Bezpečnost dat

Malware

Malware je kontaminací (portmanteau) slov “malicious“ a “software“. Označuje tedy všechen škodlivý software, není jedním z nich.

Rozdělení malware

Malware se běžně dělí na 9 typů, přičemž 7 z nich jsou software a dva zbývající jsou většinou textové.

- 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, utilitě či emailové příloze
  - Musí být spuštěn, aby mohl fungovat – .exe
  - Může krást data, instalovat backdoor, mazat data atd.
  - Nešíří se jako virus
  - V dnešní době už není tak běžný
- Počítačový červ
  - Podobný počítačovému viru, ale horší
  - Šíří se přes síť, na rozdíl od viru ale 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
- Ransomware
  - Vyděračský software (ransom – výkupné)
  - Na počítač se dostane jako nálož trojského koně, nebo červa
  - Na počítači buď zašifruje data, nebo ho zamkne
  - Funguje i na Androidu
  - Počet případů roste díky kryptoměnám – nemožnost pachatele dohledat podle platby
- Crimeware
  - Software sloužící k automatizaci kyberzločinu
  - Prostřednictvím sociálního inženýrství páchá krádež identity, nebo se snaží dostat přístup k bankovním účtů oběti

    - Obohacuje kyberzločince
- Spyware
    - Software, který bez vědomosti uživatele shromažďuje data
    - Typy sbíraných dat mají velký rozsah, může jít o cookies, či sledování prohlížení za účelem obohacení adware, až po používání keyloggerů pro kradení hesel, či jiných soukromých informací
    - Na počítač se může dostat v sharewaru, freewaru, či jako nálož jiného malwaru
- Adware
    - Na rozdíl od spywaru pouze shromažďuje o uživateli pouze jeden typ dat (cookies, procházení), za účelem zobrazování relevantních reklam
    - Může také zobrazovat vyskakující reklamy, či změnit v prohlížeči domovskou stránku
    - Na počítač se dostane stejným způsobem jako spyware
- Spam
    - Spam je nevyžádaná pošta (email), který je hromadně rozesílán emailovým adresám, které útočník získal buď pomocí jiných typů malwaru, nebo použitím bota na prohledání např.: internetových diskuzí, kde uživatel zveřejnil svůj email
    - Většinou mají reklamní, či erotický obsah; mohu však obsahovat odkazy na phishingové stránky, nebo stránky obsahující malware
    - V některých případech mohou malware obsahovat jako přílohu
    - Oproti výše uvedeným typům malwaru je spam pro zkušenějšího uživatele v podstatě neškodný
- Hoax
    - Stejně jako spam se hoax může šířit pomocí hromadného zasílání emailů, hoax se nejčastěji šíří po sociálních sítích
    - Hoax je označovaný jako falešná poplašná zpráva a na rozdíl od spamu se snaží uživatele vystrašit, varovat, či sdělit uživateli, jak vydělat opravdu moc peněz, až ho banky budou nenávidět
    - 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 a způsoby šíření

Projevy

Přítomnost malware v počítači je nejčastěji zjistitelná nenadálou, viditelně ničím nezpůsobenou, ztrátou výkonu

zařízení či zamrzáním, v případě počítačového červa zpomalením sítě a/nebo její vyšší spotřebou.
Adware se projevuje vyskakujícími okny, bannery nebo notifikacemi v oznamovacím centru.
Spam se projevuje “neprázdností“ spamové složky vašeho emailu, jelikož tam je automaticky vytříděn.

Způsoby šíření
Počítačový virus a červ se šíří sami – virus duplikací a skrýváním v jiných programů, červ po síti.
Trojský kůň se šíří jako zdánlivě neškodný program, buď je dostupný někde ke stažení, nebo může být poslán jako příloha emailu
Ransomware, crimeware, spyware a adware se šíří jako nálož počítačového červa nebo trojského koně. Spyware a adware navíc mohou být obsaženy ve freeware nebo shareware programech.
Spam je označení pro nevyžádanou poštu, a tedy se šíří emailem.
Hoax může šířit emailem, ale nejčastěji se šíří po sociálních sítích.

Zabezpečení dat před poškozením či zneužitím

Software
Nejčastějším a nejsnazším způsobem softwarové ochrany je použití antivirového programu – antiviru. Přes svůj název pomáhá proti všem typům malwaru, nejen virům. Existují však i specializované programy proti specifickým typům malwaru – antispyware, antispam, antimalware. Tyto programy zabraňují např.: modifikacím programů, spouštění v pozadí, skrytému monitorování a mohou i odhalit nebezpečný soubor, než ho stáhnete, či nebezpečnou stránku, než ji navštívíte.
Zatímco antiviry často monitorují pouze programy a systém, firewall vytváří “bezpečnostní bránu“ a odděluje vnitřní provoz sítě a posléze počítače od veřejného internetu. Firewall monitoruje data procházející skrz něj od uživatele a k uživateli, a podle specifických a uživatelem nastavitelných kritérií data buď propustí, či zablokuje. Tím brání buď průniku červů, či odesílání dat spywarem.

Hardware

Nejsnazším typem hardwarové ochrany dat je jejich uložení na (ideálně zašifrovaný) externí disk, který se k počítači připojí jen v případě potřeby.
Dále existuje možnost použití “bezpečnostních karet“, které obsahují klíč, pomocí kterého se počítač odemkne, či se odšifrují data. Jelikož je karta fyzická, klíč tedy není uložen na počítači, což prakticky znamená, že data nelze zneužít, jelikož by vám hacker musel fyzicky kartu ukrást.
Poslední způsob “ochrany“ dat je jejich zničení, v tomto případě fyzické zničení disku, na kterém jsou uložena, což znemožňuje jejich obnovu.

Antivirové programy

Antivirové programy se spolu s firewallem, antispawarem, antimalwarem, antispamem apod. řadí mezi aktivní prvky ochrany zařízení – tedy využívají k ochraně softwarové prvky.

Základní funkce

Moderní antiviry mají spoustu bonusových funkcí ke zvýšení ochrany uživatele a jeho zařízení –VPN, správce hesel, adblock, ochrana periferií atd. I ty nejzákladnější verze ovšem obsahují sadu základních ochranných funkcí.

- Kontrola integrity
  - Vytvoří si databázi disku a poté kontroluje a dává pozor na změny – především v systémových souborech
- Databáze
  - Každý antivirus má databázi známého malwaru, která mu pomáhá hledat a určovat viry
- Skenování
  - Vyhledává posloupnost příkazů, které jsou typické pro viry, výsledky porovnává s databází
- Odvirování
  - V případě zjištění viru ho automaticky, či po vyžádání akce uživatelem deaktivuje a odstraní
- Heuristická analýza

    - Emuluje činnost programu a monitoruje jeho činnost, např.: zda se snaží ukrýt, duplikace, hledání spustitelných souborů apod.
    - Případné podezřelé chování porovnává s databází
    - Další metodou je podezřelý program dekompilovat a zkontrolovat přímo zdrojový kód
    - Je pomalejší, a přestože dokáže odhalit neznámé viry, účinnost je většinou poměrně nízká, jelikož má tendenci působit plané poplachy
- Rezidentní štít a kontrola
    - Sleduje aktivitu spouštěných programů a kontroluje je na přítomnost malwaru, v případě nalezení malwaru program zablokuje
    - Prověřuje připojená datová úložiště – CD, DVD, Flash disk, HDD atd.
    - 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
- Firewall
    - Firewall se pomalu stává součástí antivirových programů
    - OS sám o sobě firewall obsahuje, antivirové programy si ovšem často berou jeho správu na starost a zlepšují jeho funkcionalitu
- Aktualizace antiviru a databází
    - Jelikož tvůrci malwaru vyvíjí stále nové a lepší viry, je nutné své databáze udržovat aktuální, stejně jako antivir sám o sobě, který se může stát terčem útoku
- Pravidelná kontrola
    - Možnost nastavit typ, frekvenci a rozsah

Bezpečné chování

Bezpečné chování uživatele a práce s počítačem se označuje jako pasivní ochrana, jelikož nevyužívá softwarových prvků.

Chování uživatele

Ani ten nejlepší antivir ovšem nedokáže ochránit uživatele, který se o ochranu a bezpečnost nezajímá. Jsou určité zásady, které by každý uživatel měl dodržovat.

Používat pouze legálně získaný software, z oficiálních zdrojů, ne ze Slunečnice, ulož.to, The Pirate Bay apod. Nestahovat nelegálně – cracknuté programy, warez, torrenty.
Udržovat aktuální antivir a systém (bezpečnostní aktualizace).
Navštěvovat pouze zabezpečené internetové stránky, jejichž adresa začíná “https“.
Neotevírat soubory a internetové stránky v emailech z neznámých zdrojů.
Neklikat na náhodně vyskakující reklamy, které slibují výhru, jsou erotické, nebo které vám gratulují, že jste x-tý návštěvník dané stránky.
Používat jedinečná dlouhá hesla a/nebo správce hesel. Správce náhodně vygeneruje změť čísel, písmen a znaků dlouhou podle nastavení uživatelem.
S nikým nesdílet své přihlašovací údaje.
Zálohování a šifrování dat.
Používat běžný účet na počítači – bez administrátorských práv, pokud to není nutné pro práci s počítačem.