok

- definice týmu specialistů,
- bezpečnostní správa je odpovědná za řízení bezpečnosti organizace,
- např. v resortu MO je tento tým nazýván bezpečnostní správa, v literatuře se ale více užívá pojem bezpečnostní management,

BA 1.krok

- vedoucí pracovník týmu, v čele musí být určená osoba, v rezortu MO je bezpečnostní manažer,
- bezpečnostní správa pokrývá všechny druhy zajištění OUI a je odpovědná za vypracování analýzy bezpečnosti organizace,
- např. bezpečnostní správa je v resortu MO tvořena rolemi:

BA 1.krok

- bezpečnostní manažer organizačního celku,
- bezpečnostní a provozní správa IKS a elektronických zařízení:
  - bezpečnostní správce utajovaného systému;
  - správce utajovaného systému;
  - místní bezpečnostní správce utajovaného systému;
  - místní správce utajovaného systému;
  - bezpečnostní správce terminálové oblasti utajovaného systému;
  - osoba odpovědná za elektronické zařízení.

BA 1.krok

- bezpečnostní správa kryptografické ochrany:
  - bezpečnostní správce kryptografické ochrany,
  - správce kryptografického materiálu,
  - zástupce správce kryptografického materiálu,
  - bezpečnostní správce kryptografické ochrany utajovaného systému,
  - pracovník určený k vedení dokumentů KRYPTO,
  - speciální obsluha kryptografického prostředku,
  - kurýr určený k přepravě kryptografického materiálu.

BA 1.krok

- registr, pomocný registr nebo kontrolní bod,
- pracoviště ochrany informací,
- bezpečnostní pracovník pro personální bezpečnost,
- správce technických prostředků.

BA 2. krok

- stanovení rozsahu analýzy
- vymezíme se do oblasti OUI, a to v návaznosti na tři základní bezpečnostní aspekty:
  - důvěrnost,
  - dostupnost a
  - autentičnost aktiv.
- při řešení problematiky bezpečnosti si musíme uvědomit, jakých cílů chceme v oblasti bezpečnosti dosáhnout:

BA 2. krok

- Bezpečnost musí být:
  - nezávislá,
  - řízená a
  - oceňovaná.
- Informace jsou chráněným aktivem společnosti.
- Bezpečnost je zajišťována nepřetržitě a nesmí dojít k narušení OUI.
- Bezpečnost je akceptovatelná pro všechny zaměstnance i přes nasazení technických prostředků.

BA 3.krok

- identifikace aktiv a jejich ocenění,
- provedeme nejprve výčet aktiv a nesmíme opomenout provést jejich ocenění.
- jedná se o následující aktiva:
  - Informace (jakákoliv znalost v jakékoliv podobě, na jakémkoliv nosiči), které lze rozdělit např. na:
    - UI,
    - citlivé informace, které vyžadují zvláštní přístup, tyto informace jsou představovány osobními údaji osob,
    - dále se můžeme setkat s informacemi z oblasti krizového řízení, tyto informace nejsou utajované, ale nejsou určeny pro veřejnost, vyžadují zvláštní stupeň nakládání s nimi.

BA 3.krok

- informace organizace jsou zpravidla dokumenty vypracovávané organizací,
- např. v resortu MO bychom neměli opomenout rozkazy, předpisy a nařízení.
- cenu informací lze rozdělit do dvou skupin:
  - informace interní, dokument je vypracován vlastními zaměstnanci, tuto informaci je těžké vyčíslit.
  - informace pocházet z externího zdroje, lze konkretizovat cenu externích nakoupených zdrojů,
  - problematické je ohodnotit cenu vlastních dokumentů, pro samotnou organizaci je cena nevyčíslitelná, a pro ostatní může být cena různá.

BA 3.krok

- Majetek představuje:
  - hmotné i nehmotné statky organizace,
  - movitý majetek, nemovitý majetek, finance organizace, ale patří zde také prestiž firmy, její pověst, případně i logo firmy.,
  - výhodou je, že u většiny z těchto aktiv máme pořizovací cenu a můžeme definovat hodnotu.

- Procesy jsou:
  - děje, které je nutno provádět, zpravidla periodicky a jež slouží k řízení bezpečnosti a jejich plněním jsou naplněny požadavky právních norem,
  - určit konkrétní cenu je problematické, procesy jsou vykonávány rutinně vyškolenými pracovníky a kvalita procesů je závislá na kvalitě pracovníků.

BA 3.krok

- Lidské zdroje jsou:
  - osoby podílející se na bezpečnosti vlastní organizace,
  - bezpečnostní správa a všichni zaměstnanci organizace,
  - nesmíme zapomenout na osoby vystupující jako podnikatelé v oboru, který je nazýván průmyslová bezpečnost.,
  - zaškolení a odpovědní vlastní pracovníci mají pro organizaci nevyčíslitelnou cenu z pohledu kvality lidských zdrojů.,
  - cena externích pracovníků se dá vyhodnotit na základě uzavřených smluv.

BA 4. krok

- identifikování hrozeb,
- je zapotřebí zjistit hrozby, které jsou reálné a mohou narušit OUI a jaká je pravděpodobnost jejich výskytu,
- zhodnocení dopadu hrozeb na aktiva organizace,
- posoudit a analyzovat každé aktivum zvlášť,
- zjistit stav ohrožení systému.

BA 5. krok

- identifikace a ocenění zranitelnosti systému,
- zranitelností chápeme stav, kdy se hrozba naplní a může dojít ke ztrátě aktiva nebo k jeho poškození,
- hlavním cílem činnosti bezpečnostní správy je OUI,
- zranitelnost představuje situaci, která může vést k narušení OUI,
- možná místa zranitelnosti lze určit analýzou situací, které mohou vést ke ztrátě utajení určité hodnoty.

BA 6. krok

- definovat protiopatření pro eliminování působení hrozeb na aktiva v oblasti bezpečnosti,
- v praxi se pro eliminaci působení hrozeb často používá pojem zvládání rizik,
- protiopatření mohou rizika působící na aktiva:
  - akceptovat,
  - snížit,
  - maximálně eliminovat,
  - přesunout jinam.

BA 6.krok

- protiopatření dělíme do 2 základních kategorií:
  - procedurální protiopatření, je zde zahrnut styl řízení bezpečnosti organizace.
  - technická protiopatření, týkají se problematiky nasazených technických prostředků.

ANALÝZA HROZEB

- pro nastavení systému bezpečnosti organizace musíme znát hrozby, které mohou způsobit ztrátu aktiv organizace,
- použití nejvýhodnější analýzy hrozeb je důležité pro komplexní posouzení celé problematiky a stává se významným faktorem úspěchu,
- bezpečnost organizace v otázce UI je nutno komplexně zajistit ve všech druzích zajištění OUI,
- právě tyto druhy jsou vystaveny mnoha hrozbám, které je nutno identifikovat, analyzovat,
- v rozsáhlých systémech mohou existovat desítky hrozeb.

ANALÝZA HROZEB

- hrozbu lze definovat jako úmyslně vyvolanou událost nebo náhodnou událost.
- hrozba může mít negativní dopad na aktiva z hlediska jejich bezpečnostních aspektů.
- hrozby se nejčastěji dělí na hrozby podle úmyslu a podle zdroje.
  - dělíme-li hrozby podle úmyslu:
    - náhodné hrozby - jedná se o hrozby, které byly způsobeny zcela náhodně,
    - úmyslné hrozby - jedná se o hrozby, které byly naplánovány.
  - Budeme-li dělit hrozby podle zdroje:
    - vnitřní hrozby - zdroj (příčina) hrozby se nachází uvnitř organizace,
    - vnější hrozby - zdroj (příčina) hrozby se nachází mimo organizaci.
- jiné dělení hrozeb je podle dopadu na systém kdy sledujeme aspekt bezpečnosti:
  - důvěrnost;
  - integrita;
  - dostupnost.

ANALÝZA HROZEB

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

ANALÝZA HROZEB

- V současné době se také 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.
  - 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.

ANALÝZA HROZEB

- 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,

ANALÝZA HROZEB

- Řada hrozeb v sobě totiž obsahuje společné elementární hrozby (např. elementární hrozba krádeže kryptografického prostředku je obsažena jak v hrozbě na dostupnost kryptografického prostředku tak i v hrozbě na důvěrnost klíčů uložených v daném prostředku).
- Vzniklý graf je kompaktní a přehledný.
- V důsledku požadavku členění hrozeb na nepřekrývající se dílčí hrozby je zajištěno, že dílčí hrozby vytvářejí nadřízenou hrozbu pouze logickým součtem (OR) a nikdy logickým součinem (AND).
- To umožňuje přehlednější a automatizovanou analýzu protiopatření na základě výrokové logiky nebo přehlednější volbu protiopatření při ručním postupu.
- Tento způsob analýzy vede k minimalizaci chyb způsobených tvůrcem grafu hrozeb, protože pravidlo členění hrozeb na úplný soubor navzájem disjunktních dílčích hrozeb, minimalizuje možnost přehlédnutí některých hrozeb, opominutí některých bezpečnostních aspektů nebo naopak překrývání hrozeb.

ANALÝZA HROZEB

- Výhodou takto vypracovaného grafu je grafická názornost a strukturovanost analyzovaných hrozeb v rámci uceleného systému. Ve vypracovaném grafu jsou případné rozpory nebo opominutí snadněji patrné a odstranitelné.
- Je vytvořen relativně úplný seznam navzájem nezávislých elementárních hrozeb, jejichž kombinací můžeme vytvořit složené hrozby.
- V této souvislosti je zapotřebí zdůraznit fakt, že absolutně spolehlivá metoda pro analýzu hrozeb neexistuje.
- Neodstranitelným rizikem každé metody je opomenutí některé hrozby, protože autor analýzy nemusí příslušnou hrozbu znát nebo příslušná hrozba vznikne později v souvislosti s rozvojem lidského poznání nebo technologií.
- To ale neznamená, že tato hrozba neexistuje nebo v budoucnosti nemůže existovat.
- Je nutné respektovat nutnost revizí analýzy hrozeb v periodických intervalech.

ANALÝZA HROZEB - NÁVRH

- pro analýzu použijeme výše zmíněný algoritmus,
- při praktickém vypracovávání grafu elementárních hrozeb nejdříve definujeme vrchol grafu, tím je hrozba pro bezpečnost analyzovaného systému.
- pod ní se nachází dílčí hrozby, které označíme jako hrozby 1. vrstvy podle jednotlivých aktiv:
  - hrozba pro bezpečnost informací,
  - hrozba pro bezpečnost lidských zdrojů
  - hrozba pro bezpečnost procesů,
  - hrozba pro bezpečnost majetku.

ANALÝZA HROZEB

- hrozbami 2. vrstvy budou označeny dílčí hrozby podle bezpečnostních aspektů a mohou jimi být:
  - hrozba pro důvěrnost aktiva;
  - hrozba pro autentičnost (integritu) aktiva;
  - hrozba pro dostupnost aktiva.

ANALÝZA HROZEB

- hrozbami 3. vrstvy budou označeny dílčí hrozby podle nositele hrozby a mohou jimi být:
  - vnitřní útočník,
  - vnější útočník.

ANALÝZA HROZEB

- Dále lze bezpečnostní hrozby rozčlenit podle mechanismů naplnění hrozby.

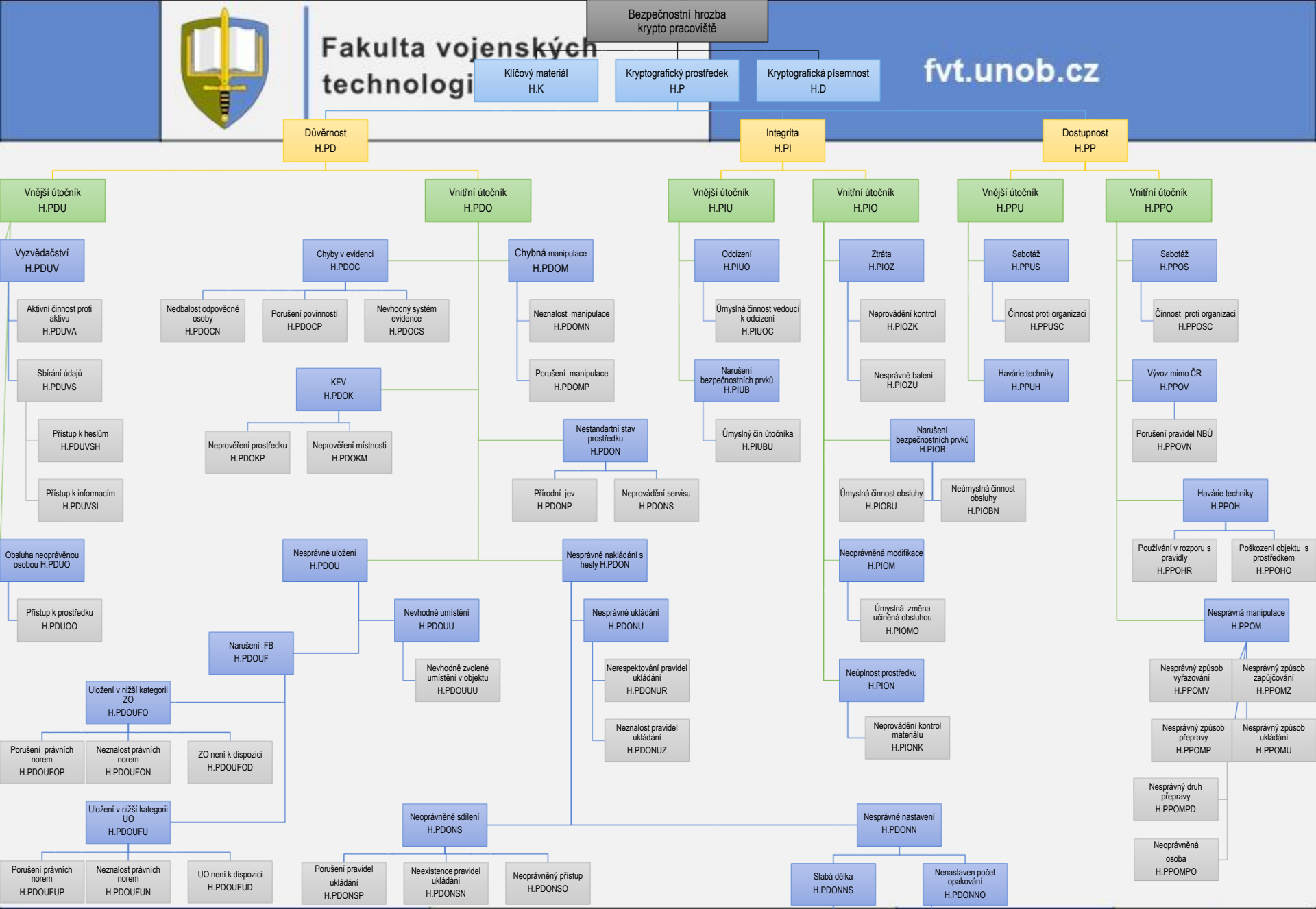
- Výše zmíněným postupem analýzy hrozeb pomocí grafu elementárních hrozeb nalezneme velkou skupinu hrozeb.

- Jako příklad pro snadnou orientaci v grafu můžeme tyto hrozby kódovat.

ANALÝZA HROZEB

H.ABC, kde

- symbol H reprezentuje hrozbu;
- symbol A = I/L/P/M reprezentuje aktivum, přičemž
  - I = informace;
  - L = lidské zdroje;
  - R = procesy;
  - M = majetek.
- symbol B = reprezentuje bezpečnostní aspekt aktiva, přičemž
  - D = důvěrnost;
  - I = autentičnost (integrita);
  - P = přístup (dostupnost).
- symbol C = reprezentuje nositele hrozby, přičemž
  - U = vnější útočník;
  - O = vnitřní útočník.


Bezpečnostní hrozba krypto 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
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 uložení H.PDOU
Narušení FB H.PDOUF
Nevhodné umístění H.PDOUU
Nevhodně zvolené umístění v objektu H.PDOUUU
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
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
Nenastaven počet opakování H.PDONNO
Nestanovení délky hesla H.PDONNSN
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

Zranitelnost

- okolnost nebo soubor okolností umožňující realizaci hrozby a tím dojde k poškození aktiv organizace.
- pozornost musíme zaměřit na identifikaci zranitelnosti.
- chce - li organizace zjistit zranitelnost, musí zaměřit pozornost na místa, jež mají vztah k aktivům:
  - fyzické prostředí organizace;
  - vedení a zaměstnanci organizace;
  - administrativní postupy organizace;
  - vnitřní chod organizace;
  - dodávka služeb pro organizaci;
  - KIS.
- aby došlo k incidentu, musí hrozba a zranitelnost působit současně. Následně dojde k poškození aktiva. Je proto nezbytné pochopit vztah mezi hrozbami a zranitelnostmi, tj. jaká hrozba může těžit z určité zranitelnosti.
- po identifikaci hrozeb a zranitelností je nezbytné posoudit pravděpodobnost, že se „setkají“ a vytvoří riziko.
- Při analýze oblasti kryptografické ochrany byly identifikovány zranitelnosti:

Zranitelnost

- **Zranitelnosti procedurálního charakteru**:
  - není definovaná bezpečnostní politika;
  - není definován management a bezpečnostní správa organizace;
  - není definována odpovědnost jednotlivých rolí v organizaci;
  - nejsou vytvořeny pravidla pro přístup k utajovaným informacím;
  - není definován režim spolupráce externích dodavatelů zboží a služeb;
  - absence systému přípravy uživatelů a vedení organizace;
  - nedostatečná příprava zaměstnanců organizace;
  - nízké bezpečnostní povědomí;
  - není vedena evidence o činnosti organizace;
  - neznalost a důvěřivost zaměstnanců;
  - nejsou pravidelně vyhodnocovány bezpečnostní incidenty;
  - neprovádění kontrolní činnosti;
  - chybné nastavení přístupových práv.

Zranitelnost

- Zranitelnosti technického charakteru:
  - nevhodné prostory pro ukládání informací;
  - nevhodné umístění aktiv organizace;
  - nefunkční technické prostředky;
  - problémy s dodávkami energií;
  - používání necertifikovaných zařízení;
  - používání neautentizovaných pomůcek;
  - zastaralé prostředky KIS;
  - nechráněný přístup ke kabelovým rozvodům;
  - používání nelegálního softwaru;
  - nesprávný způsob ničení prostředků organizace.

Protiopatření

- základní filozofie při navrhování a aplikaci protiopatření je předcházení možného vzniku škod,
- při navrhování protiopatření musí organizace pamatovat na fakt, že zvolené opatření by nám mělo pomoci k překonání následků, které mohou vzniknout.
- účelem protiopatření je nastavení:
  - postupů,
  - mechanismů,
  - praxí, a
  - pravidel, jejichž cílem je maximální eliminace vzniku a průběhu hrozeb.
- cílem je zabránění vzniku bezpečnostního incidentu či kompromitace kryptografického materiálu při maximálním snížení vzniklých škod.
- protiopatření mají svůj základ v dokumentech tvořících bezpečnostní politiku pro tuto oblast.

Protiopatření

- Protiopatření dle způsobu jejich provedení je možné rozdělit na 2 skupiny:
  - procedurální protiopatření,
  - technické protiopatření.

Protiopatření

- **Procedurální protiopatření** zahrnuje aktivity, které musí být vykonány pro OUI:
  - v oblasti **kryptografické** ochrany:
    - definování typu kryptografického pracoviště;
    - definování typu kryptografického materiálu;
    - stanovení bezpečnostní správy kryptografické ochrany;
    - vypracování bezpečnostní politiky pro oblast kryptografické ochrany:
    - vypracování pravidel používání kryptografických prostředků pro oprávněné osoby;
    - způsob evidování oprávněných osob;
    - zajištění a provádění zkoušky zvláštní odborné způsobilosti;
    - definování způsobu manipulace s kryptografickým materiálem;
    - definování bezpečnostního incidentu a kompromitace;
    - definování evidence KRYPTO materiálu;
    - vypracování režimových směrnic pro kryptografické pracoviště.

Protiopatření

- v oblasti **personální** bezpečnosti:
  - stanovení podmínek přístupu fyzické osoby k utajované informaci stupně utajení VYHRAZENÉ, DŮVĚRNÉ, TAJNÉ a PŘÍSNĚ TAJNÉ;
  - provedení Poučení zaměstnance organizace;
  - definování povinností vedoucího organizace;
  - definování povinností zaměstnance;
  - definování oprávněných osob v oblasti kryptografické ochrany;
  - výběr osob;
  - určení k výkonu kryptografické ochrany;
  - zpracování personálního projektu organizace.

Protiopatření

- v oblasti **administrativní** bezpečnosti:
  - stanovení, vyznačení, změna a zrušení stupně utajení informace;
  - stanovení způsobu vedení evidence;
  - definování způsobu přepravy či přenášení zásilky;
  - provádění obsahu kontrolní činnosti;
  - určení a používání administrativních pomůcek;
  - určení podmínek pro provádění opisu, kopie, překladu a výpisu;
  - určení osoby odpovědné za vedení písemností oblasti kryptografické ochrany;
  - dokumentární kontrola.

Protiopatření

- v oblasti **fyzické** bezpečnosti:
  - určení odpovědné osoby za projekt fyzické bezpečnosti,
  - stanovení hranice objektu, hranice zabezpečené oblasti, zařazení do třídy,
  - stanovení pravidel ke vstupu do objektu, zabezpečené oblasti nebo jednací oblasti,
  - stanovení pravidel pro ostrahu,
  - stanovení pravidel pro manipulaci s klíči, a identifikačními daty od zabezpečené oblasti (ZO) a úschovného objektu (UO).

Protiopatření

- Procedurální protiopatření musí determinovat způsoby, metody a praxe integrovaného řízení bezpečnosti organizace.

- Musí být definována bezpečnostní správa s výčtem rolí, které budou odpovědné za řízení bezpečnosti organizace, prosazování bezpečnostních cílů, řešení incidentů a zjištěných pochybení a nedostatků.

- Definování odpovědnosti rolí bezpečnostní správy je podstatným faktorem pro prosazení a aplikování adekvátní praxe v této oblasti, dále k realizaci bezpečnostních mechanismů.

Protiopatření

- **Technické protiopatření**
  - V oblasti technických protiopatření je pozornost zaměřena na zajištění OUI na pracovištích organizace při použití dostupných technických zařízení.

Protiopatření

Oblast technických protiopatření zahrnuje aktivity:

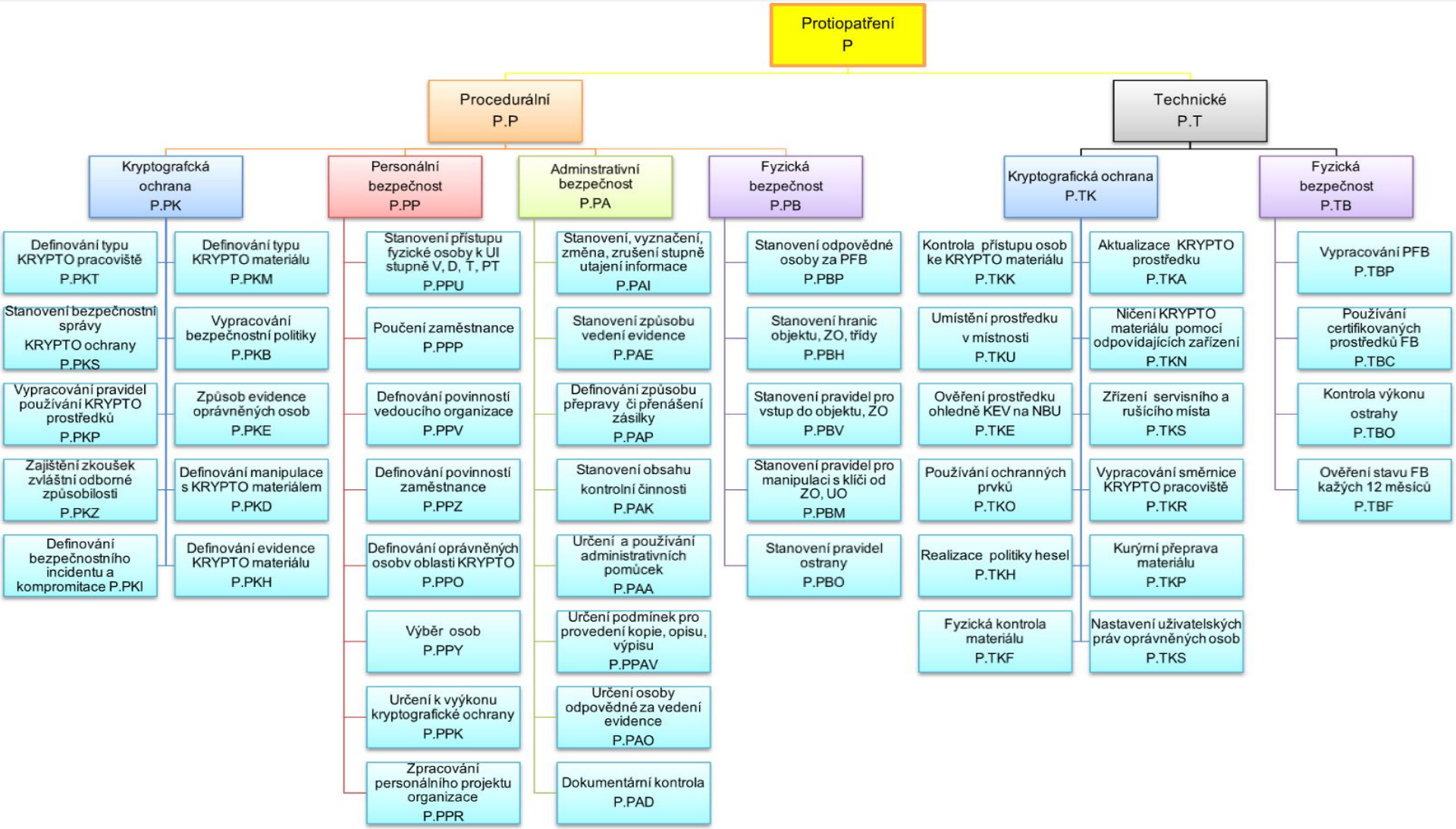
- v oblasti **kryptografické** ochrany:
  - kontrola přístupu osob ke kryptografickému materiálu včetně kontroly oprávněných činností v oblasti kryptografické ochrany;
  - pravidelné provádění kontrolní a preventivní činnosti v oblasti kryptografické ochrany;
  - zabezpečení aktualizace s nadřízeným stupněm, výrobcem, se servisním střediskem v oblasti:
    - hardwaru;
    - softwaru;
    - dokumentace ke kryptografickému prostředku.
    - umístění kryptografického prostředku v místnosti ve stanovené vzdálenosti od KIS a rozvodů elektrické energie;
    - ničení kryptografického materiálu předepsaným způsobem na odpovídajícím zařízení;
    - ověření kryptografického prostředku NBÚ z hlediska kompromitujícího vyzařování (KV);
    - zřízení servisního a rušícího místa kryptografického materiálu;
    - používání ochranných prvků;
    - vypracování režimové směrnice kryptografického pracoviště;
    - realizace politiky hesel;
    - kurýrní přeprava KRYPTO materiálu;
    - fyzická kontrola materiálu;
    - nastavení uživatelských práv oprávněných osob.

Protiopatření

- v oblasti **fyzické** bezpečnosti:
  - vypracování projektu fyzické bezpečnosti (PFB);
  - používání certifikovaných technických prostředků;
  - kontrola výkonu ostrahy a funkčnosti technických prostředků;
  - ověřování stavu fyzické bezpečnosti nejméně však každých 12 měsíců.

Protiopatření

- Přehled procedurálních a technických protiopatření systematicky rozdělených po jednotlivých druzích zajištění bezpečnosti je nutno znázornit přehledně:
  - procedurální protiopatření je označeno jako P.P;
  - procedurální protiopatření po jednotlivých druzích zajištění ochrany informací bylo označeny jako P.PK, P.PP, P.PA a P.PB a dále označeno dle konkrétního protiopatření;
  - technické protiopatření je označeno jako P.T;
  - technická protiopatření po druzích zajištění ochrany informací bylo onačeny jako P.TK a P.TPB a dále označeno dle konkrétního protiopatření.


Protiopatření
P
Procedurální
P.P
Technické
P.T
Kryptografcká ochrana
P.PK
Personální bezpečnost
P.PP
Adminstrativní bezpečnost
P.PA
Fyzická bezpečnost
P.PB
Kryptografická ochrana
P.TK
Fyzická bezpečnost
P.TB
Definování typu KRYPTO pracoviště
P.PKT
Definování typu KRYPTO materiálu
P.PKM
Stanovení bezpečnostní správy KRYPTO ochrany
P.PKS
Vypracování bezpečnostní politiky
P.PKB
Vypracování pravidel používání KRYPTO prostředků
P.PKP
Způsob evidence oprávněných osob
P.PKE
Zajištění zkoušek zvláštní odborné způsobilosti
P.PKZ
Definování manipulace s KRYPTO materiálem
P.PKD
Definování bezpečnostního incidentu a kompromitace P.PKI
Definování evidence KRYPTO materiálu
P.PKH
Stanovení přístupu fyzické osoby k UI stupně V, D, T, PT
P.PPU
Poučení zaměstnance
P.PPP
Defnování povinností vedoucího organizace
P.PPV
Definování povinností zaměstnance
P.PPZ
Definování oprávněných osobv oblasti KRYPTO
P.PPO
Výběr osob
P.PPY
Určení k vyýkonu kryptografické ochrany
P.PPK
Zpracování personálního projektu organizace
P.PPR
Stanovení, vyznačení, změna, zrušení stupně utajení informace
P.PAI
Stanovení způsobu vedení evidence
P.PAE
Definování způsobu přepravy či přenášení zásilky
P.PAP
Stanovení obsahu kontrolní činnosti
P.PAK
Určení a používání administrativních pomůcek
P.PAA
Určení podmínek pro provedení kopie, opisu, výpisu
P.PPAV
Určení osoby odpovědné za vedení evidence
P.PAO
Dokumentární kontrola
P.PAD
Stanovení odpovědné osoby za PFB
P.PBP
Stanovení hranic objektu, ZO, třídy
P.PBH
Stanovení pravidel pro vstup do objektu, ZO
P.PBV
Stanovení pravidel pro manipulaci s klíči od ZO, UO
P.PBM
Stanovení pravidel ostrany
P.PBO
Kontrola přístupu osob ke KRYPTO materiálu
P.TKK
Umístění prostředku v místnosti
P.TKU
Ověření prostředku ohledně KEV na NBU
P.TKE
Používání ochranných prvků
P.TKO
Realizace politiky hesel
P.TKH
Fyzická kontrola materiálu
P.TKF
Aktualizace KRYPTO prostředku
P.TKA
Ničení KRYPTO materiálu pomocí odpovídajících zařízení
P.TKN
Zřízení servisního a rušícího místa
P.TKS
Vypracování směrnice KRYPTO pracoviště
P.TKR
Kurýrní přeprava materiálu
P.TKP
Nastavení uživatelských práv oprávněných osob
P.TKS
Vypracování PFB
P.TBP
Používání certifikovaných prostředků FB
P.TBC
Kontrola výkonu ostrahy
P.TBO
Ověření stavu FB každých 12 měsíců
P.TBF

Samostudium otázky

- Na Vámi zvoleném příkladu aplikujte základní kroky bezpečnostní analýzy (např. mobilní telefon, notebook, stolní PC nebo sídlo firmy 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.
- HROMADA, Martin. Systém a způsob hodnocení odolnosti kritické infrastruktury. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013. ISBN 978-80-7385-140-8.
- LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-05-7.
- POŽÁR, Josef a Milan KNÝ. Reflexe funkcí bezpečnostního managementu: Výzkumné centrum bezpečnostního managementu. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-445-8.
- PROCHÁZKOVÁ, Dana. Bezpečnost, krizové řízení a udržitelný rozvoj. Praha: Univerzita Jana Amose Komenského, 2010-. ISBN 978-80-86723-97-6.
- KRULIŠ, Jiří. Jak vítězit nad riziky: aktivní management rizik - nástroj řízení úspěšných firem. Praha: Linde, 2011. ISBN 978-80-7201-835-2.