Ochrana dat v PC

Základní pravidla pro ochranu dat na počítači:

1. Antiviriový program
2. Firewall
   * Je to síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje.
3. Pravidelná aktualizace software
   * Aktualizace software je postup, při kterém je do počítače instalována novější verze jeho prog. Vybavení. Aktualizace se provádí buď z bezpečnostních důvodů nebo z důvodů přechodu na novější vverzi software, která obvykla poskytuje nové vlastnosti.
4. Zálohování dat

Zálohování – zálohování znamená vytvoření kopie důležitých dat a jejich uložení na bezpečném místě

Archivace- archivace je dlouhodobé uložení dat

PROČ zálohovat?!!!

* Chráníme se před krádeží PC – data nekoupíme
* Chráníme se před SW chybami – nejsou tak ojedinělé ale mohou poškodit cokoliv
* Chráníme tím uživatele před jeho vlastními chybami.
* Chráníme se před selháním HW části PC
* Chráníme se před vnějšími vlivy – povodně atp..

Kdy a co

Zálohujeme v případě, že si ceníme své práce a svých dat. Je třeba brát na zřetel, jak často pracuji s PC a daty.

* Záloha operačního systému spolu se základními programy, můžeme si udělat jednorázovou kompletní zálohu. Zde se nepředpokládá, že byste tak často měnili data. Po havárii systému pak nemusíte procházet zdlouhavé instalační procedury.
* Záloha dat. Data, která se budou měnit velmi často, pak zálohujeme tzv. přírůstkovou metodou

Kam zálohujeme

Zařízení, kam uschovat data, je velké množství. Spíše záleží na finančních podmínkách a druhu dat.

Záloha velkých serverů:  
- nejčastěji se používají tzv. magnetopáskové zálohovací jednotky (kapacita 1,6 – 144 GB)   
+ nízká cena na daný objem dat

Disková pole (RAID 0,1,10,5)

Domácí záloha dat:

* Výměnné nebo externí pevné disky
* CD RW
* DVD R
* Blu-ray disky
* Fleshka

Obecný popis základních metod ochrany dat

1. Zálohování a archivace dat – vytvoření důležitých dat.
2. Identifikace a autentizace uživatele – identifikace je prohlášení uživatele o totožnosti, autentizace je proce nebo výsledek ověření této totožnosti. Autentizaci lze provádět různými metodami, např.
   1. Přístupovým jménem a heslem
   2. Pomocí předmětů (čipové karty)
   3. Pomocí biometrických metod (uživatel prokazuje svoji identitu některou bio. Vlastností)
   4. Kombinace metod
3. Kryptografická ochrana – úkolem šifrování je spolehlivě řešit utajení informace, zajistit důvěrnost dat, autentizovat autora informace a zajistit integritu dat (TrueCrypt)
4. Antivirová ochrana (AVG, NOD32, KASPERSKY)
5. Ochrana dat na úrovní sítě – postupy, které slouží k řízení komunikace s okolními sítěmi za účelem zvýšení bezpečnosti. Jako příklad uveďme firewall oddělující dvě komunikující sítě ( KERIO –CZ)
6. Zálohováni napájecího napětí – UPC ( systém nepřetržitého napájení – Uninterruptable Power Supply).
7. Účinná likvidace nepotřebných dat na paměťových médiích.

Viry a Antivirová ochrana

Počítačový virus : Je to program vytvořený uživatelem se zlými úmysly.

Druhy virů:

Trojský kůň

Je většinou program, který se na první pohled chová jako zcela legální program, ve skutečnosti však tajně provádí škodlivé operace. Důležitou skutečností je, že trojský kůň není na rozdíl od viru schopen replikace (Množení) a nepřipojuje se k hostitel – souboru. Trojský kůň se tak nejčastěji vyskytuje na počítači pouze v jednom exemplář – souboru, který v sobě obsahuje právě jen toho troj. Koně.

Červi (Worms)

Červi jsou v dnešní době velice rozšířené. V dnešní době pojem „červ“ označuje takový typ infiltrace, která se do počítače dostane elektronickou poštou (e-mailem). Červ má několik věcí společných s troj. koněm. Na počítači se opět vyskytuje nejčastěji pouze v jednom exempláři – souboru, který sv sobě ukrývá červa. Vyskytuje se pouze jednou, kdyby jich bylo těchto napadených souborů více, riskují tak odhalení některým antivirovým programem. Pokud ten soubor v mailu otevřeme, červ se potom zavrtá v počítači a potom odesílá další takové maily.

Backdoory

Z překladu názvu jako „zadní vrátka“ vyplývá co tento typ virů bude dělat. Chování těcthvo virů je velice podobné trojanu. Ale nesnaží se na sebe vůbec upozorňovat. On „zaleze“ do systému a čeká až se jeho tvůrce k němu připojí a bude z PC cucat data.

Spyware a další internetová havěď

Tracking cookie

Jako cookie (koláček) se v protokolu http označuje malé množství dat, která WW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět server

Spyware

Spyware je program, který využívá Internetu k odesílání dat z PC bez vědomí jeho uživatele. Na rozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek atd.

Antivirový program

* Je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého SW. K zajištění této úlohy se používají dvě odlišné techniky:
  + Prohlížení soubor na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi
  + Detekci podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.