Co je virus

Je to škodlivý program, který se obvykle připojuje k jiným souborům. Po spuštění se může šířit dál nebo poškodit, smazat data.

Dělení malware (Adware, Spyware, Hoax, Phishing)

- Adware
  - Nejvíce rozšířený typ viru
  - Zobrazuje nechtěné reklamy a propagace (vyskakovací okna, bannery)
  - Může sledovat aktivitu uživatele a poté cílit reklamy
  - Obvykle neškodný, zpomaluje PC
- Spyware
  - Tajně sleduje uživatele (shromažďuje data bez souhlasu)
  - Sleduje např. klávesy, historii vyhledávání nebo hesla
  - Data může odesílat jiné osobě (útočníkovi)
  - Těžko se odhaluje, pracuje na pozadí
- Hoax
  - Nejedná se o virus, ale o falešnou zprávu (často šířená e-mailem)
  - Příklad: varování přes neexistujícím virem
  - Není škodlivý, ale může šířit paniku
- Phishing
  - Snaha získat citlivé údaje (hesla, čísla karet, pin)
  - Využívá falešné e-maily a podvodné weby, které se tváří jako originál
  - Může vést ke krádeži identity nebo peněz

Rootkity, Backdoory, Trojský kůň

- Rootkity
  - Speciální druh viru, má za úkol skrýt svou přítomnost nebo jiného viru
  - Může skrýt soubory, procesy nebo síťová připojení před uživatelem
  - Používá se k udržení přístupu hackera v systému bez odhalení
- Backdoory
  - Program, který vytváří tajný přístup do systému
  - Snaží se obejít běžné zabezpečení (hesla, firewall)
  - Umožňuje vzdáleně ovládat počítač nebo síť
  - Obvykle se instaluje s jiným
- Trojský kůň
  - Tváří se jako normální program, ale obsahuje škodlivý kód. Uživatel ho spustí nevědomě sám
  - Po spuštění může poškodit systém, instalovat další viry, otevřít backdoor

Ohrožení

- Poškození systému a dat
- Krádež osobních údajů
- Špehování a sledování aktivity
- Ovládání počítače na dálku
- Finanční ztráty

Šíření virů

- E-mailové přílohy
  - Nejčastější způsob šíření
  - Uživatel otevře infikovanou přílohu (dokument, obrázek)
  - Příloha se tváří jako zpráva od známého nebo jako oficiální dokument
- Webové stránky
  - Stránky se škodlivým kódem (exploit)
  - Uživatel může stáhnout virus bez jeho vědomí
- Stažený software
  - Nelegální programy, cracky, filmy
  - Skrytý malware v instalačních nástrojích
  - Trojské koně bývají často obsažené v těchto programech
- USB disky
  - Připojením nakaženého USB se může virus automaticky spustit
  - Může se sám kopírovat na další zařízení

Šíření poštou

- Nejčastější způsob šíření; přípony jako .exe .zip .js .bat
- Po otevření přílohy se automaticky malware spustí
- Odkazy na škodlivé weby
- Virus poté může za pomocí ukradené e-mailové adresy tento malware rozesílat
- Často se takový email tváří jako sledování zásilky, reset hesla nebo ověření účtu

Antivirové programy

Chrání počítač před škodlivými softwary. Detekují, blokují a odstraňují viry, trojské koně, ransomware… Je důležité neustále program aktualizovat. (Avast, ESET, AVG…)

Hlavní funkce:

- Skenování souborů – hledání známého malware
- Ochrana v reálném čase – kontroluje aktivitu na pozadí
- Kontrola e-mailů a příloh – detekce škodlivého obsahu
- Ochrana webového prohlížeče – blokuje nebezpečné stránky a stahování
- Karanténa – izoluje podezřelé soubory

Metody detekce:

- Srovnávání s databází virů
- Hledání podezřelého chování
- Analyzování struktury kódu

Princip antivirových serverů

- Centrální server ve firmě nebo síti
- Spravuje antivirovou ochranu všech připojených zařízení
- Na každém počítači je nainstalován klient antiviru
- Klient komunikuje v reálném čase – dostává pokyny a aktualizace
- Výhody: snadná správa více zařízení z jednoho místa, rychlá reakce na hrozby
- Vhodné pro školy a firmy

Vytváření balíčků

Balíček = upravená instalace antivirového programu pro konkrétní PC

Může obsahovat: – Samotný antivirový program
– Přednastavené firemní politiky
– Informace o připojení nebo licenci

Hromadná instalace na lokální stanice

Jedná se o proces, kdy se antivirový program instaluje na více PC najednou.

Typické pro firmy, školy, úřady – desítky a více počítačů.

Správce vytvoří instalační balíček a použije nástroje pro vzdálenou instalaci.

Updatování serveru

Antivirový server si pravidelně stahuje aktualizace.

- Virové databáze – nové hrozby a viry
- Moduly programu – oprava chyb
- Bezpečnostní politiky – nastavení

Updatování stanic

Stanice (počítače) si automaticky stahují aktualizace antivirového programu

- Virové databáze
- Moduly antiviru
- Nastavení od serveru

Forefrot Client Security

- Bezpečnostní řešení od Microsoftu pro firmy
- Slouží k ochraně PC před malwarem
- Využívá kombinaci Windows Server a Active Directory
- Dnes je tento systém zastaralý; novější varianty jsou například Microsoft System Center Endpoint Protection nebo Microsoft Defender

Navrhni postup při napadení virem

1. Spustit test počítače pomocí antivirového programu
2. Zjištění příznaků virů
3. Obnovení systému (pokud je to nutné)
4. Změna hesla
5. Aktualizace ochrany (2FA)

Navrhni antivirovou ochranu firmy o 25 počítačích

1. Výběr antivirového programu (dle potřeby zvolit příslušný software)
2. Instalace antivirového programu do všech PC (automaticky nebo manuálně)
3. Instalace politiky ochrany – pravidla pro antivirový program
4. Záloha a obnova systému
5. Pravidelná kontrola a aktualizace programu