STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Bezpečonsť na počítačových sieťach**

**NIKOLAS SÉLEŠ**

2024

Obsah

[1 Úvod 4](#_Toc164115181)

[2 Teoretická analýza bezpečnosti počítačových sietí 5](#_Toc164115182)

[2.1 História bezpečnosti počítačových sietí 5](#_Toc164115183)

[2.1.1 Prvý firewall a antivírus 5](#_Toc164115184)

[2.2 Identifikacia hlavnyck hrozieb a utokov 5](#_Toc164115185)

[2.2.1 Phishing 6](#_Toc164115186)

[2.2.2 Spyware 6](#_Toc164115187)

[Zoznam použitej literatúry 7](#_Toc164115188)

Anotácia

**Annotation**

1. Úvod

Bezpečnosť na počítačových sieťach je dosť dôležitou súčasťou dnešného digitálneho sveta. Technologické inovácie sa stávajú obvyklou súčasťou nášho každodenného života, a s nárastom zariadení pripojených na internet sa zvyšuje aj zraniteľnosť počítačových sietí. Preto je nevyhnutné aby sme porozumeli významu a potrebe bezpečnosti, aby sme chránili nie len naše údaje, siete ale aj digitálnu infraštruktúru pred rôznymi formami útokov a zneužitia.

V súčasnej dobe digitálneho sveta je bezpečnosť počítačových sietí kľúčovým prvkom pre zabezpečenie dôveryhodnosti, dostupnosti a integrity digitálnej komunikácie a informácií. Bezpečnosť počítačových sietí nie je len otázkou technickej ochrany, ale aj stratégie, procesov a politík, ktoré zabezpečujú ochranu údajov a sietí pred rôznymi hrozbami.

V nasledujúcich kapitolách sa povenujem teoretickému skonštatovaniu problematiky o bezpečnosti na počítačových sieťach. V nasledujúcej kapitole sa presnejšie zameriam na históriu bezpečnosti a identifikáciu hlavných hrozieb a útokov, ktoré ohrozujú bezpečnosť sietí, ako aj na predstavenie najdôležitejších metód a nástrojov na ich ochranu. Potom sa budem venovať bezpečnostným stratégiám a politikám, ktoré organizácie a jednotlivci môžu implementovať na zvýšenie bezpečnosti svojich sietí a údajov. Ku koncu sa budem zaoberať aktuálnymi trendmi a výzvami v oblasti bezpečnosti počítačových sietí a budem poskytovať predpovede budúceho vývoja.

1. Teoretická analýza bezpečnosti počítačových sietí

V tejto kapitole sa budem podrobne venovať mnohým aspektom zabezpečenia siete. Mojím cieľom bude vymenovať základné nebezpečenstvá, vybrať najúčinnejšie spôsoby obrany proti nim a preskúmať najnovší vývoj a problémy v oblasti kybernetickej bezpečnosti. Pre lepšie pochopenie toho, ako sa bezpečnostné opatrenia a metódy vyvíjali od začiatku počítačových sietí, si najprv prejdem históriu bezpečnosti počítačových sietí. Potom podrobne opíšem, ako rozpoznať základné nebezpečenstvá a útoky, ktoré ohrozujú bezpečnosť počítačových sietí. Súčasťou bude stručné charakterizovanie rôznych druhov útokov, ako sú malvér, phishing a distribuované útoky typu DoS (distributed denial of service) a DDoS (distributed denial of service). Venovať sa budem aj tomu ako sa pred nimi chrániť .

* 1. História bezpečnosti počítačových sietí

Tak ako som spomenul v kapitole 2, tak ako prvej sa budem venovať histórií bezpečnosti počítačových sietí. Histórií bezpečnosti počítačových sietí siaha od počiatkov ich využívania. V 70. a 80. rokoch prevládali na sieti ARPANET neškodné žarty, no zvýšená aktivita viedla k hľadaniu bezpečnostných riešení. Vznik organizácie CERT v roku 1988 a nástup prvého počítačového červa Morris Worm ukázali, že ochrana sietí je nevyhnutná. [1]

* + 1. Prvý firewall a antivírus

V reakcii na narastajúce hrozby sa začal vyvíjať prvý firewall a antivírusové programy. Prvý firewall je často pripisovaný výskumníkovi z centra NASA v Kalifornii, ktorý v roku 1988 vytvoril metódu na ochranu sietí podobnú fyzickému "firewallu". Tento mechanizmus oddeľoval siete pomocou routerov, čím bránil šíreniu útokov na všetky počítače naraz.

Súčasne s vývojom firewallu sa začali vyvíjať aj prvé antivírusové programy. Vzhľadom na narastajúci počet škodlivého softvéru sa stala ochrana pred vírusmi kľúčovou súčasťou bezpečnosti sietí. Tieto nástroje boli nevyhnutné na zachovanie integrity a bezpečnosti počítačových systémov v rastúcom digitálnom prostredí.

* 1. Identifikacia hlavnyck hrozieb a utokov

Identifikáciou hlavných hrozieb a útokov sa zaoberáme procesom rozpoznávania a pochopenia najbežnejších hrozieb a techník útokov, ktoré ohrozujú bezpečnosť počítačových sietí a systémov. Tento proces je kľúčový pre efektívne vypracovanie stratégií a opatrení na ochranu sietí a dát. Podkapitoly tejto časti sa zameriavajú na špecifické typy hrozieb a útokov, ako sú phishing, spyware, ransomware, keylogging, DoS a DDoS útoky, poskytujúc informácie o ich charakteristike, spôsobe fungovania a možnostiach obrany.

* + 1. Phishing

Phishing je pojem pre podvodný útok, ktorého cieľom je vylákať dôverné informácie od užívateľa prostredníctvom falošného e-mailu alebo webových stránok.[7] Útočník sa snaží manipulovať obeť prostredníctvom e-mailov alebo napodobených webových stránok, ktoré pôsobia ako dôveryhodné zdroje, napríklad banky. Cieľom je získať citlivé informácie, ako sú heslá, čísla bankových účtov alebo prístupové údaje.

Obranou proti phishingu môže byť použitie antispyware na odchytávanie podvodných e-mailov alebo softvér na internetovú bezpečnosť, ktorý môže zabrániť prístupu na podvodné webové stránky. Avšak najdôležitejšou obranou je opatrnosť samotného užívateľa. Identifikovanie podvodných e-mailov a webových stránok a vyhýbanie sa poskytovaniu citlivých informácií je kľúčové pre ochranu pred phishingom.

* + 1. Spyware

Spyware je softvér, ktorý zhromažďuje informácie o používateľovi a jeho správanie alebo mení nastavenia zariadenia tak, aby bolo zraniteľnejšie.[7] Často sa inštaluje bez vedomia užívateľa a maskuje sa ako potrebný doplnok k inému softvéru. Je to stredné až závažné bezpečnostné riziko, keďže slúži na špehovanie užívateľa a jeho aktivít.

Spyware môže škodiť tým, že zhromažďuje dáta o užívateľovi, ktoré neskôr zasliela majiteľovi spyware. Tieto údaje sa často využívajú na sledovanie zvykov užívateľov a cielenie reklamy. V závažných prípadoch môže meniť nastavenie počítača alebo získavať osobné dáta užívateľov.

Ochrana proti spyware spočíva v inštalácii bezpečnostného softvéru, najmä Antispyware, Antivirus a Firewall, a opatrnosti pri inštalácii nového softvéru z neoverených zdrojov.

Zoznam použitej literatúry

1. History of Network Security Methods [online]. Dostupné na internete: <<https://www.radware.com/resources/network_security_history.aspx/>>
2. Vaidotas Januška: Infographic: The History of Network Security [online]. Dostupné na internete: <<https://www.ipxo.com/blog/infographic-history-of-network-security/>>
3. Martin Holovský: Seznamte se – DoS a DDoS útoky [online]. Dostupné na internete: <<http://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky>>
4. <https://www.eset.com/sk/distribuovany-utok-odmietnutia-sluzby/>
5. <https://isocertifikat.sk/iso-27001-identifikacia-hrozieb-a-zranitelnosti/> obrazok graf
6. <https://www.europarl.europa.eu/topics/sk/article/20220120STO21428/kyberneticka-bezpecnost-hlavne-hrozby-v-roku-2021-infografika> obrazky pre poster
7. <https://managementmania.com/sk/informacne-a-pocitacove-hrozby> a podstránky

Prílohy (štýl Nadpis Kapitoly, bez čísla)

Zoznam príloh záverečnej práce:

* Príloha A – CD médium
* Príloha B – <názov prílohy>
* Príloha C – <názov prílohy>

Táto časť záverečnej práce obsahuje zoznam všetkých príloh. Číslovanie strán príloh nadväzuje na číslovanie strán v hlavnom texte.

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla)

Priložené CD médium **povinne** obsahuje text záverečnej práce vo formáte PDF. CD môže obsahovať edukačný hypertext, metodické listy, dotazníky a ukážky projektov atď. CD médium zabalené do papierového obalu sa vlepí na vnútornú stranu zadnej obálky záverečnej práce.

Príloha B – <názov prílohy>

<popis prílohy>

Príloha C – <názov prílohy>

<popis prílohy>