Bezpečnost dat

Malware

- Kontaminace (portmanteau) slov ‘malicious‘ a ‘software‘
- Označuje všechen škodlivý software
- Běžně se dělí na 9 typů
  - 7 z nich jsou software
  - Zbývající 2 jsou textové

Rozdělení malware – software

Počítačový virus

- Skrytý uvnitř jiného programu
- Software, který se šíří bez vědomí uživatele
- Upravuje kód jiných aplikací a tím se množí
- Může mazat data

Trojský kůň

- Škodlivý program skrytý v na první pohled normálním programu
- Musí být spuštěn, aby mohl fungovat
- Může krást data, instalovat backdoor, mazat data atd.
- Nešíří se jako virus
- V dnešní době už není tak běžný

Rozdělení malware – software

- Počítačový červ
  - Podobný počítačovému viru, ale horší
  - Šíří se přes síť, už jen svou přítomností v síti způsobuje problémy
  - Stejně jako trojský kůň má nějakou “nálož“
  - Může dělat změny v registru, nainstalovat backdoor, fungovat jako ransomware, mazat data atd.
  - V dnešní době nejrozšířenější typ malwaru

Rozdělení malware – software

Ransomware

- Vyděračský software (ransom – výkupné)
- Na počítač se dostane jako nálož
- Na počítači buď zašifruje data, nebo ho zamkne
- Funguje i na Androidu
- Počet případů roste díky kryptoměnám

Crimeware

- Software sloužící k automatizaci kyberzločinu
- Prostřednictvím sociálního inženýrství páchá krádež identity
- Snaží dostat přístup k účtům oběti
- Obohacuje kyberzločince

Rozdělení malware – software

Spyware

- Software, který bez vědomosti uživatele shromažďuje data
- Typy sbíraných dat mají velký rozsah
- Na počítač se dostane v sharewaru, freewaru, či jako nálož

Adware

- Na rozdíl od spywaru pouze shromažďuje o uživateli pouze jeden typ dat
- Mohou také zobrazovat vyskakující reklamy, či změnit v prohlížeči domovskou stránku
- Na počítač se dostane stejně jako spyware

Rozdělení malware – text

Spam

- Spam je nevyžádaná pošta (email)
- Většinou mají reklamní, či erotický obsah
- V některých případech mohou malware obsahovat jako přílohu
- Pro zkušenějšího uživatele v podstatě neškodný

Hoax

- Může se šířit mailem, ale většinou se šíří po sociálních sítích
- Hoax je označovaný jako falešná poplašná zpráva
- Hoax se často odvolává na “důvěryhodné“ zdroje a uživatele přímo oslovuje
- Pokud si nejsme jistí, zda je něco hoax, můžeme se podívat na stránku http://www.hoax.cz

Projevy malwaru

- Náhodné, nenadálé zpomalení počítače
  - Ztráta výkonu; zamrzání
- V případě červa vyšší spotřeba sítě a/nebo její zpomalení
- Adware se projevuje reklamními okny
- Spam se projevuje “neprázdností“ spamové složky vašeho emailu

Způsoby šíření

- Virus a červ se šíří sami
- Trojský kůň je někde dostupný ke stažení, nebo je posílán jako příloha
- Ransomware, crimeware, spyware a adware se šíří jako nálož
  - Spyware a adware mohou být obsaženy ve freeware nebo shareware programech
- Spam se šíří emailem
- Hoax se může šířit emailem, ale většinou se šíří po sociálních sítích

Zabezpečení dat - software

Antivirus

- Pomáhá proti všem typům malwaru
- Existují i specializované antiviry

Firewall

- Monitoruje datový průchod mezi počítačem a internetem
- Vytváří “bezpečnostní bránu“
- Kritéria jsou nastavitelná uživatelem

Zabezpečení dat - hardware

Externí disk

- Ideálně zašifrovaný
- Připojí se jen když je třeba

Bezpečnostní karta

- Obsahuje speciální klíč
- Bez klíče počítač nelze odemknout/odšifrovat data

Zničení dat

- Fyzické zničení disku na kterém jsou uložena

Antivirové programy

Aktivní prvek ochrany zařízení

Využívá k ochraně softwarové prvky

Moderní antiviry mají dlouhou řadu funkcí

VPN, správce hesel, adblock, ochrana periferií atd.

I ten nejzákladnější antivir by měl obsahovat základní sadu funkcí

Základní funkce antivirů

Kontrola integrity

- Vytvoří si databázi disku
- Kontroluje a dává pozor na změny – především v systémových souborech

Databáze

- Každý antivirus má databázi známého malwaru

Skenování

- Vyhledává posloupnost příkazů, typických pro viry
- Výsledky porovnává s databází

Základní funkce antivirů

Odvirovací

- V případě zjištění viru ho automaticky deaktivuje a odstraní

Heuristická analýza

- Emuluje činnost programu a monitoruje jeho činnost
- Případné podezřelé chování porovnává s databází
- Může podezřelý program i dekompilovat a zkontrolovat přímo zdrojový kód
- Je pomalejší – dokáže odhalit neznámé viry
- Účinnost je většinou poměrně nízká, jelikož působí plané poplachy

Základní funkce antivirů

Rezidentní štít a kontrola

- Sleduje aktivitu spouštěných programů – kontroluje je na přítomnost malwaru
- Prověřuje připojená datová úložiště
- Detekuje i stránky, či emaily obsahující malware, než je otevřete

Léčky

- Simuluje aktivitu, na kterou by viry normálně reagovaly a monitoruje reakci

Karanténa

- Uchování infikovaného souboru bez odstranění viru
- Virus nemá možnost infikovat nic dalšího
- Antivir následně soubor desinfikuje a pokusí se zachovat původní data

Základní funkce antivirů

Firewall	• Firewall se pomalu stává součástí antivirových programů • OS sám o sobě firewall obsahuje • Antivirové programy si berou jeho správu na starost a zlepšují jeho funkcionalitu
Aktualizace antiviru a databází	• Nutnost udržovat databáze aktuální – nové viry • Antivir sám o sobě se může stát terčem útoku, nutnost bezpečnostních aktualizací
Pravidelná kontrola	• Možnost nastavit typ, frekvenci a rozsah

Bezpečné chování

- Označováno jako pasivní ochrana
  - Nevyužívá softwarových prvků
- Uživatel by se měl zajímat o bezpečnost a ochranu svých dat a svého zařízení
  - Proto existují určité zásady, které bychom měli dodržovat

Chování uživatele

Používat pouze legální software z oficiálních zdrojů
Udržovat aktuální OS a antivir
Navštěvovat pouze stránky, jejichž adresa začíná “https“
Neotevírat soubory a stránky v emailech z neznámých zdrojů
Neklikat na náhodné vyskakující reklamy
Používat jedinečná dlouhá hesla a/nebo správce hesel
Nesdílet přihlašovací údaje
Zálohovat (a ideálně šifrovat) data
Používat běžný účet na počítači

Děkuji za pozornost