STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Ako surfovaŤ po internete bezpečne**

**Matúš Lupták**

2024

Obsah (štýl Nadpis Kapitoly, bez čísla)

Obsah (štýl Nadpis Kapitoly, bez čísla) 2

1 Prečo je bezpečnosť na sieti dôležitá 3

1.1 Ochrana údajov 3

1.2 Prevencia finančných strát 3

1.3 Ochrana siete a služieb 3

1.4 Dôvera užívateľov 3

1.5 Dodržiavanie predpisov 3

2 Základy bezpečnosti na sieti 5

2.1 Silné heslá 5

2.2 Aktualizácie systémov a softvérov 5

2.3 Zálohovanie údajov 5

2.4 Používanie zabezpečených sietí 5

2.5 Overovanie dvojfaktorovou autentifikáciou 5

2.6 Vzdelávanie používateľov 5

3 Firewally a antivírusy 7

3.1 Firewally 7

3.2 Typ firewallu 7

3.3 Funkcie a možnosti firewallu 7

3.4 Akutalizácie a podpora 7

3.5 Nastavenie pravidiel 7

3.6 Monitorovanie a správa 8

4 Antivírusy 9

4.1 Typ detekcie 9

4.2 Časté aktualizácie 9

4.3 Správne nastavenie skenovania 9

5 Zhrnutie 10

1. Prečo je bezpečnosť na sieti dôležitá

Bezpečnosť koncových zariadení na sieti je nevyhnutná nielen pre ochranu údajov, súkromia a stability celej siete, ale aj pre udržanie dôvery užívateľov a dodržiavanie právnych predpisov. Každý aspekt digitálneho sveta je prepojený a zraniteľný, a preto je kritické venovať osobitnú pozornosť ochrane koncových zariadení, ktoré sú často prvým cieľom útokov. Bezpečnosť zariadení je základným pilierom pre stabilnú a spoľahlivú prevádzku siete, a jej zanedbanie môže mať vážne následky pre jednotlivcov aj pre organizácie.

* 1. Ochrana údajov

Koncové zariadenia obsahujú dôležité údaje, ako sú osobné informácie, obchodné tajomstvá a finančné údaje. Bez riadnej ochrany by tieto údaje mohli byť ohrozené kybernetickými útokmi a zneužitím.

* 1. Prevencia finančných strát

Útoky ako ransomware môžu spôsobiť vážne finančné straty pre jednotlivcov aj organizácie. Bezpečnostné opatrenia môžu minimalizovať riziko takýchto útokov a ich následkov.

* 1. Ochrana siete a služieb

Útoky na koncové zariadenia môžu mať škodlivé následky na celú sieť. Napríklad, zneužitie zariadenia pre vytvorenie botnetu môže spomaliť alebo výrazne znemožniť prístup k službám pre ostatných používateľov.

* 1. Dôvera užívateľov

Užívatelia očakávajú, že ich údaje budú chránené a ich zariadenia budú bezpečné pri používaní siete. Nedostatočná bezpečnosť môže viesť k strate dôvery užívateľov a negatívnej reputácii pre organizáciu.

* 1. Dodržiavanie predpisov

V mnohých oblastiach existujú zákony a predpisy, ktoré vyžadujú, aby organizácie zabezpečili ochranu údajov a súkromia svojich zákazníkov. Nedodržanie týchto predpisov môže mať za následok pokuty a právne konzekvencie.

Celkovo je bezpečnosť dôležitá pre udržanie integrity siete, ochranu citlivých údajov a dôveru užívateľov. Preto je nevyhnutné venovať dostatočnú pozornosť bezpečnostným opatreniam a nástrojom na ochranu koncových zariadení osobných či organizačných.

1. Základy bezpečnosti na sieti

Ochrana pred kybernetickými je kľúčová v dnešnej dobe. Preto už len malé zaváhanie alebo nepozornosť môže spôsobiť veľký problém. Pravidlá, ktoré sú zväčša dodržiavané a veľmi odporúčané môžu uplatniť vo svojich životoch ľudia, ktorý nechcú utrácať peniaze alebo sa namáhať zložitými bezpečnostnými softvérmi a inými systémami.

* 1. Silné heslá

Používanie silných, unikátnych hesiel pre každý účet alebo aplikáciu je prvým krokom k zabezpečeniu koncových zariadení. Heslá by mali byť dlhé, obsahovať kombináciu veľkých a malých písmen, číslic a špeciálnych znakov.

* 1. Aktualizácie systémov a softvérov

Pravidelné inštalácie bezpečnostných aktualizácií a záplat sú nevyhnutné na odstránenie známych zraniteľností a zabezpečenie, že zariadenia sú chránené pred najnovšími hrozbami.

* 1. Zálohovanie údajov

Pravidelné zálohovanie dôležitých údajov a súborov pomáha minimalizovať straty v prípade útoku alebo havárie zariadenia.

* 1. Používanie zabezpečených sietí

Pri pripájaní k verejným WiFi sieťam je dôležité používať VPN alebo iné zabezpečené pripojenia, aby sa minimalizovalo riziko odposluchu a útokov typu man-in-the-middle.

* 1. Overovanie dvojfaktorovou autentifikáciou

Aktivácia dvojfaktorovej autentifikácie pre účty a aplikácie poskytuje ďalšiu vrstvu bezpečnosti, ktorá zabezpečuje, že aj keď sa heslo dostane do rúk útočníka, bude stále potrebné ďalšie overenie.

* 1. Vzdelávanie používateľov

Poučenie používateľov o základných bezpečnostných praktikách, ako sú rozpoznávanie phishingových e-mailov, bezpečné stiahnutie súborov a informovanie o rizikách používania neoverených zdrojov, môže značne prispieť k celkovej bezpečnosti siete.

1. Firewally a antivírusy

Firewally a antivírusový softvér sú kľúčové nástroje pre ochranu koncových zariadení a siete pred rôznymi kybernetickými hrozbami. Čo to je ? Ako to funguje ? Prečo by som to mal mať ? Čo to zahŕňa ?

* 1. Firewally

Firewall je základným prvkom zabezpečenia siete, ktorý monitoruje a kontroluje prúdenie sieťovej prevádzky na základe definovaných pravidiel. Existujú dva hlavné typy firewallu: smerovacie a aplikačné. Smerovacie firewally pracujú na úrovni IP adries a portov, zatiaľ čo aplikačné firewally sú schopné rozpoznávať konkrétne aplikácie a ich prevádzku.

* 1. Typ firewallu

Rozhodnite sa medzi hardvérovým a softvérovým firewallom. Hardvérové firewally sú fyzické zariadenia umiestnené medzi vašou sieťou a internetom, zatiaľ čo softvérové firewally sú implementované na existujúcom hardvéri, ako sú servere alebo koncové zariadenia.

* 1. Funkcie a možnosti firewallu

Vyberte firewall, ktorý ponúka potrebné funkcie a možnosti podľa vašich potrieb. Medzi dôležité funkcie patrí filtrovanie prevádzky, ochrana pred DoS útokmi, VPN podpora a podpora pre viacvrstvové zabezpečenie.

* 1. Akutalizácie a podpora

Zabezpečte sa, že firewall má pravidelné aktualizácie a dostupnú technickú podporu, aby bol schopný reagovať na nové hrozby a zraniteľnosti.

* 1. Nastavenie pravidiel

Definujte pravidlá pre prúdenie sieťovej prevádzky pomocou firewallu. Tieto pravidlá určujú, ktorá prevádzka je povolená a ktorá je blokovaná na základe zdrojových IP adries, portov a aplikácií.

* 1. Monitorovanie a správa

Vyberte firewall, ktorý umožňuje jednoduchú správu a monitorovanie sieťovej prevádzky. Tieto funkcie vám umožnia sledovať bezpečnostné udalosti, upozornenia a auditovateľnosť.

Najpoužívanejšie a najlepšie firewally na svete zahŕňajú produkty od spoločností ako Cisco, Palo Alto Networks, Check Point, Fortinet a Sophos. Každá z týchto spoločností ponúka rôzne modely firewallu s rôznymi funkciami a možnosťami.

1. Antivírusy

Antivírusový softvér je ďalší dôležitý prvok v ochrane koncových zariadení. Tieto programy skenujú súbory a prevádzku na zariadeniach a snažia sa odhaliť a odstrániť škodlivý softvér.

* 1. Typ detekcie

Vyberte antivírus, ktorý používa kombináciu statickej analýzy, heuristiky a správania sa k detekcii malvéru.

* 1. Časté aktualizácie

Antivírus musí byť pravidelne aktualizovaný, aby mal aktuálne informácie o najnovších hrozbách.

* 1. Správne nastavenie skenovania

Nastavte antivírus tak, aby pravidelne skenoval súbory, priečinky a prevádzku na zariadení.

Najlepšie antivírusy na trhu zahŕňajú produkty od spoločností ako Kaspersky, Bitdefender, Norton, McAfee a Avast. Každý z týchto antivírusov ponúka rôzne funkcie a úrovne ochrany, preto je dôležité vybrať si ten, ktorý najlepšie vyhovuje vašim potrebám a prostrediu.

1. Zhrnutie

* Firewally a antivírusy sú kľúčové nástroje v ochrane koncových zariadení a siete pred kybernetickými hrozbami.
  + Pri výbere firewallu je dôležité zvážiť typ (hardvérový vs. softvérový), funkcie a možnosti, aktuálne aktualizácie a podporu, nastavenie pravidiel a monitorovanie a správu.
    - Najpoužívanejšími a najlepšími firewally na svete sú produkty od spoločností ako Cisco, Palo Alto Networks, Check Point, Fortinet a Sophos, ktoré ponúkajú širokú škálu funkcií a možností.
  + Pri výbere antivírusu je dôležité zvážiť typ detekcie, časté aktualizácie a správne nastavenie skenovania.
    - Najlepšími antivírusmi na trhu sú produkty od spoločností ako Kaspersky, Bitdefender, Norton, McAfee a Avast, ktoré poskytujú rozmanité funkcie a úrovne ochrany.
  + Správne nakonfigurované firewally a antivírusy sú nevyhnutné pre efektívnu ochranu koncových zariadení a siete pred hrozbami ako sú malvéry, phishing, ransomware a ďalšie kybernetické útoky.