STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Bezpečnosť na internete**

Vonkajšia aj vnútorná

**Michal Halagačka**

2013

Obsah (štýl Nadpis Kapitoly, bez čísla)

Obsah (štýl Nadpis Kapitoly, bez čísla) 2

Anotácia (štýl Nadpis Kapitoly, bez čísla) 3

1 Internetová bezpečnosť 4

1.1 Prečo je Internetová bezpečnosť dôležitá 4

1.1.1 Krádež identity 4

1.1.2 Krádež údajov 4

2 VPN siete 5

2.1 Čo je to VPN 5

2.2 Čo robia VPN a prečo ich používať 5

2.3 Ich využitia 5

3 Ochrana Firewallom 6

3.1.1 Typy Firewallov 6

3.1.2 Spôsoby ochrany Firewallom 6

3.2 Záleží na type Firewall pri spôsoboch ochrany? 6

Ilustrácie, tabuľky, rovnice 8

3.3 Ilustrácie 8

3.4 Tabuľky 8

3.5 Zdrojový kód programu 9

3.6 Rovnice, vzorce 9

4 Záver 10

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 11

Prílohy (štýl Nadpis Kapitoly, bez čísla) 12

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla) 12

Príloha B – <názov prílohy> 12

Príloha C – <názov prílohy> 12

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

Anotácia (štýl Nadpis Kapitoly, bez čísla)

**Annotation**

1. Internetová bezpečnosť

Internet je plný nebezpečenstiev. Pomaly každý má osobné údaje niekde uložené na internete, či ich tam mať chceme a či nie, ale málo z nás si uvedomuje spôsoby, ktorými sú chránené pred hackermi a ďalšími nežiadanými osobami. Spôsoby ochrany dokážeme kategorizovať na vonkajšie (VPN) a vnútorné (Firewall).

* 1. Prečo je Internetová bezpečnosť dôležitá

Bez zavedených bezpečnostných opatrení je možné prezerať, zachytávať a dokonca ukradnúť súkromné ​​alebo dôverné informácie alebo správy. V závislosti od zámeru vniknutia sa môže čin hackera pohybovať od neškodných, ako je prieskum trhu, až po zničujúce, ako je krádež identity alebo iný podvod. Vlády a spoločnosti s citlivými informáciami sú tiež ohrozené, pretože ich vlastné informácie sú často cenné a tiež uchovávajú súkromné ​​informácie o jednotlivcoch, ako sú zákazníci alebo zamestnanci.

* + 1. Krádež identity

Krádež identity je prevládajúcim problémom v informačnom veku, pretože ľudia nakupujú, predávajú a vymieňajú si informácie online. Bez dostatočného zabezpečenia môžu online transakcie viesť k tomu, že podvodníci získajú informácie o vašej kreditnej karte, osobné údaje a dokonca aj číslo sociálneho poistenia. S týmito informáciami môžu vykonávať podvodné poplatky a nákupy, brať si pôžičky, žiadať o štátne dávky a spôsobiť zmätok vo vašom súkromnom živote. Aj keď vo všeobecnosti môžete všetko vyriešiť, odstránenie škody spôsobenej zlodejom identity si vyžaduje čas, úsilie a v niektorých prípadoch aj náklady.

* + 1. Krádež údajov

Ďalším problémom je krádež údajov, pri ktorej sa digitálne kradnú citlivé alebo osobné údaje, ako sú videá, dokumenty a fotografie. Tieto informácie sa potom môžu ďalej predávať alebo distribuovať na nezákonné účely. Spoločnosti riskujú stratu dôležitých testovacích údajov, dôverných finančných súborov, obchodných tajomstiev, návrhov produktov a ďalších údajov od zlodejov údajov. Vládam hrozí odcudzenie citlivých materiálov vrátane údajov o prebiehajúcich výskumných projektoch, osobnej korešpondencie medzi jednotlivcami a zoznamov s podrobnosťami o vojenských rozmiestneniach, stratégiách a menách agentov v zahraničí.

1. VPN siete
   1. Čo je to VPN

VPN (Virtual Private Network) vytvára digitálne spojenie medzi vaším počítačom a vzdialeným serverom vo vlastníctve poskytovateľa VPN, čím vytvára point-to-point tunel, ktorý šifruje vaše osobné údaje, maskuje vašu IP adresu a umožňuje vám obísť bloky webových stránok a brány firewall na internete. . To zaisťuje, že vaše online skúsenosti sú súkromné, chránené a bezpečnejšie.

* 1. Čo robia VPN a prečo ich používať

VPN alebo virtuálne súkromné ​​siete umožňujú používateľom bezpečný prístup k súkromnej sieti a zdieľanie údajov na diaľku prostredníctvom verejných sietí. Podobne ako brána firewall chráni vaše údaje vo vašom počítači, siete VPN ich chránia online. A zatiaľ čo VPN je technicky WAN (Wide Area Network), frontend si zachováva rovnakú funkčnosť, bezpečnosť a vzhľad ako v súkromnej sieti.

Zvyčajne sa používajú v menej zabezpečených sieťach, ako je napríklad verejný internet. Poskytovatelia internetových služieb (ISP) majú zvyčajne dosť veľký prehľad o činnostiach zákazníka. Navyše, niektoré nezabezpečené prístupové body Wi-Fi (AP) môžu byť pre útočníkov pohodlnou cestou, ako získať prístup k osobným údajom používateľa. Používateľ internetu by mohol použiť sieť VPN, aby sa vyhol týmto zásahom do súkromia.

* 1. Ich využitia

Sieť VPN možno použiť na skrytie histórie prehliadača používateľa, adresy internetového protokolu (IP) a geografickej polohy, webovej aktivity alebo používaných zariadení. Nikto v rovnakej sieti nebude môcť vidieť, čo robí používateľ VPN. Vďaka tomu sú siete VPN ideálnym nástrojom na ochranu súkromia online.

1. Ochrana Firewallom
   1. Čo je to Firewall \*

Firewall je sieťové bezpečnostné zariadenie, či software, ktorý sleduje prichádzajúcu a odchádzajúcu sieťovú prevádzku. Z môjho výskumu na internete majú Firewally 4 limitácie. 1) Nezastaví používateľov od získavania údajov na zlomyseľných stránkach. 2) Nevedia ochrániť organizácie od sociálneho inžinierstva. 3) Ak systém už bol nainfikovaný tak Firewall vírus nenájde pokiaľ nevyšle niečo cez sieť, ktorú sleduje Firewall. 4) Firewall nevie zabrániť hackerom používať.

* 1. Začiatky Firewallov

Firewall bol prvou ochranou pre sieťové komunikácie. Existovali asi tak dlho ako routere, od približne 1985 avšak prvý papier rozoberajúci filtrovací proces používaný, v tej dobe ešte novým, ochranným spôsobom nevyšiel až do 1988. Napísal ho Jeff Mogul z Digital Equipment Corporation. V rokoch 1989-1990, Dave Presotto a Howard Trickey z AT&T Bell Laboratories vynašli druhú generáciu firewall štruktúry, taktiež nazývané ’Firewally na úrovni okruhu’ (circuit level firewalls) a taktiež implementovali prvý fungujúci model tretej generácie firewallov.

* 1. Typy Firewallov

Firewally môžeme rozlišovať na dva druhy, a to sú Hardware Firewall a Software Firewall. Fungujú dosť rozlične od seba ale spĺňajú ten istý ciel a to je bezpečnosť na internete. Software Firewally ochraňujú hosťa, teda zariadenie na ktorom bežia ako napríklad stolný počítač, či mobilný telefón. Hardware Firewall naopak ochraňuje sieť, ku ktorej je pripojená. Vďaka týmto rozdielom ich občas voláme hosťovská Firewall a sieťová Firewall. Ďalší rozdiel by bol v tom, že software Firewall je program, ktorý beží na osobnom zariadení a hardware býva samostatné zariadenie

* + 1. Ako ochraňuje hosťovská Firewall

Ochraňuje len jedno zariadenie, ale príde pribalená s operačným systémom. Softwarové Firewally ochraňujú. Najbežnejší druh Firewallu, ktorý je možné nájsť na väčšine osobných funguje tým, že prehľadáva si prichádzajúce či odchádzajúce údaje a porovnáva ich s listom nebezpečenstiev. Ak sa data packet rovná profilu známeho nebezpečenstva, zahodí ho.

* + 1. Ako ochraňuje sieťový Firewall

Hardware Firewall funguje ako samostatný spotrebič, ktorý sleduje 3. a 4. OSI vrstvy a skenuje prevádzku medzi vonkajšími zdrojmi a lokálnou sieťou alebo medzi segmentami v sieti. Pakety monitorujú hlbokou inšpekciou. Ak paket nespĺňa predtým vybraté kritéria, podľa pravidiel vybraných správcom siete, komunikácia bude odmietnutá a zablokovaná.

1. Produkt

Podarilo sa mi spraviť prezentáciu pripravenú ako edukačný materiál. Cieľom bolo dať ľudom možnosť sa naučiť niečo nové a užitočné. Z dokumentačných dôvodov by som chcel rozobrať môj proces pri tvorbe tohto projektu.

* 1. Myšlienka

Celý projekt začal myšlienkou ochrany a bezpečnosti na internete. Bol som dosť inšpirovaný hodinami počítačovej vedy, kde sme preberali, aj keď len zľahka oproti nejakému sieťarskému odboru, sieťové technológie a veľkým počtom reklám, ktoré bolo nemožné si nevšimnúť, všetky rozprávajúce o VPN-kách a Firewalloch. Chcel som nielen aby to bolo niečo z témou internetovej bezpečnosti, ale aby to bolo aj niečo dostatočne komplexné, nech sa mi oplatí naučiť sa o danej téme vo voľnom čase. Popravde mi prišlo ako zaujímavá látka, ktorú som nikdy neskúsil študovať aj keď som celkom dosť chcel.

* 1. Prezentácia

Na môj produkt som si vybral učebný materiál, práve pretože som sa cítil sebavedomo o tvorení niečoho, z čoho by sa mohli iný ľudia niečo naučiť. Rozhodoval som sa medzi tvorením semi-dokumentácie na celú túto látku a dizajnovaním prezentácie, ako nám tvoria, alebo nájdu, naši učitelia. Finálne som sa rozhodol, že učebný materiál bude prezentácia, ktorá preberie hlavné myšlienky tejto témy tak, aby sa z nej mohol naučiť aj niekto mimo školy. To znamenalo, že text by nemal byť moc komplexný a nemalo by ho tam byť až moc veľa, ak by zas text bol moc krátky alebo moc zjednodušený na to, aby sa z neho dalo niečo užitočné naučiť, musel by som celý produkt prerábať. V poslednej dobe som taktiež viacej experimentoval z prezentáciami, čo som chcel už dlhšiu dobu a tento učebný materiál bol hlavný motivátor, prečo som sa v PowerPointe začal viacej realizovať.

* + 1. Obsah Prezentácie

Obsah prezentácie je nakoniec tvorený siedmimi stranami edukačného textu. Rozdelil som ho na dve hlavné časti, generálne a viacej upresnené informácie. Prvý slide uvádza názov učebného materiálu “Bezpečnosť na internete”, rovnako ako aj meno autora, mňa. Aby čitateľ mohol aspoň približne zistiť čo sa môže potenciálne naučiť, na druhom slide nasleduje obsah prezentácie. Ďalej je prvý slide s edukačným textom, ktorý otvára z jemným čitateľa, teda úvod do prezentácie, kde spomínam ako používatelia internetu môžu byť v nebezpečenstve bez ich vedomosti, v snahe dať nalákať ich do pokračovaného čítania. Bez žiadnych klamstiev v tomto slide som veril, že ak bol niekto zaujatý prvou textovou stranou, kde spomeniem potenciálnu hrozbu internetu a prečíta si ďalší slide, v ktorom môžem toto tempo dôležitých informácií pokračovať. Je dôležité pre asi každého autora vedieť čitateľa zaujať dostatočne na to, aby si prečítal hlavné, alebo aj dlhšie časti učebného materiálu. Myslím si, že dobre vysvetlená látka je tá, ktorá nielen ide do podrobností, ale ide do nich pomocou nepreťažovania čitateľa rovnako ako aj zaujímavým či zábavným spracovaním. Z mojich skúseností, ľudia sú prirodzene zvedaví, predsa činnosť učenia sa nových vecí môže byť celým dobrodružstvom. Niektorí ľudia sa dokážu pokúšať o seba zlepšenie a učenie sa nových vecí celý ich život. Avšak na to aby títo ľudia o sebe vôbec zistili, že danú činnosť zbožňujú, je potrebné ich nejak zaujať. Koľkokrát sme predsa všetci čítali či aj videli osobu, ktorá začala žiť pre niečo čoho sa nechcela ani dotknúť po náhodne inšpiratívnom momente.

* ----- STAREEE -----
  1. Záleží na type Firewall pri spôsoboch ochrany?

Yes, the distinction between hardware and software firewalls is relevant to the type of packet filtering employed, as each type serves a specific purpose and is implemented differently:

Hardware Firewall with Packet Filtering:

1. A hardware firewall is typically a standalone device designed to protect an entire network. It is often deployed at the perimeter, between an organization's internal network and the external network (usually the internet). Hardware firewalls can perform packet filtering, inspecting individual packets of data based on predetermined rules. These rules define what types of traffic are allowed or blocked. The hardware firewall evaluates packets at the network or transport layer, and its decisions impact all devices connected to the network.
2. Software Firewall:

A software firewall, on the other hand, is installed directly on an individual device, such as a computer or a server. It operates at the operating system or application layer, providing a more granular control over the traffic that enters or leaves the specific device. Software firewalls also employ packet filtering techniques, but they focus on the traffic specific to the device on which they are installed. They can filter packets based on application-specific criteria, providing additional security at the device level.A

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>