# **4. Zabezpečení operačních systémů**

## - Bezpečnostní hrozby,

## - malware a ochrana proti malwaru

## - síťové útoky

## - sociální inženýrství

### Bezpečnostní hrozby

#### A. Malware

* Programy, které na počítači běží bez vědomí uživatele a nějakým způsobem ho poškozují

##### Počítačový virus

* Nejběžnější typ malwaru
* Vyžaduje akci uživatele k šíření (otevření přílohy emailu, souboru na USB disku nebo stažení souboru).
* Virus se skrývá v počítačovém kódu, softwaru nebo dokumentech a spuštěním se aktivuje a infikuje zařízení
* Virus může:
  + Změnit, poškodit nebo smazat soubory či celé disky
  + Způsobit problémy při spouštění počítače nebo poškodit aplikace
  + Zachytit a odesílat citlivé informace útočníkům

##### Trojský kůň (Trojan Horse)

* Užitečně vypadající program, který obsahuje škodlivý kód
* Nejčastěji jsou součástí bezplatných online programů (např. počítačové hry)
* Typy trojských koní:
  + **Remote-access** - umožní neoprávněný vzdálený přístup
  + **Data-sending** - poskytuje útočníkovi citlivé informace (např. hesla)
  + **Destructive** - poškodí nebo odstraní soubory
  + **Denial of Service (DoS)** - zpomalí nebo zahltí síť
  + **Keylogger** - snaha ukrást důvěrné informace, jako čísla platebních karet, zaznamenáváním při vyplňování např. webových formulářů

##### Adware

* Distribuován obvykle při stahování online softwaru
* Zobrazuje nevyžádané reklamy pomocí pop-up oken nebo přesměrovává webové stránky na jiné adresy

##### Ransomware

* Brání uživateli přístupu k souborům jejich zašifrováním a následně vyžaduje výkupné za dešifrovací klíč
* Platba probíhá obvykle prostřednictvím bankovního převodu nebo kryptoměn

##### Rootkit

* Používán útočníky ke získání administrátorského přístupu na zařízení
* Velmi obtížně detekovatelný – může měnit firewall, antivirus, systémové soubory i příkazy OS, aby skryl svou přítomnost
* Poskytuje útočníkům tzv. backdoor přístup, umožňuje instalovat nový software nebo použít zařízení k DDoS útokům
* Vyžaduje speciální nástroje pro odstranění nebo kompletní reinstalaci OS

##### Spyware

* Podobný adwaru, ale slouží ke sběru informací o uživateli a jejich odesílání útočníkům

##### Červ (Worm)

* Samoreplikující program, který se šíří automaticky bez akce uživatele zneužitím zranitelností v legitimním softwaru
* K šíření využívá síť, aby našel další oběti se stejnou zranitelností

#### Ochrana proti malwaru

* **Antivirový program** - schopný detekovat a blokovat trojské koně, rootkity, ransomware, spyware, keyloggery a adware
* **Zodpovědný přístup uživatele** - uživatel musí znát možné hrozby a vyvarovat se stažení malwaru nebo zadáváním citlivých informacích na podvodných stránkách
* **Pravidelná aktualizace antivirového programu a operačního systému** - nové malwary jsou neustále vyvíjeny a proto je potřeba pravidelně udržovat antiviry a operační systém aktuální
* Využití **sandboxingu** pro testování podezřelých souborů.

#### B. Síťové útoky

##### Průzkumné útoky (Reconnaissance Attacks)

* Průzkum (reconnaissance) slouží ke shromažďování informací o cíli
* Neoprávněné zjišťování a mapování systémů, služeb nebo zranitelností
* Předchází přístupovým útokům
* Techniky průzkumu:
  + **Dotazování na informace o cíli** – vyhledávání počátečních informací o cíli (přes Google, z webových stránek organizace, whois, atd.)
  + **Pingování sítě** – zjištění aktivních IP adres v síti
  + **Skenování portů** – identifikace dostupných portů nebo služeb (Nmap, SuperScan, Angry IP Scanner)
  + **Skenery zranitelností** – zjištění z identifikovaných portů typ a verze aplikace a operačního systému běžící na hostiteli (Nipper, Core Impact, Nessus, Open VAS)
  + **Nástroje pro zneužití zranitelností** – snaha objevit zranitelné služby a zneužít je za použití nástrojů jako Metasploit, Core Impact, Sqlmap, atd.

##### Přístupové útoky (Access Attacks)

* Útočníci používají přístupové útoky na síťová zařízení a počítače k získání dat, přístupu nebo k eskalaci přístupových práv na administrátora
* Cílem je získat přístup citlivým informacím
* Typy přístupových útoků:
  + **Útoky na hesla (Password Attacks)** - snaha odhalit kritická systémová hesla za pomoci nástrojů na prolamování hesel
  + **Spoofing útoky (Spoofing Attacks)** - zařízení útočníka se vydává za jiné zařízení falšováním dat (IP spoofing, MAC spoofing, DHCP spoofing)
  + **Zneužití důvěry (Trust exploitations)** - útočník využívá neoprávněná oprávnění k získání přístupu do systému a případnému ohrožení cíle
  + **Přesměrování portů (Port redirections)** - útočník používá napadený systém pro útoky na jiné cíle (např. na PC-A se útočník připojí přes SSH (port 22) a na PC-B se může připojit přes Telnet (port 23), protože PC-A je důvěryhodný pro PC-B)
  + **Man-in-the-Middle útoky** – útočník umístí mezi dvěma stranami komunikace, aby mohl číst nebo měnit data

##### DoS útoky

* DoS (Denial of Service) útok přeruší přístup k síťovým službám uživatelům, zařízením a aplikacím
* Dva hlavní typy DoS útoků:
  + **Přetížení provozem** – útočník zpomalí nebo vyřadí zařízení nebo službu odesíláním obrovského množství dat
  + **Škodlivě formátované pakety** – útočník odešle paket, který cílové zařízení nedokáže zpracovat a tím dojde k jeho zpomalení nebo výpadku
* DoS útoky jsou velmi rizikové, protože jsou poměrně snadné provést i nezkušeným útočníkem a výsledkem je přerušení komunikaci a časové a finanční ztráty

##### DDoS útoky

* DDoS útoky jsou podobné jako DoS útoky, ale pocházejí z více koordinovaných zdrojů
* Útočník vytvoří síť infikovaných zařízení (zombies) pomocí bot malwaru
* Útočník používá příkazový a řídící systém (CnC) pro řízení zombies
* Zombies neustále skenují a infikují další zařízení bot malwarem a vytváří tak botnet (síť zombies)
* Jakmile je útočník připraven, zadá pokyn CnC systému, aby botnet provedl DDoS útok

#### C. Sociální inženýrství

* Manipulace uživatelů, aby poskytli citlivé informace nebo provedli určité akce
* Některé techniky se používají osobně, jiné mohou využívat telefonu nebo internetu
* Důsledkem může být zneužití osobních informací, finanční podvody nebo získání neoprávněného přístupu
* Techniky sociálního inženýrství:
  + **Pretexting** – útočník předstírá, že potřebuje osobní nebo finanční údaje, aby potvrdil totožnost příjemce
  + **Phishing** – útočník odešle podvodný email, který se tváří jako email z legitimního a důvěryhodného zdroje, aby příjemce přiměl k instalaci malwaru do jeho zařízení nebo ke sdílení osobních či finančních informací
  + **Spear phishing** – cílený phishingový útok přizpůsobený na konkrétního jednotlivce nebo organizaci
  + **Spam** – nevyžádané emailové zprávy obsahující škodlivé odkazy, malware

## Základní postupy při zabezpečení operačních systémů

### A. Zásady zabezpečení

* **Zásady identifikace a autentizace** – definují postupy ověřování a specifikují, kteří uživatelé mohou mít přístup k síťovým prostředkům
* **Zásady hesel** – zajišťují, že hesla splňují minimální požadavky na bezpečnost (např. délka, složitost), a že jsou pravidelně měněna
* **Zásady vzdáleného přístupu** – specifikují, jakým způsobem mohou vzdálení uživatelé přistupovat k síti a jaké zdroje mohou používat
* **Aktualizace a patch management:** Pravidelné instalování bezpečnostních záplat a aktualizací.
* **Bezpečnostní politika**: Dokumentace a implementace pravidel, které definují bezpečnostní standardy organizace.

### B. Fyzické zabezpečení

* **Kontrola přístupu:** Zabezpečení serveroven a datových center pomocí fyzických zámků, bezpečnostních karet a kamer.
* **Ochrana hardware:** Udržování zařízení v kontrolovaném prostředí (klimatizace, UPS, ochrana proti požáru).
* **Zabezpečení koncových zařízení:** Fyzické zabezpečení notebooků, mobilních zařízení a externích disků.

### C. Metody ochrany a bezpečného odstraňování dat

#### Data

* Pravděpodobně nejcennějším majetkem firmy
* Zahrnují výzkum a vývoj, prodejní údaje, finanční informace, informace o zaměstnancích a zákaznících, atd.
* Proti ztrátě dat lze chránit pomocí záloh, šifrování souborů a složek nebo nastavení přístupových oprávnění

#### Ochrana dat

* **Šifrování:** Ochrana dat pomocí silných šifrovacích algoritmů při přenosu i na úložištích.
* **Bezpečné mazání dat:**
  + Softwarové metody (přepsání dat opakovanými náhodnými vzory).
  + Hardwarové metody (demagnetizace, fyzická destrukce disků).
* **Zálohování a obnova**: Pravidelné zálohování dat a testování obnovovacích procedur, aby bylo možné rychle reagovat na incidenty.

## Konfigurace zabezpečení a zásad zabezpečení serverů a klientských stanic

**A. Konfigurace zabezpečení serverů**

* **Hardening serverů**:
  + Odstranění nebo zakázání nepotřebných služeb a aplikací.
  + Konfigurace firewallů a přístupových seznamů (ACL) na úrovni operačního systému i síťových zařízení.
  + Nastavení přísných pravidel pro autentizaci a autorizaci.
  + Pravidelné monitorování systémových logů a auditování přístupů.
  + Použití nástrojů pro detekci anomálií a bezpečnostní monitoring (SIEM).
* **Bezpečnostní zásady**:
  + Implementace politiky aktualizací a záplat.
  + Použití šifrování pro komunikaci a ukládání citlivých dat.
  + Nastavení zálohovací politiky a plánů obnovy po havárii.

**B. Konfigurace zabezpečení klientských stanic**

* **Bezpečnostní software**:
  + Nasazení antivirového/antimalwarového softwaru.
  + Použití osobních firewallů.
  + Instalace aktualizací a bezpečnostních záplat pravidelně.
* **Uživatelské zásady**:
  + Nastavení silných hesel a využití vícefaktorové autentizace.
  + Omezení uživatelských práv – běžní uživatelé by neměli mít administrátorská oprávnění.
  + Vzdělávání uživatelů v oblasti bezpečnostních praktik a prevence sociálního inženýrství.
* **Konfigurace a správa**:
  + Použití centralizovaného managementu (např. Active Directory, Group Policy, SCCM pro Windows nebo správy pomocí nástrojů jako Ansible, Puppet, Chef pro Linux).
  + Pravidelné zálohování a monitorování aktivit na stanicích.
  + Nasazení endpoint security řešení pro detekci a reakci na hrozby.

**Shrnutí**

Zabezpečení operačních systémů vyžaduje komplexní přístup, který zahrnuje:

* **Identifikaci a mitigaci bezpečnostních hrozeb**: Malware, síťové útoky a techniky sociálního inženýrství představují hlavní rizika, proti kterým je třeba chránit systémy.
* **Implementaci základních bezpečnostních zásad**: Použití principu nejmenších práv, pravidelných aktualizací, fyzického zabezpečení a šifrování dat.
* **Korektní konfiguraci zabezpečení serverů i klientských stanic**: Zahrnující hardening, firewall, monitorování a vzdělávání uživatelů, které společně s bezpečným odstraňováním dat a zálohováním tvoří základ moderní IT bezpečnosti.