STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Zabezpečenie koncových Zariadení**

**Matúš Lupták**

2024

Obsah (štýl Nadpis Kapitoly, bez čísla)

Úvod 4

1 Jadro práce 5

1.1 Názov podkapitoly 5

1.1.1 Názov časti podkapitoly 5

2 Ilustrácie, tabuľky, rovnice 6

2.1 Ilustrácie 6

2.2 Tabuľky 6

2.3 Zdrojový kód programu 7

2.4 Rovnice, vzorce 7

3 Záver 8

Zoznam použitej literatúry 9

Prílohy 10

Príloha A – CD médium 10

Príloha B – Metodické listy 10

Príloha C – Dotazník 10

Poznámka: Obsah formátujte tak, aby sa zmestil celý na stranu 2

Anotácia

Táto práca sa zameriava na súčasné trendy a výzvy v oblasti zabezpečenia koncových zariadení v informačnej technológii. Analyzujeme metódy a nástroje na ochranu koncových zariadení, vrátane antivírusových programov, firewallov, softvéru EDR a MDM. Rovnako sa venujeme 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 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 pomáha chrániť ich 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.

* 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 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.

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 hakerom 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 (trojanský 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 podezrivé 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 podezrivé 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.

* 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
     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 detegovať 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. Ako funguje moderné riešenie kybernetickej bezpečnosti ?

1. Ilustrácie, tabuľky, rovnice

V práci sa môžu vyskytovať okrem slovného textu aj informácie vyjadrené v obrazovej forme a symbolmi.

* 1. Ilustrácie

**Ilustrácie** sú obrázky obsahujúce **grafy**, **diagramy**, **mapy**, **schémy** a pod. Nie je potrebné rozlišovať rozličné typy ilustrácií, stačí, ak sa všetky označia ako „Obrázok”. Všetky ilustrácie musia byť očíslované súvislým radom číslic v celej práci a musia mať titulky (názov obrázku) pri každom obrázku. Text titulku musí byť pochopiteľný aj bez kontextu. Majú sa zaradiť bezprostredne za textom, kde sa spomínajú po prvýkrát (najlepšie na tej istej strane). Obrázok by mal byť podľa možnosti centrovaný. Pri odkazovaní na daný obrázok v texte použijeme odkaz uvedený v zátvorke (napr. Obr. 1).



Obr. 1 Názov obrázka (štýl Popis, Popiska-Caption)

* 1. Tabuľky

Tabuľky prezentujú myšlienky a tvrdenia popisované v práci. Akýkoľvek tabuľkový materiál, ktorý sa skladá z viac než štyroch alebo piatich riadkov, by mal byť spracovaný do formy tabuľky. Popis a záhlavie tabuľky má byť zrozumiteľné samostatne bez odkazu na text. Záhlavia majú vyjadrovať druh veličiny a typy jednotiek vo forme „veličina/jednotka”, je potrebné používať rovnaké symboly a skratky ako v texte. Každá tabuľka musí mať poradové číslo a titulok, umiestnený zvyčajne nad tabuľkou. Tabuľka by mala mať rovnakú orientáciu, ako text práce.

Tab. 1 Názov tabuľky (štýl Popis, Popiska-Caption)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1.A | 1.B | 1.C | 1.D |
| prezentácie | 10 | 12 | 13 | 11 |
| videá | 7 | 4 | 6 | 3 |
| počítačové hry | 5 | 6 | 3 | 4 |
| blogy | 6 | 8 | 7 | 8 |
| postery | 4 | 3 | 5 | 6 |

* 1. Zdrojový kód programu

Na zápis zdrojového kódu programu použijeme štýl kód (písmo Courier New 11, zarovnanie vľavo, orámovanie s tieňom).

viem hľadajCestu

  kým [farbabodu <> "čierna] [vz 1]

  do 1 vp 90

  kým [farbabodu <> "červená] [

   vp 90 do 1

   ak farbabodu = "čierna [

    vz 1 vl 90 do 1

    ak farbabodu = "čierna [vz 1 vl 90]

   ]

   čakaj 1

  ]

koniec

* 1. Rovnice, vzorce

Rovnice sa uvádzajú v strede riadka, vysvetlivky symbolov na začiatku riadku. Vysvetlivky symbolov sa uvádzajú od začiatku riadka. Ak je v práci viac vzorcov, uvádzame číslo vzorca do okrúhlych zátvoriek bez medzier umiestnených na pravom konci riadka. Pre písanie fyzikálnych veličín a matematických premenných sa používa kurzíva. Používame sústavu jednotiek SI (ISO 31 a ISO 1001). Pri písaní rovníc používame **editor rovníc (musíme ho mať nainštalovaný)**.

1. Záver

Záver obsahuje vecné závery, sumarizáciu, vlastný prínos alebo pohľad autora, odporúčania pre prax (výučbu). Záver je uvedený na maximálne 1 stranu.

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla)

Všetky dokumenty, ktoré v práci použijete, je potrebné zoradiť do zoznamu pozostávajúceho z  bibliografických odkazov, ktorý označujeme **Zoznam použitej literatúry**. Pre tvorbu zoznamov použitej literatúry platia štandardy. Cieľom je, aby zo zoznamu použitej literatúry bolo možné jasne identifikovať použitý zdroj a aby ho bolo možné bez ťažkostí opäť vyhľadať.

Hlavným zdrojom údajov pre tvorbu bibl. odkazov je **titulný list** (tzn. prvý list v knihe, kde sú uvedené údaje o názve autorovi atď.), príp. jeho rub. Odkazy sa môžu týkať knižných, časopiseckých a iných zdrojov informácií (zborníky z konferencií, patentové dokumenty, normy, odporúčania, kvalifikačné práce, osobná korešpondencia a rukopisy, odkazy cez sprostredkujúci zdroj, elektronické publikácie), ktoré boli v práci použité.

**Technika citovania** určuje spôsob, akým označujeme citácie v dokumente, pričom podľa normy (pozri STN ISO 690) existuje viacero spôsobov citovania. Pri metóde **číselných citácií** sa v zozname bibliografických odkazov každé citované dielo uvádza v tom poradí, v akom bolo uvedené a číslované v texte. Číslované odkazy v texte sú uvedené v zátvorkách [3] a odkazujú na dokumenty v takom poradí, v akom sa citujú po prvýkrát. Nasledujúce citácie dostávajú také isté číslo, ako má prvá citácia. Ak sa citujú osobitné časti dokumentu, môžu sa za číslom citácie uviesť čísla strán.

**Príklad zoznamu použitej literatúry:**

1. KALAŠ, Ivan – BLAHO, Andrej: *Tvorivá informatika. 1. zošit z programovania.* Bratislava: SPN - Mladé letá, 2007. 48. s. ISBN 80-10-01723-2
2. CIMBALA, Roman – BALOGH, Jozef – DŽMURA, Jaroslav: Diagnostika výkonových transformátorov s využitím prvkov umelej inteligencie 1. In: *Elektrotechnický magazín ETM*. roč. 14, č. 1 (2004), s. 8-9.
3. Kolektív autorov: *Štátny vzdelávací program*. [online] Bratislava: ŠPU v Bratislave, 2008. Aktualizované 14.2.2010 [cit. 2010-02-17]. Dostupné na internete: <http://new.statpedu.sk/sk/filemanager/download/987>
4. Elektronické diplomové a dizertačné práce SR: ETD SK. [online]. Košice : ETD SK, 2004. Aktualizované 14-2-2005 [cit 2005-03-10]. Dostupné na internete: <http://www.etd.sk/>.
5. KATUŠČÁK, Dušan: *Ako písať záverečné a kvalifikačné práce*. Nitra: Enigma, 2004. 162 s. il. ISBN 80-89132-10-3

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>