Anatomie informační bezpečnosti

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

Předmět ochrany – aktiva

- aktivum – předmět, myšlenka, informace, . . .
  mající pro organizaci hodnotu
  - ✓ Něco, co přináší vlastníkovi aktiva nějaký výnos
    nebo se očekává, že výnos přinese v budoucnu
  - ✓ 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 . . .

Předmět ochrany – Aktiva

- Informační aktivum dle zákona o kybernetické bezpečnosti
  - ✓ informace nebo služba,
    kterou zpracovává nebo poskytuje
    informační nebo komunikační systém,
  - ✓ zaměstnanci a dodavatelé
    podílející se na provozu, rozvoji, správě
    nebo bezpečnosti informačního a/nebo komunikačního systému,
  - ✓ technické vybavení,
  - ✓ komunikační prostředky,
  - ✓ programové vybavení a
  - ✓ objekty informačního a/nebo komunikačního systému

Předmět ochrany – Aktiva

- aktivum nelze nahradit bez vynaložení nákladů, úsilí, času, ...
- aktiva musí být individuálně identifikovatelná
- aktiva formují vnější identitu organizace, poškozením identity organizace by činnost organizace mohla být ohrožena
- Příklad jiné možné kategorizace aktiv
  - ✓ informační aktiva – data v jakékoliv formě (soubory dat, kopie plánů, dokumentace, originály manuálů, školící materiály, provozní procedury, plány zachování činnosti organizace, plány zálohování, perzonální data, účetní data, ...
  - ✓ softwarová aktiva – aplikační software, operační systémy, sítě, ...
  - ✓ fyzická aktiva – hardware, areálové vybavení, komunikační spoje, ...
  - ✓ služby – dodávky energií, ...
  - ✓ lidé – jejich kvalifikace, zkušenosti, dovednosti, ...
  - ✓ formální, nehmotná aktiva – pověst, značka, reputace, ...

Klasifikace (informačních) aktiv

- (Informační) aktiva se klasifikují
  - ✓ Výběr efektivních opatření plnících proces zvládání rizik lze učinit až po klasifikaci aktiv
- první přiblížení pojmu klasifikace aktiv
  - ✓ citlivá aktiva – aktivum mající nepominutelnou hodnotu z hlediska plnění činnosti organizace, škoda na citlivém aktivu ovlivňuje dosažitelnost cílů činnosti organizace
    - bankovní IS je pro banku citlivé aktivum, blogy a diskusní fora zákazníků mohou být aktiva, nikoli však citlivá
  - ✓ ostatní aktiva
- Útoky na citlivá aktiva je nutno řešit efektivnějšími (vesměs nákladnějšími) opatřeními než na ostatní aktiva

Klasifikace (citlivých) aktiv

- citlivá aktiva se mnohdy dále klasifikují, např.
  - ✓ důvěrná aktiva (pouze pro vnitřní potřebu) – jejich zveřejnění mimo organizaci je nepatřičné/nevhodné (rutinní informace, se kterou organizace chce zacházet jako s privátní informací)
    - platy/odměny, vnitřní předpisy, . . .
  - ✓ tajná aktiva – informace, jejíž zveřejnění i v rámci organizace by mohlo narušit zájmy organizace
    - tajná data ze zákona, osobní data, hodnocení konkurentů, marketingové informace, informace o zákaznících, . . .
  - ✓ přísně tajná aktiva – informace, jejíž zveřejnění i v rámci organizace by mohlo vážně poškodit organizaci
    - info o akvizicích, konceptuální strategie zvyšování konkurenční schopnosti, přísně tajná data ze zákona, . . .)
- síla (přísnost) opatření chránících aktiva se odvozuje od jejich klasifikační třídy (důvěrná, tajná, přísně tajná, . . .)

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení důvěrnosti aktiv

- Nízká
  - ✓ Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění
    např. na základě zákona o svobodném přístupu k informacím.
    Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy odpovědných orgánů a osob
  - ✓ Není vyžadována žádná ochrana
- Střední
  - ✓ Aktiva nejsou veřejně přístupná a tvoří know-how odpovědných orgánů a osoby, ochrana těchto informací není vyžadována žádným právním předpisem nebo smluvním ujednáním.
  - ✓ Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení důvěrnosti aktiv

- Vysoká
  - ✓ Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními
  - ✓ Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
- Kritická
  - ✓ Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. strategické obchodní tajemství, citlivé osobní údaje apod.).
  - ✓ Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující kompromitaci ze strany administrátorů.

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení integrity aktiv

- Nízká
  - ✓ Aktivum nevyžaduje ochranu z hlediska integrity.
    Narušení integrity aktiv neohrožuje oprávněné zájmy odpovědných orgánů a osob
  - ✓ Není vyžadována žádná ochrana
- Střední
  - ✓ Aktivum může vyžadovat ochranu z hlediska integrity.
    Narušení integrity aktiva může vést k poškození oprávněných zájmů odpovědných orgánů a osob a může se projevit méně závažnými dopady na ostatní aktiva.
  - ✓ Pro ochranu integrity jsou využívány standardní nástroje např.
    omezení přístupových práv pro zápis

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení integrity aktiv

- Vysoká
  - ✓ Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů odpovědných orgánů a osob s podstatnými dopady na ostatní aktiva.
  - ✓ Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu
- Kritická
  - ✓ Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů odpovědných orgánů a osob s přímými a velmi vážnými dopady na ostatní aktiva.
  - ✓ Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu např. pomocí technologie digitálního podpisu

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení dostupnosti aktiv

- Nízká
  - ✓ Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
  - ✓ Pro ochranu dostupnosti je postačující pravidelné zálohování.
- Střední
  - ✓ Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů odpovědných orgánů a osob
  - ✓ Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.

Klasifikace (citlivých) aktiv dle zákona o kyb. bezp.

Stupnice pro hodnocení dostupnosti aktiv

- Vysoká
  - ✓ Narušení dostupnosti aktiva by nemělo překročit dobu několika málo hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů odpovědných orgánů a osob. Aktiva jsou považována jako velmi důležitá.
  - ✓ Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy či výměnou technických aktiv
- Kritická
  - ✓ Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů odpovědných orgánů a osob. Aktiva jsou považována jako kritická.
  - ✓ Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Zranitelnost, *Vulnerability*

- slabina využitelná ke způsobení škod / ztrát organizaci
  útokem – materializací hrozby provedenou útočníkem
  - ✓ zanechávání hořlavého materiálu (papíru) v servrovně je zranitelností využitelnou externí hrozbou – požárem, ohněm
  - ✓ zranitelnosti se mohou nacházet

    ve fyzickém uspořádání
    v organizačních schématech
    v administrativních opatřeních
    v personální politice
    v logických a technických opatřeních
    v hardware, v software, v datech
    v návrhu architektury systému,
    v systému řízení informační bezpečnosti informací, . . .
- Konkrétní příklady viz Příklady zranitelností dle zákona o kybernetické bezpečnosti v dodatku přednášky

Hrozba, útok / bezpečnostní incident, riziko

Hrozba

- ✓ něco může špatně fungovat, něco může ,,útočit'' na informační aktiva
- ✓ co je hodnotné pro vlastníka aktiva,
  je pravděpodobně hodnotné i pro někoho jiného
- ✓ potenciální možnost využití zranitelného místa k útoku útočníkem
- ✓ tj. potenciální příčina bezpečnostní události/incidentu,
  jejímž důsledkem může být poškození aktiva
  z hlediska zajištění jeho důvěrnosti, integrity a/nebo dostupnosti
- ✓ hrozby je nutné identifikovat, pokud se je cílem jejich eliminace

Hrozba, útok / bezpečnostní incident, riziko

- Útok, incident (bezpečnostní incident)
  - ✓ realizovaná hrozba
  - ✓ akt využití zranitelného místa útočníkem ke způsobení škody – snížením hodnoty, zničením, znepřístupněním, . . . aktiva, . . . zveřejněním důvěrného aktiva, . . .
- Generická kategorizace útoků
  - ✓ přírodní katastrofy – hurikán, zemětřesení, požár, . . . mohou zničit nezálohovaná data (zálohovat ve vzdálené lokalitě !)
  - ✓ Externí útoky – krádeže dat o kartách, lidech, . . . hackery, profesionály
  - ✓ Interní útoky – např. web Wikileaks vznikl z interně zcizených dat
  - ✓ Selhání, neúmyslné lidské chyby – výpadek napětí, spojů, disků, . . . vylití kávy do klávesnice, omylem zrušená data, . . .

Hrozba, útok / bezpečnostní incident, riziko

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)
- ✓ Management organizace pověřuje jednotlivce nebo některé oddělení odpovědností za monitorování a případné snižování každého konkrétního rizika
  - snižováním pravděpodobnosti
  - snižováním potenciální škody

  Každé riziko má mít svého vlastníka rizika

Typy hrozeb

- Odhalení (*Disclosure*) citlivých důvěrných dat, postupů, . . .
  - ✓ slídění, špehování, . . . , kryptoanalýza
  - ✓ monitorování komunikací
    – pasívní zjišťování kdo s kým kdy co komunikuje
- Podvod, klamání (*Deception*)
  - ✓ modifikace, falšování identity, popírání autorství (zprávy, dat . . .), odmítání faktu přijetí zprávy, hoaxs (šíření falešných zpráv), . . .
  - ✓ maškaráda (*Masquerade*)
    – útočník vystupuje jako legitimní uživatel
  - ✓ diseminace zlomyslného software (*Planting*)
    – Trojský kůň, vir, . . .
  - ✓ modifikace systému, příprava předmostí pro příští útoky

Typy hrozeb

- Narušení, ničení (*Disruption*)
  - ✓ modifikace (dat, programu, chování technického prostředku, . . .)
    – neautorizovaná osoba získá přístup do systému a modifikuje v něm uložená data, neoprávněně používá zdroje, . . .
  - ✓ modifikace přenášených dat
    – neoprávněné aktivní zásahy do komunikací autorizovaných entit
- Uchvácení, přisvojení (*Usurpation*)
  - ✓ zpožďování provedení služby,
    odmítnutí poskytnutí služby, *Denial of Service* (DoS), . . .
  - ✓ narušení autorizačních pravidel (*Authorisation violation*)
    – osoba autorizovaná pro akci A provádí akci B,
    pro kterou nemá autorizaci
- Konkrétní příklady viz dodatek na konci přednášky

  Příklady hrozeb dle zákona o kybernetické bezpečnosti

Hrozba sémantických útoků

- Vyvolává významné riziko díky ,,prosíťování'' světa
- Lidé mají tendenci věřit tomu co čtou
  - ✓ na potvrzování věrohodnosti ,,není čas''
  - ✓ lidé jsou často obětmi chybných/falšovaných statistik, legend a podvodů
- Podfuk se s velkou pravděpodobností rozšíří síťovým prostředím extrémně rychle
  - ✓ Komunikační média se používají pro šíření věrohodných stupidností již po celou věčnost
  - ✓ Současné- a blízko-budoucí počítačové sítě spuštění takových útoků usnadňují a zprávy diseminují extrémně rychle
  - ✓ digitální podpisy, autentizace, integritní opatření . . .
    šíření podfuků nezabrání – sémantické útoky jsou vedeny na HCI, nejméně bezpečné rozhraní Internetu

Hrozba sémantických útoků, 2

- Pouze amatér útočí na počítače a software
- Profesionál útočí na lidi
  - ✓ ochrana proti sémantickým útokům musí být cílená na sociální řešení, ne na matematicko-logická (a technická) řešení
- Nastupuje fenomén kybernetického prostoru,
  je nutné fenomén informační bezpečnosti rozšířit na fenomén kybernetické bezpečnosti

Principy e-comm usnadňující devastující podvody

- Snadnost automatizace procesů
  - ✓ stejná automatizace, která činní e-comm efektivnější než klasický byznys, zefektivňuje i provádění podvodů
  - ✓ podvod vyžadující vynaložení desítek minut času v papírovém systému lze snadno provést „na jedno kliknutí"
    resp. lze snadno jej periodicky opakovat principem 24×7
  - ✓ singulární podvod s nízkou škodou ignorovatelný v papírovém systému může být hrozbou s velkým rizikem v e-comm systému
- Izolovanost jurisdikce v místech zdroje a cíle útoku
  - ✓ Geografie v elektronickém světě nehraje žádnou roli
  - ✓ Útočník nemusí být fyzicky blízko systému, na který útočí.
    Útočit může ze země,
    – která „nevydává zločince",
    – která nemá adekvátní policejní aparát,
    – která nemá potřebné právní zázemí vhodné ke stíhání, . . .

Principy e-comm usnadňující devastující podvody, 2

- Rychlost šíření ,,prosíťovaným světem''
  - ✓ padělatel papírových peněz monetární systém nezdevastujíe
    - široká diseminace padělatelského nástroje je nereálná,
    - rychlé šíření padělků je obtížné
  - ✓ zpráva jak podvést široce používaný e-comm systém ,,diseminovaná Internetem'' (příp. s připojeným adekvátním softwarovým nástrojem) umožní ,,si vhodně kliknout''statisícům lidí během několika dní
    - znalost jak podvést získal 1 člověk, útočit mohou statisíce lidí

Hrozba enormního nárůstu složitosti a rozsahu

- Enormě narůstá složitost vnitřních algoritmů (jádra) OS
- počty instrukcí spotřebovaných ve Windows
  (a to už před 10 lety) při
  - ✓ Zaslání zprávy mezi procesy: 6K – 120 K podle použité metody
  - ✓ Vyvtoření procesu: 3M
  - ✓ Vytvoření vlákna: 100K
  - ✓ Vytvoření souboru: 60K
  - ✓ Vytvoření semaforu: 10K – 30K
  - ✓ Nahrání DLL knihovny: 3M
  - ✓ Obsluha přerušení/výjimky: 100K – 2M
  - ✓ Přístup do systémové databáze *Registry*: 20K
  - ✓ . . .

Kdo může útočit ? Klasifikace útočníků

Pořadí výčtu odráží kombinaci pravděpodobnosti útoku a výši možných škod max $\longrightarrow$ min

- Nespokojený zaměstnanec – člen týmu, vývojář aplikace / systému, . . .
  - ✓ Typicky motivovaný útočník, často s detailní znalostí systému zevnitř
- Řízený útok na konkrétní systém, konkrétní aktivum
  - ✓ boční efekt nebo přímý důsledek útoku virem, červem, Trojským koněm
  - ✓ automatizovaný škodlivý software (programy, skripty) hledající známé zranitelnosti a využívající je nebo sdělující o nich informaci na vhodné centrální místo sběru zpráv
  - ✓ Příklad: *Stuxnet* – červ útočící na řízení průmyslových systémů pomocí systémů *SCADA*, (*supervisory control and data acquisition*, *dispečerské řízení a sběr dat*)

Kdo může útočit ? Klasifikace útočníků

Pořadí výčtu odráží kombinaci pravděpodobnosti útoku a výši možných škod max $\longrightarrow$ min

- Motivovaný kriminálník, organizovaný zločin
  - ✓ útočník s širokou škálou znalostí potřebných pro úspěšný útok, často s bohatým technologickým a silným ekonomickým zázemím
  - ✓ příp. zaplacený profesionální útočník
  - ✓ Typická motivace organizovaného zločinu – silný finanční zájem, cílem je finanční zisk, orientace na rozlousknutí aplikací typu e-commerce, veřejné bankovní aplikace,...

Kdo může útočit ? Klasifikace útočníků

Pořadí výčtu odráží kombinaci pravděpodobnosti útoku a výši možných škod max $\longrightarrow$ min

- Útočník bez motivace proti zabezpečované organizaci, vandal, skriptový hračička, hacker, . . .
  - ✓ útočník často s širokou škálou znalostí potřebných pro úspěšný útok
  - ✓ obvykle s nižším technologickým a ekonomickým zázemím
- Náhodný útočník
  - ✓ útočník obvykle bez hlubších znalostí napadaného systému, útočných technik, . . .
  - ✓ typicky použije náhodně objevenou zranitelnost, často i nezáměrně

Použitá míra pro klasifikaci útočníků

- slabí útočníci, náhodní útočníci, amatéři, . . .
  - ✓ Využívají náhodně objevená zranitelná místa při běžné práci
  - ✓ Vesměs jsou omezeni znalostmi, penězi, časem (prostředky)
  - ✓ Útoky lze charakterizovat jako náhodné, neúmyslné útoky
  - ✓ Potřebná úroveň ochran – slabá opatření
- středně silní útočníci, hackeři, skriptoví hračičkové, . . .
  - ✓ Vesměs nebývají omezeni znalostmi,
    bývají omezeni penězi, časem (prostředky)
  - ✓ Úmyslné útoky, cíl – provést něco, k čemu nejsem autorizován
  - ✓ Útoky lze charakterizovat jako běžné útoky
  - ✓ Potřebná úroveň ochran – opatření střední síly
- silní útočníci, profesionálové, autority (státní / politické), konkurence
  - ✓ Nejsou omezeni ani znalostmi, ani penězi, ani časem (prostředky)
  - ✓ Úmyslné útoky, a navíc útoky vymykající se běžné praxi
  - ✓ Potřebná úroveň ochran – silná opatření

Bezpečnostní cíl, bezpečnostní funkce / (proti)opatření

- bezpečnostní cíl
  - ✓ dosažení požadované minimální hladiny jistého rizika tak, aby se zajistila požadovaná úroveň informační bezpečnosti v rovinách důvěrnosti / integrity / autentičnosti / dostupnosti / odpovědnosti / / spolehlivosti / neopiratelnosti / . . . informací
- bezpečnostní funkce, opatření, Security Enforcing Function
  - ✓ také:

    funkce prosazující bezpečnost, bezpečnostní opatření, bezpečnostní protiopatření, opatření, protiopatření, . . .
  - ✓ funkce prosazující plnění jednoho nebo několika bezpečnostních cílů
  - ✓ proces, procedura, technický prostředek apod., navržený ke snížení pravděpodobnosti uskutečnění hrozby např. snížením zranitelnosti, zamezením přístupu útočníků nebo snížením dopadu hrozby.

Opatření – nástroj pro snižování rizik

- Zranitelnost může být zdrojem hrozby
  - ✓ uplatněná hrozba (útok) může mít škodlivý dopad (finanční, provozní, . . .)
- Možnost uplatnění a dopadu hrozby představuje riziko (hrozba $\neq$ riziko)
  - ✓ rizika mohou být různě závažná (katastrofická/velká, akceptovatelná, nevýznamná, . . .)
- Problém eliminace či snižování rizik řeší uplatňování / prosazení opatření
  - ✓ plné odstranění rizika bývá vesměs neefektivní
  - ✓ opatření typicky rizika redukují/snižují, neodstraňují je
  - ✓ opatření se mají implementovat pouze pro řešení specifických, identifikovaných rizik

Klasifikace, typy opatření

- klasifikace podle technologie implementace:
  administrativní, logická, technická, fyzická, . . . opatření
- konceptuální klasifikace opatření:
  preventivní, heuristická, detekční a opravná, podpůrná
- klasifikace opatření podle oblasti jejich nasazení:
  řízení a správa bezpečnosti, technologická bezpečnost, bezpečnost provozního prostředí
- 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 . . .

Klasifikace, typy opatření

- 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
- Pro volbu opatření dává návod k volbě nejlepších praktik standard ISO 27002

Typová klasifikace opatření podle technologie implementace

- opatření fyzického charakteru
  - ✓ stínění, trezory, zámky, strážní, visačky – jmenovky, protipožární ochrana, záložní generátory energie, . . .
- opatření technického charakteru (hardware)
  - ✓ autentizátory na bázi identifikačních karet, autentizační kalkulátory, šifrovače, firewally, archivační paměť páskového typu, . . .
- opatření logického charakteru (software)
  - ✓ funkce řízení přístupu, kryptografické utajování, digitální podepisování, antivirové prostředky, . . .

Klasifikace opatření podle technologie implementace

- opatření administrativního charakteru
  - ✓ normy pro návrh, kódování, testování, údržbu programů
  - ✓ směrnice pro výběr a školení důvěryhodných osob, pro tvorbu hesel, pro autorizační postupy, pro přijímací a výpovědní postupy
  - ✓ právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politiky
- v čase působící opatření
  - ✓ řízení opakovaného použití objektů,
  - ✓ zamykání objektů pro zajištění logické konzistence objektů zpracovávaných paralelními transakcemi
- opatření budované na bázi biometrických dat

Klasifikace opatření podle oblasti jejich nasazení

- Oblast technologické bezpečnosti, technická opatření
  - ✓ Prostá až komplexní opatření na bázi architektur systémů, inženýrských disciplin, bezpečnostních balíků založených na mixu hardware, software, firmware
- Oblast řízení a správa bezpečnosti, řídicí opatření
  - ✓ Jsou orientovaná na tvorbu a garantování politik, návodů, standardů
  - ✓ Jsou prováděná formou provozních procedur, jsou vesměs předepsaná vnitřními předpisy organizace
- Oblasti bezpečnosti provozního prostředí, provozní opatření
  - ✓ Používají se, společně s technickými opatřeními a dobrými industriálními praktikami, pro opravu provozních nedostatků, které by mohli útočníci využít

K jednotlivým kategoriím dále podrobněji:

Technická opatření

- Preventivní technická opatření
  - ✓ autentizace, autorizace, řízení přístupu, podpisování, ochrana komunikací, . . .
- Detekční technická opatření
  - ✓ audit, detekce útoků, návraty do bezpečného stavu, detekce virů, . . .
- Podpůrná technická opatření
  - ✓ identifikace, správa krypto-klíčů, . . .

Řídicí opatření

- Preventivní řídicí opatření
  - ✓ přidělení adresné odpovědnosti za bezpečnost kritických podnikatelských procesů
  - ✓ vypracování a udržování aktuálních plánů bezpečnosti systému dokumentujících používaná opatření a uvádějící plánovaná opatření
  - ✓ implementace personálních opatření typu ,,rozdělení oprávnění'', ,,přidělování nejmenších potřebných oprávnění'', povolení přístupu pouze po registraci, . . .
  - ✓ průběžné vedení školení cílených na zvyšování bezpečnostního uvědomění a technický výcvik zaměstanců a uživatelů systému
- Detekční řídicí opatření
  - ✓ periodické zkoumání efektivnosti bezpečnostních opatření
  - ✓ periodický audit systému
  - ✓ vedení průběžného řízení rizik pro ohodnocování a zvládání rizik
  - ✓ zmocnění systému k určení a akceptování zbytkového rizika

Řídicí opatření

- Opravná řídicí opatření
  - ✓ plán zachování kontinuity činnosti po havárii, . . .
  - ✓ plán činnosti po detekci incidentu (útoku na bezpečnost)

Provozní opatření

- Preventivní provozní opatření
  - ✓ řízený fyzický přístup k datovým médiím
  - ✓ virové ochrany
  - ✓ bezpečné strukturované vodiče
  - ✓ procedury pro uchovávání a zajištění bezpečnosti archivů dat
  - ✓ protipožární ochrana
  - ✓ zajištění trvalosti dodávky energie
  - ✓ . . .
- Detekční provozní opatření
  - ✓ Zajištění fyzické bezpečnosti
    (detektory pohybu, televizní sledování, . . .)
  - ✓ Zajištění bezpečnosti prostředí (detektory kouře/ohně, . . .)

Klasifikace opatření podle ISO/IEC 27001/27002

Bezpečnostní mechanismy

- (bezpečnostní) opatření musíme účinnou formou implementovat vhodnými (bezpečnostními) mechanismy
  - ✓ mechanismy administrativního, technického, logického, . . . charakteru
  - ✓ opatření řešící problém nepopiratelnosti – digitální podpis

    mechanismus = asymetrická kryptografie
  - ✓ opatření řešící řízení přístupu
    v souladu s přijatou politikou řízení přístupu

    mechanismus = fyzické klíče, idenfikační karty, biometriky, . . .
  - ✓ opatření řešící problém důvěrnosti
    v souladu s přijatou politikou zajištění důvěrnosti

    mechanismus = šifrování, trezory, smluvní závazek (NDA), . . .

Klasifikace bezpečnostních mechanismů podle odolnosti

- mechanismy základní síly, slabé bezpečnostní mechanismy
  - ✓ ochrana proti náhodným, neúmyslným útokům
  - ✓ ochrana proti amatérům, náhodným útočníkům
  - ✓ lze narušit kvalifikovaným („běžným“) útokem / útokem střední síly
- bezpečnostní mechanismy střední síly
  - ✓ ochrana pro úmyslným útokům vedeným s omezenými příležitostmi a možnostmi
  - ✓ ochrana proti hackerům, ochrana proti „běžným“ útokům
- silné bezpečnostní mechanismy
  - ✓ ochrana proti útočníkům s vysokou úrovní znalostí, s velkými příležitostmi, s velkými prostředky
  - ✓ ochrana proti profesionálům
  - ✓ ochrana proti útokům vymykající se běžné praxi

Aplikační systém, specifikace bezpečnosti systému

- Architektura aplikačního systému
  - vesměs nebývá daná
    požadavky na bezpečnostní opatření
  - vesměs bývá daná hlavními aplikačními cíli
- Požadavky na bezpečnostní opatření se typicky odvozují
  ze struktury systému procesem analýzy rizik
- Tudíž specifikace bezpečnosti typicky sestává
  - ✓ z definování, jak se provozují jisté komponenty celého systému s ohledem na bezpečnost
  - ✓ z definování podsystémů souvisejících s bezpečností

  a nedefinuje celkovou architekturu systému

Typické komponenty systému relevantní s bezpečností

- kryptografické funkce
  v hardwarové i softwarové implementaci
- bezpečnostní funkce
  poskytované jako služby a rysy OS
  - ✓ řízení přístupu, izolace běhu procesů, ...
- HSM, *Hardware Security Modules*
  - ✓ hardwarové moduly odolné proti falšování, průnikům, ...
  - ✓ od HSM pro správu klíčového hospodářství certifikační autority až po čipovou kartu osoby
- fyzická bezpečnostní opatření
  - ✓ bezpečné místnosti, ...

Implementace systému

- Specifikovaný systém musí být implementován, má-li být provozován
- Proces implementace mj. zahrnuje
  - ✓ nákupy hotových produktů a služeb
  - ✓ implementace prováděné na zakázku
- takže je potřeba počítat s organizováním řady výběrových řízení pro zajištění implementace systému
- Postup implementace systému má specifikovat bezpečnostní politika
- Postup implementace systému musí být auditovatelný
  - ✓ vývojové / testovací / akceptační / provozní prostředí,
  - ✓ výsledná dokumentace pro jednotlivá prostředí, . . .

Doprovodnou dokumentaci k systému obvykle tvoří

- Specifikace systému
  - ✓ definující co (někdy i jak nebo i architekturu) systém dělá
- Manuály systému
  - ✓ popisující jak konfigurovat a provozovat hardwarové a softwarové komponenty systému
  - ✓ popis jak systém může být provozovaný
  - ✓ popis všech možných voleb různých rysů chování systému
  - ✓ obvykle generický dokument vytvořený poskytovatelem systému
- Provozní procedury
  - ✓ popisující jak má být konfigurovaný a provozovaný konkrétní systém
  - ✓ popisy (krok po kroku) jak se systém provozuje v konkrétní organizaci
  - ✓ kdo je odpovědný za provedení jednotlivých úkolů, . . .

Testování

- Jakmile je systém implementovaný, je nutné získat důkazy jeho bezchybné provozovatelnosti
- Takové důkazy částečně poskytuje testování
- Testovací běhy (případy) systému musí být definované
  - ✓ nahodilé testování není korektní
  - ✓ testování podsystémů dodávaných třetí stranou je obvykle povinností dodavatele, výsledky testů by měly být odběrateli zpřístupněné
- Testování samo o sobě nedává dostatečné záruky za dosažení požadované úrovně bezpečnosti – nepominutelné jsou hodnocení plynoucí
  - ✓ z analýzy návrhu a návrhového procesu
  - ✓ z (automatické/manuální) analýzy kódu
  - ✓ z analýzy funkcionality, dokumentace, . . .

Hodnocení bezpečnosti

- Definovatelnou úroveň důvěry v dosaženou úroveň bezpečnosti systému (a jeho podsystémů) lze získat pouze pomocí formalizovaného hodnocení bezpečnosti
- Výsledkem hodnocení bezpečnosti je vyslovení záruky za dosaženou úroveň bezpečnosti
- Fundamentálním aktuálním standardem formalizovaného hodnocení bezpečnosti informační bezpečnosti jsou např.
  - tzv. Common Criteria, (CC)
    resp. standard ISO/IEC 15408
  - kritéria OWASP (Open Web Application Security Project)
- Principy hodnocení a získatelné výsledky z hodnocení podle CC (a OWASP) viz samostatná přednáška

Bezpečnostní procedury (postupy), role

- Připomínka z popisu dokumentace systému

  Provozní procedury

  - ✓ popisy (krok po kroku) jak se systém provozuje v konkrétní organizaci
  - ✓ kdo je odpovědný za provedení jednotlivých úkolů, . . .

- Složitost a rozsah procedur je daná stupněm potřebné interakce lidského činitele se systémem a požadavky na záruku spolehlivosti, důvěryhodnosti, . . .

- Typické role osob vystupujících v bezpečnostních procedurách

  - ✓ *Security architect*, bezpečnostní architekt
  - ✓ *Security manager*, bezpečnostní správce, resp. *Security officer*, bezpečnostní administrátor/úředník
  - ✓ Operátor, správce, administrátor systému
  - ✓ Auditor, nezávislá osoba na exekutivě bezpečnosti

Bezpečnostní procedury (postupy), obsah

- Definice zúčastněných rolí
- Přidělení rolí jednotlivcům
  vč. procedur zajištění kontinuity plnění rolí
- Popis instalace a iniciální konfigurace systému
- Popis provozních procedur systému
  vč. plánu činnosti po bezpečnostním incidentu
  (*Business Continuity Plan*)
- Popis zálohovacích a obnovovací procedur
  vč. havarijního plánu
  (plán činnosti po ,,katastrofickém incidentu'',
  Recovery Plan)

Politika, bezpečnostní politika

Politika

- ✓ pravidla řídicí dosažení cílů určenými způsoby
- ✓ je-li cílem řízení přístupu – pak je to politika řízení přístupu
- ✓ je-li cílem areálová bezpečnost – pak je to politika zabezpečení areálu

Bezpečnostní politika organizace

- ✓ souhrn bezpečnostních zásad a předpisů,
  množina pravidel definujících správu a ochranu aktiv
- ✓ definuje způsob zabezpečení organizace jako celku
- ✓ od fyzické ostrahy, přes ochranu soukromí,
  přes bezpečné plnění cílů činnosti organizace
  až po ochranu lidských práv . . .

Politika informační bezpečnosti (IT Security Policy)

- dokumentovaný souhrn bezpečnostních zásad, pravidel, směrnic, předpisů pro ochranu informačních aktiv
- zajišťuje potřebnou úroveň důvěrnosti, autenticity a integrity dat v organizaci vč. požadované bezpečnosti transakcí v distribuovaném prostředí (Internet)
- politika se běžně vyjadřuje neformálně, v přirozeném jazyce
  - ✓ standardizovaná hodnocení informační bezpečnosti budou IT systémy s neformálně vyjádřenou politikou informační bezpečnosti hodnotit jako systémy s nízkou úrovní záruky důvěryhodnosti politiky
- vyšší úroveň záruky za důvěryhodnost politiky poskytuje její semi-formální vyjádření
  - ✓ zvýšení úrovně důvěryhodnosti nelze dosáhnout použitím silnějších bezpečnostních mechanismů a/nebo bohatší škálou opatření

Politika informační bezpečnosti (IT Security Policy)

- vyjímečně lze použít i formální logicko–matematické jazyky pro vyjádření politiky (pro omezená prostředí a systémy)
  - ✓ pak lze dosáhnout až vysoké úrovně důvěryhodnosti

Politika informační bezpečnosti (IT Security Policy)

- má vyhovovat bezpečnostní politice organizace
- definuje bezpečné používání IT v rámci organizace
- stanovuje koncepci informační bezpečnosti organizace
  v horizontu 5–10 let
- stanovuje co jsou citlivá informační aktiva,
  jejich klasifikaci a odpovědnosti za jejich stav
- stanovuje bezpečnostní infrastrukturu organizace z pohledu
  informační bezpečnosti
  - ✓ nutná je nezávislost výkonných a kontrolních rolí
- definuje třídu (sílu) útočníků, vůči kterým se informace
  organizace zabezpečují
- je nezávislá na konkrétně použitých IT

Plán zvládání rizik

- také Systémová politika informační bezpečnosti
- stanovuje politiku informační bezpečnosti konkrétního systému v horizontu 1–2 let
- je závislý na konkrétně použitých IT
- 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

Plán zvládání 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
- Jádro/podstata plánu zvládání rizik
  - ✓ plán a program ukazující pro každé identifikované riziko
    - jak riziko organizace zvládá
    - která opatření se považují za nutná
    - časový prostor pro jejich implementaci
    - hladinu akceptovatelného rizika

Plán zvládání rizik

- má identifikovat kvalifikační požadavky a systém výchovy v bezpečnostním uvědomění
- je klíčovým dokumentem pro cyklus života ISMS, na vysoké úrovni dokumentuje pro každé riziko
  - ✓ kdo je odpovědný za splnění kterého cíle řízení rizik
  - ✓ jak se splnění dosáhne
  - ✓ s jakými zdroji lze počítat
  - ✓ jak je dosažení cíle hodnoceno a vylepšováno
  - ✓ detailní plán popisující kdo je odpovědný za kterou akci
- plán je živý dokument
  - ✓ koriguje se při každé změně práv, rizika, . . .
- má existovat řídicí proces zajišťující aktualizaci plánu
  - ✓ vč. podpisu odpovědnou rolí na úrovni vedení organizace

Generické rysy zabezpečování informací

- Kterou metodologii vývoje použít ?
  - ✓ není podstatné kterou metodologii použít,
    volba typu metodologie není tak důležitá,
    důležité je nějakou metodologii zvolit a systematicky používat
  - ✓ ad hoc vývoj je příliš nestrukturovaný na to,
    aby vytvořil bezpečnou aplikaci
  - ✓ důležité je velmi přísně a důsledně odsouhlasovat výsledky
    návrhových, testovacích a dokumentačních procesů
  - ✓ důležité je jasně stanovit, kam a kdy zařadit provedení bezpečnostních
    nástrojů typu: analýza rizik, analýza hrozeb,
    oponování dílčích výsledků, analýza programů, . . .
  - ✓ je nutné aplikovat metodologii
    - dobře fungující v podmínkách rozsahu a vyzrálosti organizace
    - mající potenciál ke snížení stávající chybovosti
    - vylepšující produktivitu vývoje
    - schopnou se přizpůsobovat růstu organizace či produkce

Generické rysy zabezpečování informací

- Které programovací standardy použít ?
- Efektivní je orientace na bázi známých nejlepších praktik
  - ✓ architekturní směrnice
    (např. Webovská vrstva nesmí přímo volat DBS)
  - ✓ specifikace minimálně požadované dokumentační úrovně
  - ✓ stanovení povinnosti a způsobů testování a požadavků na pokrytí testy
  - ✓ specifikace minimální úrovně komentářů kódu a stylu poznámek
  - ✓ stanovení požadavků na jednotné zvládání výjimek
  - ✓ určení preferovaného stylu pojmenovávání
    proměnných, funkcí, tříd, tabulek, . . .
  - ✓ požadavek preference udržovatelnosti a čitelnosti kódu
    před jeho vyšperkovaností
  - ✓ specifikace verzování, změnové řízení kódů programů, . . .
  - ✓ . . .

Generické rysy zabezpečování informací

- Aplikační architekt × bezpečnostní architekt
- Aplikační architekt
  - ✓ odpovídá za to, že návrh pokrývá jak typické používání aplikace, tak i ochrany před extrémními útoky na ni
  - ✓ zásadní rizika pro aplikaci musí aplikační architekt znát
- Bezpečnostní architekt (informační bezpečnosti)
  - ✓ odpovídá za řešení základních pilířů informační bezpečnosti (důvěrnosti, integrity, dostupnosti, . . .)
  - ✓ aplikace musí poskytovat nástroje pro tato řešení

Generické rysy zabezpečování informací

- Minimalizovat prostor využitelný pro útok
  - ✓ každá nadbytečná vlastnost aplikace zvyšuje objem rizik pro celou aplikaci
  - ✓ např. k webovské aplikace se doplní on-line help s vyhledávací funkcí
  - ✓ vyhledávací funkce může být zranitelná útokem *SQL injection*
  - ✓ když help zpřístupníme pouze autentizovaným uživatelům, riziko se sníží
  - ✓ když každý vstup vyhledávací funkce bude kontrolovat centralizovaný validační program, riziko se sníží dramaticky
  - ✓ když se odstraní vyhledávací funkce, riziko zmizí úplně a help vlastnost lze dát na veřejný Internet jako samostatnou aplikaci
- Jako implicitní řešení používat bezpečná řešení
  - ✓ Např. časové omezení platnosti hesla a nárok na minimální netriviálnost hesla má být implicitně zapnutá
  - ✓ uživatel si může tyto vlastnosti vědomě vypnout, na své riziko.

Generické rysy zabezpečování informací

- Princip nejmenších práv
  - ✓ Každému mají být přidělena ta nejmenší možná práva, která potřebuje pro řešení svých činností
  - ✓ Jestliže midlewarový server potřebuje mít přístup k Internetu, číst databázové tabulky a zapisovat logování dějů, pak má mít k tomu přidělená příslušná práva, ale nikoli práva administrátora / superuživatele
- Důkladný a komplexní princip ochran
  - ✓ Chyba v rozhraní administrátora bude pravděpodobně zřídka využita anonymním útočníkem pokud rozhraní bude správně hlídat, kontrolovat autenticitu administrátora, logovat žadatele, . . .
- Každý externí systém vůči bezpečné aplikaci musí být implicitně považovaný za nedůvěryhodný

Generické rysy zabezpečování informací

- Chybný je koncept ,,Security through Obscurity''
- Separace rolí
  - ✓ určité role mají jinou úroveň důvěry než normální uživatelé
  - ✓ administrátor systému × normální uživatel
  - ✓ administrátor nemá být normálním uživatelem aplikace:
    - administrátor OS může nastavit politiku hesel, vypnout systém, . . . ,
    - administrátor nemůže nakoupit akcie, i když je ,,superuser''
- V jednoduchosti je síla
  - ✓ dvojnásobná negace ještě nemusí v reálné praxi být pozitivem
- Správně opravovat chyby
  - ✓ vypracovat test příčiny chyby
  - ✓ porozumět bázovému problému způsobujícímu chybu
  - ✓ porozumět souvislostem – např. při odhalení chyby v návrhovém vzoru