PV017 Řízení informační bezpečnosti

Podzimní semestr 2022/2023

DŮVĚRYHODNÝ PV017
STUDIJNÍ MATERIÁL
CERTIFIKOVÁNO STUDENTY

> Poznámky vytvořené během učení se na zkoušky.
>
> 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. Jo a jestli vám to místy přijde chaotické, věřte mi, že některé materiály byly ještě víc.
>
> Používejte na vlastní riziko.
>
> WORK IN PROGRESS! 👷 Pokusím se stihnout do předtermínu
>
> `hojkas`

HojkasDoc™

PV017 Řízení informační bezpečnosti

Organizace

- Hodnocení

Přednáška 1

- Koncept bezpečnosti informací
- Anatomie informační bezpečnosti

Přednáška 2

- Standardy (normy) informační bezpečnosti
- Řízení rizik
- Řízení informační bezpečnosti v organizaci: Management, role a odpovědnosti

Přednáška 3

- Politika informační bezpečnosti
- Systém řízení informační bezpečnosti (ISMS)
- Projekt implementace ISMS

Přednáška 4

- Kyberbezpečnost
- Ochrana osobních údajů

Přednáška 5

- SDLC vs Secure SDLC
- Microsoft SDL

Přednáška 6, část 1

- Kritéria hodnocení bezpečnosti
- Common Criteria (CC)

Přednáška 6, část 2

- Praktické poznatky z posouzení stavu informační a kybernetické bezpečnosti v organizaci

Přednáška 7

- Security Operations in real life

Organizace

[Toto nezestárlo dobře, informace z mailu, které na poslední chvíli změnil.]

`30b` půlsemestrální zkouška (na první 3 přednášky), `70b` záverečná písemka
[Až na to, že půlsemka měla `32b`, takže závěrečná bude asi `68b`.]

Obojí kombinace otevřených a testových otázek.

Otevřená otázka je za `7b`. [Až na to, že na půlsemce byla za `6b`.]
Příklad:

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

Testová otázka je za `3b`. [Až na to, že na půlsemce byla za `4b`.]
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`!

Hodnocení

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

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.

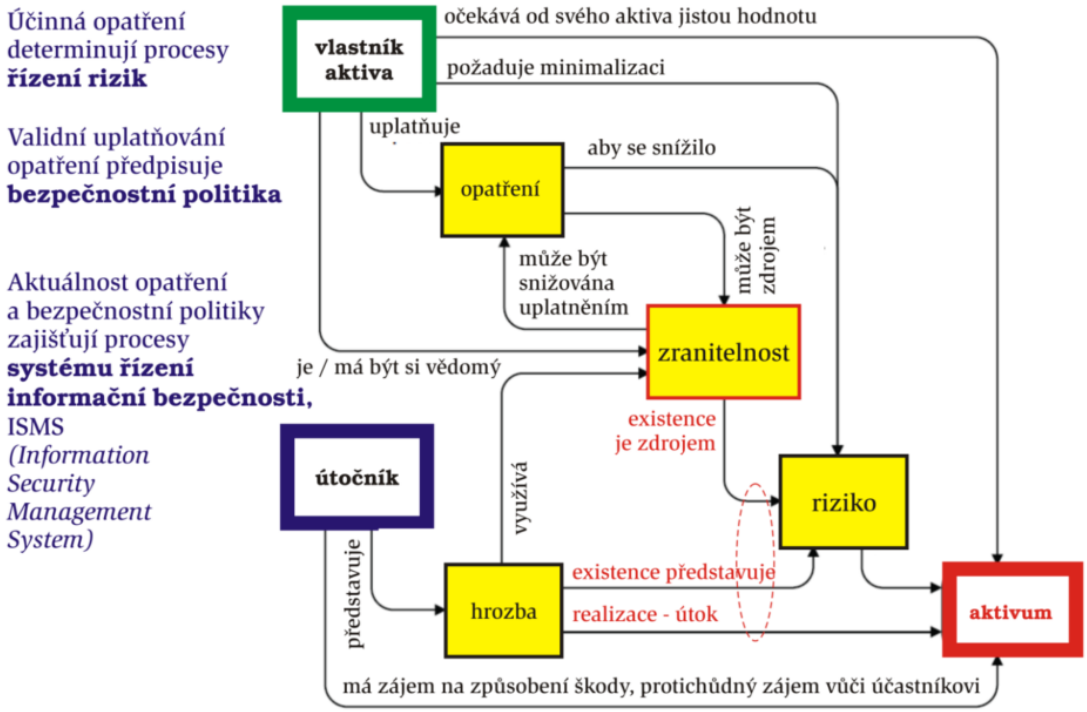
Základní pojmy informační bezpečnosti:

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

[Nebyl záznam. Vytvořeno pouze ze slidů.]

Politika informační bezpečnosti

Politika = systém pravidel řídící dosažení cílů určitými způsoby
Politika organizace: Prohlášení o celkovém záměru a směru podnikání, formálně vyjádřené vedením organizace. Organizace typicky mají řadu politik pro různé oblasti činnosti, které jsou pro ně důležité (personální, cash flow policy, sociální politika, ...)

Politika je konceptuální dokument, který má respektovat činnosti, lokality a aktiva organizace, nad tím definovat systém stanovení cílů a strategií řízení organizace a rizik + ustanovit kontext ve kterém působí a kritéria evaluace rizik a strukturu procesu jejich hodnocení.

Hierarchie bezpečnostních politik

1. **Bezpečnostní politika organizace** (nejvyšší politika)
   Souhrn bezpečnostních zásad a předpisů, množina pravidel definujících správu a ochranu aktiv organizace. Definuje způsob zabezpečení jako celku. Je typicky podpořena mnoho dalšími politikami (z oblasti ITSec - InfoSec, ISMS politika - i mimo, např. Business Continuity Plan).

   Standard `ISO/IEC 27001` (a asi `27002` pro InfoSec) žádá, aby organizace měla Politiku ISMS (vyžadovaný a Politiku informační bezpečnosti (to samé jako politika InfoSec). Obě mohou být vytvořeny jako doplňující se nebo být v libovolné závislosti.

   [Nebo je ISMS politika podle `27000 Plán zvládání rizik`, já fakt nevím, slajdy si protiřečí na 3 místech.]

2. **Politika InfoSec**: Jak a proti čemu chránit. Souhrn bezpečnostních zásad a předpisů pro ochranu informačních aktiv. Definuje bezpečné používání IT v rámci organizace. **Stanovuje koncepci informační bezpečnosti** v horizontu 5-10 let.

   Říká, co jsou citlivá informační aktiva, jakou mají klasifikaci, odpovědnost za ně, bezpečnostní infrastrukturu organizace, definujie sílu útočníků, vůči kterým se organizace zabezpečuje. **Nezávislá** na konkrétních IT technologiích.

   Bývá podpořena řadou detailních politik na konkrétní aspekty ITSec (řízení přístupu, emaily, používání síťových služeb, ...).

   Politika se běžně vyjadřuje v běžném jazyce, neformálně (ale je pak systém hodnocen jako systém s nízkou úrvoní záruky). Vyšší úroveň záruky za důvěryhodnost politiky poskytuje semi-formální vyjádření (a/nebo bohatší škála opatření), popřípadě vyjímečně i formální logicko-matematciké jazyky.

3. **Politika ISMS** (= bezpečnostní politika systému zpracování informací): Jak navrhovat, vyvíjet, provozovat a hodnotit procesy plnící politiku InfoSec.

   Určuje způsob zabezpečení informací v daném systému v horizontu 2-5 let. Definuje **konkrétní** cíle co se proti čemu chrání, konkrétní opatření, použité mechanismy pro implementaci opatření, havarijní plán a plány činnosti po útocích.

   Detailní normy, pravidla, praktiky, předpisy konkrétně definující způsob správy, ochrany, distribuce citlivé informace a jiných IT zdrojů v oblasti vymezené systémem pro zpracování informací organizace. **Musí respektovat** konkrétní IT technologie.

Tvorba politik informační bezpečnosti

- Definice politiky InfoSec a politiky ISMS je 1. krok při budování ISMS. Tvorba politik je typicky iterativní proces, finální verze musí odrážet výsledek *ohodnocení rizik* daný obsahem *prohlášení aplikovatelnosti* (specifikace vhodných opatření) - dokument vzniklý jako výsledek ohodnocení rizik.
- Musí být schválená vedením organizace a pravidelně přezkoumávaná a aktualizovaná.
- **Iniciální dokument**:
    - Deklarace politiky informační bezpečnosti odpovídá na otázky "pro koho? kde? co? proč?" na 2-3 A4, vyhlašuje ji vrcholový management, podepisuje "šéf" organizace. Má být maximálně srozumitelná, úplná (samostatně použitelná) a evidentní (nezpochybnitelná).
    - Pro koho? Je závazná pro vrcholový management (je za ni zodpovědný) a pro oblasti, kam definují, že dopadá (zaměstanci, okruhy zákazníků, ... vše má plusy a mínusy když se zahrne)
    - Kde? Nutno přesně vymezit.
    - Co? Aktiva které specifikuje, jejich relevantní rysy (důvěrnost, integrita, dostupnost). Stanovuje kritéria pro akceptování rizik.
    - Proč? (Proč se zavádí?) Srozumitelné popsání hrozeb, výše škod, ilustrační příklady.
- Později se můžou rozšiřovat a upřesňovat s novými informacemi o hrozbách a hodnocení rizik.
- Politika informační bezpečnosti má pokrývat/obsahovat:
  — Prohlášení, že vedení bude podporovat ISMS a pravidelně politiku přezkoumávat
  — Nástin přístupu k řízení rizik (určení metodiky)
  — Kritéria evaluace rizik a strukturu procesu jejich ohodnocení
  — Kdo bude za ohodnocení odpovědný
  — Strukčnou identifikaci požadavků na soubory opatření (plán ochran před viry, zálohování dat, ...)
  — Deklaraci, že požadavky na bezpečnost informací budou vyhovovat cílům organizace (a ISMS se bude trvale vylepšovat)
  — Vyjádření, že zaměstanci budou proškolování a trénováni
  — Ideálně deklaraci, že vyhovuje standardu `27002` (tj. že uplatňuje standardní opatření) (popř. certifikát o `27001`, že uplatňuje validní procesy ISMS)
- Klíčové je monitorování postupu budování politiky InfoSec, především v klíčových okamžicích jako po vypracování návrhu, implementace inic. sestavy, prvním auditu, a pak ročně

Důležitou součástí správy politik je **auditní činnost** zabezpečována nezávislými rolemi (na executivě a těch co vše navrhují)

- Cíle auditu: Kontrola správné definice bezp. procedur. Detekce neošetřených či neadekvátně pokrytých míst. Popř. po narušení jak k tomu došlo a kdo je odpovědný.
- Postup auditu se definuje jako součást procedur správy a provozu systému. Auditor musí být schopný audit vykonat bez rad monitorovaných entit.

Většina organizací vytváří politiku informační bezpečnosti dle standardu `ISO/IEC 27002` (politika založená na řízení rizik).

Systém řízení informační bezpečnosti (ISMS)

Důvěryhodná bezpečnostní politika zpracování informací je základní kámen **systému řízení informační bezpečnosti** (**ISMS**, Information Security Management System).

- Systém ISMS jako součást celkového systému řízení organizace (ve všech podčástech jako strutkura, politiky, odpovědnosti, procesy, zdroje, …)
- Cílem ISMS je zajistit trvalou aktuálnost politiky informační bezpečnosti a trvalou úroveň zabezpečení informací. Je buď nadřazenea politice informační bezpečnosti (InfoSec) nebo její přímou součásti. Výstupem ISMS by měly být **správně fungující procesy** podporující informační bezpečnost v relevantních činnostech organizace.
- **Základní idea**: Plan → Do → Check → Act → (repeat)
  Zavedení a provozování opatření v kontextu s činností organizace, neustálé zlepšování na základě objektivního měření.
- Bází pro budování ISMS jsou standardy `ISO 27001` (jak navrhnout ISMS a co má obecně dělat) a `ISO 27002` (která konrétní bezpečnostní opatření může/má systém ISMS obsahovat).
- ISMS z definice je systém řízení, který je dokumentovaný, systematicky implementovaný a řízený, trvale přezkoumávaný a auditovaný, trvale vylepšovaný, důvěryhodný (důvěryhodnost poskytuje certifikace nezávislou certifikační autoritou).
- **Dokumentace** by měla obsahovat: info o kontextu působení ISMS (oblast, politika bezpečnosti, cíle), o rizicích (jak se ohodnocují, zvládají, jak na ně jde aplikovat opatření), info o aktivech, info o podpory ze strany organizace. K tomu by měla mít info o protokolech různých věcí, jako o školeních, monitorováních, auditech, korekcí… A různé politiky (např. hesel, likvidace věcí, klasifikace informací, work from home, …)

Role v ISMS

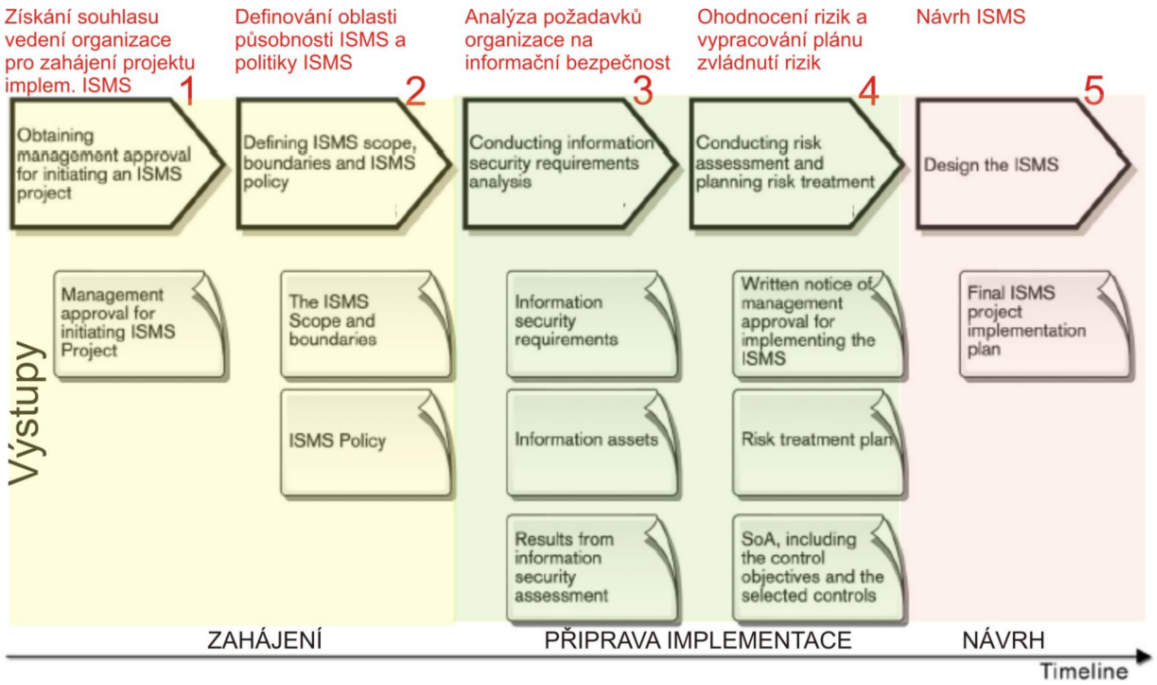
- ISMS vede *šéf projektu ISMS*.
- Za ISMS je odpovědný typicky *CEO*. Vrcholový management si musí vzít ISMS projekt "k srdci" (jinak se nic nepohne). Podpora od managementu/vedení organizace je klíčová. CEO musí chápat, proč je projekt třeba, a prosazovat ho.
- *CISO* má zopovědnost za zajišťování informační bezpečnosti obecně, tedy i za ISMS.

Budování ISMS

- Na začátku ideál vypracovat *seznam aktuálních relevantních bezpečnostních problémů* (nejlépe s odkazem na standard).
- Zredukovat v zadání ISMS vše, co je moc složité, náročné, obtížné. [Aby to nevypadalo tak děsivě.] Lidi nemají rádi změny obecně, počítat s tím, že někteří budou kopat proti.
- Vymezit oblast toho, kde ISMS bude působit.
- Ideálně jet podle standardu `27001` a `27002`, případně se i nechat certifikovat podle `27001` skrz certifikační autoritu, která je akreditována u Národní akreditačního úřadu (NAU). V některých případech může certifikace podle `27001` dána legislativou. Pro úspěšnost auditu certifikační autority je dobré mít dostupnout úplnou dokumentaci ISMS, zprávy z interních auditů a testů, vstřícnost k auditorů, přístup k vyššímu managementu.

Projekt implementace ISMS

Fáze projektu:



Úspěch projektu je splnění cílů věcných (co), časových (kdy) a nákladových (za kolik).

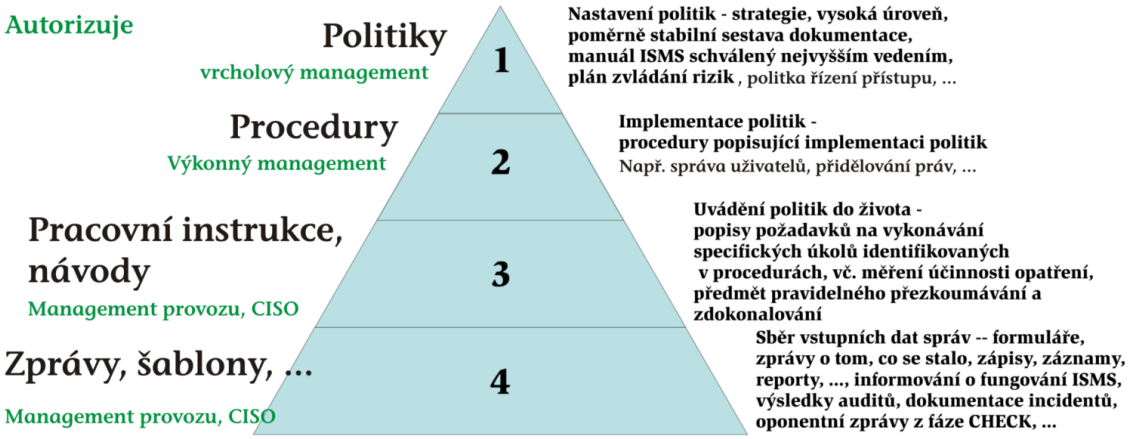
Projekt je potřeba řídit polde nějakých plánů projektu. Metodou řízení realizace ISMS je podle `27001` **PDCA** (plan - do - check - act), ale lze použít i jiné.

- **Plan**: Definice oblasti, politiky, přístupu, procedur řešících hodnocení rizik, vybrání možností jak zvládat rizika, výběr opatření, vypracování prohlášení o těchto věcech.
- **Do**: Implementace vybraných opatření zvládání rizik, implementace procedur, zaškolení zaměstnanců, zajištění zdrojů, formulace plánu zvládání rizik.
- **Check**: Sledování a posuzování výkonu ISMS. Monitorování, testování, audity, měření výkonu, shromažďování výsledků, vytváření zpráv pro management.
- **Act**: Provedení oprav na základě posouzení mangementem. Identifikace a implementace vylepšení.

Pro implementaci ISMS by měl být sestaven tým z klíčových business manažerů a technických expertů na InfoSec, vést by ho měl člen středního nebo nižšího managementu s delší praxí (ideálně ne IT manažer).

Dokumentace je časově nejnáročnější, musí být úplná, odpovídat firemnímu prostředí, dostupná, použitelná, adekvátně chráněná. Dokumentace má být v souladu s `ISO 27001` (obsahovat politiku informační bezpečnosti, oblast ISMS, hodnocení rizik, cíle, popis řídící struktury ISMS, důkazy provedených akcí, plány zvládání rizik, procedury implementující opatření, procedury řízení a inspekce).

4-vrstvá struktura dokumentové základny ISMS



Další dokumenty v ISMS

- z oblasti správy informační bezpečnosti
  - soupis citlivých inf. aktiv
  - hodnocení zranitelností, hrozeb a rizik pro tato aktiva
  - manuál ISMS obsahující prohlášení o aplikovatelnosti (opatření prosazujících bezpečnost)
- z oblasti nástrojů pro plnění správy InfoSec
  - sestava popisu procesů, politik, procedur a návodů k činnostem v oblasti InfoSec
- Dokumenty tvořící manuál ISMS (dostupný všem zaměstnancům)
- Důkazy provedených akcí organizací při vedení ISMS (zápisy ze schůzí, zprávy specialistů, ...)
- Popis systému řízení informační bezpečnosti
- Plán zvládání rizik
  Včetně podpůrných procedur obsahujících detaily o tom kdo má co dělat za jaké situace.
- Procedury řící správu a inspekci ISMS
- Pracovní instrukce
- Formuláře, šablony, zprávy o auditech, ...

Testování ISMS

Funguje to jak bylo zamýšleno?

Možnosti testování: důkladný audit (interní, externí), papírové testování (analýza dokumentů), reálné testování, penetrační testování, rozsáhlé zcénářově orientované testy, ...

Přednáška 4

[Nebyl záznam. Vytvořeno pouze ze slidů.]

Kyberbezpečnost

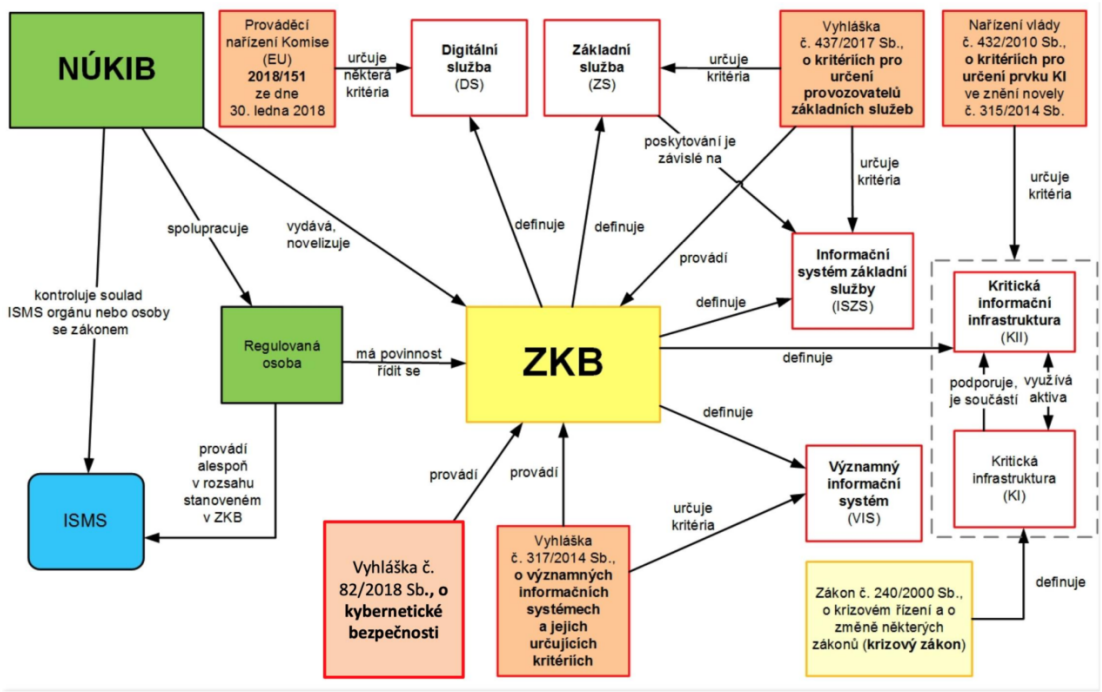
2 modely:

- **Identifikační model**: USA + jihoamerické státy.
  + Efektivní, univerzální.
  - Velká míra zásahu do informačního soukromí. Problém výpadků, nedostatek mezinárodní podpory.
- **Model ochrany prostředí**: EU, ČR
  + Performativní pravidla, chytrá regulace. Menší zásah do informačního soukromí.
  - Méně efektivní, institucionální oddělení.

Právní úprava kyberbezpečnosti:

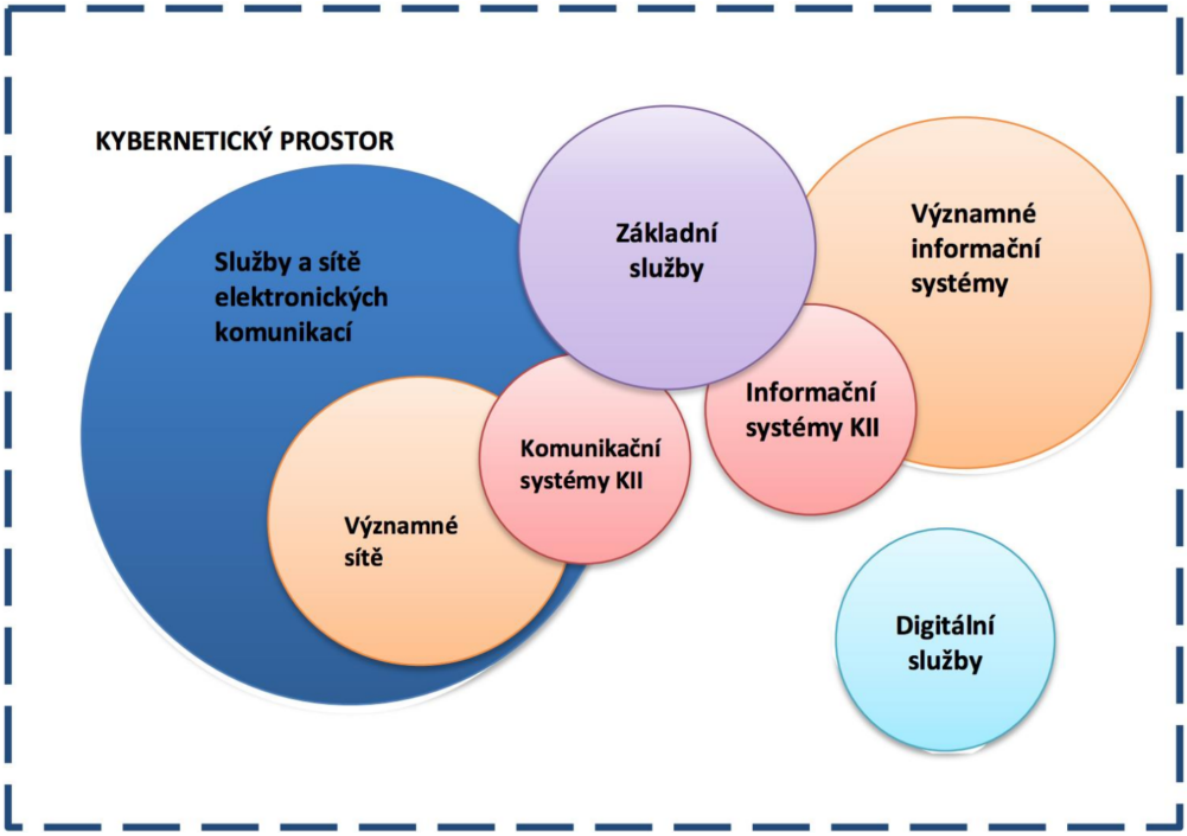
`Zákon č. 181/2014 Sb.`, **o kybernetické bezpečnosti** (ZKB/ZoKB)
`Zákon č. 240/2000 Sb.`, **o krizovém řízení** a o změně některých zákonů (krizový zákon)
`Zákon č. 365/2000 Sb.`, **o IS veřejné správy** (ISVS)
`Směrnice (EU) 2016/1148` o opatřeních zajištění vysoké společé úrovně bezpečnosti sítí a informačních systémů v Unii (**směrnice NIS**)
`Nařízení (EU) 2019/881` o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií ("**akt o kybernetické bezpečnosti**")
Sektorová regulace (např. energetika, bankovní a finanční služby), obecná regulace

Graf účastníků a akcí v ZKB (zákonu o kybernetické bezpečnosti):



[NÚKIB = Národní úřad pro kybernetickou a informační bezpečnost]

Povinné osoby dle ZoKB



- **Služby a sítě elektronických komunikací**
  - Určování neprobíhá, osoby jsou definovány zákonem o elektronických komunikacích
  - Sféra Národního CERTu. Povinnost nahlásit konktaktní údaje.
- **Významné sítě** = "síť elektronických komunikací zajišťujících přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře"
  - Určování neprobíhá, povinný subjekt určen přímo definicí v ZKB.
  - Sféra Národního CERTu. Povinnost hlásit kontaktní údaje, detekovat kybernetické bezpečnostní události a hlásit incidenty.
- **Kritická informační struktura** (KII) = prvek nebo systém prvků kritické infrastruktury (KI), komunikační a informační systémy v oblasti kybernetické bezpečnosti.
  - Komplex informačních a komunikačních systémů, jejichž narušení by mohlo mít vážný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatel, zdraví osob nebo ekonomiku státu. Systémy důležité pro chod státu a ekonomiky.
  - Určena podle stanovených kritérií v oblasti kybernetické bezpečnosti a krizového zákona.
    Týká se veřejnoprávních i soukromých subjektů.
  - Sféra Vládního CERTu, určuje/navrhuje NÚKIB.
  - Nejpřísnější regulace - povinnost plnit celý ZKB. Hlásit kontaktní údaje, detekovat a hlásit incidenty, povinnost zavést bezpečnostní opatření podle vyhlášky č. 82/2018 Sb. Nutno provádět ochranná a reaktivní opatření vydané NÚKIBem.
- **Významný informační systém** = systém spravovaný orgánem veřejné moci, který není kritickou informační infrastukturou ani informačním systémem základní služby, a u kterého narušení informační bezpečnosti může omezit/ohrozit působnost daného orgánu veřejné moci.
  - Pouze státní sektor.
  - Určeno: Buď automaticky pokud je systém zahrnut do přílohy vyhlášky č. 317/2014 Sb, nebo pokud orgán/osoba usoudí, že systém naplňuje kritéria této vyhlášky, a nahlásí se

NÚKIBu.

- **Základní služby** = služby, jejichž poskytování je závislé na informačních systémech/sítích elektronických komunikací, a jejichž narušení by mohlo mít významný dopad na zabezpečení společenských/ekonomických činností v určitém odvětví (energetika, doprava, bankovnictví, finanční trhy, zdravotnictví, vodohospodářství, digitální infrastruktura nebo chemický průmysl).
    - Určuje NÚKIB na základě kritérií z vyhlášky š. 437/2017 Sb, poté osloví relevantní subjekty a zahájí správní řízení o určení provozovatele dané služby.
- **Digitální služby** = služby informační společnosti spočívající v provozování online-tržiště, internetového vyhledávače nebo cloud computingu.
    - Určeno: Sám orgán/osoba posoudí naplnění kritérií a případně se nahlásí Národnímu CERT.
    - Regulace se netýká malých a mikro podniků (<50 lidí, <10 milion € obrat).

Instituty ZoKB:

- Mají **obecné povinnosti**: Sbírat kontaktní údaje, sdělovat bezpečnostní opatření (organizační, technická)
- Mají **operativní povinnosti**: Řešit hlášení incidentů (kybernetický bezpečnostní incident = KBI), varování před možnými hrozbami, protiopatření (reaktivní, ochranná)
    - reaktivní protiopatření: reaguje na KBI, rozhodnutí nebo opatření obecné povahy
    - ochranná protiopatření: reakce na výsledek analýzy KBI, opatření obecné povahy
- Řeší **stav kybernetického nebezpečí** = stav, kdy je ve velkém rozsahu ohrožena bezpečnost informací nebo služeb elektronických komunikací nebo bezpečnost a integrita sítí elektronických komunikací (a tím by mohlo dojít k porušení nebo ohrožení zájmu České republiky ve smyslu zákona o ochraně utajovaných informací)
    - Rozhoduje ředitel NÚKIB, povinnost zveřejnění, max 7/30 dnů, možnost navazujícího nouzového stavu.
- Stanovují **požadavky na dodavatele**
- Vydávají **certifikace**

Ochrana osobních údajů

GDPR: Nařízení Evropského parlamentu a rady (EU) `2016/679` o ochraně fyzických osob v souvislosti se zpracováním osobních údajů

Zákon `č. 110/2019 Sb.` Zákon o zpracování osobních údajů.

> Osobními údaji (se rozumí) veškeré informace o indentifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Zpracování osobních údajů: Jákakoliv operace nebo soubor operací s osobními údaji.

Zásady zpracování osobních údajů platí pro kohokoliv, kdo je zpracovává.

- Osobní údaje musí být ve vztahu k subjektu zpracovávány korektně a zákonným a transparentním způsobem.
- Zásada limitace účelem.

- Zásada minimalizace údajů (pouze nezbytný rozsah).
- Zásada přesnosti.
- Zásada omezení uložení (právo být zapomenut).
- Zásada integrity a důvěrnosti.
- Zásada odpovědnosti.

Zákonnost zpracování v GDPR: [situace kdy je zpracování osobních údajů OK]

- Existuje souhlas se zpracováním.
- Zpracování nezbytné pro plnění smlouvy.
- Zpracování nezbytné pro dodržení právní povinnosti správce.
- Ochrana životně důležitých zájmů subjektu údajů (souhlas bez zbytečného odkladu)
- Zpracování nezbytné pro plnění úkolu ve veřejném zájmu, nebo při výkonu veřejné moci, kterým je pověřen správce [Např. policie?]
- Nezbytnost zpracování pro ochranu práv a právem chráněných zájmů správce, příjemce, nebo jiné dotčené osoby.

Práva subjektů údajů [v GDPR]

- Právo být informován o zpracování osobních údajů
- Právo na přístup k údajům
- Právo na opravu, výmaz (“právo být zapomenut”)
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo vznést námitku
- Právo na ochranu před automatizovaným individuálním rozhodování, včetně profilování

AI Act - návrh nařízení Evropského parlamentu a rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci

Přednáška 5

SDLC vs Secure SDLC

SDLC = **S**oftware **D**evelopment **L**ife**C**ycle (např. waterfall-based SDLC, agilní SDLC, ...)

Typicky fáze: (akorát třeba u agilních v cyklu)

$$Requirements \rightarrow Design \rightarrow Implementation \rightarrow Verification \rightarrow Release \rightarrow Respose$$

Cílem **Secure SDLC** je zavést do všech fází klasického SDLC bezpečnostní prvky (kterými se zajistí, že se s bezpečností počítá od začátku, zákazník bude mít bezpečný sw, data atd.)

Microsoft SDL

Jenom jeden příklad SDLC, uvádíme se proto, že Microsoft byl tak trochu pionýr v oblasti, řešil to jako jeden z prvních (a svoje metodiky zveřejnil ostatním firmám).

Secure developement integrovali 1998-2007. (Změnit metodiky celé firmy není otázka na chvíli, trvá typicky měsíce spíše roky změnit mentalitu firmy a všeho ohledně toho. Navíc Microsoft jak byl první, museli si spoustu nástrojů, metodik, praktik... vyvíjet sami.)

Praktiky v SDL podle fází vývoje:

Requirements

- Definice bezpečnostních požadavků na základě:
  - Standardů firmy.
  - Legálních požadavků (např. GDPR, NIST, ISO, OWASP...), industry standardů.
  - **OWASP ASVS** = **A**pplication **S**ecurity **V**erification **S**tandard
    OWASP je organizace zabývající se bezpečností webových aplikací, sdružuje lidi z celé světa (má oddíly, jeden je i v Brně). OWASP pod sebou má desítky až stovky security-related projektů, jeden z jejich flagship projektů je právě ASVS.

    Dokument ASVS obsahuje 69 stran požadavků v 14 různých oblastech (např. autentikace, session management, řízení přístupu, kryptografie, errors, logy, požadavky na hesla, ...). Dokument může sloužit jako checklist věcí na testování produktu, že vyhovuje bezpečnosti.
- Definice a použití kryptografických standardů
  - Cryptography Review Board (skupina lidí ve firmě, kteří aktivně sledují stav a použitelnost různých technologií kryptografie) vydávají kryptografické doporučení (např. SSL/TLS verze, typy šifer, algoritmů, délky klíčů, RNG, ...).
  - Microsoft tato doporučení zveřejňuje (takže menší firmy bez dedikovaných lidí na cryptography review se mohou inspirovat tímto).

Design

Zároveň s vymýšlením toho, jak aplikace bude vypadat, přemýšlíme nad tím, jestli tam někde není chyba/bezpečnostní díra. Čím dřív se na to přijde, tím méně stojí to opravit.

Threat Modeling (Modelování hrozeb): Brainstorming všeho, co se může pokazit/může být špatně. Kromě free flow brainstormingu je dobré použít jako podporu nějaký tool nebo existující seznamy, aby se na něco nezapomnělo (aby se nesoustředilo na jeden detail a nepřehlédlo celou jinou oblast).

- Při této fázi je dobré se zaměřit na to, aby se pouze generoval seznam hrozeb, a diskuzi "je toto vůbec třeba řešit? a neřešíme to už metodou XY?" nechat až na později. (V této fázi vytvořit obsáhlejší seznam a seškrtat to až později.)
- Výsledkem bude velký seznam hrozeb. Co implementovat jako první je možné rozhodovat např. pomocí DREAD skóre. (Nicméně nejlépe by bylo zaintegrovat všechno co jde, protože ve fázi designu to obvkyle nebývá takový problém.)
    - **D**amage, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability

      $RiskValue$ = (Damage+ AffectedUsers) $\times$ (Reproducibility + Exploitability + Discoverability)
- Možné nástroje:
    - *Data Flow Diagram*. Tým dostane přehled o celém systému, a lépe se určí, kde se co řeší/kde se co má zabezpečovat/kontrolovat. Součástí je dobré určit "trust boundaries" - podcelky, kde si komponenty navzájem věří (potom hranice trust boundaries určují body, na které je třeba se při zabezpečování zaměřit nejvíce).
    - *Microsoft STRIDE*. **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of privileges.

      Tento seznam (a oblasti, kterých se týká) je fajn při brainstormingu projít nad každou interakcí mezi komponentami v našem Data Flow Diagramu a ptát se: "Může nastat Spoofing mezi uživatelem a management konzolí? Případně jak tomu zamezit?".

      Při omezeném času (pokud není žádoucí procházet takto detailně každou interakci), je fajn udělat to aspoň pro všechny interakce co překračují trust boundaries.
    - *Microsoft Threat Modeling Tool*. Nástroj, ve kterém lze vytvořit diagram interakce komponent i zadat konkrétní typ (např. databáze na této technologii v cloudu). Nad vloženým diagramem tool automaticky vygeneruje (obsáhlý) seznam možných hrozeb. (Může vést k tomu, že se tým přestane zamýšlet nad hrozbami nad rámec tohoto seznamu, nebo je přestane kvůli velikosti toho seznamu bavit to modelovat a procházet.)
    - *OWASP Threat Dragon*. Nástroj umožňující vytvořit diagram interakce komponent a vepisovat k nim možné hrozby. Neprovádí automatickou analýzu hrozeb, pouze umožňuje lépe zaznamenat vlastní hrozby než klasické Data Flow Diagramy.
    - *LINDDUN*. **L**inkability, **I**dentifiability, **N**on-repudiation, **D**etectability, **D**isclosure of information, **U**nawareness, **N**on-compliance. Zase jde hlavně o seznam bodů, které se mohou projít, zamyslet se nad každým z nich, a tím checknout, že se na nějakou důležitou oblast nezapomnělo.
    - *Mozilla Rapid Risk Assessment*. Používá se spíš na to zjistit, jestli je nějaká služba z pohledu bezpečnosti zajímavá nebo ne - jestli je třeba ji projít podrobněji. 30-60 minut, zaměří se na data a CIA (Confidentiality, Integrity, Availability). Vyhodnocuje dopad na reputaci, produktivitu a finanční stránku. Pokud něco vyjde s velkým dopadem, rozebere se to jiným nástrojem více.

Implementation

- Manage the Security Risk of Using Third-Party Components

    - Než se použije knihovna třetí strany, zamyslet se a vyhodnotit ji (známé zranitelnosti, podpora vývojáři, frekvence updatů).
    - Pravidelné skenování codebase, pravidelný update komponent (u kterých byly objeveny nové zranitelnosti).
    - Je mnoho nástrojů pro takovou analýzu, např. OWASP Dependency Check (Java, .NET).
- Use Approved Tools
    - Definovat a udržovat seznam povolených toolů (ověřených, že neobsahují samy o sobě zranitelnosti), používat nejnovější updaty (s fixy nově objevených bezpečnostních zranitelností).
- Perform Static Analysis Security Testing
    - Ideálně už nad ještě nemergnutým kódem co je právě vyvíjen (čím dříve je vývojář upozorněn, tím větší šance, že se to vážně opraví). Např. plugin do IDE, job nad merge requestem, ...
    - Nástroje např. SonarQube.
    - Při výběru toolu na analýzu je třeba myslet na to, jaké mají nástroje false positive & false negatives rates. Moc false positives naučí lidi ignorovat všechny warningy a přestat to používat.

Verification

- Perform Dynamic Analysis Security Testing
    - Dynamická se dělá v runtime. Např. analýza otevřených portů, použitých komunikačních protokolů, atd.
    - Nástroje generické (např. Burp Suite, OWASP ZAP) nebo specifické (např. SQLmap pro zjištění možné SQL injection).
- Perform Penetration Testing
    - Penetrační testy provádí experti na inf. bezpečnost, simulují útok hackerů a používají k tomu veškeré možné prostředky, které by mohli mít skuteční hackeři (statické analýzy pokud je k dispozici kód, dynamické analýzy, atd.).
    - Existují guidbooky, např. OWASP Security Testing Guide.

Response

- Ideálně se potenciální problémy odhalí proaktivně už dříve, ale stejně je potřeba mít zavedené postupy pro případ, že ne a musí se reagovat.
- Establish a Standard Incident Response Process

Other

- Provide Training
    - Snaha naučit vývojáře automaticky přemýšlet o tom, jak vyvíjet bezpečně
- Define Metrics and Compliance Reporting
    - Sbírat statistiky, analyzovat je, vyvozovat z nich případně změny do postupů.
    - Možné metriky: Počet externě/interně reportovaných zranitelnost. Fix rate. False positives. Coverage.
    - **BSIMM 12** (**B**uilding **S**ecurity **I**n **M**aturity **M**odel): Software security framework.

      Řeší metriky v 4 doménách, 12 praktikách, 119 aktivitách. Každý rok osloví firmě a ptají se, co za praktiky ohledně bezpečnosti dělají. Firma dostane zpětnou vazbu nejen kolik z nich dělá/nedělá, a jak si na tom stojí oproti ostatním 128 anonymizovaným společnostem. (To se dá použít jako guide co je fajn zavést jako další.)

- OWASP SAMM 2: Podobné jako projekt BSIMM 12, ale ještě neposkytují srovnání s ostatními firmami.

Přednáška 6, část 1

Kritéria hodnocení bezpečnosti

Vývoj kritérii

- Začátek v USA koncem 60. let – potřeba ověřených systémů pro vladní organizace, ale individuální hodnocení byla nákladná – snaha minimalizovat náklady na hodnocení zavedením obecných kritérií.

  Tzv. “Orange Book” (1985, Trusted Computer System Evaluation Criteria), dávalo třídy D (žádná bezpečnost) až A1 (nejvyšší).

- V Evropě se vyvinulo ITSEC (oddělení funkčnosti a záruk) v Kanadě CTCPEC (funkčnost dělena na důvěrnost, integritu, zodpovědnost, dostupnost), v US Federal Criteria.

  Více standardů $\rightarrow$ mezinárodně prodávaný sw potřeboval více kontrolami projít, opět snaha mít nějaký common ground.

- **Společná kritéria** (Common Criteria) – slouží jako celosvětový standard, `ISO/IEC 15408`.

  (To neznamená, že předchozí instituce/standardy vymizely, na některý software mohou být kladena i jiná kritéria než tato, a USA si trochu jede vlastní věci, ale je to rozšířený common grounds, na jehož základě se mnoho hodnocení provádí.)

Pojmy

- **Akreditace**: Oficiální souhlas (pověření) s prováděním určité činnosti.
- **Certifikace**: Vydání daného osvědčení na základě provedeného hodnocení.
- **Hodnocení** (evaluace): Ověření shody deklarovaných vlastnostní (dle kritérií). Hodnocení (autoritou) vždy pouze kontroluje, že deklarované vlastnosti sedí. Neověřuje systém celkově ani nic takového.
- **Validace**: Ověření platnosti/souladu, v US terminologii “hodnocení”.

Common Criteria (CC)

Pojmy:

- **TOE** – Target of Evaluation (**Předmět hodnocení**): Produkt nebo systém (popř. jeho část), který je předmětem hodnocení
- **ST** – Security Target (**Specifikace bezpečnosti**): Cílová kombinace komponent spojených s konkrétním produktem nebo systémem [Cíl úrovně bezpečnosti, který se prověřuje?]
- **PP** – Protection Profile (**Profil bezpečnosti**): Implementačně nezávislá skupina bezpečnostních požadavků určité skupiny TOE.

Certifikáty CC se dříve zaváděly na dobu neurčitou, brzy ale bylo jasné, že platnost dané úrovně bezpečnosti s časem klesá, a nyní jsou vydávány na 5 let.

Certifikace se ve velkém množství provádí například na oblast produktů typu čipové karty, kde banky, které je budou používat, nutí výrobce, aby měly podle CC konkrétní úroveň záruky.

CC tvoří požadavky na *funkčnost* (functionality) a *záruky* (assurance).

- **Funkčnost**: Popis, co za funkce v oblasti bezpečnosti produkt umí (na papíře).
  “Co vlastně za bezpečnost ten produkt dělá, jestli chrání integritu, autenticitu, atd. a na jaké úrovni to dělá.”

- **Záruky**: Jakou důvěru můžeme mít v to, jak dobře zařízení splňuje bezpečnostní funkce. "Jak dobře byl produkt vyvíjen, aby umožňoval tu úroveň bezpečnosti, kterou má umožňovat."

  (Neplést s **robustností**: To je charakteristika síly konkrétní bezpečnostní funkce a záruka, že je dobře naimplementovaná.)

  > [Subjektivní vložka toho, jak jsem to pochopila já, protože ty definice zní strašně. Ale nemusím mít pravdu.]
  >
  > Lidsky řečeno: Funkčnost je na papíře co systém umí pro bezpečnost, např. že řeší autorizaci pro přístup k tomuto, integritu dat, atd. A záruka je, jak moc můžeme věřit, že to ten systém vážně dělá (a že to dělá spolehlivě), neboli že produkt dostál svým bezpečnostním cílům.
  >
  > Např. Systém má požadavek na funkčnost, že bude zajišťovat důvěrnost dat přenesených při uživatelově přihlášení. Úroveň záruky je taková, že je to implementováno tak dobře, aby to odradilo pokusy běžného útočníka.

Příprava na evaluaci v CC

- Definování produktu/systému, co bude evaluován
- Specifikace funkcionality
- Specifikace úrovně záruky, který produkt/systém tvrdí, že splňuje
- Zjistit si, co je potřeba mít ready pro hodnocení u certifikační autority
- Připravit produkt a dokumentaci na evaluaci

Proces ohodnocení úrovní záruky může mít tyto body:
(záleží, na jakou úroveň se míří, vyšší úroveň → více kroků)

- analýza a kontrola procesů a procedur použitých při vývoji produktu
- kontrola, že tyto procesy/procedury byly vážně aplikované
- analýza, jak moc sedí návrh produktu a skutečný stav
- analýza, jak moc sedí návrh produktu a požadavky na něj
- důkazy verifikace
- analýza guidance dokumentů
- analýza testů na funkčnost a jejich výsledků
- nezávislé testy na funkčnost
- analýza zranitelností
- penetrační testování

CC úroveň záruky → záruka se zakládá na hodnocení (aktivním zkoumání produktu a jeho podkladů), které je prováděno experty (kteří s rostoucí úrovní záruky zkoumají do většího rozsahu, hloubky, ...)

7 úrovní záruky (EAL)

- Hierarchický systém, EAL1 (nejnižší) až EAL7+ (nejvyšší), čím vyšší stupeň, tím víc věcí to musí splňovat a tím naročnější a obsáhlejší je proces hodnocení. Produktů, co mají EAL7 je na světě jen v řádu desítek. Pro výrobce nemá cenu dělat si vyšší EAL než kolik po nich chce klient.

  EAL1 – functionally tested.
  EAL2 – structurally tested.
  EAL3 – methodically tested and checked.
  EAL4 - methodically designed, tested and reviewed.

EAL5 – semiformally designed and tested.
EAL6 – semiformally verified design and tested.
EAL7 – formally verified design and tested.

- Prakticky:
    - EAL1-3: Nevýznamná úroveň bezpečnosti, je to takové, že to ty systémy dosáhnou i spíš omylem nebo s relativně málo úsilím, nemá cenu na tyto úrovně cílit. Takové "nějaká bezpečnost tam je", často se tam dodává až jako afterthought nebo aby byl aspoň nějaký certifikát.
    - EAL4-5: Už významná úroveň, na ni se certifikuje nejvíc produktů, např. čipové/identiifkační karty jsou požadované, aby měly tuto úroveň. V těchto produktech už se typicky na bezpečnost myslelo od začátku.
    - EAL6-7: Systémy s velkým důrazem na bezpečnost.

Záruky znamenají…

- pro zákazníka: jakou úroveň zabezpečení mám garantovanou v daném výrobku?
- pro vývojáře: co všechno bude můj tým muset provést a poskytnout pro hodnocení?
- pro hodnotitele: dostal jsem všechny potřebné podklady a zdroje, proběhly všechny testy na danou úroveň v pořádku, abych mohl potvrdit certifikát?

Význam kritérií

- Usnadňují nasazení a používání bezpečných systémů (jednodušší srovnávání a výběr dle skutečných potřeb)
- Usnadňují specifikaci požadavků
- Ujasňují požadavky na návrh a vývoj

Přednáška 6, část 2

Praktické poznatky z posouzení stavu informační a kybernetické bezpečnosti v organizaci

Proč řešit posouzení?
3 možnosti: Buď to je přímo dané zákonem, klienti by bez toho přestali spolupracovat, nebo to sama firma vnitřně vnímá jako dobrý business krok.

1. **Požadavky jsou vynucené primárně**, např. zákonem o kybernetické bezpečnosti, zákonem o krizovém řízení, GDPR, zákon o IS ve veřejné správě, o ochraně utajovaných informací, občanský zákoník, trestní zákoník, atd.
2. **Požadavky jsou vynucené sekundárně**, zpravidla tlakem ze strany klientů, kteří mají sami zavedený ISMS (ISMS = Information Security Management System) (např. ISO 27001 stanovuje požadavky na soulad – trvají na tom, aby spolupracující software měl stejný důraz na bezpečnost)
3. **Zajištění business kontinuity a odpovědnost dobrého hospodáře**: Dávat důraz na bezpečnost pro firmu znamená ochranu aktiv, zajištění lepšího provozu, atd.

Rámec pro posouzení: Záleží podle účelu, proč se posouzení dělá.

- Povinné osoby (z pohledu ZoKB - Zákonu o kybernetické bezpečnosti) mají rámec posouzení jasný, podle tohoto zákona
- Nepovinné osoby (z pohledu ZoKB) buď potřebují audit (podle ISO 27001), kde rámec určuje tato norma, nebo nepotřebují audit podle této normy, a pak se posuzuje např. podle norem NÚKIBu (Národní úřad pro kybernetickou a informační bezpečnost)

Průběh posouzení

Iniciační fáze → Vyžádání dokumentace → Sběr informací → Studium/načtení a posouzení předaných informací → Pohovory se zainterestovanými stranami → Zpracování podkladů → Vyhodnocení podkladů → Vypracování posouzení s doporučeními k nápravě → Předání závěrečné zprávy, prezentace zákazníkovi

- **Iniciační fáze**
    - Posuzovaný subjekt si objedná posouzení stavu informační a kybernetické bezpečnosti u své organizace, s hodnotitelem sepíše smlouvu a NDA (důraz na důvěrnost, protože informace, ke kterým se hodnotitel dostane, jsou citlivé).
    - Následuje kick off meeting, kde jsou přítomni zástupci vedení a zainteresovaných stran. Stanoví se cíle, priority, časový rámec posouzení, míra spolupráce posuzovaného subjektu (jaké zdroje se vyhradí, kam všude se hodnotitel pustí, ...). Hodnotitel seznámí posuzovaný subjekt s průběhem posouzení a vysvětlí tyto fáze. Zároveň se vyjasní komunikační matice a způsob předávání informací mezi hodnotitelem a subjektem (opět důraz na důvěrnost).
- **Vyžádání dokumentace**
    - Posuzovaný subjekt je vyzván k předložení veškeré dokumentace a záznamů, které má hodnotitel zkoumat a hodnotit.
- **Sběr informací**
    - Sběr informací a podkladových materiálů potřebných ke zjištění stávajícího stavu a k ujasnění rozsahu ISMS.

    - Věci, co jsou relevantní k bezpečnosti informací, jako je:
      Práva a povinnosti rolí v organizaci, směrnice, politiky, metodiky, informace o řízení bezpečnosti informací, záznamy, seznam dodavatelů ICT a jejich smlouvy, topologie infrastruktury, provozní informace, popis IS, vše kolem zpracování osobních údajů, fyzická bezpečnost, dodržování předpisů, úroveň povědomí o nich, …
- **Studium/načtení a posouzení předaných informací**
    - Časově nejnáročnější fáze.
    - Hodnotitel vše přečte, přičemž si vytváří komplexní obreaz o fungování posuzované organizace. Pokud mu nějaké informace chybí, požádá o jejich doložení (pokud existují).
- **Pohovory se zainterestovanými stranami**
    - Hodnotitel od zaměstnanců posuzovaného subjektu vyžaduje informace, které v předložených materiálech postrádá, doptává se na věci, které je potřeba ujasnit nebo které jsou sporné.
    - Je potřeba počítat s tím, že zaměstnanci nemusí důležité informace sdělit (protože je to např. nenapadlo, předpokládají, že to je obecná znalost, nechtějí to sdělit, nebo nebyly otázky položeny správně).
- **Zpracování podkladů**
    - Hodnotitel získané informace zkompletuje, utřídí si je tak, aby mohl posoudit dobře relevanci ve vztahu ke zvolenému rámci posuzování.
- **Vyhodnocení podkladů** a **vypracování posouzení s doporučeními k nápravě**
    - Zjištěný faktický stav je porovnán s požadavky stanoveného rámce.
    - Vyhodnocení zjištěného stavu bod po bodu, jak slovním komentářem, tak i zdůvodněním a uvedením grafického semaforu (barva podle toho jestli je to ok, nebo ne, a jak moc závažné), včetně případných doporučení k nápravě nedostatků.
- **Předání závěrečné zprávy, prezentace zákazníkovi**
    - Závěrečná zpráva předána v elektronické, případně i písemné podobě s dostatečným předstihem (cca 14 dní) následovaná prezentací výsledů ve formě prezentace, v rámci které hodnotitel ukáže výsledky (stravitelnou formou) představitelům hodnocené organizace a následně proběhne diskuze nad zjištěními a možnými opravnými prostředky.

Proč bývají tyto věci problematické a jaké se v implementaci ISMS skrývají **překážky**

- Čím větší rozsah ISMS, tím více práce a peněz.
- Často se setkáme se špatnými předsudky ohledně IT oddělení a jeho sféry působení.
    - IT je provozní, nikoliv bezpečnostní oddělení, ani nejde o univerzální support. Zájmy IT mohou jít proti bezpečnostním zájmům (např. když je vyžadována častá složitá aktualizace). IT nemůže být zodpovědné za bezpečnost, protože by tím kontrolovalo samo sebe.
    - Na IT oddělení často padne nejvíc peněz (kromě personálu pod ně spadá celá technika firmy umožňující fungování ve všech ostatních odvětvích), ve vedení může být nechuť utrácet na “IT věcech” jako bezpečnost ještě víc peněz.
- Potenciální legislativní překážky, např. výklad zákonů a nebo spor o tom, který zákon je nadřazený.
- Potenciální organizační překážky: Nemusí existovat osoba zodpovědná za oblast ISMS, nebo v bezpečnostních rolích nemusí být odborníci na dostatečné úrovni, zaměstnanci neradi přijímají zodpovědné bezpečnostní role, …

- Odpor lidí k tomu být kontrolován, dokumentován. Management nemusí chápat důležitost informační bezpečnosti, řádoví zaměstnanci nemají rádi změny a nechtějí více odpovědnosti.

Vydáním posudku to nekončí

- Posuzovaný subjekt by dál měl pokračovat. Pravidelné skeny zranitelností, pentesty, opatření, analýzy rizik, učit se z chyb, které se časem ukážou, …
- Informační bezpečnost je kontinuální proces, který nikdy nekončí, a posouzení je jeho součástí.

Přednáška 7

[Nebyl záznam. Vytvořeno pouze ze slidů. Které byly v angličtině.]

Security Operations in real life

V **malé firmě**

- Typicky bez dedikovaného týmu na bezpečnost. Přinejlepším je řešení bezpečnosti one-man show (který to řeší spíš z vlastní iniciativy), často ani to ne. Bezpečnost se řeší v rámci IT oddělení, popřípadě IT adminem. Není vnímána jako až tak důležitá část, spíš jde jen o zálohy a autentizace.
- Když je tam aspoň jeden člověk, co řeší bezpečnost, je to lepší než nic, ale je to potom pochopitelně limitované na zkušenosti/znalosti pouze jedné osoby.
- Typicky přístup vedení takový, že se bezpečnost banalizuje (“proč by na nás někdo útočil”), dává se jí minimální budget a minimální lidské zdroje.
- V takovýchto podmínkách se začne informační bezpečnost brát vážně až po skutečném útoku, nebo po nevydařelém auditu.

Ve **středně velké firmě**

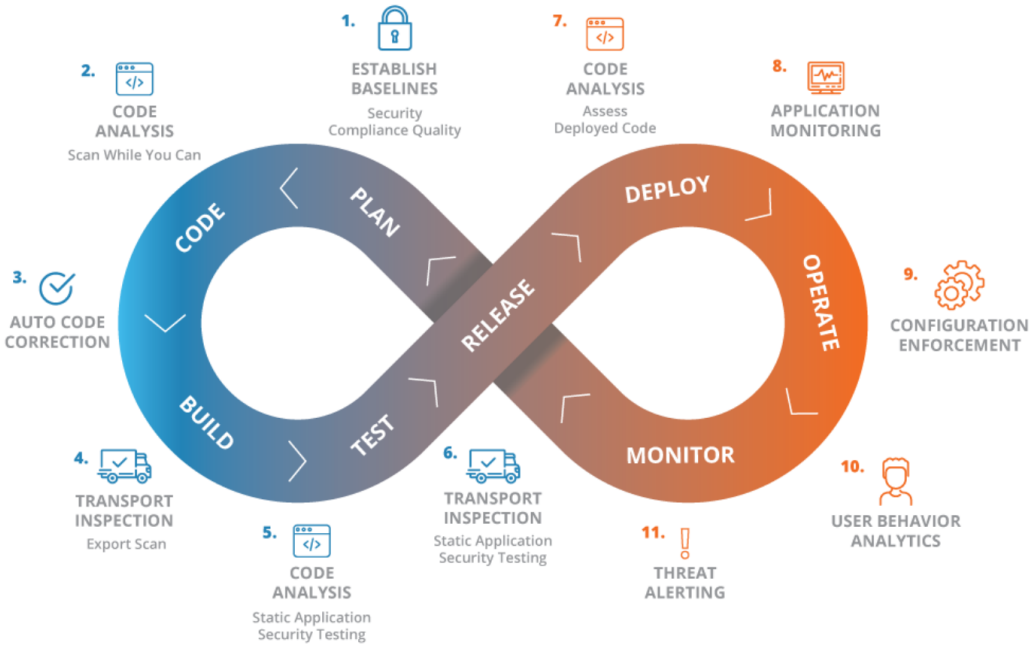
- Malý tým, který je “na všechno” ohledně bezpečnosti a řeší i infrastrukturu, operační aspekty, atd. Není specializovaný, pořád má mezery v kolektivních znalostech.
- Bezpečnost vnímána jako nezbytné zlo, tým bývá často limitován zdroji a pořádné dostane až pokud dojde k nějakému útoku.

Ve **velké firmě**

- Velký dedikovaný tým/týmy, ne všichni se soustředí pouze na bezpečnost, ale třeba i důvěrnost dat, atd.
  Už mají prostor soustředit se na různé oblasti bezpečnosti, např.:
  - **Security Architecture** definuje bezpečnostní politiky/standardy/procesy, provádí analýzu rizik (před vývojem SW především), zabraňuje špatnému návrhu aplikací nebo volbě technologií, co se nehodí do existujícího tech stacku.
  - **Security Engineering** řeší, aby nástroje a metody, pomocí kterých se vyvíjí a udržují systémy, byly bezpečné.
  - **Security Operations Centre** řeší operační aspekty informační bezpečnosti. Koordinují reakci na případné hrozby/incidenty, monitorují je a reportují o nich, analyzují rizika a zranitelnost (za běhu produktu, narozdíl od Sec. Architecture), analyzují bezpečnostní události, řeší notifikace na případné hrozby, …
  - Další, např. Pentesting tým, CISO, Security Consulting Team, …

Životní cyklus provedení změn v řízení bezpečnosti:
Navrhnutí změny → Analýza dopadu → Schválení/Zamítnutí → Zavedení změn → Zhodnocení/Reportování → … (nový cyklus)

Koncept DevSecOps



Security Framworks, příklady

- CIS control v8: Zaměřuje se na aktivity (ne na to, kdo spravuje zařízení), obsahuje 153 safeguards a 18 oblastí, kterými pokrývá kritické procesy/aktivity v organizaci (např. data protenction, penetration testing, account management, malware defenses, data recovery, ...)
- The Cybersecurity Framwork (NIST) má tři primární části: *Core* (hierarchický seznam žádoucích výsledků cybersecurity, který funguje jako návod a kontrola), *Profiles* (sladění požadavků, cílů a zdrojů organizace s ideálními výsledky z Core) a *Implementation Tiers* (poskytuje možnosti měření, jak dobře je cybersecurity risk management implementovaný do organizace, úrovně 1 Partial, 2 Risk Informed, 3 Repeatable, 4 Adaptive)
    - Záznamy v části Core se skládají z popisu výsledku, kterého chceme dosáhnout (např. důvěrnost dat), a popisu, co se bude dělat, aby se nežádoucímu výsledku předešlo, jak bude probíhat případná detekce, reakce a zotavení se.
    - Framework je založený na rizicích. Vychází z mezinárodních standardů. Adaptovatelný na různé technologie, oblasti, uživatele. Living document.
- MITRE ATT&CK: The **A**dversial **T**actics, **T**echniques **& C**ommon **K**nowledge, cílem je popsat a klasifikovat cyberattacks (based on real-world). Používá se pro zavedení obranných a útočných akcí, monitorování, reportování, atd.