Metody ochrany před malware:

- Firewall: Firewall je síťové zařízení nebo software, který monitoruje a kontroluje provoz přicházející a odcházející z organizace na základě nastavených pravidel. Firewall může být konfigurován tak, aby blokoval přístup z neznámých nebo nedůvěryhodných zdrojů, což pomáhá chránit síť a servery před malware.
- HIDS (Host Intrusion Detection System): HIDS je software, který monitoruje a detekuje neobvyklou činnost na konkrétním zařízení, jako jsou servery nebo koncové stanice. HIDS může identifikovat pokusy o neoprávněný přístup, neobvyklé změny v systémových souborech nebo aplikacích a další potenciálně škodlivou činnost.
- Whitelisting: Whitelisting je metoda, která omezuje přístup pouze na povolené seznamy souborů, aplikací nebo webových stránek na koncových zařízeních. To zabraňuje spuštění nebo provádění neznámého nebo neověřeného softwaru, což snižuje riziko infekce malwarem.
- Sandboxing: Sandboxing je technika, která izoluje neznámý software nebo soubory v omezeném a kontrolovaném prostředí, zvaném "sandbox". Tím se minimalizuje riziko infekce malwarem, protože software nebo soubory nemají přístup ke kritickým systémovým zdrojům nebo datům.

Přednosti profilování sítě a serverů:

- Detekce anomálního chování: Profilování sítě a serverů umožňuje identifikovat neobvyklou nebo anomální činnost, která může být známkou pokusu o neoprávněný přístup nebo infekce malwarem.
- Rychlá detekce hrozeb: Profilování sítě a serverů umožňuje rychlé detekování hrozeb na základě předem definovaných pravidel a vzorů chování, což umožňuje rychlou reakci na potenciální bezpečnostní incidenty.
- Prevence šíření hrozeb: Profilování sítě a serverů může zabránit šíření hrozeb na další části sítě nebo serverů a minimalizovat tak rozsah poškození v případě infekce malwarem.

Běžné typy útoků na koncová zařízení a opatření proti nim:

- Malware - útočníci mohou použít malware k infikování koncového zařízení a ovládnutí jejich dat. Ochrana před malwarem zahrnuje instalaci antivirového softwaru a pravidelné aktualizace softwaru a operačního systému.
- Phishing - útočníci mohou využít e-mailové zprávy, které se zdají být legitimní, aby uživatele podvedli k zadání citlivých informací. Ochrana proti phishingu zahrnuje výuku uživatelů o bezpečnosti e-mailů a také použití technologií jako je antispamový software a e-mailové filtry.
- Sociální inženýrství - útočníci mohou využít lidské chyby a důvěry k získání přístupu k citlivým informacím. Opatření proti sociálnímu inženýrství zahrnují vzdělávání uživatelů, implementaci politik pro přístup a ověření totožnosti a zákaz sdílení citlivých informací.
- Ransomware - útočníci mohou použít ransomware k šifrování dat na koncovém zařízení a vydírat uživatele za jejich dešifrování. Ochrana před ransomwarem zahrnuje pravidelné zálohování dat a instalaci bezpečnostního softwaru.
- DDoS útoky - útočníci mohou využít distribuovaného útoku na odmítnutí služby k přetížení koncového zařízení. Ochrana proti DDoS útokům zahrnuje implementaci bezpečnostních opatření na úrovni sítě a infrastruktury.
- Zero-day útoky - útočníci mohou využít zranitelnosti v softwaru, které dosud nebyly objeveny nebo opraveny v rámci aktualizací. Ochrana před zero-day útoky zahrnuje pravidelné aktualizace softwaru a operačního systému a použití bezpečnostního softwaru.

Vysvětli použití systému CVSS k popisu zranitelností

- CVSS (Common Vulnerability Scoring System) je framework používaný k hodnocení zranitelností softwaru na základě jejich závažnosti. Skóre CVSS se pohybuje na škále 0-10, kde vyšší skóre značí vyšší závažnost zranitelnosti. CVSS zahrnuje různé metriky, jako jsou výskyt a vliv zranitelnosti, složitost provedení útoku, vliv na důvěrnost, integritu a dostupnost systému, atd.

Popiš způsoby řízení bezpečnosti zařízení

- Politiky a postupy: Vytvoření a implementace firemních politik a postupů pro zabezpečení zařízení, včetně pravidel pro používání, správu a monitorování zařízení, zálohování dat, šifrování komunikace a dalších bezpečnostních opatření.
- Správa oprávnění: Správa oprávnění a přístupových práv k zařízením, která zajišťuje, že pouze oprávnění uživatelé mají přístup ke koncovým zařízením a jejich funkcím.
- Aktualizace a záplatování: Pravidelné provádění aktualizací a záplatování koncových zařízení, aby se odstranily známé zranitelnosti a udržela se jejich bezpečnost na aktuální úrovni.
- Monitorování a detekce: Nasazení systémů monitorování a detekce, které sledují koncová zařízení a identifikují potenciální bezpečnostní hrozby, jako jsou anomální aktivity, podezřelý provoz nebo neobvyklé chování uživatelů.
- Zálohování a obnova dat: Pravidelné zálohování dat z koncových zařízení a plánování obnovy dat v případě jejich ztráty nebo poškození.
- Správa hesel: Stanovení silných hesel pro přístup k koncovým zařízením a pravidelná změna hesel, a také omezení počtu uživatelů s administrátorskými právy.
- Audity a revize: Pravidelné provádění auditů a revizí koncových zařízení, které kontrolují jejich bezpečnostní stav a dodržování bezpečnostních politik a postupů.
- Školení zaměstnanců: Provádění pravidelných školení zaměstnanců ohledně bezpečnostních postupů a hrozeb, které mohou ohrozit bezpečnost koncových zařízení.
- Celkově je řízení bezpečnosti zařízení komplexní proces, který zahrnuje kombinaci technických opatření, politik, postupů, správy oprávnění, monitorování a školení zaměstnanců s cílem zajistit vysokou úroveň ochrany koncových zařízení a minimalizovat riziko bezpečnostních hrozeb.