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.

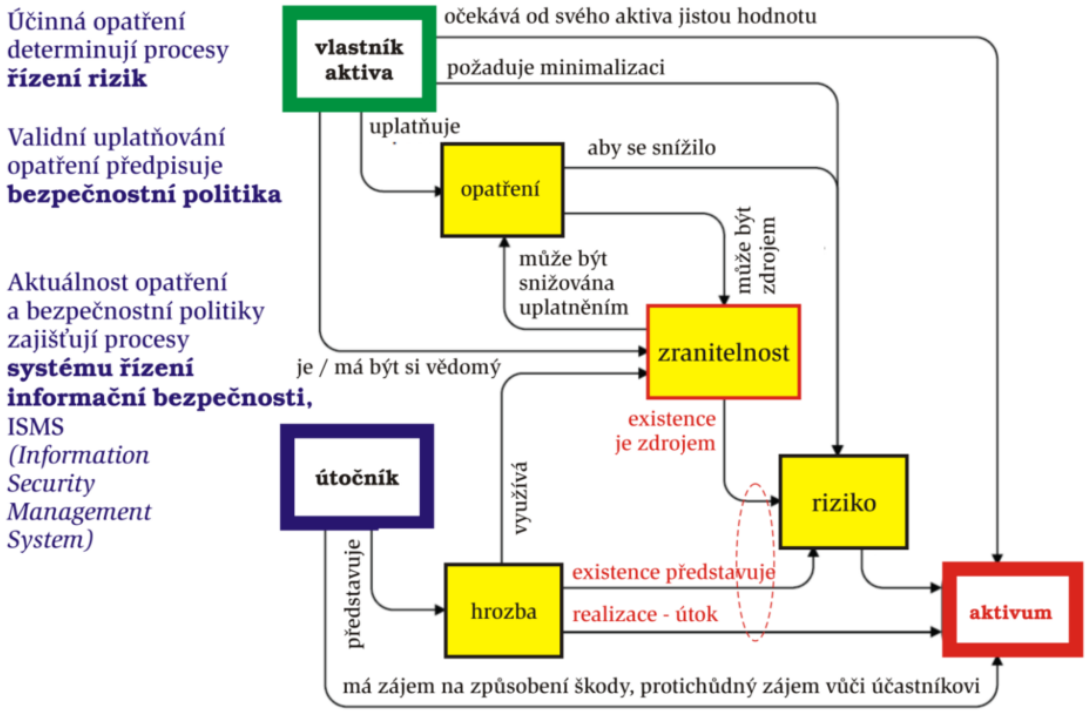
Základní pojmy informační bezpečnosti:

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

Standardy (normy) informační bezpečnosti

Norma se v Česku (hlavně mimo IT) používá z historických důvodů, v oblasti IT se spíše používá slovo **standard** (je to ale v našem kontextu to samé). **Doporučení** je termín používaný některými organizacemi vydávajících standardy místo termínu “standard”.

De facto standard je standard vyvinutý na bázi konsensu komunity (místo nařízení jedné organizace jde o souhlas určité komunity, např. RFC).

De iure standard je standard “podle práva”, úmluva schválená uznávanou institucí, např. ISO.

De facto standardy se vydávájí rychleji. Vyzrálé de facto s. bývají často přepracovány časem (nebo přebrány jejich rysy) do de iure standardů.

Žádný standard **není** sám o sobě **právně závazný**. Avšak může být (např. státem) zavede právní předpis, který dodržování některých standardů dává povinně, např. povinnost vyhovění určitému standardu technologie, pokud chce výrobce svoje produkty prodávat v EU.

Produkt, služba, proces, … může **vyhovovat standardu** (prohlášení, že splňuje podmínky standardu) nebo může být **certifikovaný** (existuje certifikát vydaný neutrální třetí stranou, který potvrzuje, že to vyhovuje standardu).

Problémy standardů

- Musí být odsouhlasený všemi členy komunity, mnoho pohledů na to, co je správné. Pokud je ve standardu mnoho optional věcí nebo hodně možností, blbě se implementuje.
- Standard je **jenom** dokument, jehož interpretace se může lišit (obzvlášť při překladech do jiných jazyků).

De facto standardy

- **RFC** (Request for Comment). Internetové standardy. V pozadí působí **ISOC** (Internet Society), internet repreztuje a dělá konečné rozhodnutí o přijetí **IAB** (Internet Activities Board), hlavní zodpovědnost za vývoj a posuzování RFC je delegován na technickou poradní komisi **IETF** (Internet Engineering Task Force).
- **ISACA** (Information Systems Audit and Control Association). Mezinárodní organizace auditorů výpočetních systémů. Roku 1996 vydala **COBIT** (the Control Objectioves for Information and related Technology), set best practices pro it management.
- **OWASP** (the Open Web Application Security Project). Otevřená komunita soustředěná na vylepšování bezpečnosti SW. Standard vývoje bezpečné webové aplikace. Standard testování bezpečné webové aplikace. Standard hodnocení kritéria záruk za bezpečnost webové aplikace.
- **ISF** (Information Security Forum). Mezinárodní nezávislá neziskovka věnující se měření a rozvoji praktik v IT bezpečnosti.
- **Firemní/propriertární standardy**. Typicky standardy patentovaných technik, nástroj pro udržení trhu silnou společností. Např. PKCS (Public-Key Cryptography Standards) z RSA Labs.

ISO standard (de iure standard). ISO - International Organization for Standardization.

- V současné době především rodina standardů ISO/IEC 27000, která je celosvětově uznávaný základní standard zajišťování informační bezpečnosti.

- Odpovědnost za tvorbu norem mají **technické výbory** (Technical Committees, TC), kterých je cca 200.
- **Životní cyklus** ISO standardu:

  Návrh nové pracovní položky → Committee Draft (2 měsíce) → Draft International Standard (6 měsíců) → Final Draft International Standard (2 měsíce)

  Obvykle pětiletá perioda hodnocení mezinárodního standardu (po které se přehodnocují existující standardy, ale když se odhalí vada dřív, jsou přijímána opatření, aby standardy byly revidovány i dříve).
- Standardy ISO rodiny 27000 zvýrazněné ve slidech:
  - `ISO/IEC 27000 Information security management systems - Overview and vocabulary`
  - `ISO/IEC 27001:2013 Information Security Management System - Requirements`.

    Definuje požadavky na funkcionalitu a vlastnosti systému řízení informační bezpečnosti (ISMS - Information Security Management System). Detailní popis požadavků, které ISMS *musí/má* (*must*, *shall*) splňovat, aby standardu vyhověl. Standard nezávisí na technologii, určený pro všechny typy, velikosti a sektory působení organizací.

    V dodatku je seznam cílů opatření (definovaných blíže v 27002), povinností pro splnění 27001 je porovnat zvolená opatření při zvládání rizik s tímto seznamem (aby se na nic nezapomnělo, seznam ale není úplný, lze použít i jiné věci). 27001 nařizuje použít 27002 jako zdroj návodů pro volbu a implementaci opatření (ale nezakazuje použití dalších zdrojů).

    Organizace se může certifikovat na vyhovění 27001.
  - `ISO/IEC 27002:2013 Code of practise for information security management`

    Doporučení jak navrhovat, implementovat, udržovat a vylepšovat opatření prosazující informační bezpečnost. Používá slova *may*, *should*. Návod, jak implementovat ISMS, rady pro budování bezpečného systému.

    Mezinárodně uznávané nejlepší praktiky řízení informační bezpečnosti.

    Certifikace vyhovění se nedělá, jenom se vyhovění deklaruje.
  - `ISO/IEC 27003 Information security management system implementation guidance`

    Ozkoušené rady pro implementování ISO rodiny 27000, detailnější vysvětlení částí 27001.
  - `ISO/IEC 27004 Information security management - Measurement`
  - `ISO/IEC 27007 Guidelines for information secruity management systems auditing` O auditování řídících systémů v ISMS.
  - `ISO/IEC 27008 Guideliness for auditors on security management controls` O auditování prvků informační bezpečnosti v ISMS.
  - `ISO/IEC 27014 Governance of information security`
  - `ISO/IEC 27034-2 2016 Guideliness to plan and prepare for incident response`
  - `ISO/IEC 27037 Guidelines for identification, collection, acquisition, and preservation of digital evidence` One of the IT forensics standards.

NIST Special Publications (SP)

- rodina `SP 800 Computer security`: guidelines o počítačové/kybernetické/informační bezpečnosti, doporučení a materiály
- rodina `SP 1800 NIST Cybersecurity Practice Guides`: doplňuje rodinu SP 800, soustředí se na konkrétní výzvy kybersecurity, praktické návody jak adoptovat přístupu ke kybersecurity založené na standardech
- rodina `SP 500 Computer Systems Technology`: obecnější

Řízení rizik

Rizika reprezentují negativní dopad na systém využitím zranitelnosti, přičemž zohledňují pravděpodobnost útoku i dopad (škody).
Rizika mohou plynout z: cílů a řešení podnikatelských procesů, nedokonalého vyhovění zákonným/smluvním závazkům, úrovně kvality návrhových, implementačních a provozních procedur aplikačních systémů.
Mohou existovat nezávisle na naší vůli (výpadek energie, požár, zemětřesení, ...)

Standard `ISO/IEC 27001` požaduje, aby organizace přistupovala k výběru a k provozování bezpečnostních opatření **na základě** znalosti rizik. Nejen na bázi aktiv, ale i scénářů, co se jim může stát. Rizika je potřeba zvažovat napříč celé chráněné oblasti.

Riziko má **pravděpodobnost** a **dopad hrozby**.

Generická úroveň rizika:
$uroven\_rizika = F(pravdepodobnost\_utoku) \times F'(dopad\_utoku)$

Rizika se zvládají volbou a uplatňováním vhodných **opatření**. Abychom riziko zvládli (eliminovali ho nebo snížili jeho úroveň), musíme ho nejprve ohodnotit – **identifikovat**, **analyzovat** a **vyhodnotit** (určit úroveň).

Tento proces usnadní např. použití **tabulky rizik aktiv** (kde jsou aktiva v relaci s faktory určujícím rizika). Faktory určující riziko: hrozba, zranitelnost, id, osoba zodpovědná za zvládání rizika, výše možné škody, pravděpodobnost útoku, typ útočníka.

`ISO/IEC 27005 Information technology - security techniques - Information security risk management`

Procesy řízení rizik

- Ustanovení kontextu (oblasti, kritérií, ...)
  Vymezení účelu provedení řízení rizik, spravované oblasti a hranic, zajištění zdrojů pro řízení rizik, stanovení kritérií pro vyhodnocování dopadu útoků, úrovní rizik, akceptovatelnosti rizik, stanovení organizačního zajištění a odpovědnostních rolí za řízeneí rizik.
- Ohodnocení rizik: identifikace rizik $\rightarrow$ Analýza rizik (určení velikosti) $\rightarrow$ Vyhodnocení rizik (určení úrovní rizik porovnáním se stanovenými kritérii)
  Výstupem je prioritně řazený seznam ohodnoceneých rizik a prohlášení o aplikovatelnosti vhodných opatření, která tato rizika budou řešit.
- Zvládnutí rizik: Proces modifikující rizika, výběr a implementace opatření snižujících rizika. Rizika jsou zvládnutá, když jsou identifikovaná, analyzovaná a posouzená pro aktiva z pohledu důvěrnosti, integrity a dostupnosti.

  Cílem je určit rizika:
  — která se eliminují
  — která nelze eliminovat a která se sníží na akceptovatelnou úroveň implementací určitých opatření

— tolerovaná rizika, pro které se odmítla opatření – akceptovatelná rizika (do byznys modelu se zabudují náklady na škody)
— která se přenesou smluvně nebo pojištěním na jinou organizaci (sdílení nákladů na škody)

- Akceptace rizik: Rozhodování o přijatelnosti rizika dle stanovených kritérií. Odsouhlasení plánu zvládání rizik managementem organizace.
- Informování o rizicích: Sdělení informace o rizicích všech, kdo je může ovlivnit nebo být jimi ovlivněn. Aka managementu a zaměstancům. Následuje implementace zvolených opatření do procesů organizace.
- Monitorování a přezkoumávání rizik a procesu řízení rizik: Rizika nejsou statická, je třeba odhalovat změny v kontextu, rizicích, faktorech… při běžné činnosti organizace.

Řízení informační bezpečnosti v organizaci: Management, role a odpovědnosti

Aktivity managementu organizace při zabezpečování informací: Vypracování a prosazování bezpečnostních politik, identifikace rolí a odpovědností, řízení rizik, výběr a implementace adekvátních bezpečnostních opatření, správa konfigurace IT systémů, plán činnosti po incidentu, školení v oblastní ITSec, zajišťování provozních činností (údržba, audit, monitorování, reakce na incidenty).

`ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security`

V organizaci musí fungovat systém procesů, standardů a praktik, kterými se řídí a ovládají aktivity zajišťující informační bezpečnost.

Řízení informační bezpečnosti musí:
— sladit cíle, strategie informační bezpečnosti s podnikatelskými cíly a strategiemi
— dodržovat legislativu, právní předpisy a smlouvy
— být posuzováno, analyzováno a implementováno principy řízení rizik, které jsou podporovány řídícím a kontrolním systémem organizace

Vrcholový management organizace (nejvyšší vedení odpovědné za chod organizace jako celku). Vytváří celkové podnikání, strategie, postup rozvoje, definuje cíle, které nižší vrstvy managementu rozkládají a uvádějí v chod.

Tradiční struktura velké organizace má *dualistický* model řízení, kde vše řídí správní rada rozdělená na dozorčí radu a výkonné vedení (představenstvo).

Správní rada (Governing Body), skupina osob odpovědných vlastníkům organizace, určuje strategie a politiky řídící činnosti a zajišťuje jejich prosazování. Tvořena obvykle dozorčí radou a výkonným vedením.

- **Dozorčí rada** (Supervizory Board) se typicky schází několikrát do roka, aby odsouhlasila zásadní změny ve společnosti.
- **Výkonné vedení** (představenstvo; Executive Management) je osoba nebo skupina lidí, na které dozorčí rada přenáší odpovědnost za implementaci strategií a politik pro dosažení cílů organizace. Veškerý chod organizace je delegovaný na **výkonného (generálního) ředitele** (CEO).

Příklady rolí ve výkonném vedení:
— Board of Directors (rada ředitelů, nejvyšší management, CEO, CFO Financial, COO Operating)
— Board of Directors 1 (střední management, CIO Chief Information Officer, **CISO** Chief Information Security Officer, další ředitelé)

Zásady řízení informační bezpečnosti organizace

- Bezpečnost se zavádí v rámci celé organizace, plně integrováním aktivit informační bezpečnosti do procesů organizace. Rozhodování o informační bezpečnosti musí přihlížet k podnikatelským záměrům a dalším skutečnostem.
- Zavedení informační bezpečnosti vychází z výstupů procesů řízení rizik. Ty určí, jak silné zabezpečení dává smysl, vyvažování rizika ztráty a nákladů na zabránění tomu.
- Zajištění shody s interními a externími požadavky, aby informační bezpečnost byla ve shodě s právními předpisy, smluvními závazky, atd.
- Hodnocení efektivity informační bezpečnosti sleduje podnikatelské cíle (jak moc fungují opatření se nesleduje izolovaně, ale naopak v kontextu s podnikatelskou výkonností)
- Musí se podporovat pozitivní přístup k informační bezpečnosti. Informační bezpečnost je vystavena na lidech, kterým je potřeba cíle informační bezpečnoosti dobe komunikovat, vzdělávat a koordinovat je.

Co se hodnocení procesů řízení informační bezpečnosti v organizaci týče:

- Správní rada musí zajistit, aby podnikatelské záměry zohledňovaly problémy informační bezpečnosti. Musí prioritizovat a zahajovat požadované akce.
- Výkonný management musí zajistit, aby informační bezpečnost podporovala plnění podnikatelských cílů.

Co se řízení týče:

- Správní rada musí vymezit akceptovatelnou výši rizik, schvalovat strategii informační bezpečnosti, přidělit zdroje.
- Výkonný management musí rozvíjet a realizovat strategii a politiku informační bezpečnosti, sladit cíle bezpečnosti a podnikatelské, prosazovat pozitivní kulturu.

Co se monitorování týče:

- Správní rada musí posuzovat účinnost řízení informačních činností, zajistit shodu s interními/externími požadavky, brát v úvahu dopad měnících se podnikatelských záměrů a prostředí na informační rizika.
- Výkonný management musí monitorovat na základě metrik relevantních k podnikání, poskytovat správní radě zpětnou vazbu o výsledcích měření výkonu opatření informační bezpečnosti a jejich dopadů, a upozorňovat radu na nové relevantní skutečnosti.

Co se komunikace týče:

- Správní rada musí komunikovat úroveň bezpečnosti s externími stranami, sdělovat výkonnému managementu výsledky externích přezkoumání a požadovat napravení nedsotatků, rozpoznávat legislativní závazky a očekávání zainteresovaných stran a potřeby podnikání.
- Výkonný management musí informovat radu o záležitostech vyžadující rozhodnutí a instruovat příslušné strany ve vykonávání akcí na podporu prosazení směrnic a rozhodnutí správní rady.

Co se získání záruk týče:

- Správní rada spouští nezávislé objektivní přezkoumávání, audity a certifikace. Musí objednat nezávislé a objektivní názory na to, jak plní své odpovědnosti za zajištění a udržení požadované úrovně informační bezpečnosti.
- Výkonný management musí podporovat provádění auditou, hodnocení nebo certifikace.

Řízení informační bezpečnosti podle `ISO/IEC 27002`

- `ISO/IEC 27002` je (neúplným) výčtem použitelných opatření pro řízení informační bezpečnosti (cca 150 nástrojů v 11 skupinách). Vesměs orientované na zpracování informací vlastním týmem nebo třetí stranou.
- Aby uplatnění standardu bylo ok, musí být *vypracována bezpečnostní politika* reflektující bezpečnostní cíle, *management musí politiku prosazovat* a má být *implementovaný měřící systém* pro hodnocení řízení informační bezpečnosti.
- Standard vyžaduje na vysoké úrovni abstrakce bezpečnostní politiku
  — bezpečnostní cíle organizace
  — systém pro analýzu a vyhodnocení rizik a volbu opatření
  — požadavky na vyhovění specifickým politkám, zákonným standardům, smluvním požadavkům, …
  — odpovědnost za správu bezpečnosti

  Tato politika je odsouhlasena managementem, předložena zaměstnancům a třetím stranám, je pravidelně přezkoumávána a obsahuje jasně definované odpovědnosti za informační bezpečnost.

Řídící výbor informační bezpečnosti (popř. samostatný architekt informační bezpečnosti) je ustanovený nejvyšším managementem organizace, fórum členů napříč funkční strukturou organizace. Informační bezpečnost má být koordinována představiteli různých částí organizace působících v relevantních pracovních funkcí. **Bezpečnostní architekt** je člen výboru pověřený péčí o celkovou architekturu.

- Stanovuje:
  Cíle informační bezpečnosti.
  Oblast působení ISMS.
  Hodnoty akceptovatelného rizika pro aktiva.
  Metriky vyhovění bezpečnostním politikám a jejich periodické kontrolování.
- Odsouhlasuje:
  Role, odpovědnosti, metodologie a procesy použité pro dosažení informační bezpečnosti.
  Validnost funkce ISMS.
  Přidělení rolí a odpovědností stanovených bezpečnostní politikou.
  Hlavní iniciativy vylepšování informační bezpečnosti v organizaci.
- Zajišťuje:
  Aby si celá organizace byla vědoma toho, jak se řeší informační bezpečnost.
  Dostatečné zdroje pro vývoj, implementaci a provozování ISMS.
  Koordinaci implementací bezpečnostních opatření napříč organizací.
  Provedení adekvátních kroků cílených na vylepšení ISMS.
  Posuzování ISMS managementem.
- Posuzuje:
  Adekvátnost opatření a koordinování jejich implementací.
  Význam bezpečnostních incidentů.
  Bezpečnostní politiku, schvaluje ji.
- Sleduje:
  Změny klíčových informací aktiv a jejich vystavení hrozbám.

- Kontroluje:
  Existenci zdrojů pro dosažení cílů.
  Dostatečnou integraci ISMS do procesů organizace.
  Plnění programu bezpečnostního uvědomnění a chápání ISMS.

Manažer informační bezpečnosti (CISO - Chief of Information Security Officer)

- Většinou ustanoven řídícím výborem informační bezpečnosti. Je třeba, aby byl v oddělení bez konfliktu zájmů. (V malých firmách ale role často sdružena s šéfem IT, ve velkých samostatná role pod CEO nebo jiným oddělením). Nesmí být z interního auditu.
- Musí znát nejen informační bezpečnost obecně, ale i byznys procesy v organizaci.
- Koordinuje činnosti o ochraně dat, schvaluje metody ochrany zařízení a komunikací. Navrhuje metody autentizace, šifrování, pravidla práce z domova. Definuje požadavky na bezpečnostní vlastnosti služeb, na bezpečný vývoj IS. Analyzuje činnost uživatelů pro odhalení podezřelého chování. Provádí posuzování kvality ISMS, monitoruje vyhovění standardům. Řeší co jsou zainteresované strany v ITSec a jaké mají požadavky.
- Oblasti práce:

  Vyhovění legislativním, regulačním a smluvním požadavkům

  Oblast řízení rizik: Navrhuje výběr opatření, identifikuje změny rizik a zajišťuje reakci, koordinuje ohodnocování rizik, iniciální posouzení rizik, zajišťuje že vrcholový management odsouhlasuje vše potřebné (rizika, plán zvládání, přístup k řízení, ...)

  Oblast řízení lidských zdrojů: Ověřuje uchažeče o zaměstnání z hlediska ITSec, vypracovává plán školení v oblasti ITSec, zvyšuje povědomí o ITSec, navrhuje disciplinární řízení.

  Ve vztahu s vrcholovým managementem: Komunikuje. Navrhuje opatření, náklady a zdroje, sděluje důležité info, rizika, poskytuje rady.

  Navrhuje rozpočet, vylepšení a opravy ITSec, sděluje výsledky, dohlíží na opravné akce (a zodpovídá za ně), informuje o postupu. Eviduje info o aktivech. Bezpečně likviduje stará zařízení.

  U třetích stran: Ohodnocuje rizika, kontroluje vhodnost kandidátů, definuje položky do smlouvy týkající se ITSec.

  Definuje akceptovatelné komunikační kanály.

  Koordinuje analýzy dopadů katastrofických indidentů a plán činnosti po nich, koordinuje cvičení a testování plánů. Po incidentu oponuje plán obnovy.

  V technické bezpečnosti: Odsouhlasuje metody ochrany dat mobilních zařízení, sítích, kom. kanálech. Navrhuje metody autentizace, politiku hesel, šifrování, ... Definuje principy bezpečného vývoje, vlastnostni online služeb. Analyzuje záznamy o činnosti uživatelů (hledá podezřelou).

  V oblasti správy dokumentů: Navrhuje drafts dokumentů v ITSec (politiky, metody řízení rizik, plán zvládání, ...). Odpovídá za oponování a aktualizaci těchto dokumentů.

  Oblast správy bezpečnostních incidentů: Přijímá zprávy o bezpečnostních incidentech, koordinuje reakce na ně, zprávy o nich, připravuje důkazy pro právní řízení po incidentech. Analyzuje incidenty (vč. prokázání příčin s cílem prevence), určí adekvátní opravné/preventivní akce. Spolupracuje na plánu zachování činnosti po incidentech, navrhuje korekce toho plánu, a školí o tom.

Další odpovědné role za informační bezpečnost

- **Oddělení IT** odpovídá za zajištění výkonu bezpečnostních opatření systémů v jejich správě, bezpečnost servroven, spolupráce při identifikace hrozeb, hodnocení rizik, ...
- **Lokální adminstrátoři** odpovídají za registrace a rušení uživatelů ze systému, monitorování systémů, připravu bezpečných procedur, zálohování dat, navrhování aplikační bezpečnosti, implementace vnitřních opatření, testování nouzových plánů.
    - **Správci systémů** za to odpovídají na úrovni systémů (implementace opatření, identifikace hrozeb, nastavování správy uživatelů, hesel, aktualizování procedur, ...)
    - **Správci sítí** za to odpovídají na úrovni domény nebo sítě (hrozby v síti, hodnocení rizik, implementace síťových opatření jako firewall, bezpečná konfigurace sítě, ...)
- **Správci areálů** odpovídají za identifikaci hrozeb, implementaci vybraných fyzických opatření, detekci a likvidaci požáru, veřejné služby (elektřina, plyn) a jejich zálohování, dodávky, expedice, ...
- **Uživatelé IT** musí znát a dodržovat politiku informační bezpečnoosti organizace
- **Třetí strany** mají odpovědnosti stanoveny ve smlouvě

Přednáška 3

[TODO]

Přednáška 4

[TBD]

Přednáška 5

[TBD]

Přednáška 6

[TBD]