PV017 Řízení informační bezpečnosti

> Poznámky z učení se. Některé věci mohou být vynechané protože jsem je znala, nebo mi přišly nedůležité, nebo se mi nechtělo je vypisovat. A taky vám nikdo nezaručí, že jsem někde neudělala chybu nebo něco špatně nepochopila. Používejte na vlastní riziko.
>
> - hojkas

Organizace

`30b` půlsemestrální zkouška (na první 3 přednášky), `70b` záverečná písemka

Obojí kombinace otevřených a testových otázek.

Otevřená otázka je za `7b`.
Příklad:

> Popište politiku a obsah (cíl) procesu správy reakcí na bezpečnostní události.

Testová otázka je za `3b`. Má alespoň jednu správnou odpověď, musí být vybrány VŠECHNY správné odpovědi pro zisk bodů.
Příklad:

> Faktory determinující velikost rizika pro aktivum jsou
> a) zranitelnost aktiva
> b) počet aplikovaných bezpečnostních opatření pro zajištění ochran aktiva
> c) existence potenciálních útočníků
> d) hodnota aktiva
> e) klasifikační kategorie aktiva

Nesprávně zodpovězená otázka: `-1b`!

[200 IQ výpočet: 30b půlsemka ~ 3 otevřené 3 testové otázky]

Hodnocení

A 90-100
B 80-89
C 70-79
D 60-69
E 50-59

Osnova předmětu

Přednáška 1

- Co se rozumí bezpečností a informační bezpečností zvlášťě
- Koncept a anatomie informační bezpečnosti

Přednáška 2

- Jak významná je role standardů, bez nich ani ránu
- Legislativní rámec
- Co se rozumí řízením rizik - stručně
- Kdo má v instituci na starosti dosažení informační bezpečnosti

Přednáška 3

- Politiky jako specifikátory toho co a jak dělat
- Systém procesů zajišťující kontinuální efektivitu zabezpečování
- Jak takový systém procesů projektovat

Přednáška 4

- Jak zajistit provozní bezpečnost - pohled z praxe

Přednáška 5

- Jak zajistit aplikační bezpečnost - pohled z praxe

Přednáška 6

- Jak hodnotit bezpečnost
- Praktické poznatky z posuzování kyberbezpečnosti - pohled z praxe

Přednáška 1

safety vs **security**

- **safety**, bezpečí - stav bytí, ve kterém platí, že za definovaných podmínek někdo či něco nezpůsobí škodu (aka chránění proti nahodilým událostem)
- **security**, bezpečnost - ochránění proti úmyslným škodám na aktivech (v širším myslu ochránění před poškozením osob nebo aktiv v důsledku úmyslných činů)
- **information security** (informační bezpečnost) je ochrana proti úmyslným škodám, nežádoucím akcím na **informačních aktivech**

ISO standardy na kterých tu stavíme:
— `ISO/IEC 27001`: 2014 – IT – Bezpečnostní techniky – Systémy řízení bezpečností informací – Požadavky
— `ISO/IEC 27002`: 2014 – IT – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
— `ISO/IEC 27003`: 2018 – IT – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny
— `ISO/IEC 27004`: 2018 – IT – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení
— `ISO/IEC 27005`: 2019 – IT – Bezpečnostní techniky – Řízení rizik bezpečnosti informací
— `ISO/IEC 27014`: 2021 – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Správa a řízení bezpečnosti informací
— `ISO/IEC 15408`

Koncept bezpečnosti informací

> Security - the state of being free from danger or injury (Oxford Dictionary)

Bezpečnost = zajištění, jak něco NEDĚLAT

- abychom ji efektivně zajistili, musíme **znát co se nesmí dělat** (znát hodnotu majetku, jaké škody mu mohou nastat, ...)
- vývoj bezpečnostních opatření zajišťujících bezpečnost je podmíněný znalostí technologií, které lze použít k zajištění bezpečnosti, a jejich implementaci - **musíme znát, jak opatření dělat**

Nelze se bránit proti účinkům škodících akcí na bázi dosud neexistujících/neznámých technologií.

Informační bezpečnost podle standardu (27002):

> Informace je bezpečná, když je přístupná pouze oprávněným subjektům, modifikovatelná pouze oprávněnými subjekty, dostupná oprávněným subjektům (do stanovené doby).

Informace je bezpečná, je-li zajištěna její:

- důvěrnost (confidentiality)
- integrita (integrity)
- dostupnost (availability)

Také se k tomu řadí udržování dalších vlastností:

- autenticita (authenticity)
- zodpovědnost, prokazatelnost (accountability)

- nepopiratelnost (non-repudiation)
- spolehlivost (reliability)

Problém informační bezpečnosti

- Informační věk → systémy zpracovávající informace jsou každodenní věc v současné společnosti
- Počítače jsou jen systémy na zpracování informací, pouze manipulují s posloupnostmi bitů kde všechny bity mají stejné vlastnosti, po změně bitu samo o sobě nejde poznat kde ke změně došlo, sledy bitů jde nezjistitelně mnohanásobně kpírovat.
- A my přitom chceme takovým systémům důvěřovat.

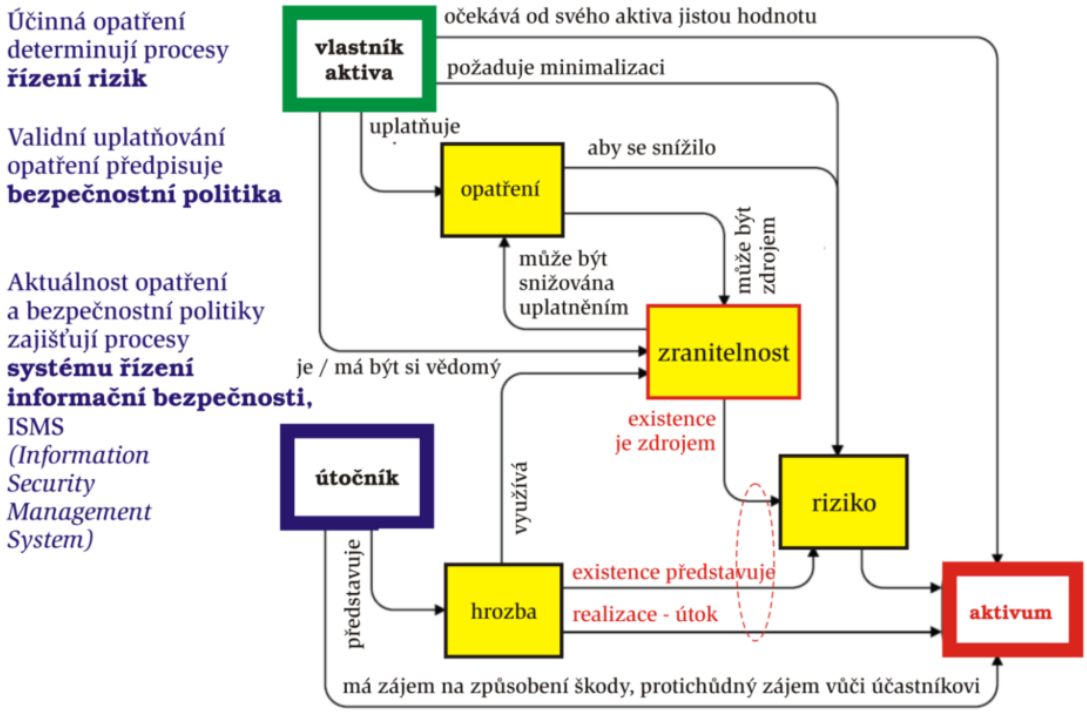
Základní pojmy informační bezpečnosti:

1. **Aktivum** (Assets): Cokoliv hodnotného, užitečného… Hlavní tři kategorie aktiv: data, lidské zdroje, systémy a komunikační infrastruktra. Něco, co vlastníkovi aktiva produkuje nebo bude produkovat pozitivní ekonomickou hodnotu.
2. **Zranitelnost** (Vulnerability): Slabina využitelná k způsobení škod/ztrát organizaci útokem.
   Zranitelné místo: Slabina v návrhu, implementaci, provozu…
   Zranitelnost: Existence zranitelného místa + potenciálních útočníků
3. **Hrozba** pro aktiva (Threats): Potenciální možnost využití zranitelného místa k útoku útočníkem. Pokud je chceme eliminovat, je nutné je identifikovat.
4. **Útok, bezpečnostní incident** (Atack, Security incident): Útok provádí útočník využitím zranitelnosti informačního aktiva (realizovaná hrozba). Způsobuje škodu na aktivech.
   Kategorie: Přírodní katastrofy. Externí útoky. Interní útoky. Selhání/lidské chyby.
5. **Riziko** (Risk): Užší význam – pravděpodobnost, že se v daném zranitelném místě uplatní hrozba. Širší význam – velikost rizika je daná pravděpodobnosti výskytu incidentu krát způsobená škoda (dopad incidentu).
6. **Opatření** (Control, Measure, Security enforcing function): Nástroj pro snížení/eliminaci rizika. Typicky rizika snižují, neodstraňují. Měla by se implementovat pouze pro řešení specifických identifikovaných rizik (a ne random “secure” věci jen proto, že je budget). Pro implementaci se používají mechanismy na bázi vhodných technologií (sw, hw, administrativa).

- **Účastník** prostředí: Vlastník aktiva
- **Škoda**: Důsledek (dopad) útoku na aktivum/hodnotu aktiva
- **Mechanismus**: (Obecná) metoda/technologie zajištění ochrany (např. šifrování, zákon, ochrana přístupu, …)

[Přeskočeno: Mechanismy pro implementaci opatření zajišťujících důvěrnost, integritu, … – symetrické/asymetrické šifrování.]

Obecný model zabezpečování



Systém bude úspěšný (bezpečný), když bude zajišťovat ochranu proti všem možným útokům (včetně takových, které v době vytváření systémů ještě neexistují).

Útočník bude úspěšný, když pro útok využije jedinou nedokonalost v bezpečnostních ochranách. Může přitom vyčkávat na dosud neexistujcící zranitelnost/technologii. Nikdy nemáme kompletní přehled o tom, co může hrozit, ani kompletní nástroje k zajištení všeho. S postupem času nyní implementované bezpečnostní nástroje mohou přestat efektivně plnit svůj cíl.

Zajištení informační bezpečnosti je komplexní problém.
Nelze ji zajistit jedním opatřením, ale kombinací několika současně. Nejen v IT, ale je třeba řešit i problémy v organizaci, řízení lidských zdrojů, fyzické bezpečnosti, legislativních omezení, ...
Zajištění informační bezpečnosti vyžaduje vytvoření a **udržování** komplexního bezpečného prostředí. (Taková prostředí jsou již definována standardy: ISO 27001, COBIT, ...)

Standard: katalog bezpečnostních opatření a způsob správy prostředí pro zabezpečování informací ve všech jejích formách, návod, jak důkladně a pečlivě řešit informační bezpečnost.

Analýzou rizik poznáme hrozby, jimž jsou aktiva vystavena. Komplexní soubor hrozeb vyžaduje systematické, promyšlené, kontextově závislé pořadí uplatňování opatření → pravidla uplatňování opatření v jistém prostředí definuje **politika** toho prostředí.

Politika – pravidla řídící dosažení cílů určenými způsoby. Jde o promyšlený systém principů. Obvykle dokument implementovaný jako procedura. **Politiky organizace** jsou prohlášení o celkovém záměru a směru podnikání vyjádřené vedením organizace, v jedné org. může být řada politik pro různé oblasti činnosti (personální politika, politika působení na trhu, sociální politika, politika informační bezpečnosti, ...).

Chybně definovaná nebo neprosazovaná bezpečnost může způsobit větší riziko než nedefinovaná bezpečnost (zatímco bezpečnost je to jak si myslíme, že jsme chráněni, skutečné bezpečí tomu nemusí odpovídat; riziko placebo efektu).

Politika informační bezpečnosti definuje bezpečné používání IT v rámci organizace, stanovuje koncept inf. bezp. org. v horizontu 5-10 let, určuje, co jsou citlivá informační aktiva (klasifikaci, odpovědnost za jejich stav), stanovuje bezpečnostní infrastrukturu (nutná nezávislost výkonných a kontrolních rolí), definuje třídu útočníků, vůči kterým se aktiva organizace zabezpečují (např. proti běžným hackerům, ale ne proti overpowered FBI...). Politika IT bezpečnosti je nezávislá na konkrétně použitých IT prostředcích.

Složitost **bezpečnostních procedur** je dána tím kolik lidské interakce se systémem probíhá + jaké jsou požadavky na spolehlivost, důvěryhodnost, ...
Typické role v bzepčnostních procedurách: Chief Security Officer (CSO), Chief Information Security Officer (CISO), security architect, security manager/officer, operátor, správce, admin, auditor.

Dosahování informační bezpečnosti: nutnou úroveň určuje kontext - počet a síla potenciálních útočníků, potenciální výše škod, jak moc to lze vylepšit implementací dostupných opatření.

- **Detekční opatření** - cílem odhalit a napravit selhání (kterému nešlo zabránit preventivně)
- **Reakční opatření** - cílem zajistit správné chování během incidentu a po něm (ohodnocení rozsahu, akce k minimalizaci dopadu, reportování o incidentu)

Bezpečnostní politika (BP): Soubor pravidel specifikující účinný způsob uplatňování opatření potřebných pro dosažení akceptovatelné úrovně rizika. BP říká, proti čemu/komu chrání, jaké jsou bezpečnostní cíle, jak se ochrana prosazuje, a způsob dosažení cílů pomoci opatření implementovaných vhodnými mechanismy.

- Pro validní prosazování informační bezpečnosti IS je nutné definovat BP odpovídající hrozbám a rizikům pro daný IS!
- BP co **konceptuálně** zavádí bezpečnost informací v organizaci musí být rozhodnutím vedení organizace. Typicky jde o několikastránkový dokument nezávislý na používaných technologiích, zavedený každých cca 5-10 let.
- BP stanovující **konkrétní** opatření v konkrétních systémech chrání konkrétní IS, je závislá na IT technologiích, reviduje se obvykle každý 1-2 roky.

Chceme, aby byly BP důvěryhodné (**trustworthy**; tj. aby prokazatelně jejím uplatňováním docházelo k dosažení požadované úrovně ochrany), a ne jen **trusted** (něco co dostává důvěru ať už zaslouženě nebo ne).

Perfektní bezpečnost neexistuje, vše je otázkou času a energie. Cílem BP je **zajistit každé aktivum "dostatečně"** (akceptovatelně).

Dosahování bezpečnosti informací je nekonečný **proces** (nikoliv jednorázový čin). Je třeba držet krok s technologií, formami útoků, legislativou. Na to je třeba udržovat BP aktivní a plánovat procesy, skrz které se BP pravidelně vypracovává a prosazuje. O to se typicky bude starat manažerský systém - **systém řízení informační bezpečnosti**.

Systém řízení informační bezpečnosti (ISMS - Information Security Management System)

- pro systematické řízení informační bezpečnosti v organizaci
  nejlépe procesově orientovaný, jako podmnožina procesů pro řízení IT a procesů podporujících plnění cílů organizace
  orientace na ochranu a zabezpečení informačních aktiv organizace
- uvnitř ISMS jde o systematické posuzování vlastností systémů, technologií a médií používaných pro informační aktiva, odhadování nákladů narušení inf. bezpečnosti, a vývoj a nasazování protiopatření vůči známým hrozbám
- zajišťování informační bezpečnosti je třeba manažersky řídit, protože:
  — management rozhodl závaznou strategii pro organizaci

— je nutné, aby zákazníci měli důvod organizaci důvěřovat
— organizace musí reagovat na zákonné předpisy
— je nutné trvale udržovat efektivnost řízení IT
- součástí je organizační struktura, politiky, plánovací činnosti, odpovědnosti, metody, procedury, procesy, zdroje

Anatomie informační bezpečnosti

Aktivum (podrobněji)

- *Hmotné* aktivum (Tangible): Peníze, budovy, SW, HW, data, lidé…
- *Nehmotné* aktivum (Intangible): Patenty, autorská práva, licence, pověst firmy, …
- **Informační aktivum** (dle zákona o kyb. bezp.):
  Informace nebo *služba*, kterou zpracovává nebo poskytuje informační/komunikační systém.
  Zaměstanci a *dodavatelé* podílejícíc se na provozu, rozvoji, správě, bezpečnostni systému.
  Technické vybavení.
  Komunikační prostředky
  Programové vybavení
  Objekty systému.

Klasifikace aktiva:

- **Důvěrnost aktiv**

  Nízká: Aktiva jsou veřejně přístupná nebo určena ke zveřejnění (např. zákonem o svobodném přístupu k informacím). Není třeba ochrana.

  Střední: Aktiva nejsou veřejně přístupná, tvoří know-how odpovědných orgánů/osob, jejich ochrana *není* vyžadována žádným právním předpisem/smluvním ujednáním.
  Pro ochranu využívány prostředky pro řízení přístupu.

  Vysoká: Aktiva nejsou veřejná, jejich ochrana *je* vyžadována právními předpisy/smlouvami.
  Pro ochranu využívány prostředky pro řízení přístupu a zaznamenávání přístupu. Přenosy informací chráněny kryptograficky.

  Kritická: Aktiva nejsou veřejná a vyžadují nadstandardní míru ochrany (např. obchodní tajemství, citlivé osobní údaje, …).
  Pro ochranu třeba evidence osob, které k aktivům přistoupily, a metody ochrany proti kompromitaci ze strany adminů.

- **Integrity aktiv**

  Nízká: Nevyžaduje integritní ochranu. Narušení integrity nic neohrožuje.

  Střední: Může vyžadovat ochranu. Narušení integrity může vést k poškození oprávněných zájmů odpovědných orgánů a osob a může se projevit méně závažnými dopady na ostatní aktiva.
  Pro ochranu využívány standardní nástroje, např. omezení práva k zápisu dat.

  Vysoká: Vyžaduje ochranu. Narušení vede k poškození oprávněných zájmů s podstatnými dopady na ostatní aktiva.
  Ochrana: Speciální prostředky na sledování historii změn a identitu toho, kdo je provedl.

  Kritická: Vyžaduje ochranu. Narušení vede k vážnému poškození oprávněných zájmů s velmi vážnými přímými dopady na ostatní aktiva.
  Ochrana: Speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. digitální podpis).

- **Dostupnost aktiv**

Nízká: Narušení dostupnosti není důežité, v případě výpadku je ok delší čas na nápravu (např. týden).
Ochrana: Pravidelné zálohování.

Střední: Narušení dostupnosti by nemělo překročit dobu pracovního dne, dlouhodobější výpadek by vedl k ohrožení oprávněných zájmů osob a odpovědných orgánů.
Ochrana: Běžné metody zálohování a obnovy.

Vysoká: Narušení dostupnosti by nemělo překročit několik hodin. Výpadek je třeba řešit ihned, protože vede k přímému ohrožení zájmů.
Ochrana: Záložní systémy, obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnnou technických aktiv.

Kritická: Narušení dostupnosti aktiva není přípustné ani krátkodobě (v řádu minut) protože vede k vážnému ohrožení zájmů.
Ochrana: Záložní systémy, obnova poskytování služeb automatizovaná a krátkodobá.

Zranitelnosti se mohou nacházet v: fyzickém uspořádání, organizačních schématech, admin. opatřeních, personální politice, technických opatřeních, HW, SW, datech, návrhu, systému řízení informační bezpečnosti [how the turntables].

Typy hrozeb

- **Odhalení** (Disclosure) citlivých důvěrných dat, postupů. Např. skrz špehování, kryptoanalýzu.
- **Podvod** (Deception): Modifikace dat, falšování identity, popírání autorství, hoaxes, masquarade (tváření se jako legitimní uživatel), planting (trojský kůň, vir), modifikace systému (pro budoucí útoky)
- **Narušení** (Distruption): Modifikace dat, programu, chování, neoprávněné využití zdrojů, nebo modifikace přenášených dat.
- **Uchvácení** (Usurpation): Zpoždění služby, DoS, narušení autorizace…
- Vnitřní
- Vnější

Automatizace business světa usnadňuje podvod (který by papírově byl komplikovaný). Geografie nehraje roli, možnost útoků odkdekoliv na velké množství cílů, nedostatečná jurisdikce v některých zemích.

Útočník

- Atributy: Cíle, metody, schopnosti, financování, outsider/insider.
- Klasifikace dle IBM (třídy):

  0: script kiddies bez znalosti systému, využívají pouze existující nástroje, pokus/omyl
  1: chytří nezasvěcení bez znalosti systému, středně sofistikované vybavení, využijí existujících zranitelností
  1.5: dobře vybavení outsideři základní znalost systému, dobré vybavení
  2: zasvěcení insideři znalost systému, specifické technické znalosti, sofistikované nástroje
  3: dobře financované organizace schopné utvořit týmy specialistů s top financováním a top nástroji, schopné detailních analýz systému a vytváření nových typů útoku

Opatření = nástroj pro snižování rizik.

- Zranitelnost může být zdrojem hrozby. Možnost uplatnění a dopadu hrozby představuje riziko.
- Typicky kombinace technologie, chování a procedury. (Např. antivir – technologie: SW, chování: neotvírat přílohy junk mailů, procedura: aktualizace SW)

- Cena opatření musí být menší než výše škod.
- Klasifikace
  — dle **technologie implementace**: Administrativní (norma pro návrh, testování, kódění), logická (SW), technická (HW), fyzická (zámek, trezor, záložní generátor), …
  — dle **konceptu**: Preventivní (autentizace, autorizace, šifrování, řízení přístupu, záložní generátor), heuristická, detekční (audit, detekce útoků, virů, detekce ohně) a opravná (plán po detekci incidentu), podpůrná (identifikace, správa krypto-klíčů).
  — dle **oblasti nasazení**: Řízení a správa bezpečnosti, technologická bezpečnost, bezpečnost provozního prostředí.

Bezpečnostní opatření jsou implementovány **bezpečnostními mechanismy**

- Klasifikace dle odolnosti:
  Slabé: ochrana proti náhodným neúmyslným útokům nebo amatérům
  Střední: ochrana proti "běžným" útokům střední síly
  Silné: ochrana proti profesionálům s vysokou úrovní znalosti

Generické rysy zabezpečování informací

- Cílem minimalizovat prostor pro útok. Každá nadbytečná vlastnost aplikace může přidat riziko útoku.
- Implicitně používat bezpečná řešení (a pokud ne toli bezpečná mají být k dispozici, omezit přístup k nim a aspoň mít bezpečí opt-out místo opt-in)
- Princip nejmenších dostatečných práv, separace rolí
- Každý externí systém implicitně považovat za nedůvěryhodný (např. i balíčky třetích stran)
- Vyhnout se "Security through obscurity"
- Správně opravovat chyby (v souvislostech, prozkoumat je, ne jen "záplaty")

Přednáška 2

[TODO]

Přednáška 3

[TODO]

Přednáška 4

[TBD]

Přednáška 5

[TBD]

Přednáška 6

[TBD]