Bezpečnost informačních technologií - PV017

podzim 2013

(01)

(,,Safety" × ,,Security") × Bezpečnost

- ISO/IEC 27032: 2012, Information technology — Security techniques – Guidelines for cybersecurity
- ***Safety***, bezpečí
  - ✓ Stav bytí v chráněné oblasti, ve kterém je zajištěna ochrana proti fyzickému, sociálnímu, duchovnímu, finančnímu, politickému, emocionálnímu, pracovnímu, psychologickému, vzdělávacímu nebo jinému typu nebo důsledku selhání, poškození, chyby, nehody, poškození nebo jiné události, která by mohla být považována za nežádoucí.
  - ✓ Bezpečí může mít podobu chránění osob nebo hmotných či nehmotných hodnot (aktiv) před událostmi nebo vystaveními skutečnostem způsobujícím zdravotní, ekonomické, . . . ztráty
  - ✓ Stav bytí, ve kterém platí, že za definovaných podmínek někdo či něco nezpůsobí škodu.
  - ✓ Bezpečí se mnohdy chápe jako chránění proti nahodilým událostem
- ***Security***, Bezpečnost
  - ✓ chránění proti úmyslným škodám
  - ✓ v širším slova smyslu ochránění před poškozením osob nebo hmotných či nehmotných hodnot (aktiv) v důsledku úmyslných (trestných) činů, jako jsou přepadení, vloupání nebo vandalismu, krádež, . . .
  - ✓ ***information security***, informační bezpečnost
    ochrana proti úmyslným škodám, nežádoucím akcím na informačních aktivech

Tři cesty k zajištění informační bezpečnosti

Pro obhospodařování citlivých aktiv existují 3 možnosti:

A. Vytvořit v organizační struktuře alespoň na manažerské úrovni roli bezpečnostního manažera a informační bezpečnost zajistit outsourcingem pod jeho řízením.

B. Vytvořit v organizační struktuře bezpečnostní infrastrukturu a tým schopný plně prosazovat informační bezpečnost svými silami.

C. Nechat si bezpečnost IT zajišťovat mnohdy i velmi iniciativně vnitřními silami působícími bez systematicky řízeného vedení vhodnou politikou, často majoritně motivovanými snahou prokázat své vlastní dokonalosti.

!!! The road to hell is paved with good intentions !!!

Nevěnování bezpečnosti IT více energie než je nutné pro výběr "bezpečného"software cestu do pekel jen zkrátí. Nic jiného se tím nedosáhne.

Standard, norma, doporučení = dokumentovaná úmluva

- standard nebo norma ?
  - ✓ v Česku (mimo oblast IT) se tradičně používá pojem „norma“, což je historický vliv němčiny
  - ✓ v oblasti IT celosvětově pojem „norma“ vesměs prohrává s pojmem „standard“ – dáno vlivem progresivní globalizací angličtiny
- Doporučení (*recommendation*) – termín používaný některými organizacemi vydávající standardy místo termínu „standard“(ITU – telekomunikace, . . .)
- Standard vyvinutý na bázi konsensu jisté komunity, de facto standard
  - ✓ standard vypracovaný v rámci jisté komunity, která si před jeho vydáním odsouhlasí, že standard odpovídá jí stanoveným cílům
  - ✓ např. dokumenty RFC vydávané IETF pro oblast Internetu
  - ✓ de facto standard reprezentuje spíše liberální pohled na svět
- Standard „podle práva“ , de iure standard
  - ✓ úmluva schválená uznávanou institucí pověřenou tímto posláním legislativou, rozhodnutím státních autorit, . . .
  - ✓ standardy implicitně nejsou právně závazné, jistá právní norma ale může předepsat povinnost vyhovění (obvykle de iure) standardu
  - ✓ typicky standardy vydávané organizacemi ISO, IEC, ITU, . . .
  - ✓ de iure standard reprezentuje silně konzervativní pohled na svět
- konzervativci od liberálů přebírají co přebírat chtějí a co přebírat stačí
  - ✓ de facto standardy se vydávají rychleji
  - ✓ vyzrálé de facto standardy, které se ukázaly jako efektivní, se často přepracovávají/přebírají na de iure standardy

Oblasti zájmu de iure standardů

- univerzální oblast bez portfeje – zahrnuje vše, bez omezení
  - ✓ Celosvětové odpovědná instituce: International Organization for Standardization ISO, ISO
  - ✓ ISO – *isos*, stejný, žádný akronym !!!
  - ✓ celosvětová federace více než cca 160 členských národních (státních) standardizačních organizací (*ISO Member Bodies*) ex. od r. 1947
- oblast elektroniky a elektrotechniky
  - ✓ Celosvětové odpovědná instituce: ISO + International Electrotechnical Commission, IEC
- oblast komunikací
  - ✓ Celosvětové odpovědná instituce: ISO + International Telecommunications Union, ITU, konkrétně její T sektor, sektor standardizace, ITU-T, od r. 1993 následnický orgán CCITT ((1865) 1956–1993), *Comité Consultatif International Téléphonique et Télégraphique*

Bezpečnost informací je předmětem zájmu ve všech třech liniích.

Příklad oblasti de facto standardů – RFC (ISOC)

- RFC (*Request for Comment*)
  - ✓ název internetovských standardů, dáno historickou souvislostí
- V pozadí působí – *Internet Society*, ISOC
  - ✓ http://www.isoc.org/
  - ✓ 150 institucionálních, 6000 individuálních členů z cca 100 zemí
- Internet reprezentuje – *Internet Activities Board*, IAB
  - ✓ rada pro internetovské činnosti
  - ✓ manažersky spravuje a řídí provoz Internetu
  - ✓ provádí dohled nad architekturou protokolů a procedur
- OWASP, *The Open Web Application Security Project*
  - ✓ a worldwide free and open community focused on improving the security of application software
  - ✓ http://www.owasp.org/
  - ✓ standard vývoje bezpečné webovské aplikace
  - ✓ standard testování bezpečné webovské aplikace
  - ✓ standard hodnocení a kriteria záruk za bezpečnost bezpečné webovské aplikace
- ISF, *Information Security Forum*
  - ✓ mezinárodní nezávislá, nezisková věnující se měření a rozvoji praktik v informační bezpečnosti
  - ✓ v r. 1996 vydává volně dostupný standard (SoGP), *The Standard of Good Practice – a detailed documentation of best practice for information security*

ISO TR (Technical Reports)

- Technické zprávy typu 1
  - ✓ se vydává tehdy, když se ve výboru nenalezla dostatečná podpora pro vydání standardu
  - ✓ Říká se v definici TR 1:

    navzdory opětovné snaze není možné
    prosadit materiál k vydání jako řádný standard
  - ✓ dohoda není možná, protože názory jednotlivých národních institucí (jednotlivých členů výboru) se různí, standard nemůže být vydaný
  - ✓ TR typu 1 je během tří let po svém vydání předmětem revize, padne rozhodnutí, zda bude přeměněna v mezinárodní standard

- Technické zprávy typu 2
  - ✓ vydává se v případě, kdy standardizovaný předmět se stále ještě z technického hlediska vyvíjí a za čas bude posouzeno, zda dohoda již možná je
  - ✓ Říká se v definici TR 2:

    předmět zájmu normy je stále ve stádiu rozvoje nebo
    existuje jiný důvod, pro který není možné schválit
    mezinárodní standard okamžitě,
    v budoucnu to však zřejmě možné bude
  - ✓ TR typu 2 je během tří let po svém vydání předmětem revize, padne rozhodnutí, zda bude přeměněna v mezinárodní standard

- Technické zprávy typu 3
  - ✓ se vydávají o problémech, které běžně nepodléhají technické standardizaci, ale určitý návrh je natolik významný a po formální stránce připravený, že bylo zhledáno jeho vydání alespoň formou technické zprávy jako vhodné
  - ✓ Říká se v definici TR 3:

    technický výbor shromáždil různé podklady, ze kterých je normálně
    publikován mezinárodní standard
  - ✓ TR typu 3 není znovu posuzována, pokud informace v nich obsažené nejsou shledány neplatnými či neužitečnými
  - ✓ TR typu 3 je obvykle dokument metodického charakteru
  - ✓ skutečnost, že se jedná „pouze" o technickou zprávu a nikoli o řádný mezinárodní standard, však z věcného hlediska nijak nesnižuje význam dokumentu
  - ✓ TR 3 je např. ISO/IEC TR 13335 Směrnice pro správu bezpečnosti IT

Předmět ochrany – aktiva

- aktivum – předmět, myšlenka, informace, . . .
  mající pro organizaci hodnotu
- jedná se o ekonomický zdroj, zdroj podnikatelských procesů –
  cokoliv hmotné (*tangible*) či nehmotné (*intangible*) povahy,
  co může být vlastněno nebo ovládáno (řízeno, spravováno)
  nějakou entitou (organizací, . . .)
  s cílem produkovat pozitivní ekonomickou hodnotu
- hmotná aktiva (konkrétní, jasná, zřejmá, hmatatelná, . . .)
  peníze, budovy, pozemky, dopravní prostředky, sklady,
  zařízení, software, data, služby, lidé, . . .
- nehmotná aktiva (neurčitá, nepostižitelná, . . .)
  patenty, autorská práva, licence, obchodní známka,
  jméno, pověst . . .

Hrozba, útok / bezpečnostní incident, riziko

- Hrozba
  - ✓ potenciální možnost využití zranitelného místa k útoku útočníkem
- Útok, incident (bezpečnostní incident),
  - ✓ realizovaná hrozba
  - ✓ akt využití zranitelného místa útočníkem ke způsobení škody –
    snížením hodnoty, zničením, znepřístupněním, . . . aktiva,
    . . . zveřejněním důvěrného aktiva, . . .
- Riziko
  - ✓ v užším slova smyslu —
    pravděpodobnost, že se v daném zranitelném místě uplatní hrozba
  - ✓ charakteristika šířeji chápaného pojmu „riziko"
    – pravděpodobnost výskytu incidentu x způsobená škoda
    význam rizika se odvozuje z kombinace pravděpodobnosti výskytu a
    dopadu relevantního útoku (výše způsobené škody)

Zranitelné místo

- slabina využitelná ke způsobení škod / ztrát organizaci útokem
  - ✓ slabina ve fyzickém uspořádání
  - ✓ slabina v organizačních schématech
  - ✓ slabina v administrativních opatřeních
  - ✓ slabina v personální politice

. . .

Co je opatření ?

- Typické opatření je kombinací
  technologie, chování a procedury
  - ✓ např. anti virové opatření:
    software instalované v bráně a v počítači
    procedura zajišťující pravidelné aktualizace báze dat
    výchova uživatele k neotevírání neočekávaných příloh mailů . . .
- Podmínka efektivnosti opatření: cena opatření $\leq$ výše škody
- Vesměs platí, že s každým aktivem se druží více rizik
- Na identifikované riziko se musí vázat efektivní opatření
- Některá opatření lze aplikovat pro řešení více rizik

Organizování informační bezpečnosti v organizaci

- CISO, Chief of Information Security Officer,
  manažer / správce informační bezpečnosti
  - ✓ většinou ho ustanovuje řídicí výbor informační bezpečnosti,
    vedení organizace jmenuje řídicí výbor a
    požádá řídicí výbor o výběr CISO
  - ✓ s řídicím výborem spoluvytváří BP, určuje její cíle a strategie a stanovuje oblast působení
  - ✓ instruuje řídicí výbor o aktuálních hrozbách, zranitelnostech a o adekvátních krocích k jejich eliminaci
  - ✓ provádí iniciální posouzení rizik
  - ✓ identifikuje změny rizik a zajišťuje odpovídající reakce
  - ✓ zajišťuje, že vrcholový management a řídicí výbor odsouhlasuje rizika a přístup organizce k řízení rizik, plán zvládání rizik a nutnou úroveň záruky za bezpečnost
  - ✓ pokrač.

Odpovědnosti za informační bezpečnost, generické role

- řídicí výbor ITSec / Správce informační bezpečnosti –
  odpovědnosti viz předchozí výklad
- Oddělení IT mají odpovídat za
  - ✓ za zajištění výkonu bezpečnostních opatření systémů, za které odpovídají
  - ✓ bezpečnost servroven, . . .
  - ✓ spolupráce při identifikaci hrozeb, hodnocení rizik, řízení projektů, revizí, výkon zpravodajství
- Lokální administrátoři / správci systémů mají odpovídat za
  - ✓ registrace a rušení uživatelů systémů, monitorování systémů, přípravu bezpečnostních postupů (procedur), průběh změnového řízení v definovaných mezích, zálohování dat, navrhování aplikační bezpečnosti, implementace vnitřních opatření, testování nouzových plánů a plánů reakcí na bezpečnostní incidenty
- Správci systémů mají odpovídat (na úrovni systému) za
  - ✓ identifikaci hrozeb, hodnocení rizik, implementaci vybraných opatření, bezpečné konfigurování systémů, nastavování systému správy uživatelů (ID, hesla), nastavování monitorování bezpečnosti systémů, implementaci změnového řízení, nastavování všech nutných bezpečnostních procedur, udržování, aktualizování a testování plánů zachování činnosti organizace
- Správci sítí mají odpovídat
  (na úrovni domény nebo samostatné sítě) za
  - ✓ identifikaci hrozeb v mezích sítě, hodnocení rizik, implementaci vybraných síťových opatření (vč. firewallů), bezpečné (navrhování a) konfigurování sítí, implementaci změnového řízení, nastavování bezpečnostních procedur, udržování a testování plánů obnovy sítě

Aktivity správy reakcí na bezpečnostní incidenty

- Primární cíl
  - ✓ minimalizovat přímý negativní dopad bezpečnostního incidentu
- Sekundární cíl
  - ✓ získání poučení z výskytu incidentu, zefektivnění ochran
- Činěné kroky k jejich dosažení
  - ✓ ad1: zastavení účinku útoku a zvládnutí, zkrocení šíření škody
  - ✓ ad1: likvidace, odstavení zdroje útoku
  - ✓ ad2: analýza incidentu a vypracování zprávy o incidentu
  - ✓ ad2: podrobně zkoumání incidentu, příčiny, efektivity ochran, ...

Reakce na incident

- Reakce je v plné odpovědnosti ISIRT
- Iniciální reakce
  - ✓ identifikace akcí iniciální reakce na konkrétní incident
  - ✓ minimalizace nepříznivých dopadů na podnikatelské procesy
    - odstavení napadených systémů, služeb či sítí
    - informování managementu IT a podnikatelských činností a relevantních uživatelů
  - ✓ identifikace zdroje útoku
- Klasifikace incidentu, rozhodnutí o závažnosti incidentu
  - ✓ případné spuštění akcí podle připraveného krizového plánu
- Finální reakce po iniciálním zvládnutí incidentu
  - ✓ Obnova normální funkce napadeného systému, služby, sítě
  - ✓ Vypracování záznamu o incidentu a reakci do DB událostí, incidentů, zranitelností informační bezpečnosti

(Information Security Incident Response Team = ISIRT)

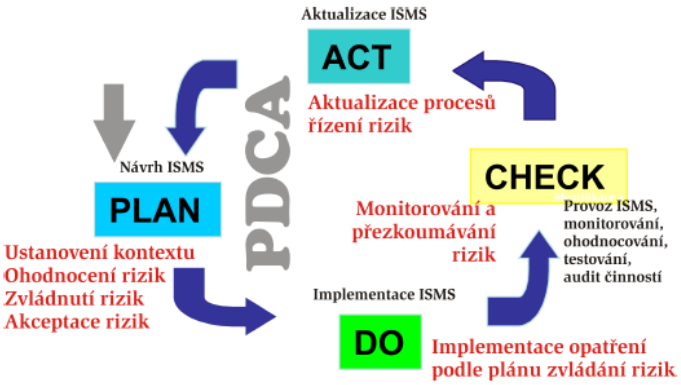
Klasifikace bezpečnostních incidentů podle významnosti

- Klasifikace
  - ✓ Very serious (Class IV)
  - ✓ Serious (Class III)
  - ✓ Less serious (Class II)
  - ✓ Small (Class I)
- Význam uvedených tříd
  - ✓ Nouzový stav: silný dopad
  - ✓ Kritický stav: střední dopad;
  - ✓ Varování: nízký dopad;
  - ✓ Informační: žádný dopad, ale analýza incidentu by mohla být použita ke zlepšení politik, procedur nebo opatření v oblasti informační bezpečnosti

Procesy řízení rizik (*Risk Management*) – výčet

- Ustanovení kontextu, stanovení oblasti, kritérií, ...
- Ohodnocení rizik, *Risk Assessment* tvoří podprocesy:
  - Identifikace rizik (*Risk Identification*)
  - Analýza rizik (*Risk Analysis*) – určení velikosti rizik
  - Vyhodnocení rizik (*Risk Evaluation*)
    – určení úrovní rizik porovnáním vůči stanoveným kritériím
- Zvládnutí rizik, *Risk Treatment*, *Risk Mitigation*
  – proces modifikující rizika, výběr a implementace opatření snižujících rizika
- Akceptace rizik, *Risk Acceptance*
  – rozhodování o přijatelnosti rizika dle stanovených kritérií
- Informování o rizicích, *Risk Communication*
  – sdělení informace o rizicích všem, kdo může rizika ovlivnit či být riziky ovlivněn
- Monitorování a přezkoumávání rizik a procesu řízení rizik

Procesy řízení rizik jsou součástí cyklu PDCA procesů ISMS



Metodologie ohodnocení rizik

- Elementární ohodnocení rizik
  - ✓ převzetí opatření na základě analogie podobných systémů a ze všeobecných standardů
- Neformální ohodnocení rizik
  - ✓ ohodnocení rizik na základě znalostí jednotlivců – odborníků na bezpečnost (interních/externích) bez použití standardních strukturovaných metod a nástrojů
- Detailní (formální) ohodnocení rizik
  - ✓ ohodnocení rizik standardními strukturovanými metodami a nástroji ve všech fázích (Identifikace aktiv, identifikace zranitelných míst, ...)
- Kombinované ohodnocení rizik
  - ✓ jak kde je to nutné (vč. ekonomických hledisek) se použije elementární, neformální nebo detailní (formální) ohodnocení rizik

Příklad odvození škály úrovní rizik

- úroveň rizika = F (pravděpodobnost útoku) × F´(dopad útoku)
  - ✓ vše ve vhodném škálování, nikdy v absolutních mírách, např.
  - ✓ pravděpodobnostní charakter rizika:

    1, (L, *Low*), zanedbatelný výskyt útoku, jednou za dekádu let
    2, (M, *Medium*), běžný výskyt útoku, jednou ročně
    3, (H, *High*), výskyt útoku hraničící s jistotou, každý den
  - ✓ dopad odpovídajícího útoku:

    1, (L) zanedbatelný / akceptovatelný , v desítkách tisíců Kč
    2, (M) běžný, ve statisících Kč
    3, (H) katastrofický, v milionech Kč
  - ✓ riziko, resp. významnost rizika: resp. tabulkou

    (L) akceptovatelné riziko, (součiny = 1,2)
    (M) běžné riziko, (součiny = 3,4)
    (H) katastrofické riziko, (součiny = 6,9)

pravděp./dopad	L	M	H
L	L	L	M
M	L	M	H
H	M	H	H

Plán zvládání rizik

- identifikuje příslušné kroky řízení, odpovědnosti a priority řízení rizik informační bezpečnosti
  - ✓ Plán je vazbou mezi opatřeními vyjmenovanými v Prohlášení o aplikovatelnosti a ohodnocením rizik zajišťující, že se budou implementovat, testovat a vylepšovat přístupy k rizikům definované vedením organizace
- má srozumitelně identifikovat
  - ✓ přístup organizace k řízení rizik
  - ✓ kritéria akceptování rizik
- je vypracováván pro kontext vymezený politikou informační bezpečnosti
- má mít formu formálního dokumentu
  - ✓ formálně definuje proces hodnocení rizik
  - ✓ formálně přiděluje (roli, ne osobě) odpovědnost za provedení, přezkoumávání a renovování procesu ohodnocení rizik

Zvládání rizik

- Plné odstranění rizika je obvykle nepraktické nebo téměř nemožné
- Odpovědné vedení organizace za účelně vysoké náklady zajistí implementaci nejvhodnějších opatření, která sníží rizika pro podnikatelské procesy na akceptovatelnou úroveň
  - ✓ škodný dopad na poslání a procesy organizace bude minimální
- Základní pravidlo
  - ✓ Vždy se řeší se největší riziko a
  - ✓ usiluje se o dostatečné snížení tohoto rizika za nejmenší možnou cenu, tak aby řešení mělo minimální dopad na ostatní způsobilosti podnikatelských procesů
- Definuje se plán zvládání rizik, harmonogram implementace opatření a definuje se výčet zbytkových rizik

Akceptace rizik

- Management odsouhlasí plán zvládání rizik
- Management odsouhlasí zbytková rizika jako akceptovatelná rizika
- Management explicitně zdůvodní ta akceptovaná rizika, která nesplňují standardní kriteria akceptovaní organizace

Informování o rizicích

- Cíle
  - ✓ poskytnout ujištění o dosažení výsledku řízení rizik v organizaci
  - ✓ shromažďovat informace o rizicích
  - ✓ prezenovat výsledky ohodnocení rizika a plán zvládnutí rizik
  - ✓ vyloučit nebo redukovat jak výskyty tak i následky porušení informační bezpečnosti díky vzájemně neporozumění mezi managementem vydávajícím rozhodnutí a ostatními zúčastněnými stranami
  - ✓ podporu rozhodování

Monitorování a přezkoumávání rizik a procesu řízení rizik

- Monitorování a přezkoumávání faktorů rizik
  - ✓ nová aktiva v oblasti působnosti řízení rizik
  - ✓ nezbytné úpravy hodnot aktiv, např. kvůli změněným požadavkům byznysu
  - ✓ nové hrozby, které by se mohly uplatnit vně i uvnitř organizace a které nebyly dosud hodnocené
  - ✓ nové nebo zvýšené zranitelnosti

ISO/IEC 27002:2005

- Information Security Management
  - ✓ *Information technology – Security techniques – Code of practice for information security management*
  - ✓ Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení informační bezpečnosti
- Struktura standardu
  - ✓ Standard obsahuje celkem 11 základních oddílů, které jsou dále rozděleny do 39 kategorií bezpečnosti
  - ✓ V každé kategorii bezpečnosti se specifikuje alespoň jedno opatření
  - ✓ Mimo to jsou ve standardu uvedeny základní informace o procesech hodnocení a zvládání rizik.
  - ✓ Oddíly jsou číslované pořadím kapitol standardu obsahujících jejich popis (5 – 15)

ISO/IEC 27002:2005, Oddíly kategorií bezpečnosti

Každý z oddílů obsahuje jednu nebo více kategorií bezpečnosti

5) Bezpečnostní politika
6) Organizace bezpečnosti – interní organizace, externí subjekty
7) Klasifikace a řízení aktiv – odpovědnosti za aktiva, klasifikace
8) Bezpečnost lidských zdrojů – přijetí do, průběh, ukončení vztahu
9) Fyzická bezpečnost a bezpečnost prostředí
10) Řízení komunikací a řízení provozu – vybraný ilustrační příklad
11) Řízení přístupu – vybraný ilustrační příklad
12) Nákup, vývoj a údržba informačního systému
13) Zvládání bezpečnostních incidentů
14) Řízení kontinuity činností organizace
15) Soulad s požadavky – práva, politik, smluv, . . . , audit

Tvorba politiky bezpečnosti informací, iniciální dokument

- Deklarace politiky bezpečnosti informací
  - ✓ Maximální rozsah – 2 až 3 strany A4
  - ✓ Odpovědi na klíčové otázky – Pro koho ? Kde ? Co ? Proč ?
  - ✓ Deklaruje vrcholový management, podepisuje, „šéf" organizace
- Pro koho bude politika bezpečnosti informací závazná ?
  - ✓ odpovědnost za politiku (za každou revizi) má vrcholový management, musí existovat důkaz, že tomu tak je – zápisy z vedení, . . .
  - ✓ vrcholový management / řídicí výbor musí zvážit a vymezit dopad politiky na konkrétní okruhy zaměstnanců, zákazníků, dodavatelů, . . . vč. přínosů/negativ pro byznys, . . .
  - ✓ vytvářená politika má být maximálně srozumitelná, úplná (samostatně použitelný dokument) a evidentní (nezpochybnitelná), aby se v průběhu implementace nemusely opakovaně odsouhlasovat všechny dílčí alternativy politiky
- Kde bude oblast působnosti politiky bezpečnosti informací?
  - ✓ Nutno přesně vymezit podle org. řádu / geograficky / funkčně / . . .
  - ✓ špatně se prosazuje ITSP v oblasti, která nepodléhá jednotnému řízení
  - ✓ mnohdy nestačí jednostranné vymezení např. na bázi organizační struktury či geografické lokality, do oblasti musí být zahrnuty všechny související kritické funkce
- Co politika bezpečnosti informací chrání ?
  - ✓ specifikace informačních aktiv pokrytých politikou
  - ✓ specifikace relevantních rysů bezpečnosti chráněných aktiv (důvěrnost, integrita, dostupnost, . . .)
  - ✓ stanovení kritérií pro akceptování rizik a identifikace úrovně akceptovatelného rizika
- Proč se politika bezpečnosti informací zavádí ?
  - ✓ srozumitelné vyjádření podstaty hrozeb pro organizaci
  - ✓ srozumitelné vyjádření výše škod způsobených narušením bezpečnosti informací (ve finančních i nefinančních pojmech)
  - ✓ ilustrační příklady důsledků incidentů podporující zavedení ISMS

Systém řízení informační bezpečnosti

- Information Security Management System, ISMS,
  Systém řízení informační bezpečnosti
- Součást celkového systému řízení organizace
- Reprezentace – projev přístupu organizace
  k rizikům daným orientací na informační ekonomiku
- Cíle řízení pomocí procesů ISMS:
  - navržení, implementace, zavedení,
  - provozování,
  - monitorování,
  - přezkoumávání,
  - udržování a
  - zajišťování urovně zaručitelnosti

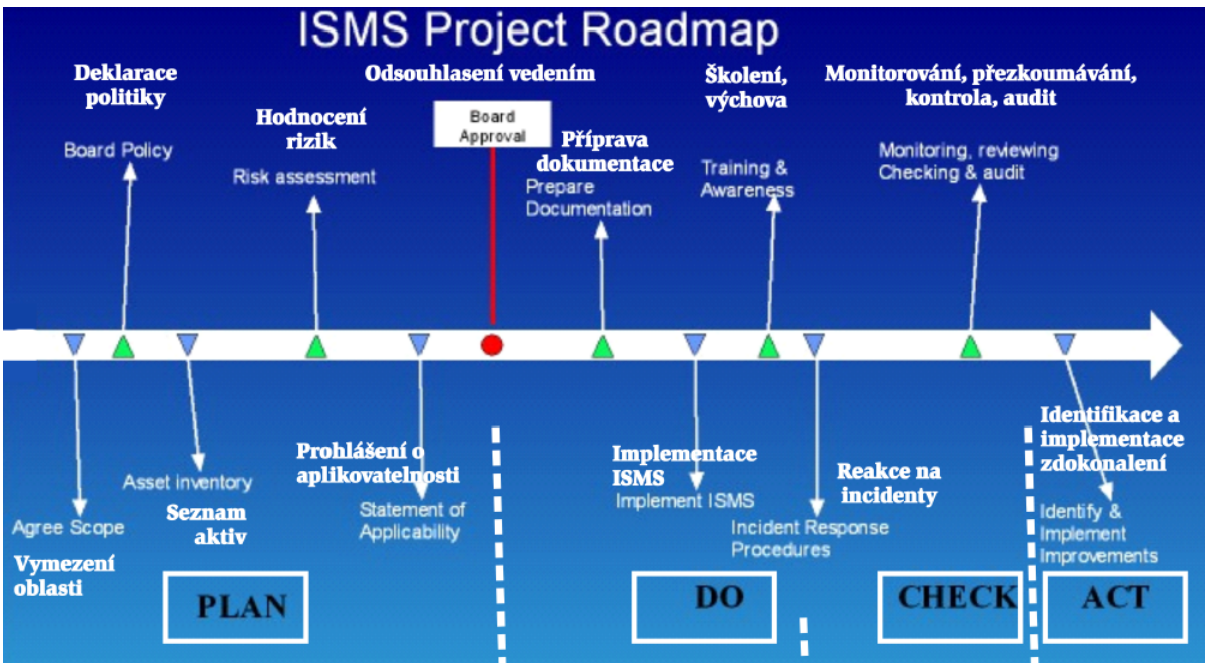
  informační bezpečnosti

Jedná se o

- systematicky implementovaný a řízený,
- trvale přezkoumávaný, auditovaný a kontrolovaný a
- trvale vylepšovaný (aktualizovaný) systém řízení.
- Předmětem jeho řízení je informační bezpečnost.
- Důkazem důvěryhodnosti ISMS je jeho certifikace
  - ✓ certifikací ISMS se získává důkaz úplnosti a kvality ISMS
  - ✓ pro podnikání je certifikace ceněná, nikoli však vždy nezbytná
  - ✓ certifikace přispívá k dosažení
    maximální, dlouhodobě platné, hodnoty podnikatelských procesů
  - ✓ vždy jde o finální etapu vývoje ISMS
  - ✓ certifikaci provádí třetí, nezávislá certifikační instituce (autorita)

Metodologie návrhu a implementace ISMS

- ISO 27001 prosazuje pro návrh, implementaci a
  prosazení ISMS procesní přístup
  - ✓ používá se model PDCA – *Plan–Do-Check-Act*
  - ✓ model PDCA je široce uplatňovaný v podnikání, v řízení kvality, . . .



Fáze projektu implementace ISMS

- ISO/IEC 27003 : 2010
  Information technology — Security techniques — Information security management system implementation guidance

Implementací ISMS se rozumí zahájení, naplánování a definice projektu zavádějícího ISMS formou zakázky řešené organizací. Fáze zakázky projekt implementace ISMS jsou:

1. ***Získání souhlasu vedení organizace pro zahájení projektu implementace ISMS***
2. ***Definování oblasti působnosti ISMS a politiky ISMS***
3. ***Analýza požadavků organizace na informační bezpečnost***
4. ***Ohodnocení rizik a vypracování plánu zvládnutí rizik***
5. ***Návrh ISMS***

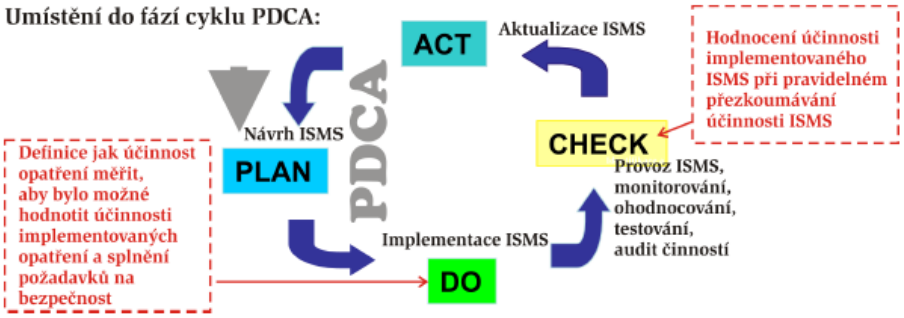
Dílčí kroky fází projektu implementace ISMS

1. Získání souhlasu vedení organizace pro zahájení implem. ISMS
   - 1.1 Objasnění priorit organizace pro projekt ISMS
   - 1.2 Předběžná definice oblasti působnosti ISMS
   - 1.3 Vytvoření zakázky a plánu projektu implementace ISMS pro odsouhlasení vedením organizace
2. Definování oblasti působnosti ISMS a politiky ISMS
   - 2.1 Definování oblasti a hranic inf. bezpečnosti v organizaci
   - 2.2 Definování oblasti a hranic informačních a komunikačních technologií (ICT)
   - 2.3 Definování fyzické oblasti a hranic
   - 2.4 Integrace všech oblastí a hranic do oblasti a hranic ISMS
   - 2.5 Vývoj politiky ISMS a získání souhlasu od vedení
3. Analýza požadavků organizace na informační bezpečnost
   - 3.1 Definování požadavků organizace na inf. bezpečnost
   - 3.2 Identifikace aktiv v oblasti působnosti ISMS
   - 3.3 Ohodnocení informační bezpečnosti
4. Ohodnocení rizik a vypracování plánu zvládnutí rizik
   - 4.1 Ohodnocení rizik
   - 4.2 Výběr cílů opatření a opatření
   - 4.3 Získání souhlasu vedení organizace s implementací a provozováním ISMS
5. Návrh ISMS
   - 5.1 Návrh informační bezpečnosti v organizaci
   - 5.2 Návrh fyzické a ICT informační bezpečnosti
   - 5.3 Návrh informační bezpečnosti specifické pro ISMS
   - 5.4 Vytvoření finálního plánu projektu ISMS

Metriky, měření informační bezpečnosti a ISMS

- ✓ ISO/IEC 27004: 2009, Information technology — Security techniques — Information security management — Measurement
- ✓ stanovují se míry a metody měření pro posouzení efektivnosti ISMS
  - to je nutné pro zlepšování výkonnosti informační bezpečnosti z pohledu celkových podnikatelských rizik organizace
  - dodávání vstupů pro přezkoumávání ISMS managementem s cílem usnadnit jeho rozhodování související s ISMS rozhodování a získání důkazů pro zlepšení implementovaného ISMS

Umístění do fází cyklu PDCA:



Pragmatické úvahy o návrhu měření bezpečnosti

- Co měřit ?
  - ✓ jen to, co chceme opakovaně, systematicky, rutinně vyhodnocovat
  - ✓ sbíráme jen ta data, která budeme analyzovat
  - ✓ děláme jen ty analýzy, jejichž výsledky prakticky využijeme
- Jak měřit ?
  - ✓ kdo dělá měření ?
  - ✓ jak bezpečně se uchovávají výsledky měření ?
  - ✓ začít s „polibkem", a měření rozšiřovat až když se ukáže nutnost, KISS (*Keep It Simple and Stupid*)
- Jak dokumentovat, jak prezentovat výsledky měření ?
  - ✓ viz systém zpráv na následující stránce
  - ✓ jak implementovat zpravodajský systém ?

Základní metriky a metody měření

- Příklad
  - ✓ Měření trendu vyhovění politice *Zajišťování vědomí zaměstnanců o informační bezpečnosti*
  - ✓ Předmět (objekt) měření – plán školení
  - ✓ Měřená vlastnost – zaměstnanci identifikovaní v plánu školení
  - ✓ Metoda měření – čítání zaměstnanců s úspěšně složenou závěrečnou zkouškou po školení
  - ✓ Základní metriky – počty plánovaných/úspěšně proškolených osob
  - ✓ Trend proškolování v průběhu roku je odvozenou metrikou, získanou vhodnou měřící funkcí ze základních metrik
  - ✓ Pro odvození indikace problematického trendu se použijí vhodný analytický model, metriky a adekvátní rozhodovací kritéria

Digitální důkaz

- Informace nebo data, uložené nebo přenášené v binární formě, která lze chápat jako důkaz

Digitální důkaz – tři fundamentální principy

- Digitální důkaz musí být
  - ✓ relevantní – lze ho použít k prokázání nebo vyvrácení jistého prvku konkrétně šetřeného případu
  - ✓ spolehlivý – je tím, čím má být, je skutečně důkazem
  - ✓ dostatečný – nemusí být shromažďována všechna data související s šetřenou událostí, ale musí se shromáždit dostatečné množství potenciálních digitálních důkazů, aby to, co se řeší, mohlo být patřičně prověřeno nebo prošetřeno
- Fundamentální principy důkazů jsou důležité pro každé vyšetřování, nejen pro použití u soudu

Role pracující s digitálními důkazy

- ***Digital Evidence First Responder***, DEFR, „detektiv"
  - ✓ fyzická osoba, která je oprávněná, vyškolená a kvalifikovaná jednat jako první na scéně incidentu při shromažďování a získávání digitálních důkazů,
  - ✓ je odpovědná za manipulaci s důkazy
  - ✓ musí zaručit, že shromažďování a získávání důkazů neporušuje legislativní omezení
- ***Digital Evidence Specialist***, DES, „vyšetřovatel"
  - ✓ fyzická osoba, která může provádět úkoly detektiva a má navíc odborné znalosti, dovednosti a schopnosti zvládnout širokou škálu technických problémů (síťový specialista, specialista na operační systém, . . .

Vlastnosti digitálních důkazů

Relevance digitálního důkazu

- ✓ Musí být možné prokázat, že získaný materiál se vztahuje k šetření, obsahuje informace napomáhající vyšetřování konkrétní události a jsou dobré důvody pro to, aby byl získán
- ✓ detektiv musí být schopný popsat použité postupy získání důkazu a vysvětlit uvedením dostatečných důvodů, proč bylo rozhodnuto získávat jednotlivé důkazové materiály

Spolehlivost digitálního důkazu

- ✓ Všechny procesy použité při manipulaci s potenciálními digitálními důkazy mají být auditovatelné a opakovatelné.
- ✓ Výsledky uplatňování těchto procesů musí být reprodukovatelné.

Dostatečnost digitálního důkazu

- ✓ detektiv si musí být vědomý, že shromáždil dostatečné množství materiálu umožňující řádné vyšetřování, které které se má provést
- ✓ detektiv musí být schopný dostatečně zdůvodnit množství shromažďovaného materiálu, použité procedury a rozhodnutí kolik jaký materiálu se získává

Auditovatelnost digitálního důkazu

- ✓ Nezávislý posuzovatel nebo jiné autorizované zúčastněné strany musí mít možnost vyhodnotit činnosti zajišťované DFER a DES.
- ✓ Všechny akce DFER a DES musí být adekvátně dokumentované.
- ✓ DFER a DES musí být schopni odůvodnit rozhodovací proces výběru použitého postupu akcí.
- ✓ Procesy vykonávané DFER a DES musí být k dispozici pro nezávislé hodnocení určující, zda se použila vhodná vědecká metoda, technika nebo procedura.

Opakovatelnost digitálního důkazu (výsledku testu)

- ✓ dosahuje se pokud se (testováním) získávají stejné výsledky testu provedených za následujících podmínek:
  - byla použitá stejná procedura a metoda měření / testování
  - použily se stejné nástroje za stejných podmínek a
  - test lze kdykoliv po originálním testu zopakovat
- ✓ Kvalifikovaný a zkušený DFER musí být schopen provádět všechny procesy popsané v dokumentaci a dojít ke stejným výsledkům bez návodů nebo interpretací

Reprodukovatelnost digitálního důkazu (výsledku testu)

- ✓ dosahuje se pokud se (testováním) získávají stejné výsledky testu provedených za následujících podmínek:
  - byla použitá stejná metoda měření / testování
  - použily se jiné nástroje za jiných podmínek a
  - výsledky testu lze kdykoliv po originálním testu reprodukovat

Ospravedlnění, zdůvodnění digitálního důkazu (justifikace)

- ✓ DFER má být schopný zdůvodnit veškeré činnosti a metody používané při manipulaci s potenciálními digitálními důkazy.
- ✓ Zdůvodnění může být dosaženo tím, že prokáže, že učiněná rozhodnutí byla ta nejlepší volba získání všech potenciálních digitálních důkazů.
- ✓ Toto zdůvodnění by měl rovněž prokázat jiný DFER nebo DES úspěšnou reprodukcí nebo validací použité akce a metody.
- ✓ Je v nejlepším zájmu organizace zaměstnávat DFER nebo DES, který má základní dovednosti a kompetence.
- ✓ Tím je zajištěno, že jsou při manipulaci s potenciálními digitálními důkazy používané správné procesy a procedury zajišťující jejich důkazní hodnotu.

Soulad s požadavky

- Cíl
  - ✓ Návrh, provoz a používání IS může být předmětem zákonných, podzákonných nebo smluvních (bezpečnostních) požadavků.
  - ✓ Organizace se musí vyvarovat porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a (bezpečnostních) požadavků.
- Dvě linie dosažení souladu
  - ✓ Soulad s právními normami
    - Specifické požadavky vyplývající ze zákona by měly být konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky.
    - Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle zemí.
  - ✓ Soulad s bezpečnostními politikami, normami a technická shoda
- Nástrojem ověření dosažení souladu je audit

Audit

- Audit (z lat. ***auditus***, slyšení) znamená úřední přezkoumání a zhodnocení dokumentů a jiných objektů nezávislou osobou.
- Účelem auditu je zjistit, zda doklady podávají platné a spolehlivé informace o skutečnosti a obvykle také zhodnotit kvalitu vnitřní kontroly firmy.
- Vzhledem k rozsahu dokumentace se audit obvykle zabývá jen vzorky a jeho výsledek tedy neznamená naprostou jistotu, nýbrž jen rozumnou pravděpodobnost konečného hodnocení.
- Cíl auditu ISMS – vyhodnocení,
  - zda ISMS adekvátně identifikuje a řeší požadavky informační bezpečnosti
  - trvalé přiměřenosti cílů ISMS stanovených vedením a
  - postupů pro údržbu a pro účinné zlepšování ISMS.
  - ✓ Účelem auditu bezpečnostních opatření (politik, ...) je zjistit,
    - zda jejich dokumentace podává platné a spolehlivé informace o skutečnosti a
    - zda jejich implementace a provozování odpovídá jejich specifikaci

Metody přezkoumávání

- Vyšetřování
  - ✓ Podle typu: Všeobecné, cílené, detailní
  - ✓ Podle rozsahu, šíře šetření: Reprezentativní, specifické, úplné (vyčerpávající)
- Interview
  - ✓ Podle typu: Všeobecné, cílené, detailní
  - ✓ Podle rozsahu, šíře šetření: Reprezentativní, specifické, úplné (vyčerpávající)
- Test
  - ✓ Blind, black-box, na slepo
  - ✓ Double blind, dublovaně na slepo
  - ✓ Gray-box, s částečným odhalením objektu
  - ✓ Double gray-box,
  - ✓ Tandem, white-box, s plným odhalením
  - ✓ Reversal, simulovaný útok

Common Criteria, ISO/IEC 15408

- Evaluation criteria for IT security
  - ✓ ISO/IEC 15408-1: Part 1: Introduction and general model
  - ✓ ISO/IEC 15408-2: Part 2: Security functional requirements
  - ✓ ISO/IEC 15408-3: Part 3: Security assurance requirements
- Předmětem hodnocení může být produkt nebo systém (dále nerozlišujeme)
- Pokud lze produkt/systém lze používat více způsoby pak předmětem hodnocení, ***Target of Evaluation***, TOE, je konkrétní mód jeho použití (podle návodu)
- Hodnocením podle CC se ověřuje, zda TOE vykazuje deklarované bezpečnostní vlastnosti a to jak z funkční skladby tak i z hlediska realizace
- Hodnocení stanovuje úroveň záruky za dosaženou bezpečnost

Specifikační dokument CC, Protection Profile

- profil ochran, ***Protection Profile***, PP
  - ✓ dokument typicky vytvářený uživatelem nebo nějakou uživatelskou komunitou
  - ✓ identifikuje požadavky na bezpečnost pro jisté prostředí
  - ✓ efektivně definuje třídu bezpečnostních zařízení, např.
    - použití čipových karet pro dosažení nepopiratelnosti (podpisování)
    - síťové firewally (pro řízení přístupu), . . .
  - ✓ výrobce se může rozhodnout vyrábět zařízení vyhovující konkrétnímu PP, výrobek lze certifikovat jako vyhovující PP
  - ✓ PP lze použít jako šablonu pro definici bezpečnostního cíle (specifikaci bezpečnostních vlastností konkrétního produktu/systému)
  - ✓ zákazník si může vybírat z produktů, které deklarují vyhovění jistému PP, resp. které vlastní certifikát vyhovění jistému PP

Specifikační dokument CC, Security Target

- bezpečnostní cíl, ***Security Target***, ST
  - ✓ dokument definující bezpečnostní vlastnosti produktu/systému, tzv. Security Functional Requirements (SFRs)
    - specifikace bezpečnostních funkcí poskytovaných produktem
    - součástí CC je standardní katalog těchto funkcí
    - např SFR může definovat, jak se má konkrétní role autentizovat
    - CC nepředpisují žádné povinné SFR v ST
    - některé SFR se mohou podmiňovat – např. schopnost omezovat přístup rolím vyžaduje nutnost mít možnost identifikovat jednotlivé role
  - ✓ produkt/systém se obvykle hodnotí jak splňuje zadaný/deklarovaný ST, – je hodnocený proti SFRs deklarovaným v ST
  - ✓ lze rovněž hodnotit ST, zda vyhovuje zadanému PP
  - ✓ ST je mnohdy reklamním materiálem výrobce

Common Criteria, hodnocení produktu a PP

- Hodnocení produktu/systému (TOE) typicky sestává ze 2 kroků
  - ✓ hodnocení ST, o kterém TOE sděluje, že ho splňuje, aby se získala jistota, že problém řešený produktem je problémem, který je potřeba řešit
  - ✓ vlastní hodnocení TOE proti tomuto ST, aby se získala jistota, že TOE splňuje bezpečnostní úroveň definovanou v ST
- Hodnocení PP
  - ✓ probíhá před formální deklarací PP relevantní autoritou odpovědnou za bezpečnost IT
  - ✓ cílem hodnocení je získání jistoty, že PP správně identifikuje požadavky na bezpečnost

EALs, Evaluation Assurance Levels, přehled

- úrovně záruky za dosažení informační bezpečnosti v TOE
- 7 definovaných úrovní záruky za dosažení informační bezpečnosti v TOE (přibližný ekvivalent dle TCSEC)
  - ✓ EAL1, funkčně testovaný TOE
  - ✓ EAL2, strukturálně testovaný TOE (∼ TCSEC C1)
  - ✓ EAL3, metodicky testovaný a kontrolovaný TOE (∼ TCSEC C2)
  - ✓ EAL4, metodicky navržený, testovaný a přezkoumaný TOE (∼ TCSEC B1)
  - ✓ EAL5, semiformálně navržený a testovaný TOE (∼ TCSEC B2)
  - ✓ EAL6, semiformálně navržený se semiformálně ověřeným návrhem a testovaný TOE (∼ TCSEC B3)
  - ✓ EAL7, formálně navržený s formálně ověřeným návrhem a testovaný TOE (∼ TCSEC A1)
- s růstem čísla EAL se zvyšuje úplnost a přísnost hodnocení dosažené kvality plnění požadavků na bezpečnost
  - ✓ nic více, nic méně
  - ✓ vyšší číslo EAL neznamená dosažení vyššího bezpečí, silnější mechanismy apod.

EALs, Evaluation Assurance Levels, přehled

- Stačí pouhé ověření, že bezpečnostní funkčnost odpovídá manuálovému popisu ?
  - ✓ E1 – evidence DKP, běžné zpracování osobních údajů
- Je navíc požadovaná ověření, zda bezpečnostní funkčnost ošetřuje známé zranitelnosti
  - ✓ E2 – podnikové účetnictví
- Požaduje se navíc kontrola prostředí, ve kterém byl TOE vyvíjen ?
  - ✓ E3 – bankovní software, software CA v PKI
- Požaduje se navíc ohodnocení detailního návrhu TOE vč. zdrojových kódů bezpečnostních funkcí a neformálního modelu bezpečnostní politiky ?

  Požaduje se prokazatelnost odolnosti vůči penetraci útočníky s nízkým potenciálem pro útok (hackři, amatéři)
  - ✓ E4 – některé, propracované, univerzální OS (pro business)
- Požaduje se navíc ohodnocení úplné implementace TOE, demonstrace korespondence implementace vůči návrhu TOE, formální model politiky, analýza skrytých kanálů ?

  Požaduje se prokazatelnost odolnosti vůči penetraci útočníky s středním potenciálem pro útok (organizovaní hackři)
  - ✓ E5 – čipové karty, specializované OS
- Požaduje se navíc ohodnocení úplné implementace TOE, demonstrace korespondence implementace vůči návrhu TOE, formální model politiky, . . . ?

  Požaduje se prokazatelnost odolnosti vůči penetraci útočníky s vysokým potenciálem pro útok (profesionálové)
  - ✓ E6
- Požaduje se navíc plné otestování na úrovni ***white-box***, plná formalizace politiky, bezpečnostních funkcí, detailního návrhu a korespondence implementace s návrhem

  Požaduje se prokazatelnost odolnosti vůči penetraci útočníky s extrémně vysokým potenciálem pro útok (organizovaný zločin)
  - ✓ E7