STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Bezpečnosť na počítačových sieťach**

**NIKOLAS SÉLEŠ**

2024

Obsah

Anotácia 3

Úvod 4

1 Teoretická analýza bezpečnosti počítačových sietí 5

1.1 História bezpečnosti počítačových sietí 5

1.1.1 Prvý firewall a antivírus 5

1.2 Identifikácia hlavných hrozieb a útokov 6

1.2.1 Phishing 6

1.2.2 Spyware 7

1.2.3 Ransomware 7

1.2.4 Keylogging 8

1.2.5 DoS útok 9

1.2.6 DDoS 9

2 Tvorba plagátu 11

2.1 Výber veľkosti plagátu 11

2.2 Voľba nástroja na tvorbu plagátu 11

2.3 Výber druhu ilustrácie 12

2.4 Farebná paleta 13

2.5 Použitý text v plagáte 13

2.6 Cieľová skupina 14

3 Záver 15

Zoznam použitej literatúry 16

Anotácia

Táto ročníková práca sa zaoberá problematikou bezpečnosti počítačových sietí v súčasnom digitálnom svete. V úvode je zdôraznený význam bezpečnosti v kontexte rastúcej zraniteľnosti sietí v dôsledku technologických inovácií a rozšírenia pripojených zariadení. Ďalej sa práca venuje teoretickej analýze bezpečnosti počítačových sietí, zahŕňajúcej históriu bezpečnosti, identifikáciu hlavných hrozieb a útokov, ako aj metódy obrany. Súčasťou práce je aj tvorba plagátu, ktorý slúži ako nástroj na zvýšenie povedomia o bezpečnosti počítačových sietí. V práci sa zdôrazňuje dôležitosť vhodného výberu veľkosti plagátu, použitého nástroja na tvorbu, farebnej palety a textu, pričom je venovaná pozornosť aj cieľovým skupinám a ich potrebám. Celkovo je práca zameraná na poskytnutie komplexného pohľadu na problematiku bezpečnosti počítačových sietí a prezentáciu relevantných informácií a odporúčaní prostredníctvom vhodných vizuálnych a textových prostriedkov.

**Annotation**

This year's work deals with the issue of computer network security in today's digital world. The introduction to this work highlights the importance of security in the context of the increasing vulnerability of networks due to technological innovation and the rapid increase of connected devices. Next, the work discusses a theoretical analysis of computer network security, covering the history of security, the identification of major threats and attacks, as well as methods of defense. The work also includes the creation of a poster that serves as a tool to raise awareness of computer network security. The work emphasises the importance of choosing the appropriate size of the poster, the tool used to create it, the colour palette and the text, while attention is also paid to the target groups and their needs. Overall, this year’s work aims to provide a comprehensive view of the issue of computer network security and to present relevant information and recommendations through appropriate visual and textual means.

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. Identifikácia hlavných hrozieb a útokov

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.

Obrázok, na ktorom je text, snímka obrazovky, softvér, webová stránka

Automaticky generovaný popis

Obr. 1 Príklad falošného e-mailu, ktorý nie je prepojený so Slovenskou Poštou [12]

* + 1. Spyware

Spyware je softvér, ktorý zhromažďuje informácie o používateľovi a jeho správanie alebo mení nastavenia zariadenia tak, aby bolo zraniteľnejšie.[8] 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 zasiela 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.

Tab. 1 Tabuľka s efektami spywaru (Prevzaté a preložené z [16])

|  |  |  |  |
| --- | --- | --- | --- |
| Hrozba | Užívateľ | Počítač | Sieť |
| Mierna | Komerčne predajné údaje | Spotreba kapacity | Spotreba šírky pásma |
| Vážna | Osobné údaje | Šírenie podradného kódu | Distribúcia malvéru |
| Devastujúca | Kritické údaje | Prevzatie zariadenia | Breakdown |

* + 1. Ransomware

Ransomware je typ počítačového vírusu, ktorý užívateľovi obmedzí prístup k počítaču alebo k dátam. Jeho autor následne vyžaduje zaplatenie výkupného za poskytnutie kľúča. [9]

Ransomware funguje tým, že sa infikuje na počítač a zašifruje dáta. Autor následne žiada výkupné, často prostredníctvom Bitcoinu, a po zaplatení poskytne kľúč na obnovenie dát. Bez zaplatenia užívateľ nemá prístup k svojim dátam.

Na obranu pred ransomware sa odporúča udržiavať zariadenie a webový prehliadač aktuálne, vyhýbať sa podozrivým webovým stránkam a neotvárať podozrivé e-maily. Dôležitý je aj bezpečnostný softvér, ako antivírus, a pravidelné zálohovanie dát.

Obrázok, na ktorom je text, snímka obrazovky, logo, písmo

Automaticky generovaný popis

Obr. 2 Príklad ako môže vyzerať ransomware útok [13]

* + 1. Keylogging

Keylogging je typ kybernetického útoku, pri ktorom útočník sleduje stlačené klávesy na vašom počítači. Môže tak napríklad zaznamenať vaše heslo alebo iné citlivé údaje. [10] Existujú dva hlavné spôsoby, ako keylogging funguje: cez špeciálny škodlivý softvér nazývaný Keylogger, alebo cez hardvérové zariadenie nainštalované do klávesnice. Keylogger môže byť využitý aj ako legálne monitorovacie zariadenie v firemných prostrediach.

Obrana proti nechcenému keyloggingu vyžaduje použitie kvalitného softvéru na ochranu proti vírusom a malware, ako sú antivírusy, internet security a firewally. Preventívne opatrenia, ako je vyhýbanie sa podozrivým webovým stránkam a e-mailom, sú tiež kľúčové pre ochranu pred touto formou útoku.

Graf. 1 Graf zobrazujúci typy dát, ktoré boli ukradnuté organizáciám v tretej štvrtine roka 2023 (Prevzaté z [17])

* + 1. DoS útok

Denial of Service (DoS) je kybernetický útok, ktorý je zameraný na znemožnenie prístupu k zdrojom alebo službám na počítačovej sieti. Útočník používa rôzne techniky na zahltenie cieľového systému, čím spôsobuje výpadok alebo znemožnenie jeho normálneho fungovania pre legitímnych používateľov.

DoS útoky sa môžu realizovať pomocou viacerých metód, vrátane oneskorenia, zablokovania alebo vyradenia cieľového systému z prevádzky. Útočník môže využívať veľké množstvo požiadaviek na spojenie, aby zahltil sieťové zdroje, alebo vytvárať chybné požiadavky na služby, čím vyčerpáva dostupné systémové zdroje.

Obrana proti DoS útokom zahŕňa implementáciu ochranných mechanizmov a softvéru, ktoré monitorujú sieťovú prevádzku a identifikujú potenciálne útoky. To môže zahŕňať použitie firewallu, sieťových filtrov alebo softvérových nástrojov na detekciu anomálií v prevádzke. Ďalšie opatrenia zahŕňajú distribuovanú ochranu, ktorá rozloží záťaž medzi viaceré zdroje, aby sa minimalizoval dopad DoS útokov.

* + 1. DDoS

Distributed Denial of Service (DDoS) je závažná forma kybernetického útoku, ktorý využíva množstvo zariadení alebo počítačov na súčasné zaslanie veľkého množstva požiadaviek na jeden cieľový systém alebo sieť. Cieľom je preťažiť zdroje cieľového systému, čím sa znemožní jeho normálne fungovanie pre legitímnych používateľov.

DDoS útoky sú oveľa účinnejšie ako klasické DoS útoky, pretože využívajú distribuovanú sieť zariadení, ktoré sú často infikované malvérom a slúžia ako tzv. „botnet“. Tieto botnety môžu byť veľmi veľké a schopné generovať enormné množstvo sieťovej prevádzky, čo robí detekciu a obranu proti DDoS útokom ešte ťažšou.

Obrana proti DDoS útokom vyžaduje pokročilé bezpečnostné opatrenia, ktoré zahŕňajú nasadenie špecializovaných DDoS ochranných riešení, ktoré dokážu identifikovať a filtrovať nelegitímnu sieťovú prevádzku. Tieto riešenia môžu zahŕňať rôzne techniky, ako sú detekcia anomálií, geografické filtrovanie, správu prístupu a ďalšie.

Okrem toho je dôležité mať aj plán na zvládanie DDoS útokov, ktorý zahŕňa monitorovanie a rýchlu reakciu na odhalené útoky, spoluprácu so sieťovými poskytovateľmi a implementáciu ochranných mechanizmov na viacerých úrovniach siete. Bez týchto opatrení môže DDoS útok vážne poškodiť dostupnosť a spoľahlivosť služieb a systémov na počítačovej sieti.

1. Tvorba plagátu

Táto kapitola je venovaná procesu tvorby plagátu, ktorý slúži ako prostriedok pre zvýšenie povedomia o bezpečnosti počítačových sietí. Plagát je vizuálny nástroj, ktorý umožňuje jasné a prehľadné zobrazenie kľúčových aspektov a odporúčaní týkajúcich sa bezpečnosti počítačových sietí.

Budem sa snažiť poskytnúť podrobný prehľad toho, ako som postupoval pri tvorbe plagátu, vrátane návrhu, výberu obsahu, grafického dizajnu a ďalších dôležitých aspektov tvorby. Plagát slúži nielen ako prostriedok na šírenie informácií, ale aj ako nástroj na zvyšovanie povedomia o bezpečnosti počítačových sietí medzi širokou verejnosťou.

V nasledujúcich podkapitolách sa povenujem detailne popíšem jednotlivé fázy tvorby plagátu, vrátane návrhu a realizácie. Budem diskutovať o mojich rozhodnutiach a postupoch, ktoré som pri tvorbe plagátu prijal, a budem sa snažiť prezentovať ich praktický prínos a význam v kontexte bezpečnosti počítačových sietí.

* 1. Výber veľkosti plagátu

Veľkosť plagátu hrá kľúčovú úlohu v jeho účinnosti a viditeľnosti, a preto je dôležité vybrať správnu veľkosť, ktorá bude najvhodnejšia pre daný účel. Rozhodoval som sa medzi niekoľkými veľkosťami plagátov, vrátane formátov 24" x 36", 11" x 17" a 18" x 24. Veľkosť 24" x 36" síce poskytuje veľa priestoru pre obsah, no môže byť príliš veľká a nepraktická na umiestnenie v rôznych prostrediach. Naopak, formát 11" x 17" je príliš malý a obmedzuje možnosti prezentácie informácií.

Veľkosť 18" x 24" ponúka dostatočne veľký priestor na umiestnenie textových informácií a grafiky, zatiaľ čo zostáva dostatočne kompaktná na to, aby bola praktická na umiestnenie na stenách, výveskách alebo stojanoch. Preto sa táto veľkosť javí ako najlepšia možnosť pre účely tvorby plagátu.

* 1. Voľba nástroja na tvorbu plagátu

Pri rozhodovaní sa, ktorý nástroj použiť na tvorbu plagátu, som zvážil niekoľko faktorov, ktoré ovplyvňujú výber vhodného prostriedku pre realizáciu môjho projektu. Nakoniec som sa rozhodol použiť program Figma. Prečo?

* Skúsenosť a znalosť: Už mám skúsenosti s používaním nástroja Figma. Vďaka tejto znalosti budem mat prácu ľahšiu, pretože som s ním už pracoval a cítim sa v ňom pohodlne. Môžem efektívne využiť svoje znalosti a skúsenosti na vytvorenie plagátu s minimálnym časovým investovaním do učenia sa nového nástroja.
* Flexibilita: Figma je veľmi flexibilný nástroj, ktorý umožňuje tvorbu rôznych typov dizajnov. Môžem vytvárať nielen plagáty, ale aj webové stránky, mobilné aplikácie a ďalšie digitálne projekty. Táto flexibilita mi dáva možnosť prispôsobiť dizajn plagátu podľa mojich potrieb a predstáv.
* Dostupnosť a cena: Figma je dostupná ako online nástroj a je zadarmo pre jednotlivcov. Tento faktor zohľadňuje moje finančné možnosti a umožňuje mi pracovať na svojom projekte bez nutnosti investovať do drahých softvérových licencií.

Z týchto dôvodov som sa rozhodol použiť Figmu na tvorbu plagátu. Jeho kombinácia skúseností, flexibility, dostupnosti a schopnosti spolupracovať je pre mňa ideálnym riešením pre úspešnú realizáciu môjho projektu.

* 1. Výber druhu ilustrácie

Pri tvorbe plagátu som sa rozhodol použiť formu ilustrácie nazývanú Vector Art (Obr. 4). Vector. Art je typ digitálneho umenia, ktorý je vytvorený pomocou vektorových grafických programov, ako je napr. Figma. Tento druh umenia je výrazný a ľahký na pochopenie, pričom umožňuje vytvárať škálovateľné obrázky bez straty kvality.

Pre svoju tvorbu som využil platformu Flaticon, ktorá poskytuje širokú škálu vektorových ikon a obrázkov. Flaticon umožňuje upravovať tieto obrázky podľa potreby a prispôsobovať ich štýl, farbu a veľkosť, čo mi poskytlo dostatočnú flexibilitu pri vytváraní dizajnu plagátu.

Obrázok, na ktorom je vták, zobák, rybárik

Automaticky generovaný popis

Obr. 4 Jednoduchý príklad toho ako vyzerá Vector Art (Prevzaté z [15])

* 1. Farebná paleta

Pri tvorbe plagátu som sa zameriaval na vhodný výber farieb, ktoré by vytvorili atraktívny a vizuálne príjemný dizajn. Rozhodol som sa použiť kombináciu žltej a gradientov fialovej farby, aby som dosiahol vyváženú a zaujímavú farebnú paletu.

Fialová farba bola jednou z hlavných farieb použitých na plagáte. Zvolil som gradienty fialovej a jemne odtienené fialovej, aby som vytvoril hladký prechod medzi rôznymi časťami dizajnu. Tieto gradienty dodávajú plagátu hĺbku a zároveň mu dodávajú moderný vzhľad.

Na vyváženie fialovej som použil niekoľko výrazných odtieňov žltej. Tieto žlté prvky slúžili ako kontrastné prvky voči fialovej palete a pridávali do dizajnu energiu a dynamiku. Kontrast medzi fialovou a žltou farbou pritiahne pozornosť diváka a robí plagát výrazným a zaujímavým.

* 1. Použitý text v plagáte

Text, ktorý som použil na plagáte, bol formulovaný tak, aby bol stručný a ľahko zrozumiteľný. Každý textový blok obsahoval esenciálny obsah, ktorý bol dôležitý pre pochopenie každého typu útoku. Cieľom bolo osloviť divákov a zaujať ich bez zbytočného preplnenia informáciami.

Okrem samotného opisu každého typu útoku som sa snažil pridať aj vysvetlenie, ako daný typ útoku funguje, a uviesť konkrétny príklad. Týmto spôsobom som divákom poskytol hlbšie pochopenie problematiky a ukázal im, ako tieto útoky môžu ohroziť bezpečnosť ich počítačových sietí.

Zvolil som vhodnú veľkosť textu, ktorá umožňuje ľahké čítanie aj z väčšej vzdialenosti, keď je plagát umiestnený na stene. Text bol písaný písmom Config Condensed, ktoré navrhol Adam Ladd a je bezplatne dostupný na stiahnutie. Tento font ponúka vysokú čitateľnosť a štýlový vzhľad, čo ho robí ideálnou voľbou pre tvorbu plagátov a iných dizajnových projektov.

Použitie textu a typografie s dôrazom na jasnosť, zrozumiteľnosť a estetiku bolo hlavne kľúčové pre efektívnu komunikáciu s divákmi a úspech plagátu ako prostriedku prezentácie mojej práce a poznatkov.

* 1. Cieľová skupina

Pri tvorbe plagátu som sa snažil zohľadniť potreby a záujmy rôznych skupín ľudí, ktorí by mohli mať záujem o problematiku kybernetickej bezpečnosti.

Ľudia so záujmom v oblasti IT a kybernetickej bezpečnosti sú jednou zo zameraných skupín. Pre nich som sa sústredil na poskytnutie hlbšieho a podrobnejšieho pohľadu na rôzne formy kybernetických útokov a ochranných opatrení. Ich odborné znalosti sú vysoké, takže som sa zameral na poskytnutie komplexných informácií a možností ochrany.

Študenti tvoria ďalšiu dôležitú cieľovú skupinu. Pre nich som sa snažil vytvoriť plagát s jednoduchým a zrozumiteľným jazykom, aby im poskytol prehľad o rôznych druhoch útokov a opatrení na ochranu. Ich záujem o rozšírenie vedomostí o kybernetickej bezpečnosti ma motivoval k tomu, aby som poskytol relevantné a zaujímavé informácie.

Zamestnanci a bežní používatelia počítačov predstavujú ďalšiu cieľovú skupinu, ktorej som sa snažil osloviť. Plagát bol navrhnutý tak, aby bol prístupný a relevantný pre každodenné použitie. Zameranie na praktické tipy a rady týkajúce sa ochrany pred kybernetickými hrozbami môže pomôcť zvýšiť povedomie o bezpečnosti a zabezpečiť lepšiu ochranu ich digitálnych zariadení.

Zohľadnenie potrieb a záujmov cieľovej skupiny bolo kľúčové pre úspešnú tvorbu plagátu, ktorý dokáže osloviť a informovať široké spektrum užívateľov s rôznymi úrovňami znalostí.

1. Záver

Bezpečnosť počítačových sietí je neustále sa rozvíjajúcim a kľúčovým aspektom v dnešnom digitálnom svete. Počítačové siete sú základným pilierom pre komunikáciu a vymieňanie informácií, čo ich robí nevyhnutnými pre fungovanie dnešných spoločností, podnikov aj jednotlivcov. S nárastom digitálnej transformácie a závislosti na technológiách však rastie aj riziko útokov a kybernetickej kriminality.

Hľadanie spôsobov, ako chrániť počítačové siete, si vyžaduje pohľad nielen na súčasné hrozby, ale aj na históriu bezpečnostných incidentov a technologický vývoj. Od prvých počítačových vírusov a malwaru až po sofistikované kybernetické útoky, ako sú ransomware či pokročilé phishingové techniky, sme svedkami neustálej evolúcie kybernetických hrozieb.

Identifikoval som niekoľko kľúčových hrozieb, ktoré ohrozujú bezpečnosť počítačových sietí, a to vrátane phishingu, spyware, ransomware, keyloggingu a distribuovaných odmietnutí služby (DoS a DDoS) útokov. Každý z týchto typov útokov vyžaduje individuálnu stratégiu na ochranu a prevenciu, zahŕňajúcu technické opatrenia, ako aj výchovné a osvetové aktivity.

Okrem technických opatrení je dôležité aj zvýšiť povedomie o bezpečnosti počítačových sietí medzi širokou verejnosťou, zamestnancami a manažérmi IT. Vytvorenie plagátu ako osvetového nástroja nám umožnilo vizuálne komunikovať hlavné bezpečnostné zásady a postupy, čím sme prispeli k zlepšeniu kybernetickej gramotnosti a povedomia o bezpečnosti v digitálnom prostredí.

Záverom môžeme konštatovať, že bezpečnosť počítačových sietí je dynamickou a neustále sa meniacou oblasťou, ktorá vyžaduje neustálu pozornosť a inovácie. Bezpečnosť počítačových sietí je záležitosťou každého, a preto je kľúčové, aby sme si uvedomili výzvy, ktoré predstavuje, a aktívne sa podieľali na ochrane našich digitálnych zdrojov a informácií. Len tak môžeme zabezpečiť bezpečnosť a dôvernosť digitálneho sveta pre súčasných aj budúcich používateľov.

Zoznam použitej literatúry

1. Radware, History of network security methods, Radware. Available at: <https://www.radware.com/resources/network_security_history.aspx/>
2. Januška, V. (2023) Infographic: The History of Network Security, IPXO. Available at: <https://www.ipxo.com/blog/infographic-history-of-network-security/>
3. Holovský, M. (2013) *Seznamte SE – dos a ddos útoky*. Available at: <https://www.security-portal.cz/clanky/seznamte-se-%E2%80%93-dos-ddos-%C3%BAtoky>
4. *Útoky ddos* (no date) *ESET*. Available at: <https://www.eset.com/sk/distribuovany-utok-odmietnutia-sluzby/>
5. Institut kvality, environmentu a B. (2022) ISO/IEC 27001 - Identifikácia hrozieb a zraniteľností, isocertifikat.sk. Available at: <https://isocertifikat.sk/iso-27001-identifikacia-hrozieb-a-zranitelnosti/>
6. Informačné a počítačové hrozby. In: ManagementMania.com [online]. Wilmington (DE) 2011-2024, 03.09.2016 [cit. 20.04.2024]. Dostupné z: <https://managementmania.com/sk/informacne-a-pocitacove-hrozby>
7. Phishing. In: ManagementMania.com [online]. Wilmington (DE) 2011-2024, 20.08.2015 [cit. 20.04.2024]. Dostupné z: <https://managementmania.com/sk/phishing>
8. Spyware. ManagementMania.com [online]. Wilmington (DE) 2011-2024, 06.10.2016 [cit. 24.04.2024]. Dostupné z: <https://managementmania.com/sk/spyware>
9. Ransomware. ManagementMania.com [online]. Wilmington (DE) 2011-2024, 03.09.2016 [cit. 25.04.2024]. Dostupné z: <https://managementmania.com/sk/ransomware>
10. Keylogging. In: ManagementMania.com [online]. Wilmington (DE) 2011-2024, 21.09.2016 [cit. 25.04.2024]. Dostupné z: <https://managementmania.com/sk/keylogging>
11. AuFayez Eliyan and AbstractSoftware Defined Networking, In SDN (2021) *DOS and ddos attacks in software defined networks: A survey of existing solutions and research challenges*, *Future Generation Computer Systems*. Available at: <https://www.sciencedirect.com/science/article/pii/S0167739X21000911>
12. Mudroň, M. (2020) *Vaše Balenie Je Pripravené na Doručenie: Podvodným E-mailom SA darí*, *MojAndroid.sk*. Available at: <https://www.mojandroid.sk/slovenska-posta-podvod-email/>
13. Abrams, L. (2017) *The week in Ransomware - September 1st 2017 - Locky, Exploit Kits, & more*, *BleepingComputer*. Available at: <https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-1st-2017-locky-exploit-kits-and-more/>
14. Kybernetická bezpečnosť: Hlavné hrozby v Roku 2021 (infografika): Témy: Európsky parlament (2022). Available at: <https://www.europarl.europa.eu/topics/sk/article/20220120STO21428/kyberneticka-bezpecnost-hlavne-hrozby-v-roku-2021-infografika>
15. Team, D. (2022) *A simple explanation of Vector Graphics & Illustrations*, *Digitional*. Available at: <https://www.digitional.com/a-simple-explanation-of-vector-graphics-illustrations/>
16. *Exploring spyware effects Martin Boldt | semantic scholar*. Available at: <https://www.semanticscholar.org/paper/Exploring-Spyware-Effects-Martin-Boldt-Carlsson-Jacobsson/0e966af3eed20053afaa397ca9ec9ce0e63a2e6e>
17. Popova, E. (2023a) Eugeniya Popova on linkedin, The leakage of confidential information is the most common consequence of successful cyberattacks on organizations in the third quarter of 2023. . Available at: <https://www.linkedin.com/posts/eugeniya-popova-b8425741_databbeach-cybersecurity-cyberattack-activity-7141724376881590272-pEaa>