STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Zabezpečenie koncových Zariadení**

**Matúš Lupták**

2024

Obsah

Obsah 2

Anotácia 3

1 Základné pojmy 4

1.1 Čo je to koncový bod 4

1.2 Definovanie koncových bodov 4

1.3 Kybernetický útok 5

2 Typy kybernetických útokov a hrozieb 6

2.1 Malvér 6

2.2 Útok DDoS 6

2.3 Neoprávnené získavanie údajov (fishing) 6

2.4 Botnety 7

2.5 Ransomware 7

3 Firewall 8

3.1 Princíp fungovania firewallu 8

3.2 Výhody použitia firewallu 9

3.3 Dôležitosť použitia firewallov v sieti 9

4 Antivírus 10

4.1 Čo je antivírus ? 10

4.2 Jednoúčelové antivírusy 10

4.3 Balíkové jednoúčelové antivírusy 10

4.4 Komplexné antivírusové systémy 10

5 Učebný materiál 11

5.1 Implementácia silných hesiel 11

5.2 Aktualizácie systémov a softvéru 11

5.3 Pravidelné zálohovanie údajov 12

5.4 Používanie zabezpečených sietí 13

5.5 Aktivácia dvojfaktorovej autentifikácie 13

5.6 Poučenie používateľov o bezpečnostných praktikách 14

6 Záver 16

Zoznam použitej literatúry 17

Anotácia

Táto práca sa zameriava na súčasné trendy a výzvy v oblasti zabezpečenia koncových zariadení v informačných technológiách. Analyzujem metódy a nástroje na ochranu koncových zariadení, vrátane antivírusových programov, firewallov, softvéru EDR a MDM. Rovnako sa venujem ľudskému faktoru v bezpečnosti a politikám zabezpečenia. Výsledky tejto práce poskytnú odporúčania pre organizácie na zlepšenie ich bezpečnostných postupov a ochrany informácií.

**Annotation**

This work focuses on the current trends and challenges in the field of endpoint device security in information technology. We analyze methods and tools for protecting endpoint devices, including antivirus programs, firewalls, EDR software, and MDM. We also address the human factor in security and security policies. The results of this work will provide recommendations for organizations to improve their security procedures and information protection.

1. Základné pojmy

Pre pochopenie si rozdelíme niektoré názvy, ktoré budem ďalej v texte používať.

* 1. Čo je to koncový bod

Zariadenia, ktoré sa pripájajú k sieťovému systému, sa nazývajú koncové body. Patria sem mobilné zariadenia, počítače, serveri a ďalšie. Zariadenia internetu vecí, ako sú fotoaparáty, osvetlenie, chladničky, bezpečnostné systémy, inteligentné reproduktory a termostaty, sú tiež koncové body. Keď sa zariadenie pripojí k sieti, tok informácií sa podobá na konverzáciu medzi dvoma ľuďmi cez telefón.

* 1. Definovanie koncových bodov

Zabezpečenie koncových bodov alebo ochrana koncových bodov ich pomáha chrániť pred škodlivými účastníkmi a zneužitiami. Koncové body sú cieľom kybernetických útokov, pretože sú bránou k dôležitým údajom a sú prirodzene zraniteľné voči útoku. Ochrana koncových bodov pred útokmi je čoraz náročnejšia, pretože pracovná sila sa čoraz viac distribuuje. Väčšina nákladov spôsobených únikom údajov je spôsobená stratou v oblasti obchodu, fluktuáciou zákazníkov a nákladmi na získanie nových obchodov kvôli poškodenej reputácii.

Tab. 1 Top 10 kybernetických útokov za rok 2023

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meno organizácie** | **Sektor** | **Lokácia** | **Počet porušených záznamov** | **Veľkosť súborov** |
| **DarkBeam** | Kyber bezpečnosť | UK | 3800000000 |  |
| **Real Estate Wealth Network** | Nehnuteľnosti | USA | 1523776691 |  |
| **ICMR** | Zdravotníctvo | India | 815000000 |  |
| **Kid Security** | IT služby | Kazakhstan | 300000000 |  |
| **Twitter** | IT služby | USA | 220000000 |  |
| **TuneFab** | IT služby | Honk Kong | 151000000 |  |
| **Dori Media Group** | Médiá | Israel |  | 100TB |
| **Tigo** | Telekomunikácia | Honk Kong | 100000000 |  |
| **SAP SE Bulgaria** | IT služby | Bulgaria | 95592696 |  |
| **Luxottica Group** | Výroba | Italy | 70000000 |  |

* 1. Kybernetický útok

Cieľom kybernetických útokov je poškodiť alebo získať kontrolu alebo prístup k dôležitým dokumentom a systémom v rámci počítačovej siete. Kybernetické útoky môžu byť vykonané s politickými, kriminálnymi alebo osobnými zámermi zničiť utajované informácie alebo k nim získať prístup. Existuje niekoľko typov kybernetických útokov, vrátane malvéru, útokov DDoS, neoprávneného získavania údajov (phishing), útokov typu SQL injection, skriptovaných lokalít (XSS), botnetov a ransomware.



Obr 1 Kybernetický útok

1. Typy kybernetických útokov a hrozieb

Možnosti útokov a hrozieb, ktoré neskôr budem rozoberať v tejto práci.

* 1. Malvér

Malvér je škodlivý softvér, ktorý umožňuje hackerom prístup k počítačovej sieti. Môže sa šíriť cez e-maily, infikované webové stránky, USB kľúče a iné médiá. Keď sa malvér dostane do systému, môže vykonať rôzne škodlivé činnosti, ako je šifrovanie súborov (ransomware), zhromažďovanie citlivých údajov (spyware), poškodenie systému (trojský kôň) alebo zneužitie výpočtových zdrojov (botnet).

* + 1. Obrana

Na ochranu pred malvérom je potrebné používať aktualizovaný antivírusový softvér, ktorý skenuje systém a odstraňuje škodlivý softvér. Okrem toho je dôležité neotvárať e-maily od neznámych odosielateľov, neklikať na podozrivé odkazy a neprevádzkovať neoverený softvér.

* 1. Útok DDoS

Distribuovaný útok zahltením servera služby (DDoS) spočíva v snahe znemožniť prístup k určitej lokalite alebo sieti tým, že sa na neho súčasne sústredí veľké množstvo požiadaviek. To vedie k zahlteniu servera a znemožneniu prístupu legitímnym používateľom.

* + 1. Obrana

Na ochranu pred DDoS útokmi sa používajú ochranné systémy, ktoré dokážu rozpoznať a blokovať nezvyčajné prevádzky. To môže zahŕňať použitie firewallu, systémov detekcie a prevencie útokov (IDS/IPS) a služby distribuovaného odmietania služby (DDoS).

* 1. Neoprávnené získavanie údajov (fishing)

Phishing je metóda podvodu, pri ktorej sa hakeri snažia získať citlivé informácie, ako sú heslá, bankové údaje alebo osobné informácie, od používateľov tým, že sa vydávajú za dôveryhodné inštitúcie alebo jednotlivcov. Tento typ útoku sa často uskutočňuje prostredníctvom e-mailov alebo falošných webových stránok.

* + 1. Obrana

Na ochranu pred phishingom je dôležité vzdelávať používateľov o tom, ako rozpoznať podozrivé e-maily a webové stránky. Okrem toho môžu byť použité technické riešenia, ako sú filtre na spam a webové filtre, ktoré blokujú prístup k falošným stránkam.

* 1. Botnety

Botnety sú súborom počítačov, ktoré boli infikované škodlivým softvérom a môžu byť vzdialene ovládané hackerom. Tieto boty alebo „zombie“ počítače môžu byť využité na vykonávanie rôznych činností, ako sú distribúcia spamu, útoky na webové stránky, šírenie ďalšieho malvéru alebo útoky DDoS.

* + 1. Obrana

Na ochranu pred botnetmi sa používajú antivírusové programy a firewall, ktoré dokážu identifikovať a odstrániť škodlivý softvér. Okrem toho môžu byť použité aj ochranné softvérové nástroje na monitorovanie a detekciu nezvyčajnej siete.

* 1. Ransomware

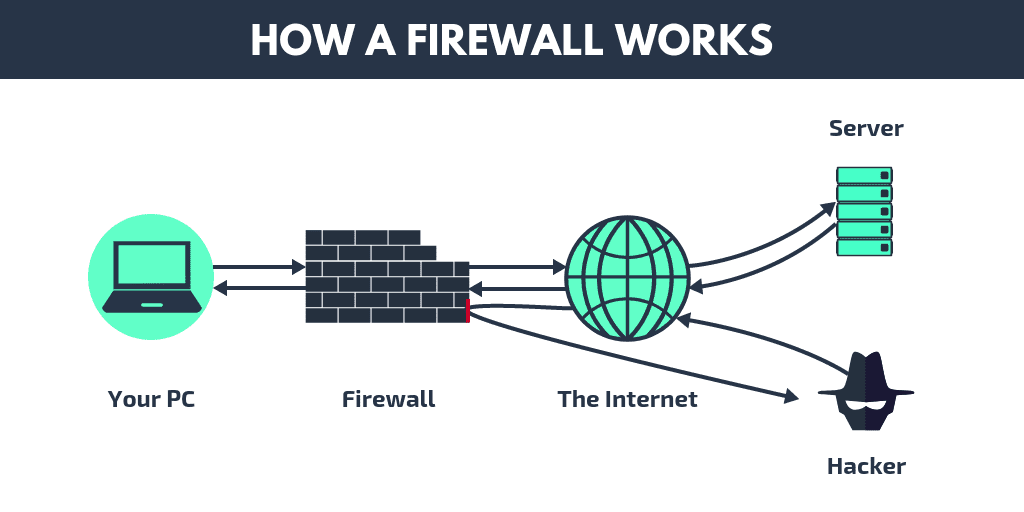
Ransomware je škodlivý softvér, ktorý šifruje súbory na počítači alebo sieťovom zariadení a vyžaduje výkupné za ich obnovenie. Tento typ útoku môže mať katastrofálne dôsledky pre jednotlivcov aj organizácie, pretože môže spôsobiť trvalú stratu dát alebo narušiť prevádzku.

* + 1. Obrana

Na ochranu pred ransomwerom je dôležité pravidelne zálohovať dôležité súbory a udržiavať ich offline, aby boli mimo dosahu ransomware. Okrem toho je dôležité používať aktualizovaný antivírusový softvér a firewall a vzdelávať zamestnancov o bezpečnostných praktikách.

1. Firewall

Firewall je základným prvkom zabezpečenia počítačových sietí a slúži na ochranu pred neoprávneným prístupom a útokmi z internetu. Jeho úlohou je monitorovať a kontrolovať komunikáciu medzi rôznymi sieťami, ako napríklad lokálnou sietou (LAN) a internetom, a zabezpečiť, aby sa neželané alebo škodlivé dáta nedostali do chránenej siete.



Obr. 2 Ako funguje firewall

* 1. Princíp fungovania firewallu

Princíp fungovania firewallu spočíva v analýze sieťovej prevádzky a aplikovaní sady pravidiel na základe preddefinovaných pravidiel a politík zabezpečenia. Existujú rôzne typy firewallov, vrátane sieťových firewallov, aplikačných firewallov a osobných firewallov.

* + 1. Sieťový firewall

Sieťový firewall je umiestnený medzi dvomi sieťami a monitoruje sieťový tok na základe IP adries a portových čísel. Vytvára virtuálnu bariéru medzi vnútornou sieťou (napríklad firemnou sieťou) a vonkajšou sieťou (napríklad internetom) a rozhoduje o tom, ktoré dáta majú povolený prístup a ktoré sú blokované.

* + 1. Aplikačný firewall

Aplikačný firewall pracuje na vyššej úrovni ako sieťový firewall a umožňuje kontrolovať a filtrovať konkrétne aplikácie alebo služby na základe ich identifikátorov (napríklad protokolov, portov alebo obsahu dát).

* + 1. Osobný firewall

Osobný firewall je softvérová ochrana nainštalovaná na jednotlivé počítače a zabezpečuje, že iba povolené aplikácie a služby majú prístup k sieťovým zdrojom. Zvyčajne poskytuje používateľovi možnosť nastaviť pravidlá pre komunikáciu medzi počítačom a sieťou.

* 1. Výhody použitia firewallu

Základné ale aj menej známe výhody.

* + 1. Bezpečnosť siete

Firewall pomáha chrániť sieť pred neoprávneným prístupom a útokmi, čím znižuje riziko úniku citlivých dát alebo poškodenia systémov.

* + 1. Kontrola a filtrovanie prevádzky

Firewall poskytuje možnosť kontrolovať a filtrovať sieťovú prevádzku, čo umožňuje blokovanie škodlivého obsahu, spamu alebo nežiaducej komunikácie.

* + 1. Ochrana pred malvérom

Firewall môže detekovať a blokovať pokusy o preniknutie malvérom, ako sú vírusy, červy, trojské kone, ransomvérové útoky a iné škodlivé programy.

* + 1. Zvýšenie dôvernosti

Firewall môže pomôcť udržať dôvernosť dát tým, že obmedzuje prístup k citlivým informáciám iba na autorizovaných používateľov.

* + 1. Monitorovanie a audit

Mnohé firewally poskytujú funkcie monitorovania a auditu siete, čo umožňuje sledovať sieťovú prevádzku, identifikovať hrozby a vyhodnocovať bezpečnostné udalosti.

* 1. Dôležitosť použitia firewallov v sieti

Je dôležité si uvedomiť, že firewall je iba jedným z mnohých opatrení zabezpečenia, a preto by sa mal používať v kombinácii s inými bezpečnostnými opatreniami, ako sú antivírusové programy, aktualizácie softvéru a správa opráv, aby sa dosiahla optimálna bezpečnosť siete.

1. Antivírus

Pojmom „antivírus“ sa v súčasnosti označuje bezpečnostný softvér zložený z viacerých ochranných vrstiev, ktoré zachytávajú, blokujú a odstraňujú nielen vírusy, ale malvér vo všeobecnosti, ako aj chránia používateľov pred ďalšími kybernetickými hrozbami.

* 1. Čo je antivírus ?

Antivírusový program pôvodne označoval softvér, ktorý slúžil na zachytávanie a niekedy aj odstraňovanie počítačových vírusov z infikovaných zariadení, pričom tiež pomáhal zastaviť ďalšie šírenie škodlivého obsahu. Platilo to hlavne v deväťdesiatych rokoch minulého storočia a krátko po roku 2000. S dramatickým nárastom v množstve malvéru rôznych druhov sa však antivírusové programy vyvinuli do komplexných bezpečnostných riešení.

* 1. Jednoúčelové antivírusy

Tieto antivírusové programy sa zameriavajú na detekciu a prípadne aj dezinfekciu jedného konkrétneho vírusu. Taktiež Poskytujú dôkladnejšiu dezinfekciu a rýchlejšiu detekciu, ale neposkytujú celkovú ochranu a sú určené len na známu hrozbu.

* 1. Balíkové jednoúčelové antivírusy

Sú schopné nájsť a odstrániť viacero bežných vírusov a malvéru. Poskytujú širšiu ochranu než jednoúčelové antivírusy, ale stále sa zameriavajú na známe hrozby.

* 1. Komplexné antivírusové systémy

Najčastejšia forma antivírusových programov, ktoré sledujú všetky hlavné vstupy, cez ktoré by sa malvér mohol do systému dostať. Zahŕňajú aj automatickú aktualizáciu cez internet a poskytujú celkovú ochranu pred rôznymi druhmi hrozieb.

1. Učebný materiál

Predstavíme praktickú aplikáciu zabezpečenia siete na základe teoretických princípov uvedených v predchádzajúcej časti. Každá podkapitola bude demonštrovať konkrétne opatrenia a kroky, ktoré sme podnikli na zabezpečenie koncových zariadení a siete ako celku. Začneme implementáciou silných hesiel, ktoré sú základným prvkom bezpečnosti, a pokračovať budeme s ďalšími opatreniami, ako sú aktualizácie systémov a softvéru, pravidelné zálohovanie údajov, používanie zabezpečených sietí, aktivácia dvojfaktorovej autentifikácie a poučenie používateľov o bezpečnostných praktikách. Každý krok je navrhnutý tak, aby zabezpečil integritu, dôvernosť a dostupnosť našej siete a údajov.

* 1. Implementácia silných hesiel

Implementácia silných hesiel je kľúčovým prvkom bezpečnosti siete. Silné heslá poskytujú ochranu pred útokmi hrubou silou a zabezpečujú, že prístup k účtom a aplikáciám je chránený. V tejto podkapitole predstavíme postup, ktorý sme zvolili na vytvorenie a implementáciu silných hesiel pre naše koncové zariadenia a účty. Prvým krokom bolo vygenerovanie unikátnych hesiel pre každý účet a aplikáciu. Heslá sme zvolili tak, aby obsahovali kombináciu veľkých a malých písmen, čísiel a špeciálnych znakov. Tento prístup zvyšuje ich odolnosť voči rôznym typom útokov, ako je hrubá sila a slovníkové útoky. Naša implementácia silných hesiel zahŕňala aj stanovenie politiky hesiel, ktorá určuje minimálnu dĺžku hesla, povolené znaky a požiadavky na jeho zmenu v pravidelných intervaloch. Tieto opatrenia zabezpečujú, že všetky heslá v sieti sú silné a zložité pre útočníkov. Okrem toho sme zabezpečili, že naše zariadenia a aplikácie neukladajú heslá v čitateľnej podobe. Použili sme metódy ako hashovanie hesiel, ktoré zabezpečujú, že aj v prípade úniku údajov by bolo veľmi ťažké ich prekonať. Implementáciou silných hesiel sme zvýšili bezpečnosť našej siete a minimalizovali riziko neoprávneného prístupu k dôležitým údajom a zariadeniam. Tento krok je nevyhnutným základom pre ďalšie opatrenia zabezpečenia siete.

* 1. Aktualizácie systémov a softvéru

Dôležitým aspektom zabezpečenia siete je pravidelná aktualizácia systémov a softvéru. Aktualizácie často obsahujú záplaty a opravy bezpečnostných chýb, ktoré môžu byť využité útočníkmi na zneužitie zariadení a únik citlivých údajov. V tejto podkapitole opíšeme postup, ktorý sme zvolili na zabezpečenie pravidelných aktualizácií pre naše koncové zariadenia. Na začiatok sme nastavili automatické aktualizácie pre všetky operačné systémy a aplikácie na našich koncových zariadeniach. Toto zabezpečuje, že všetky dostupné aktualizácie sa nainštalujú automaticky bez potreby manuálnej intervencie. Okrem toho sme vykonali inventarizáciu všetkých zariadení a softvéru v našej sieti a vytvorili sme harmonogram aktualizácií na základe kritických a dôležitých zraniteľností. To nám umožňuje zamerať sa na najdôležitejšie aktualizácie a minimalizovať riziko neaktualizovaných systémov a softvéru. Ďalším krokom bolo sledovanie a overovanie úspešnosti aktualizácií. Zabezpečili sme, že všetky aktualizácie boli úspešne nainštalované a že žiadna z nich neovplyvnila stabilitu ani funkčnosť našich zariadení a aplikácií. Tento postup nám umožnil udržať naše koncové zariadenia a softvér aktuálne a chránené pred najnovšími hrozbami. Pravidelné aktualizácie sú kľúčové pre prevenciu zraniteľností a minimalizáciu rizika kybernetických útokov.

* 1. Pravidelné zálohovanie údajov

Pravidelné zálohovanie údajov je nevyhnutnou súčasťou zabezpečenia siete, pretože umožňuje obnovenie dôležitých údajov v prípade útoku, havárie alebo straty údajov. V tejto podkapitole sa zameriame na náš postup pravidelného zálohovania údajov a opatrenia, ktoré sme prijali na zabezpečenie ich bezpečnosti. Na začiatok sme identifikovali dôležité údaje a súbory, ktoré je potrebné zálohovať. Patrili sem dôležité dokumenty, databázy, konfiguračné súbory a iné citlivé údaje, ktoré sú kľúčové pre prevádzku našej siete a podnikania. Následne sme vytvorili plán pravidelného zálohovania, ktorý zahŕňal harmonogram zálohovania, spôsob ich ukladania a miesto ich uchovávania. Zabezpečili sme, že zálohovanie prebieha pravidelne, ideálne denne, a že údaje sú ukladané na externé zariadenia alebo do cloudového úložiska. Pri implementácii sme sa uistili, že zálohovanie je plne automatizované, aby sme minimalizovali riziko ľudských chýb a zabránili neúplným alebo neaktuálnym zálohám. Ďalej sme testovali proces obnovy údajov zálohovaných zariadení, aby sme overili, že sme schopní rýchlo obnoviť dôležité údaje v prípade potreby. Tento krok je kľúčový pre zabezpečenie toho, že zálohované údaje sú skutočne použiteľné a nebudú stratene v prípade havárie alebo útoku. Pravidelné zálohovanie údajov nám poskytuje istotu, že sme schopní obnoviť naše dôležité údaje v prípade nečakaných udalostí. Je to kľúčový krok pre zabezpečenie integrity a dostupnosti našich údajov a minimalizáciu rizika v prípade straty údajov.

* 1. Používanie zabezpečených sietí

Používanie zabezpečených sietí je dôležitým opatrením na ochranu koncových zariadení pred rôznymi typmi útokov, ako je odposluch, útoky typu man-in-the-middle a iné kybernetické hrozby. V tejto podkapitole sa pozrieme na opatrenia, ktoré sme prijali na zabezpečenie používania zabezpečených sietí v našej organizácii. Začali sme implementáciou virtuálnych privátnych sietí (VPN), ktoré poskytujú šifrované a bezpečné pripojenie k verejným WiFi sieťam. Používatelia musia vždy používať VPN, keď sa pripájajú k verejným sieťam, čím minimalizujeme riziko odposluchu a útokov typu man-in-the-middle. Okrem toho sme zaviedli pravidlá pre bezpečné pripájanie k našej interné sieti z vonkajších zariadení. Používame mechanizmy autentifikácie, ako je dvojfaktorová autentifikácia a certifikáty, aby sme zabezpečili, že len oprávnení používatelia majú prístup k interným zdrojom. Tiež sme vykonali audit našich bezpečnostných politík s cieľom zabezpečiť, že siete sú správne konfigurované a chránené pred rôznymi hrozbami. To zahŕňa zabezpečenie, že bezpečnostné pravidlá a politiky sú pravidelne aktualizované a dodržiavané. V neposlednom rade sme vykonali školenie pre našich zamestnancov o bezpečnom používaní sietí a identifikácii možných hrozieb. Toto školenie zahŕňalo informácie o tom, ako rozpoznať nebezpečné siete, ako aj o tom, ako chrániť svoje účty a zariadenia pred rôznymi typmi útokov. Implementáciou týchto opatrení sme zabezpečili, že používanie sietí v našej organizácii je bezpečné a spoľahlivé. Tieto kroky nám umožňujú minimalizovať riziko kybernetických útokov a zabezpečiť, že naše koncové zariadenia sú chránené pred potenciálnymi hrozbami.

* 1. Aktivácia dvojfaktorovej autentifikácie

Aktivácia dvojfaktorovej autentifikácie je ďalším krokom k zabezpečeniu koncových zariadení a účtov. Dvojfaktorová autentifikácia poskytuje ďalšiu vrstvu bezpečnosti tým, že vyžaduje nielen niečo, čo používateľ vie (jeho heslo), ale aj niečo, čo používateľ má (napríklad mobilný telefón). V tejto podkapitole opíšeme, ako sme implementovali dvojfaktorovú autentifikáciu a prečo je to dôležité. Začali sme tým, že sme vybrali vhodnú dvojfaktorovú autentifikačnú metódu pre našu organizáciu. Používame kombináciu SMS kódov, mobilných aplikácií pre dvojfaktorovú autentifikáciu a hardvérových tokenov podľa potreby a typu účtu. Následne sme aktivovali dvojfaktorovú autentifikáciu pre všetky dôležité účty a aplikácie, ktoré obsahujú citlivé údaje alebo majú prístup k dôležitým zariadeniam. Toto zahŕňa prístup k e-mailom, cloudovým úložiskám, administrátorským účtom a iným dôležitým systémom. Okrem toho sme použili politiku povinného používania dvojfaktorovej autentifikácie pre všetkých používateľov v našej organizácii. To znamená, že každý, kto sa snaží pristupovať k dôležitým účtom alebo zariadeniam, musí prejsť procesom dvojfaktorovej autentifikácie. Ďalej sme vykonali školenie pre našich zamestnancov o dvojfaktorovej autentifikácii a jej výhodách. Poučili sme ich o tom, ako správne používať dvojfaktorovú autentifikáciu a prečo je to dôležité pre ochranu ich účtov a údajov. Implementácia dvojfaktorovej autentifikácie nám poskytuje ďalšiu úroveň zabezpečenia našich koncových zariadení a účtov. Táto vrstva ochrany pomáha minimalizovať riziko neoprávnenej prístupu a zabezpečuje, že naše dôležité údaje sú chránené pred neoprávneným prístupom.

* 1. Poučenie používateľov o bezpečnostných praktikách

Poučenie používateľov o bezpečnostných praktikách je kľúčové pre prevenciu kybernetických hrozieb a zvýšenie povedomia o bezpečnosti v našej organizácii. V tejto podkapitole sa zameriame na opatrenia, ktoré sme prijali na vzdelávanie našich zamestnancov o bezpečnostných hrozbách a najlepších praktikách v oblasti kybernetickej bezpečnosti. Na začiatok sme vytvorili bezpečnostné školenia a materiály, ktoré obsahujú informácie o rôznych typoch kybernetických hrozieb, ako sú phishingové útoky, ransomware, malware a ďalšie. Tieto školenia sme pravidelne poskytovali novým zamestnancom a vykonávali sme ich aj ako pravidelnú súčasť ďalšieho vzdelávania. Ďalej sme zorganizovali praktické cvičenia a simulácie útokov, aby sme našim zamestnancom umožnili zažiť rôzne scenáre útokov a naučili ich, ako reagovať a správne identifikovať nebezpečné situácie. Okrem toho sme vytvorili internú bezpečnostnú politiku a postupy, ktoré sme zdieľali so všetkými zamestnancami. Tieto politiky a postupy obsahovali pokyny týkajúce sa používania hesiel, zálohovania údajov, prístupu k sieti a ďalšie. Taktiež sme zabezpečili, že naši zamestnanci sú informovaní o najnovších bezpečnostných opatreniach a aktualizáciách prostredníctvom interných komunikačných kanálov, ako sú e-maily, interné webové stránky alebo informačné briefingy. V neposlednom rade sme vytvorili mechanizmus hlásenia bezpečnostných incidentov a podporovali sme kultúru zdieľania informácií o potenciálnych hrozbách medzi zamestnancami. Tieto opatrenia nám umožnili zvýšiť povedomie o kybernetickej bezpečnosti v našej organizácii a minimalizovať riziko úspechu kybernetických útokov. Poučenie používateľov je neoddeliteľnou súčasťou našej stratégie bezpečnosti a pomáha nám chrániť naše koncové zariadenia a údaje pred rôznymi typmi hrozieb.

1. Záver

V tejto praxovej časti sme preskúmali a analyzovali dôležité aspekty zabezpečenia koncových zariadení a siete prostredníctvom implementácie rôznych bezpečnostných opatrení a postupov. Každá časť našej práce zohráva kľúčovú úlohu pri zabezpečení interného a spoľahlivého fungovania našej siete a ochrane dôležitých údajov. Prvá časť našej praxe sa zameriavala na základné princípy bezpečnosti na sieti, ako je silné heslo, pravidelné aktualizácie systémov a softvéru, pravidelné zálohovanie údajov, používanie zabezpečených sietí, aktivácia dvojfaktorovej autentifikácie a poučenie používateľov o bezpečnostných praktikách. Tieto opatrenia tvoria základný pilier bezpečnosti a pomáhajú minimalizovať riziko kybernetických útokov a straty citlivých údajov. Druhá časť našej praxe sa zaoberala konkrétnymi bezpečnostnými nástrojmi, ako sú firewally a antivírusy. Implementácia týchto nástrojov je nevyhnutná pre ochranu koncových zariadení a siete pred rôznymi typmi hrozieb. Vybrali sme firewally od renomovaných výrobcov, ako sú Cisco, Palo Alto Networks, Check Point, Fortinet a Sophos, a antivírusy od spoločností ako Kaspersky, Bitdefender, Norton, McAfee a Avast, ktoré poskytujú vysokú úroveň ochrany a funkčnosti. Celkovým záverom je, že kombinácia správnych bezpečnostných opatrení, nástrojov a postupov je kľúčom k efektívnemu zabezpečeniu koncových zariadení a siete pred kybernetickými hrozbami. Pravidelná aktualizácia a vzdelávanie zamestnancov o najnovších bezpečnostných opatreniach sú kľúčové pre udržanie bezpečného a spoľahlivého prostredia.

Zoznam použitej literatúry

1. MICROSOFT, Čo je koncový bod ? [online]. 2024. [cit: 20. 04. 2024]. Dostupné na internete: < <https://www.microsoft.com/sk-sk/security/business/security-101/what-is-an-endpoint>>
2. POGG NICOLAS, Endpoint Security Risks - Why It Matters Now More Than Ever [online]. 15. 06. 2021[cit: 20. 04. 2024]. Dostupné na internete: <https://preyproject.com/blog/endpoint-security-risks>
3. CODERAMA, Firewall [online]. 2023[cit: 20. 04. 2024]. Dostupné na internete: < <https://coderama.com/slovnik/firewall>>
4. Skalka Ján, Klimeš Cyril, Lovászová Gabriela, Švec Peter, Informatika na maturity a prijímacie skúšky, Enigma, Nitra 2007, ISBN 978-80-89132-50-8.
5. Glamoslija Katarina, Antivirus and Cybersecurity Statistics, Trends & Facts 2024 [online]. 2024[cit: 20. 04. 2024]. Dostupné na internete: < https://www.safetydetectives.com/blog/antivirus-statistics/ >
6. Neil Ford, List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached [online]. 05. 01. 2024[cit: 20. 04. 2024] Dostupné na internete: < https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023 >
7. Ashwin Harish.P, How does a firewall work [online]. 20.03.2023[cit: 20. 04. 2024] Dostupné na internete: <https://www.linkedin.com/pulse/how-does-firewall-work-ashwin-harish-p>
8. FREEPICK, obrázky [online]. 2024 Dostupné na internete: <freepick.com>