Otázka číslo 9
Ochrana počítače

- bezpečný počítač = počítač, který neobsahuje žádný nežádoucí software a který není napadnutelný z Internetu
- dle specialistů je asi 1 bezpečnostní chyba na 1000 řádků kódu

Aktualizace OS a programů

- Aktualizace se někdy dělí na
    - Bezpečnostní (kritické)
    - Volitelné (přidávají nové funkce)

Aktualizace systému

- V případě odhalení chyby výrobce OS vydá opravu (záplatu, tzv patch), která chybu opravuje
- Aktualizace není třeba hlídat, stačí si zapnout automatické aktualizace
- Pokud je počítač online, OS i programy kontrolují, zda není nová verze/záplata

Firewall a další bezpečností nástroje

Firewall

- Jednotlivé služby (web, pošta, sdílení souborů) využívají jednotlivé síťové porty, jakési „brány“ do počítače – přesněji jde o číslo (0-65535), které slouží v sítích při komunikaci pomocí protokolů TCP a UDP (např web používá port 80, pošta odchází přes port 25,…)
- Portů je teoreticky 65 535 a přes všechny by se do počítače mohly dostat počítačové červy
- Využívají je také hackeři, snažící se o neoprávněný přístup o cizích systémů
- Firewall = program, který hlídá, co se na jednotlivých portech děje a povoluje jen námi vyžádanou komunikaci
    - Osobní firewall je dnes většinou součástí OS
    - Síťový firewall sleduje komunikaci mezi vnitřní (lokální) sítí LAN a vnější sítí WAN (internetem). Bývá součástí směrovače (routeru)
    - Rozdělen do 4 kategorií
        - Paketové filtry – uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket (blok přenášených dat)
        - Aplikační brány – velmi vysoká úroveň zabezpečení, velmi náročné na HW
        - Stavové paketové filtry – podobně jako paketové filtry, navíc si ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety mohou být propuštěny nebo musí znovu projít rozhodovacím procesem (rychlostí a bezpečností někde mezi výše zmíněnými)
        - Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS (systém pro odhalení průniku) – firewally jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů a aplikací (když data v hlavičce emailu nesplňují požadavky RFC (žádost o komentáře))

Antivirový program

- Antivir stále běží v paměti počítače a kontroluje každý spuštěný program a každý otevřený dokument

- Antivir na náš pokyn otestuje počítač, přesněji zkontroluje, zda v paměti počítače neběží škodlivý kód a potom zkontroluje všechny (nebo určené) soubory v počítači
- Pokud nalezne malware (škodlivý software), eliminuje ho
- Rezidentní štít: testuje soubory, které se otvírají, a pokud je nalezen virus, zablokuje přístup k nakaženému souboru
- Využívá heuristickou analýzu
    - Vykonává v podstatě dva kroky – první je totožný s antivirovým testem – s pomocí virové databáze hledá známé viry.
    - Pokud nebyl nalezen žádný známý virus, zahájí se logická analýza kódu testovaného objektu a posuzuje se, co testovaný kód v praxi znamená. Lze tedy zjistit, že objekt, který se kontroluje obsahuje instrukce, jejichž význam nelze označit za normální či běžné – např. vyhledávání jiných souborů EXE, jejich otevírání pro zápis a kopírování vlastního kódu do těchto souborů, apod
- Jak funguje:
    - Porovnává programy se svojí databází škodlivých kódů
        - Podobně porovnává adresy webů s černou listinou nebezpečných stránek
    - Sleduje podezřelé aktivity
        - Zápis do systémových souborů a jiných programů
        - Na webu obsah (javaskriptového) programu vloženého do stránky
        - Má tak šanci nalézt i dosud neznámý vir
- Pokud najde nějaký vir, má 3 možnosti
    1) Pokusit se opravit soubor odstraněním viru ze souboru
    2) Umístit soubor do karantény (virus se dále nemůže šířit, protože ho nelze používat)
    3) Smazat infikovaný soubor (i s virem)
- Aktualizace antiviru je zcela nutná, jinak by neznal nejnovější hrozby
- Všechny se aktualizují samy
- Méně rozšířená je kontrola programů vůči antivirové databázi umístěné na internetu
- Odvirování nakaženého počítače (není jednoduché, neboť mnoho virů se dokáže skrýt před antivirovým programem
    - Boot jiného OS z Live CD nebo USB disku
        - Vir pak již není aktivní a je možné ho skenováním disku najít a odstranit
    - Vyjmutí disku z nakaženého počítače, jeho umístění v čistém stroji a odvirování
- Známé antiviry: Kasperky, ESET, McAfee (placené), avast!, AVG (zdarma)

Počítačové viry a červy, malware a spyware

- Počítačový vir nebo červ je program vytvoří za účelem získání dat z Vašeho počítače, získání kontroly nad vaším počítačem nebo alespoň využití jeho zdroje, případně aby zničil Vaši práci (tvůrcům jde především o Vaše přihlašovací údaje a peníze)

Virus

- Program, který se umí vložit do jiného programu a s ním se šířit
- Spuštěním programu se nevědomky spustí i virus, který napadne další programy

Jak funguje (platí i pro červa)

- Nějakou dobu se jen šíří, rozesílá, instaluje, ale nic nedělá
- Po nějaké době provede nějakou nepříjemnou činnost
    - Ovládnutí počítače
        - Program typu backdoor otevře některé porty počítače a naslouchá na nich povelům zvenčí
    - Odcizení obsahu počítače

        - Díky vzdálenému přístupu může útočník kopírovat soubory z napadeného počítače, případně použít program typu keylogger ke sledování stisknutých kláves (např při vyplňování políček ve formulářích) nebo dataminder, program, který shromažďuje data o činnosti uživatele počítače
    - Využití počítače pro nelegální činnost
        - Vzdálený útočník může proměnit nezabezpečený počítač v server rozesílající spam nebo stránky nelegálním obsahem a uživatel přitom o ničem neví
    - Mazání obsahu počítače
        - Dnes raritní, protože krom uspokojení z toho útočník nic nemá
    - Zpomalení práce systému
    - Blokování místa
    - Nestabilita systému

Makrovirus

- Není to program, ale dokument, který může obsahovat makra, tj. vlastně v dokumentu vložené programové kódy (dnes mnoho typů dokumentů)
- Kupříkladu mnoho textových procesorů na makra spoléhá při otevírání souborů, jelikož tento proces se skládá z několika samostatných kroků
- Makrovirus tuto sadu pokynů změní tak, aby se při každém spuštění daného makra spustil také

Červ

- Má vlastní soubor a většinou se snaží přimět uživatele počítače, aby ho spustil, případně využívá bezpečnostní chybu (např prohlížeče webu) a snaží se spustit sám
- Některé internetové červy využívají chyby v zabezpečení síťového připojení operačního systému a šíří se přímo v paketech síťového protokolu
- Velmi nebezpečné, neboť je nezachytí antivirový program a protože nevyžadují k napadení počítače aktivitu uživatele
- Nejznámější červ „I Love You“ – mazal systémové soubory, upravoval registry a přepisoval určité typy souborů

Trojský kůň

- Tváří se užitečně – např hra, spořič obrazovky, jednoduchý nástroj,..
- Otevře některé porty počítače a naslouchá na nich povelům zvenčí
- Krom toho též vykonává ještě nikde neuvedené akce bez souhlasu uživatele
- Umožní útočníkovi získat přístup do počítače a pracovat s ním
- Sledování záznamu znaků zadávaných z klávesnice (a celkově víceméně to samé, co virus či červ)

Rootkit

- Škodlivý kód, který běží v jádru OS s právy administrátora počítače
- Špatně se detekuje a odstraňuje, protože je součástí jádra OS, může se skrýt před antivirovým programem
- Také maskuje přítomnost jiného malwaru

Malware

- Shrnující označení pro škodlivé kódy

Spyware

- Programy, které sledují činnost uživatele a předávají o ní někomu zprávy nebo prohledávají obsah počítače a opět o něm někoho informují
- Jako adware se často instaluje spolu s nějakým programem nebo pomocí aktivního obsahu webových stránek
- Typy:

- Adware: sleduje aktivity uživatele na internetu a cíleně mu zobrazuje reklamu, nemusí to být vždy škodlivý kód (např neustále vyskakující pop-up okna)
- Hijacker: mění domovskou stránku
- Key Loggers: sleduje každý pohyb na klávesnici, některé druhy odesílají uživatelova hesla

Metody útoků přes webové stránky a elektronickou poštu

- Umístění zavirovaného souboru o jinak užitečného programu (na web)
  - Obvyklé na webech s nelegálním obsahem (cracky, warez)
  - Uživatel si stáhne program, spustí ho a tím si zaviruje počítač
- Umístění zavirovaného souboru na zcela důvěryhodný web
  - Obvykle byl předtím napaden hackery a místo původních souborů na něm byly umístěny zavirované programy
- Umístění skriptu (programu) do kódu webové stránky
  - Pokud prohlížeč tento kód spustí, nahraje se do OS škodlivý kód
  - Prohlížeče však obsahují zabudované ochrany (zakázané skripty, spuštění pouze na dotaz), takže jde většinou o využití bezpečnostní chyby v prohlížeči, která nebyla záplatována
  - Rozšířeným útokem je nabídka falešné antivirové kontroly počítače
  - Webová stránka zobrazí upozornění na nalezení viru v počítači (fiktivní, emotivně zbarvené) a nabídne jeho odstranění, stačí pouze spustit nabízený antivir
  - Uživatel odmítne všechna bezpečnostní varování prohlížeče a vir spustí
- Vytvoření zavirovaného doplňku (plug-in) pro webový prohlížeč
  - Uživatel si s doplňkem nainstaluje i škodlivý kód
- Využití podvržené stránky
  - Uživatel je přesměrován na falešnou stránku, napodobující originál (web banky apod) kde vyplní své přihlašovací údaje a tím je poskytne útočníkům
- Další rafinované způsoby
  - Propašování viru od systému nebo získání důležitých (osobních údajů)
- Přes mail
  - Dnes méně jak 10% virů se šíří mailem
  - Obsahuje zavirovanou přílohu, jejímž spuštěním se vir spustí a dojde k nakažení počítače
  - Některé emailové servery už mají integrovaný antivirový program
  - Proto útočníci používají zprávy s odkazy na zavirované stránky

Spam a obrana proti němu

= nevyžádané, hromadné rozesílané zprávy (typicky s reklamou)

- Dnes je postižitelné i podle zákona
- Velmi levný způsob inzerce
- Šiřitelé spamu (spameři) získávají adresy mnoha způsoby
  - Pomocí specializovaných programů (robotů) prochází webové stránky a sbírají z nich adresy
  - Využívají viry, které odešlou celý adresář poštovního programu na určitou adresu
  - Kupují databáze od jiných spamerů
  - Generují náhodné adresy podle seznamů jmen a rozšířených poštovních serverů

Obrana proti spamu

- Je třeba být opatrný při zadávání své emailové adresy na různých webových serverech. Jednou z možností je mít 2 maily – jeden pro soukromé účely a druhý právě pro různé registrace
- Spamy jsou často posílány ze serverů ze zemí, kde posílání spamů není trestné

- Poskytovatelé internetu blokují počítače, ze kterých odchází množství zpráv (tzv black list). Často na to ovšem doplatí nevinní lidé, protože spam server z jejich počítače vytvořil vir
- Poštovní program je nutné doplnit o antispamový filtr
    - Ten sleduje výskyt slov indikujících spam (sex, viagra,..) a přesunuje takové zprávy do zvláštní složky
    - Navíc se většinou umí učit – sleduje, jaké zprávy sami označíte za spam, a podobné zprávy pak přesunuje automaticky
    - Občas je ale nutné složku se spamem zkontrolovat, zda v ní omylem nejsou důležité zprávy
    - Tato možnost je nejúčinnější

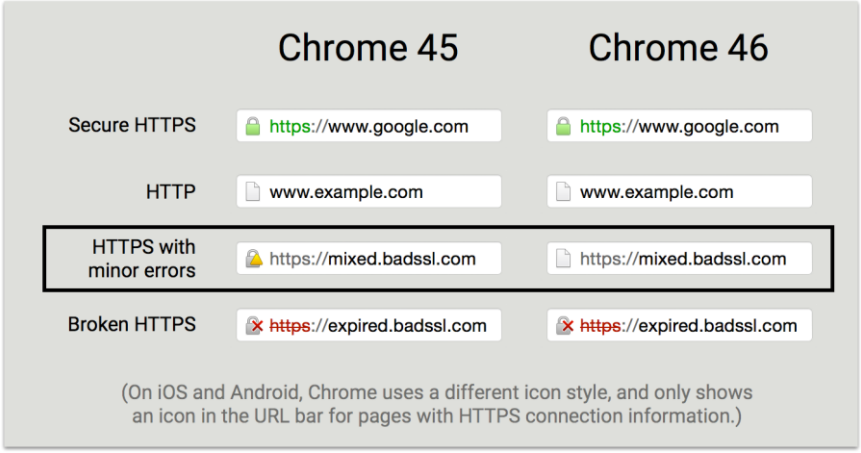
Podvody, hoaxy

Podvody (tzv techniky sociálního inženýrství)

- Útočníci spoléhají nikoliv na skvěle napsaný vir, ale na chybu člověka
- Vycházejí často ze znalostí psychologie
- Metody
    - Nabízejí zdarma erotický či tajný obsah (nahé fotky celebrity, dokumenty o machinacích,..)
    - Nabízejí velký finanční zisk při minimálním úsilí (např tzv nigerijské dopisy, slibující miliony po zaplacení pár desítek tisíc poplatků)
    - Hrají na city uživatele (můžete zachránit nemocného člověka)
    - Vzbuzují strach
    - Tváří se důvěrně (někdo ti něco poslal, stáhni si to zde)
    - Vydávají se za někoho jiného (třeba za podporu Amazonu)
    - Mnoho dalších metod, které většinou kombinují výše uvedené
    - A hlavně: nutí jednat okamžitě
- Základní obrana: vědět o jejich existenci a uvědomovat si fakt, že internet je nebezpečné prostředí

Ukradení (zneužití) identity – phishing (rybaření)

- Útočník rozešle podvodné emaily napodobující styl známé banky a vyzývající příjemce z nejrůznějších důvodů ke kontrole účtu. Po klepnutí na odkaz se zobrazí stránky vypadající přesně jako originální web banky
- Po zadání přihlašovacího jména – čísla platební karty a hesla dojde ke zdánlivě slibované akci
- Ve skutečnosti jste však zadali své přihlašovací údaje do formuláře, který jste odeslali útočníkovi
- Na uvěřitelnosti takových stránek přidává, že používají HTTPS (tento krok činí stále víc víc phishingových stránek)
- Různé techniky
    - Využití poddomén - Následující odkaz http://www.konkretnibanka.novasluzba.cz/ vypadá, jako by vedl na sekci nová služba na webu konkrétní banky; ve skutečnosti tento odkaz míří na sekci „konkrétní banka“ (tedy phishing) stránky „nová služba“
    - Překlepy a zkreslení odkazů - Běžným trikem bývají překlepy v odkazech. Dalším běžným trikem je, aby text odkazu vypadal jinak, než skutečný odkaz. Následující odkaz http://stranka.cz/X vypadá, že vede na stránku „X“, avšak ve skutečnosti vede na stránku „Y“. V levém dolním rohu většiny prohlížečů se zobrazuje skutečný cíl daného odkazu, na který právě ukazuje myš
    - Unikání filtrům - Útočníci začali používat obrázky místo textů, aby tak zkomplikovali anti-phishingovým filtrům detekovat běžně používané texty nebezpečných e-mailů
    - Telefonický phishing (vishing = voice phishing)



Hoax

- Falešná zpráva, která vás nabádá ke smazání „zcela nezjistitelného viru“ nebo k posílání zpráv pro záchranu nemocného člověka
- Pokud hoax poslechnete, smažete si sami systémový soubor nebo alespoň zahltíte poštovní schránky jiným uživatelům, může tak také přijít o důvěryhodnost