INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA STROJNÍ

ZÁKLADY INFORMATIKY

Ing. Roman Danel, Ph.D.

Ostrava 2013

ISBN 978-80-248-3052-0

Tento studijní materiál vznikl za finanční podpory Evropského sociálního fondu (ESF) a rozpočtu České republiky v rámci řešení projektu: CZ.1.07/2.2.00/15.0463, MODERNIZACE VÝUKOVÝCH MATERIÁLŮ A DIDAKTICKÝCH METOD

OBSAH

1 BEZPEČNOST IT

OBSAH KAPITOLY:

Bezpečnost IT

Analýza rizik

Obranné mechanismy a zálohování dat

MOTIVACE:

V této kapitole se seznámíte se základy počítačové bezpečnosti. Řekneme si co je to analýza rizik, jaké druhy hrozeb existují a jak se proti nim můžeme bránit. Vysvětlíme si, jaký je rozdíl mezi autorizací a autentizací, co to je biometrické ověření uživatele a k čemu je firewall. Dozvíte se, co to je bezpečnostní politika a co obsahuje havarijní plán.

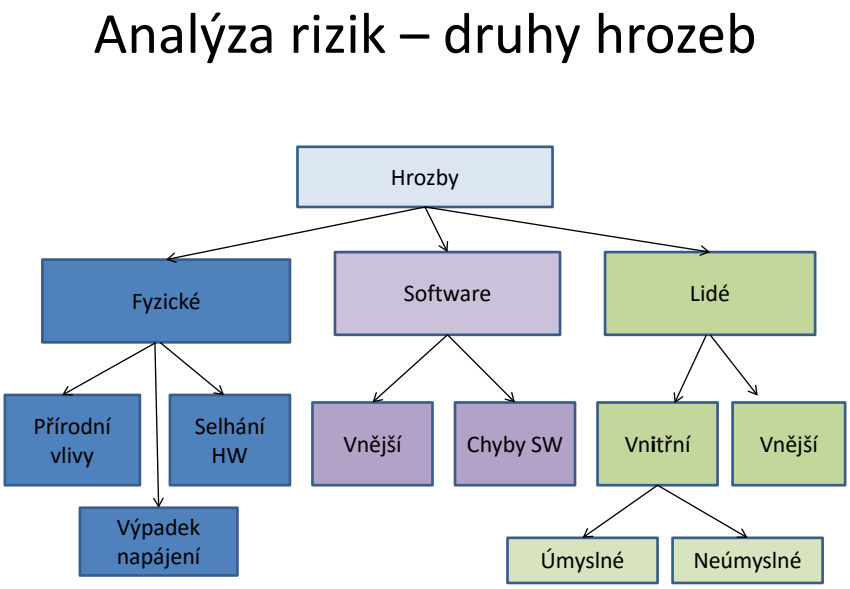
CÍL:

Po prostudování kapitoly budete umět vysvětlit, co je to fault a disaster tolerant systém. Budete znát, co se chápe pod pojmy bezpečnostní politika a havarijní plán. Získáte přehled, s jakými hrozbami se v IT můžete setkat.

1.1 BEZPEČNOST IT

Jednou z nejdůležitějších oblastí informatiky je bezpečnost. Ztráta nebo odcizení dat patří mezi události, které pro nás mohou mít nedozírné následky.

1.2 ANALÝZA RIZIK



Audio 1.1

Bezpečnost můžeme rozdělit do tří okruhů:

- Fyzická bezpečnost
  - Technické závady
  - Přírodní katastrofy – např. požár
  - Výpadek elektrické energie
  - Blesk, přepětí, podpětí…
- Softwarové ohrožení
  - Vnější – viry, červi, trojské koně a jiné škodlivé programy
  - Chyby v software
- Ohrožení lidmi
  - Vnější – hackeři, útočníci…
  - Vnitřní – vlastní zaměstnanci úmyslné poškození nebo krádež
  - Vnitřní neúmyslné – např. smazání omylem nebo poškození z neznalosti

1.2.1 Softwarové ohrožení

- Počítačové virus - program, který se šíří bez vědomí uživatele a vykonává nežádoucí nebo škodlivou činnost. Bližší informace k aktuálním virům najdete např. na http://www.antivirovecentrum.cz http://www.viry.cz
  - Druhy virů: souborové, bootovací (aktivují se při startu počítače ze zavirovaného boot sektoru), stealth, polymorfní (snaží se zabránit detekcí

antivirovým programem neustálou změnou své struktury tak, aby nemohl být nalezen charakteristický řetězec), makroviry (v kancelářském SW)

- Trojský kůň - skrytá část programu nebo aplikace provádějící funkce, se kterou uživatel nesouhlasí, na rozdíl od viru aktivuje uživatel spuštěním programu
- Červi (worms) - šíření založeno na bezpečnostních chybách operačního systému, poštovního klienta, databáze nebo aplikace
- Back-doors – vstup do systému bez hesla
- Zapomenuté funkce z doby vývoje
- Phishing - podvodný email snažící se technikou sociálního inženýrství vylákat důvěrné informace-např. hesla
- Hoax – poplašná zpráva. Seznam poplašných zpráv najdete na stránkách http://www.hoax.cz
- Spyware – software, který sleduje uživatele nebo informace o jeho počítači a data odesílá
- Rootkit – program k zamaskování určitých aktivit na počítači

1.2.2 Ohrožení lidmi

Cíle útočníků:

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

1.2.3 Typy 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, například formou phishingu
- Politický aktivista – fanatik, idealista…

Chyby, kterých 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 počítače vyjmout pevný disk a přečíst 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

1.3 OBRANNÉ MECHANISMY A ZÁLOHOVÁNÍ DAT

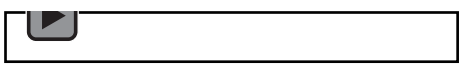
Cílem je:
- Zajištění důvěrnosti dat
- Zajištění integrity dat
- Zajištění dostupnosti

1.3.1 Ochrana proti fyzickému a přírodnímu ohrožení

- **Zálohování dat**
  - úplná nebo inkrementální záloha
  - replikace, mirroring dat
- **Zabezpečení** proti výpadku napájení – UPS, přepěťové ochrany, RAID, …
- **Cluster** - skupina počítačů nebo SW prostředků, která se navenek chová jako jediný systém
- **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 u fault-tolerant systémů je bezpečnost řešena zdvojením, ale navíc i fyzickým oddělením záložního systému (minimálně do jiné budovy nebo lépe v jiném městě).

UPS je zařízení, které obsahuje baterie, schopné dodávat po určitou dobu elektrickou energii při výpadku dodávky elektrického proudu. Další funkcí je stabilizace výstupního napětí (eliminuje předpětí a podpětí). Je třeba si uvědomit, že baterie časem stárnou a cca po 3-4 letech je nutná jejich výměna.
Citlivou komponentou počítačového systému je hard disk jakožto zařízení, na kterém jsou uložena data. Jedná se o točivé zařízení, které je ohroženo jak přepětím, tak mechanickými otřesy. Data uložená na pevném disku je tedy vždy nutné zálohovat.
Co se zálohovacích médií týče, zde je třeba upozornit, že tyto média mají omezenou životnost. Vypalovaná CD mají reálnou životnost asi deset let, ale u DVD je životnost podstatně nižší.

Audio 1.2



1.3.2 Ochrana proti softwarovému ohrožení

- Firewall
- Antivirové programy, antispyware…

- Sítě – vytvoření privátní sítě VPN (Virtual Private Network) – komunikace se symetrickým šifrováním

Firewall („bezpečnostní brána“) je zjednodušeně řečeno zařízení či software oddělující provoz mezi dvěma sítěmi (např. podniková interní 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.

Demilitarizovaná zóna - oddělení komunikace s vnějším prostředím od komunikace lokálních sítí, mezistupeň mezi chráněnou privátní sítí a veřejnou (Internetem). Součást proxy řešení - uživatelův browser pošle požadavek WWW proxy bráně, umístěné přímo v demilitarizované zóně. Ta pak požadavek znovu vyšle (nyní již svým jménem) z demilitarizované zóny do nechráněného Internetu

Antivirový program by měl být samozřejmou součástí každého počítače. Součástí antivirového programu je on-line antivirový scanner, trvale spuštěná komponenta, která kontroluje všechny činnosti a soubory.

Součástí počítačové bezpečnosti je i udržování operačního systému a dalších aplikací v aktualizovaném stavu. Je nutné pravidelně instalovat bezpečnostní aktualizace, záplaty a servisní balíčky (service packy). V systému Windows je pro tyto účely k dispozici služba **Windows Update**, která, pokud je nastavena do automatického režimu, zajišťuje automatickou aktualizaci operačního systému a dalšího software od firmy Microsoft.

1.3.3 Ochrana proti ohrožení lidmi

- Autentizace a řízení přístupových práv
- Vytvoření pravidel bezpečnostní politiky
- Vytvoření plánu obnovy činnosti po selhání

Jaký je rozdíl mezi **autentizací a autorizací**?

Autentizace je mechanismus ověření uživatele zatímco autorizace je ověření práv uživatele vykonávat určitou funkci nebo využívat určitou službu. Používají se tři autentizační metody – první jsou založené na znalosti hesla, druhé na vlastnictví tokenu (klíč, karta…) a biometrické metody.

Autentizace:

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

Audio 1.3

Ověření uživatele

- Vlastnictví určitého předmětu – karta, čárový kód, token
- Znalost hesla

- Ověření fyziologických charakteristik – biometrie (otisk prstů, hlas, barva očí…)

Problémy autentizace:
- Příliš mnoho hesel do různých systémů
- Nejednoznačnost identity (v jiném systému pod stejným uživatelským jménem vystupuje někdo jiný)
- Chyby biometrických systémů
  - Oprávněnému uživateli je odmítnut přístup do systému (**False Rejection Error**)
  - Neoprávněný uživatel je biometrickým zařízením označen jako oprávněný (**False Acceptance Error**)

Autentizační metody:
- **User-centric** - ověřuje se uživatel
  - OpenID, LiveID, OpenAuth, Facebook Connect
- **Institution-centric** - ověřuje se oprávnění k roli v rámci instituce
  - Shibboleth

1.3.4 Bezpečnostní politika

Bezpečnostní politika je soubor zásad a pravidel, které definují způsob řešení IT bezpečnosti v podniku a umožňují mu chránit svá aktiva. Je vhodné, aby byla formulována jako písemný dokument. Měla by obsahovat zejména:
- 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

Bezpečnostní politika má za úkol zajistit bezpečnost informačního systému s přihlédnutím k nákladové efektivitě a musí odpovídat na tyto otázky:
- Kdo nese zodpovědnost?
- Kdy to bude efektivní?
- Jak to bude vynuceno?
- Kdy a jak to bude uvedeno do praxe?

Analýza rizik spočívá v odpovědích na otázky:
- Co se stane, když informace nebudou chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Aktivem je cokoliv, co má pro organizaci hodnotu:
- fyzická aktiva (např. počítačový hardware, komunikační prostředky, budovy
- informace (dokumenty, databáze,...)
- software
- schopnost vytvářet určité produkty nebo poskytovat služby – know-how
- pracovní sílu, školení pracovníků, znalosti zaměstnanců, zapracování apod.
- nehmotné hodnoty (např. abstraktní hodnota firmy, image, dobré vztahy atd..)

Bezpečnostní studie:

- Odhad hrozeb
- Škoda způsobená incidentem
  - dočasná, trvalá
- Analýza zranitelnosti
- Odhad dopadů incidentu:
  - Stanovením finančních nákladů
  - Stupnice 1-10
  - Ohodnocení – nízký, střední, vysoký
- Analýza rizik: riziko je potenciální možnost, že daná hrozba využije zranitelnosti

Řešení bezpečnosti informačních systémů je **PROCES** – nutná kontinuální údržba!

Bezpečnost je kompromis mezi úrovní zabezpečení a náklady.

Nejsou věci „bezpečné“ a „nebezpečné“, jsou jen různé míry rizika. Různí lidé akceptují v různých situacích různou míru rizika.

1.3.5 Havarijní plán

- Postup a reakce v případě havárie, poruchy nebo nefunkčnosti IS
- Součást Bezpečnostní politiky
- Uživatel IS by měl vědět KOHO a JAK informovat v případě poruchy

BCM (Business Continuity Management) je manažerská disciplína, která se zaměřuje na identifikaci potencionálních dopadů, jež organizaci hrozí po havárii. Vytváří rámec pro zajištění určité míry odolnosti a schopnosti reagovat na neočekávané události.

Audio 1.4

1.4 KONTROLNÍ OTÁZKY

1. Co je to analýza rizik?
2. Jaká je klasifikace hrozeb v IT?
3. Jaký je rozdíl mezi virem a trojským koněm?
4. Co je to phishing?
5. Co je to hoax?
6. Jak se můžeme bránit proti jednotlivým hrozbám?
7. Co je to firewall?
8. Co je to autorizace a autentizace?
9. Co je to bezpečnostní politika a havarijní plán?
10. Co je to fault-tolerant a disaster-tolerant systém a jaký je mezi nimi rozdíl?
11. Co je to biometrie?
12. Jakými způsoby můžeme ověřit uživatele?