Počítačová bezpečnost

Stručný nástin problematiky

Sestavil : Ing. Jiří Franc

Zdroj informací:

http://www.bolekvrany.cz/downloads/security_cz.pdf

1. Pravidla jsou vlastně jasná

- 1. Nikdy nikam neposílejte hesla, PIN ani nic podobného
- 2. Pravidelně záplatujte systém
- 3. Používejte antivirus, firewall a detekci spywaru
- 4. Správně nastavte přístupová práva, důležitá data a maily filtrujte
- 5. Pro důležité maily používejte digitální podpis
- 6. Před prodejem disku nebo počítače smažte disk pomocí utilit, které data přepisují, ne jen prostým smazáním

- dále si je trochu rozvedeme…

2. Psychologické útoky

- **2.1 Vylákání údajů**
- **2.2 Nigerijské dopisy**
- **2.3 Hoaxy . . . . . .**

2.1 Vylákání údajů

- příkladem, který vás může stát desítky tisíc korun, je takzvaný **fishing („rybaření“)**
- *dostanete e-mailem dotazník, který vás nabádá k vyplnění čísla platební karty, pinu, doby platnosti a dalších údajů, údajně proto, že odesílatel (tvářící se jako např. společnost VISA) je potřebuje k vyřešení problému s vaší platební kartou*
- poté, co tyto údaje v dobré víře odešlete, mohou být zneužity skutečným autorem mailu k vašemu okradení
- *podobně vypadá i celá řada dalších dopisů, které se např. tváří, jako že jsou od administrátora vaší lokální sítě, a vyzývají k zaslání vašeho hesla k e-mailovému účtu*
- jsou to všechno podvody - banka samozřejmě všechny údaje zná, je přece vydavatelem, stejně tak administrátor sítě zná vše a heslo sdělené komukoliv přestává plnit základní funkci
- autor využívá našeho sklonu důvěřovat, nepřemýšlet

2.2 Nigerijské dopisy

- Dalším značně rozšířeným příkladem jsou **tzv. nigerijské dopisy**
- Jejich struktura je v podstatě následující:

- *Vážená paní, vážený pane, jsem pracovníkem banky v . . . . Před 20 lety si u nás americký občan John Smith uložil 20.000.000 USD (dvacet milionů dolarů). Pokud by si tyto peníze nevybral do 31.12. tohoto roku, vklad propadne naší zkorumpované vládě. Proto jsme hledali……Bohužel k tomu potřebujeme nějaký účet mimo naši banku……dovolujeme si proto s důvěrou obrátit na Vás a požádat Vás, zda byste nám neposkytl(a) svůj účet……za tuto laskavost dostanete provizi 2.000.000 USD (dva miliony dolarů)*

- Pokud na tento dopis naletíte, mohou následovat v podstatě **3 scénáře:**
- 1) vylákání financí na administrativní poplatky
- 2) pozvou Vás do Nigerie nebo jinam, unesou Vás a někdo zaplatí výkupné
- 3) Váš účet někdo použije k praní špinavých peněz

2.3 Hoaxy . . . . .

- na internetu se šíří celá řada **planých poplachů (hoaxů)**

- ***např. e-mailová zpráva**, která tvrdí, že nějaká holčička nutně potřebuje asi 100.000 USD na operaci rakoviny. A její otec, který nemá peníze, sháněl sponzory. Sehnal internetovou firmu, která se zavázala, že za každý mail s touto zprávou, který pošlete svým přátelům, zaplatí na příslušné konto 1 cent = **nesmysl, technicky nemožné***
- *nebo jinak - hlášky typu Microsoft varuje před souborem XYZ.EXE na vašem disku – je to virus, který ještě žádný antivir nedetekuje. Virus odstraníte tím, že tento soubor smažete. Prosíme, rozešlete všem svým přátelům =Tento soubor je ve skutečnosti obvykle nějaký systémový soubor, který má netypické jméno, **když ho smažu, nastanou potíže = ignorovat***
- nepříjemné - obsah působící na psychiku
- zahlcují a zpomalují internetový provozu
- zhroucení poštovních serverů
- zdržují a snižují produktivitu v práci
- skutečně ekonomické škody – smažu důležitý soubor

3. Volba hesla

- heslo slouží jako **nejčastější a mnohdy také jediný prostředek ochrany vašeho počítačového účtu** před neoprávněným nakládáním

- chrání před zneužitím jak ze strany osob **sedících s vámi** v kanceláři, tak ze strany **anonymního útočníka z internetu**

- bezpečná hesla jsou dostatečně dlouhé (10 a více znaků) náhodné kombinace písmen, číslic a speciálních znaků. Příkladem takového hesla je Gk@4c90$aMq...
- k dispozici 26 písmen anglické abecedy +10 číslic + cca10 speciálních znaků → vznikne **46^{10}** = 42 420 747 482 776 576 desetiznakových hesel

- slova jsou lehko uhodnutelná - cca 300 000 kombinací
- různá hesla na různých místech
- pravidelná obměna hesla
- naprosté utajení hesla nutností !!!

4. Odposlech, sledování a kradení údajů…

- 4.1 Odposlech . . . .
- 4.2 Bezpečné vymazání
- 4.3 Přístupová práva
- 4.4 Šifrování . . . . .
- 4.5 Automatické doplňování

4.1 Odposlech . . .

- **95% internetové komunikace je odposlouchávánо**
- **státní odposlech** – sledování teroristů, původců hospodářské kriminality….
- **nestátní odposlech** = problém nás všech na internetu
- **obsah e-mailů** může znát administrátor sítě, šéf nebo kdokoliv kdo má k dispozici nijak náročná technická řešení ke sledování pohybu dat sítí
- k odposlechu může dojít **kdekoliv v síti**
- *zbývá citlivé údaje pošeptat druhému do ouška někde uprostřed lesa (a co špionážní satelity ☹☹)*

4.2 Bezpečné vymazání

- např. **Internet Explorer, si pamatují historii** toho, co jste prohlíželi
- **kdokoliv u vašeho PC** tak může zjistit, kde se pohybujete
- pravidelně **mažte historii** navštívených stránek
- podobně je **nedostatečné mazání z disku** – data se dají stále ještě obnovit
- **programy typu wipe disk** soubor **přepíší nesmyslnými daty** a pak **smažou**, obnoví se tedy nesmysl

4.3 Přístupová práva

- **přístupová práva** slouží k tomu, abyste **definovali, co kdo** na daném počítači může a ke kterým souborům má přístup pro čtení, ke kterým pro zápis atd.

- přístupová práva jsou důležitá, ale **sama vás nezachrání**

- není problém disk přečíst **mimosystémovým nástrojem**, například z bootovacího CD, a získat vaše data bez ohledu na přístupová práva

4.4 Šifrování . . . .

- skutečnou ochranu poskytuje až šifrování. To ochrání nejen **data na vašem disku, ale i data přenášená po internetu**. Je však třeba používat skutečně kvalitní šifrování. V současné době tyto nároky splňují **šifry s dostatečně dlouhým asymetrickým klíčem**

- pracují **na principu veřejného a soukromého klíče**

- data, která vám někdo posílá, jsou zašifrována pomocí vašeho **veřejného klíče**. Tento klíč dáte všem, od nichž chcete přijímat šifrované e-maily

- mail pak lze rozšifrovat pouze pomocí vašeho **soukromého klíče**, který je nutné držet v tajnosti

- **podpora pro asymetrické šifrování je vestavěna přímo do Windows a Outlooku**

4.5 Automatické doplňování

- např. Internet Explorer, má standardně **zapnuté automatické doplňování formulářů**. To je zdánlivě velmi užitečné
- stačí, když zobrazíte stránku a **prohlížeč sám doplní do příslušných kolonek vaše uživatelské jméno a heslo**
- nemusíte si nic pamatovat, **vše je snadné a krásné**. Stačí však, aby se k počítači dostal někdo jiný (ať už fyzicky, nebo po internetu) a **budete se divit**
- přečte si poštu, provede vaším jménem transakci platební kartou…
- zamítnout v nastavení IE či Mozilly **Možnosti…záložka Obsah**

5. Viry, hackeři, bezpečnostní díry, spyware – souhrnné označení malware (MALign softWARE – zlý software)

- 5.1 Viry . . . . . .
- 5.2 Hackeři . . . . . .
- 5.3 Bezpečnostní díry
- 5.4 Spyware . . . . .
- 5.5 Zavirovaní mobilního telefonu

5.1 Viry . . . . . .

- programy vytvořené za účelem provádění **nežádoucí činnosti** v uživatelově počítači
- tento termín byl poprvé použit v roce **1972** v románu D. Gerolda
- virus (zatím)**nevzniká v počítači samovolně a neničí hardware**
- **1981** – první virus pro počítač Apple
- **1986** – první virus na PC, šlo o boot virus, vytvořený v Pákistánu
- **1988** – vzniká antivirová asociace Computer Virus Industry Associates
- **1988** – **odsouzen první člověk** za počítačovou infiltraci

- **1990** – vzniká česká firma Grisoft – na trhu AVG 1.0
- **1991** – popsáno přes 1000 virů, vzniká technika heuristické analýzy pro detekci virů
- vzniká první časopis o virech **Virus Bulletin**
- **2000** – objevuje se první virus schopný napadnout data pouhým **otevřením elektronické pošty**

- **původní viry** obvykle mazaly harddisk nebo prováděly nějakou podobnou činnost, protože neexistoval způsob, jak zajistit jejich tvůrci **zpětnou vazbu**, informaci o úspěšnosti

- **možnosti šíření byly omezené** – přenos disketou

- **dnešní viry** se šíří především **pomocí elektronické pošty**, resp. i**nternetu** vůbec, a jejich **cílem je zneužití vašeho počítače a dat na něm**

- **nenápadný průnik viru a jeho rezidentní (skryté) chování**

- **Vlastnosti úspěšného viru:**

- bez chyb
- nezávislý na OS a verzi programu
- nezávislý na jazykové mutaci
- Nenápadný
- umí reagovat na neobvyklé situace
- ovlivnění antivirového programu

- **Projevy působení viru:**

- **blokování paměti nebo místa na disku**
- **zpomalení práce systému**
- **neobvyklé chování systému**
- **neobvyklá chybová hlášení**
- **grafické nebo zvukové projevy**
- **změny souborů a vlastností**
- **„ padání “aplikace nebo OS**
- **nenápadné poškození dat (*vkládání nějakého slova*)**
- zničení dat (přehazování slov; smazání systémové oblasti disku; smazání FAT …)
- krádeže dat (hesel; elektronických podpisů;důvěrných dokumentů)
- šifrování dat
- speciální projevy (virus BacTime – systémové hodiny jdou nazpět = zmatky při mazání)

Viry jako zbraň:

- **závislost** světa na výpočetní technice
- stačí vyřadit zdroj elektrické energie *(Blackout, Elektrická smrt)*
- **přímý a viditelný útok**
- **nebo** nebezpečnější **modifikace dat**
- **kyberterorismus** = násilí na odpůrci až do fyzického zničení, vyhrožování a zastrašování provedené v rámci světa informačních systémů
- **modifikace dat** *(např. dokumentace)*
- **šíření dezinformace** *(kyberprostor)*
- **elektronická bomba** *(zaměstnanec je velké riziko!!!)*
- **odcizení informací**
- **zátěž komunikační infrastruktury** ***(zahlcení spamy)***
- **poškození dobrého jména**
- **neoprávněné využití kapacity** *(spam)*
- **změna identity** *(obvinění ze šíření)*
- **počítače ve válce** *(Bosna,Čína x Tchai van)*

5.2 Hackeři . . . . .

- **čtyři druhy hackerů:**
- 1) lidé, kteří si tímto způsobem prostě **rozšiřují své znalosti** a do PC se nabourávají pouze proto, aby vyzkoušeli jejich zabezpečení a své vědomosti
- 2) patnáctileté děti, které **chtějí být in** - pořádně nevědí, co dělají, mohou napáchat obrovské škody smazáním disku apod.
- 3) hackeři, kterým jde o získání citlivých údajů, v podstatě **špióni**
- 4) hackeři, kterým jde o **zneužití vašeho počítače** k aktivitám typu provozování pedofilních stránek z vašeho PC
- **co může způsobit vir, to může i hacker**

5.3 Bezpečnostní díry

- viry a hackeři se do systému dostávají pomocí bezpečnostních děr. To jsou **chyby v naprogramování nebo nastavení vašeho systému**, které jejich průnik umožňují

- **nutná pravidelná údržba a update všech částí systému!!!**

5.4 Spyware . . . . .

- existuje celá třída aplikací, které se zabývají tím, že **sledují, co děláte** - těmto věcičkám se říká spyware (spy = špion)

- obranou je **instalace antiviru, firewallu, systému pro detekci vniknutí (intrusion detection system), systému pro vyhledávání spywaru a především pravidelné aktualizace operačního systému tzv. záplatování a případně i dalších programů**. např. Internet Exploreru nebo balíku MS Office

- k detekci spywaru také existují speciální nástroje např. **Ad – Aware SE Personal** – freewarový detektor spywaru

5.5 Zavirovaní mobilního telefonu

- **hardwarová a softwarová roztříštěnost** mobilních telefonů je hlavním důvodem, proč pro ně neexistuje více virů
- **sjednocování OS** pro chytré telefony např. Symbian přinese nové hrozby
- pro šíření je největším rizikem stále **zapnuté Bluetooth**

6. Spam

- 6.1 Prevence
- 6.2 Filtrování spamu

6. Spam

- slovem SPAM se označuje **nevyžádaná reklamní pošta**
- zbytečně zahlcuje síť a brzdí provoz
- zahlcují jejich adresáty, kteří je **musí mazat a ztrácí tím čas**
- nebezpečím např. **nepřijetí důležité zprávy** plnou schránkou
- spam nerozesílají lidé, ale **automaticky počítače** – to vysvětluje množství
- obrana proti SPAMu: za prvé **prevence**, za druhé **filtrování**

6.1 Prevence

- existují **roboty**, které automaticky procházejí webové stránky, diskusní skupiny a konference a hledají e-mailové adresy a poskytují je spammerům
- neuvádějte nikde svoji **adresu v podobě čitelné pro roboty,** na webové stránky si dejte např. **obrázek**, který obsahuje vaši adresu, ale ne odkaz, kde je výslovně napsána
- své adresy pište místo ja@mojefirma.cz ve tvaru **ja zavinac mojefirma tecka cz** – to zatím roboty číst neumí, člověk tomu porozumí

- druhý způsob, jak spameři získají vaši adresu je, že posílají maily na **statisíce strojově generovaných adres**

- např. víme, že Volný je velký poskytovatel připojení – prostě si vezmou **seznam typických českých jmen** a budou generovat adresy *novak@volny.cz, jan.novak@volny.cz, petr.novak@volny.cz, ...*

- strojově zvládnutelné a některé z těchto adres **budou jistě existovat**

6.2 Filtrování spamu

- různé programy, které umí **odfiltrovat spam z vaší pošty**
- takové filtry jsou již obsaženy **např. v Outlooku 2003**

- filtry fungují na principu **statistického filtrování**: analyzuje se obsah mailu, to, kolikrát a v jaké souvislosti se v něm vyskytují jaká slova, a to se **porovnává se známými vzorky** spamu

- dle rozboru se určí **skóre** a pokud skóre překročí stanovenou hranici, je mail označen za spam
- je to jen statistická metoda (**není stoprocentní**) - spam někdy nechá projít a jindy označí jako spam i seriózní zprávu

- není dobré se **bezhlavě řídit úsudkem filtru** a všechny maily označené za spam ignorovat a smazat
- **pravidelně projít složku nevyžádané pošty a zkontrolovat**, jestli tam náhodou není něco důležitého

7. Identita a anonymita

vycházejte z toho, že **veškerá vaše činnost může být vystopována až k vaší skutečné fyzické identitě**

chovejte se podle toho

jde jen o to, jak moc někdo **bude mít zájem** toto stopování provést

dávejte si tedy pozor na zdánlivě nevinné stahování hudby, videa apod. - porušujete autorská práva a můžete být vypátráni a postaveni před soud

identita se většinou dá velmi **snadno podvrhnout**

skutečně ověřit pravost odesilatele umožňuje **digitální podpis**, pokud vám jeho kód ukradnou, existuje **databáze odvolaných kódů**

8. Různé

- 8.1 Skrytí přípon souborů
- 8.2 Rozesílání hromadných mailů

8.1 Skrytí přípon souborů

- **ve Windows je standardně nastaveno skrytí přípon souborů známých typů**. To je poněkud nebezpečné

- pokud Vám přijde například **spustitelný soubor s virem**, nevidíte příponu **.EXE**, myslíte, že jde o dokument a spustíte ho

- funkce se dá vypnout tak, že spustíte ***Tento počítač*** a z menu ***Nástroje*** vyberete ***Možnosti složky***. Zde na záložce ***Zobrazení*** zrušíte zaškrtnutí políčka ***Skrýt příponu souborů známých typů***, následně zmáčknete tlačítko ***Použít*** a pak ještě tlačítko ***Použít pro všechny složky***

- nyní se Vám **vždy budou zobrazovat** přípony souborů

8.2 Rozesílání hromadných mailů

- mnoho lidí maily rozesílá tak, že jako adresáty naklikají **všechny** , kterým chtějí mail poslat
- takovýto mail sdělí **naprosto zbytečně** každému adresátu i všechny další
- **viry**, které dokáží takto poskytnutý seznam adres využít podobně jako **adresář v počítači**. Pokud má jeden z adresátů zavirovaný počítač, může se stát, že **se virus bude rozesílat všem**, kterým jste adresovali tento hromadný mail
- jak se tedy správně rozesílají hromadné maily? Opět naťukáte všechny adresy, ale u každé z nich místo ***"Komu",*** vyberete ***"Skrytá kopie„***
- tím se mail rozešle na spoustu adres, ale **žádný adresát nebude vidět adresu toho druhého**

9. Antivirová ochrana

- použití **antivirového programu**
- pravidelná **aktualizace virové databáze**
- pozor na **přílohy e – mailů** *(nejdřív uložit na disk a prověřit)*
- pravidelné **zálohování dat**
- zálohování dat na **více než jeden nosič**
- **zálohování i starších verzí**

- pozor na **nelegální SW, shareware, freeware**
- získávejte **informace** www.viry.cz; www.aec.cz
- **obraťte se na odborníky** – odhalí bezpečnostní rizika a pomohou Vám je „záplatovat“
- **šifrujte** a elektronicky podepisujte
- **nedůvěřujte** nikdy, nikomu a ničemu

- **antivirové programy (skenery)** – pro souborové viry používají jako základní postup databáze se vzorky sekvencí známých virů tzv. **heuristickou analýzu**
- **podobný postup jako při detekci spamu**
- tyto antivirové prostředky nejsou bohužel již dostačující a důkladně nás mohou ochránit jen v kombinaci s **personal firewall** – bránícím nežádoucí komunikaci počítače s okolím a nepovolené infiltraci z vnějšku
- další již zmiňovanou nutnosti je **záplatování operačního systému**
- *tuto skutečnost odhalil masově např. červ Blaster v srpnu 2003*