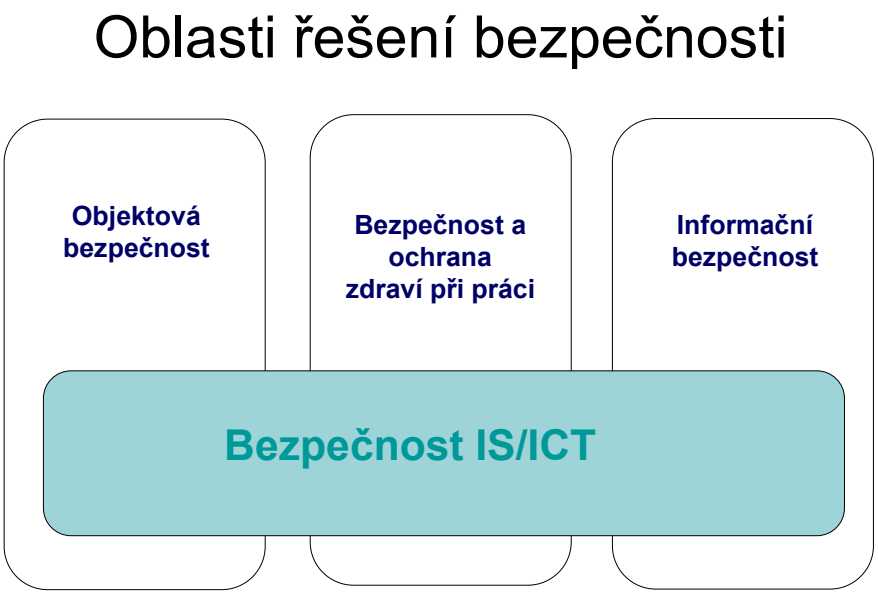
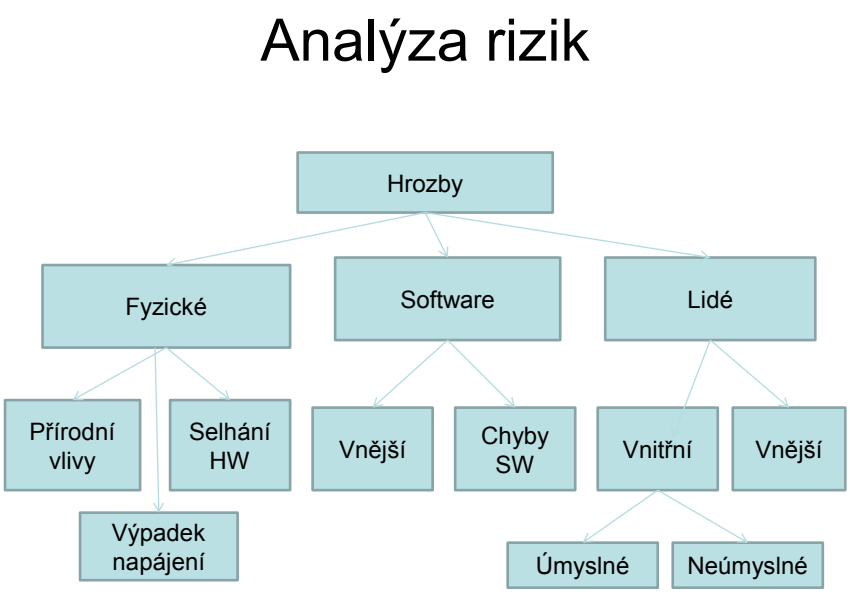
BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Termín „bezpečnost“ je poměrně široký pojem. V zásadě můžeme bezpečnost rozdělit do tří oblastí:



V následujícím textu se budeme zabývat pouze oblastí „Informační bezpečnosti“.

Základní pojmy z oblasti bezpečnosti v oblasti IT byly probírány v rámci předmětu „Základy informatiky“ v prvním semestru. Připomeňme si základní rozdělení bezpečnostních hrozeb:



DRUHY ÚTOČNÍKŮ

- Hacker
  - Začátečník -> uznání, seberealizace
  - Profesionál -> překonání intelektuálních výzev, ideál o svobodném přístupu informací...
- Virový tvůrce – „zrazení idealisté“, „nedocenění odborníci“,…
- Vnitřní nepřítel („Insider thread“) – odplata vůči zaměstnavateli, pocit křivdy, …
- Informační válečník – vlastenecké motivy – destabilizace nepřátelských zdrojů
- Zloděj – snaha o zisk financí, př. Fishing
- Politický aktivista – fanatik, idealista…

Chyby, které využívají útočníci:

- **Programátorské chyby** - vznikají při neošetření některých stavů programů, špatných výpočtech při alokaci paměti, nedostatečných kontrolách vstupu od uživatele a podobně.
- **Návrhové chyby** - vznikají při chybném úsudku návrháře programu. Často bývají obtížně odstranitelné. Příkladem může být například šifrování ve WiFi sítích podle standardu WEP. Ten je dodnes možné na všech síťových kartách a přístupových bodech

pro WiFi sítě použít, i když záhy po jeho uvedení byl zveřejněn velmi jednoduchý způsob jak jej prolomit.

- **Konfigurační chyby** - vznikají chybou nebo nevědomostí uživatele nebo administrátor, který daný program nebo zařízení nastavuje. Velká část zařízení i programů bývají kvůli co nejjednoduššímu používání od výrobců nastaveny tak, že obsahují řadu nebezpečných nastavení. Příkladem může být typický přístupový bod pro WiFi síť - naprostá většina se dodává s vypnutým šifrováním, takže po jejich zapnutí se do WiFi sítě (a tím pádem i do lokální sítě, kam je přístupový bod připojený) může připojit kdokoliv.
- **Fyzické narušení** - velká část bezpečnostních opatření lze obejít, když má útočník fyzický přístup k zařízení nebo počítači. Například může z počítač vyjmout pevný disk a přečíst a nebo upravit jeho obsah i když se k zapnutému počítači nemůže přihlásit.
- **Chyby obsluhy** - stačí omylem spustit jeden škodlivý program v okamžiku, kdy je uživatel přihlášený s administrátorskými oprávněními a počítač může být napadený bez ohledu na to, jak kvalitní firewall jej chrání před útoky z internetu

Cíle útočníků:

- Krádež dat a informací
- Zničení dat
- Destabilizace systému
- Blokování místa nebo určitých zdrojů

OBRANNÉ MECHANISMY

FYZICKÉ A PŘÍRODNÍ OHROŽENÍ

- **Zálohování** (úplná x inkrementální záloha)
- **Zabezpečení** – UPS, přepěťové ochrany,…
- **Kategorie systémů odolných vůči výpadkům:**
  - Fault-tolerant systém – systém odolný vůči výpadkům – výpadek části systému (elektřina, komponenta, síť) nezpůsobí významné přerušení funkce systému; řešení pomocí zdvojení kritických komponent
  - Disaster-tolerant systém - systém odolný vůči katastrofám; jako FT řešeno zdvojením ale i fyzickým oddělením záložního systému.

SOFTWAROVÉ OHROŽENÍ

- Firewall, antivirové programy, …
- Sítě – VPN (Virtual Private Network) –
- Autentizace a řízení přístupových práv
- Bezpečnostní politika, plán obnovy činnosti, havarijní plán (návod pro uživatele, co dělat v případě havárie – komu mají volat)

Autentizace = ověření uživatele

Autorizace = ověření práv

Firewall je tzv.„bezpečnostní brána“, je to zařízení či software oddělující provoz mezi dvěma sítěmi (např. interní podniková a veřejný internet), přičemž propouští jedním nebo druhým směrem data podle určitých předem definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.

AUTENTIZACE A BIOMETRIE

- **Přístup přes uživatelská jména a hesla nebo PIN**
  - Expirační doba hesel
  - Omezený počet pokusů přihlášení (heslo, PIN)
  - „Strong“ password – minimální počet znaků, povinné kombinace čísel a písmen, zákaz používání smysuplných slov
  - Zákaz „prázdného“ hesla

- **Ověření uživatele**
  - Vlastnictví určitého předmětu – karta, čárový kód, token
  - Ověření fyziologických charakteristik – biometrie
- **Využití časových intervalů** (automatické odhlášení při delší nečinnosti)

Problémy autentizace:

- Příliš mnoho hesel do různých systémů
- Nejednoznačnost identity (v jiném systému pod stejným uživatelským jménem vystupuje někdo jiný)

BIOMETRIE

- Otisky prstů
- Snímek oční sítnice a duhovky
- Rozpoznání obličeje, dlaně
- Rozpoznání hlasu
- Dynamika podpisu, psaní na klávesnici

Problémy biometrických metod:

- Obtížnost měření biometrických informací
- Ověření, že je uživatel živý (liveness-test)
- Závislost měření na prostředí a fyzické kondici uživatele

Chyby biometrických systémů:

False Rejection Error - oprávněnému uživateli je odmítnut přístup do systému

False Acceptance Error - Neoprávněný uživatel je biometrickým zařízením označen jako oprávněný

BEZPEČNOST DATABÁZÍ

- zabezpečení dat v databázi proti zneužití
- zabezpečování přihlašovacích informací
- zabezpečení komunikace mezi aplikací a databází
- zabezpečení dotazů proti SQL-injection

Architektury bezpečných informačních systémů:

- *Trusted Subject Architecture* - Databázový a operační systém jsou jedna entita
- *Woods Hole Architecture* - Uživatele pracují s množinou nedůvěryhodných rozhraní pro různé bezpečnostní úrovně. Ty komunikují s důvěryhodným rozhraním (front end), které funguje jako referenční monitor. Samotný databázový systém je opět nedůvěryhodný.

BEZPEČNOSTNÍ POŽADAVKY NA IS

Bezpečnostní požadavky na IS pro státní správu definuje „Národní strategie informační bezpečnosti ČR“ (www.micr.cz). Obecně je lze formulovat jako:

- zachování důvěrnosti („confidentiality“), kdy přístup k aktivům mají pouze autorizované subjekty, tj. osoba, proces nebo zařízení disponující oprávněními k provádění činností v IS/ICT.
- zachování dostupnosti („availability“), kdy autorizované subjekty mohou na své vyžádání vykonat činnosti a není jim odepřen k činnosti přístup.
- zachování integrity, kdy ke změně aktiva nemůže dojít neautorizovaným subjektem, nepovolenou činností či nekompletním provedením změn.

Vlastnosti systému ovlivňujících jeho bezpečnost:

- zajištění prokazatelnosti („authentication“), kdy lze vysledovat jakoukoliv akci, která v systému proběhla s tím, že lze zjistit původce takové akce,
- zajištění nepopíratelnosti („non-repudiation“), kdy subjekt nemůže odmítnout svoji účast na provádění nějaké akce,
- zachování spolehlivosti („reliability“), kdy reálné chování systému je konsistentní s chováním systému, tak jak je dokumentováno.

BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika je soubor zásad a pravidel (dokument), s jejichž pomocí organizace chrání svá aktiva.

Obsahuje:

- Popis informačního systému
- Cíle bezpečnostní politiky
- Definice citlivosti informací
- Definice možných hrozeb
- Zásady personální politiky
- Stanovení politiky zálohování
- Plán obnovy pro havárii
- Metodiku řešení krizových stavů

Nejsou věci „bezpečné“ a „nebezpečné“, jsou jen různé míry rizika.

Různí lidé akceptují v různých situacích různou míru rizika.

Řešení bezpečnosti je nekončící **proces**.

ANALÝZA RIZIK

- Co se stane, když informace nebudou chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

INSTITUCE SE VZTAHEM K BEZPEČNOSTI IS

- Úřad pro ochranu osobních údaj - ÚOOÚ
- Národní bezpečnostní úřad - NBÚ
- Ministerstvo vnitra – MV ČR
- Český normalizační institut - ČNI
- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví - ÚNMZ

LEGISLATIVA TÝKAJÍCÍ SE BEZPEČNOSTI IS

- Zákon č. **106/1999 Sb**., o svobodném přístupu k informacím
- Zákon č. **101/2000 Sb**., o ochraně osobních údajů
- Zákon č. **227/2000 Sb**., o elektronickém podpisu (poslední úpravy zákon č. **110/2007 Sb.**) a **304/2001 Sb.** Prováděcí vyhláška
- Zákon č. **365/2000 Sb**., o informačních systémech veřejné správy (poslední úprava . 81/2006 Sb.),
- Zákon č. **22/1997 Sb.**, o technických požadavcích na výrobky
- Zákon české národní rady č. **20/1993 Sb**., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví.
- Zákon č. **412/2005 Sb**., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

DVANÁCTKU TIPŮ K OCHRANĚ FIREMNÍCH DAT (NETWORK BOX)

12 tips to ensure company data is kept private:

- Zvolte prohlížeč a udržujte ho v aktualizované podobě tak, aby dokázal správně ohodnotit existující rizika.
- K užívání povolte jen schválené prohlížeče, a to na všech počítačích firmy (ať v práci či doma).
- Ujistěte se, že uživatelé znají význam toho aktu, když se podepisují k internetovým službám.
- Pokud vaše e-maily či uložená data obhospodařuje jiný poskytovatel, obětujete tak některá práva na vaše soukromí.
- Buďte opatrní na to, která data takto ukládáte, v některých zemích je to upraveno legislativou (třeba Německo).
- Nastavte firemní počítače tak, aby byly zakázány cookies třetích stran.
- Ujistěte se, že bezpečnostní systémy jsou v aktualizované podobě a že používáte vícevrstvý bezpečnostní přístup.
- Ověřujte aplikace ve vztahu k zranitelnosti (např. typu SQL injection).
- Ujistěte se, že zaměstnanci nepoužívají soukromý e-mail pro pracovní účely.
- Ujistěte se, že zaměstnanci pravidelně vyčistí historii používaných prohlížečů a čistí cache informací, která je uložena na počítači.
- Připomínejte uživatelům, že je třeba pravidelně měnit hesla a že tato hesla jsou dostatečně robustní. Připomeňte jim, aby nepoužívali vlastnost „Pamatuj si mne“ při logování na chráněné weby.
- Buďte ve střehu. Ujistěte se, že zaměstnanci chápou existující bezpečnostní rizika a že se nestanou obětí phishingových podvodů.