STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Zabezpečenie zariadení na sieti**

**Maxim Frühwald**

2024

Obsah (štýl Nadpis Kapitoly, bez čísla)

Obsah (štýl Nadpis Kapitoly, bez čísla) 2

Anotácia (štýl Nadpis Kapitoly, bez čísla) 3

1 Stratégie v zabezprečení 4

2 Čo je to firewall 4

2.1 História firewallu 3

2.1.1 Prvé generácie (80. a 90. roky) 3

2.1.2 Vývoj v 90. rokoch 3

2.1.3 Firewally s aplikačnou podporou 3

2.1.4 Moderné firewally 3

2.2 Sieťový firewall 4

2.3 Aplikačný firewall 3

2.4 Rovnice, vzorce 3

3 Záver 5

Zoznam použitej literatúry (Nadpis Kapitoly, bez čísla) 6

Prílohy (štýl Nadpis Kapitoly, bez čísla) 7

Príloha A – CD médium (štýl PodNadpis Kapitoly, bez čísla) 7

Príloha B – <názov prílohy> 7

Príloha C – <názov prílohy> 7

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

Anotácia (štýl Nadpis Kapitoly, bez čísla)

**Annotation**

1. Stratégie v zabezprečení

Zabezpečenie zariadení v sieti je dnes kritickým aspektom v digitálnom svete, kde sa technológie rýchlo rozvíjajú a naše spoločnosti sa stále viac digitalizujú. Zabezpečenie zahŕňa ochranu širokej škály zariadení, od osobných počítačov a smartfónov až po priemyselné zariadenia a IoT (Internet of Things) zariadenia, ktoré sa stávajú neoddeliteľnou súčasťou našich domácností aj pracovných prostredí.

S rozvojom technológií sa však zvyšuje aj počet a sofistikácia hrozieb, ktorým sú tieto zariadenia vystavené. Medzi tieto hrozby patrí malware, phishing, ransomware, DDoS útoky a mnoho ďalších, ktoré môžu ohroziť integritu, dostupnosť a dôvernosť našich údajov a informácií.

Preto je dôležité, aby sme implementovali opatrenia na minimalizovanie rizík týchto hrozieb a chránili naše zariadenia a siete. Medzi základné prvky zabezpečenia patria firewally, antivírové programy, šifrovanie údajov, aktualizácie softvéru a pravidelné zálohovanie. Tieto nástroje nám pomáhajú zabezpečiť naše zariadenia a zvýšiť úroveň ochrany pred rôznymi hrozbami.

Navyše, s rastom technológií sa vyvíjajú aj sofistikovanejšie metódy zabezpečenia, ako je biometrická autentifikácia, umelej inteligencie pre detekciu hrozieb a sieťové segmentácie. Tieto pokročilé techniky nám poskytujú ešte vyššiu úroveň bezpečnosti a umožňujú nám efektívnejšie chrániť naše zariadenia a dáta pred rôznymi typmi útokov.

Pochopenie tejto problematiky a používanie najlepších postupov v oblasti zabezpečenia zariadení v sieti je kľúčové pre ochranu našich súkromných údajov a citlivých informácií. Táto zodpovednosť sa týka nielen jednotlivcov, ale aj organizácií všetkých veľkostí, ktoré majú povinnosť chrániť údaje svojich zákazníkov a zamestnancov.

Vzhľadom na neustále sa meniacu povahu hrozieb je dôležité, aby sme sa neustále vzdelávali a informovali o nových vývojoch v oblasti kybernetickej bezpečnosti a aby sme boli pripravení čeliť novým výzvam, ktoré môžu vzniknúť v dnešnom digitálnom prostredí. To znamená, že by sme mali byť aktívne zapojení do vzdelávania a implementácie nových bezpečnostných opatrení a technológií, aby sme ochránili naše zariadenia a dáta pred neustále sa meniacimi hrozbami.

1. Čo je to firewall

Firewall je komplexný bezpečnostný nástroj, ktorý hrá kľúčovú úlohu v ochrane počítačových sietí pred neoprávnenými prístupmi a škodlivým softvérom. Jeho funkcia spočíva v monitorovaní, riadení a filtrovaní toku dát medzi rôznymi časťami siete a medzi sieťou a vonkajším prostredím, ako je internet.

Existuje niekoľko druhov firewallov, ktoré sa používajú na rôzne účely a na rôznych úrovniach komunikácie:

1. Sieťový firewall : Tento typ firewallu funguje na základe adries IP, portov a protokolov. V podstate vytvára "bránu" medzi internou a externou sieťou a rozhoduje o tom, ktoré dáta sú povolené a ktoré sú zablokované na základe preddefinovaných pravidiel. Môže fungovať ako brána medzi vnútornou a vonkajšou sieťou (tzv. "brána prehlasovania") alebo ako samostatné zariadenie.
2. Aplikačný firewall : Tento typ firewallu funguje na vyššej úrovni v sieti, na aplikačnej vrstve. Dokáže špecifikovať povolenia na základe konkrétnych aplikácií a protokolov, čím zabezpečuje kontrolu komunikácie. Napríklad môže rozumieť obsahu HTTP požiadaviek a odpovedí a môže filtrovať prístup na základe obsahu alebo typu súborov.

Firewall môže byť implementovaný rôznymi spôsobmi:

Hardvérové riešenia : To sú samostatné zariadenia navrhnuté špeciálne na účely firewallu. Majú vlastný hardvér a softvér optimalizovaný pre rýchle a efektívne filtrovanie dát.

Softvérové riešenia : Tieto sú implementované ako programy na existujúcich počítačoch alebo sieťových zariadeniach a poskytujú firewallové funkcie softvérovým spôsobom.

Firewall zohráva kľúčovú úlohu pri ochrane sietí pred rôznymi hrozbami, vrátane útokov typu DDoS, malware, ransomware, phishing a ďalších. Jeho konfigurácia sa zvyčajne riadi súborom pravidiel, ktoré administrátor nastavuje podľa potrieb a požiadaviek siete. Aktívne a efektívne používanie firewallu je jedným z najzákladnejších prvkov pre zabezpečenie moderných počítačových sietí.

* 1. História firewallu

História firewallu sa začína v 80. a 90. rokoch minulého storočia, keď sa siete začali rozvíjať a komunikácia cez internet sa stala štandardom. Prvé formy firewallu boli základné, a často sa jednalo o softvérové nástroje vykonávajúce jednoduché filtrovanie dát na úrovni IP adries a portov.

* + 1. Prvé generácie (80. a 90. roky)

Prvé firewally sa objavili ako softvérové aplikácie na operačných systémoch Unix a boli známe ako "packet filter" firewally. Tieto nástroje boli schopné filtrovať sieťový tok na základe IP adries, portov a protokolov. V tejto dobe neboli firewally považované za samostatné zariadenia, ale skôr za súčasť sieťového softvéru

* + 1. Vývoj v 90. rokoch

V 90. rokoch sa začali objavovať firewally s lepšími možnosťami kontroly, ako napríklad Stateful Inspection. Tieto firewally boli schopné sledovať stav sieťovej komunikácie a povoliť alebo zablokovať dáta na základe kontextuálnych informácií o spojeniach.

* + 1. Firewally s aplikačnou podporou

V 2000. rokoch sa začali objavovať firewally s pokročilejšou aplikačnou kontrolou. Tieto firewally mohli robiť rozhodnutia na základe obsahu dát a súvislostí s konkrétnymi aplikáciami, nie len na základe IP adries a portov. Tento typ firewallu umožňuje presnejšie filtrovanie dát a je schopný identifikovať a blokovať škodlivý obsah.

* + 1. Moderné firewally

Dnešné firewally kombinujú rôzne techniky filtrovania dát, vrátane aplikačnej kontroly, detekcie hlbokých údajov (DPI), protokolovania a správy udalostí. Okrem toho sú firewally často integrované s ďalšími bezpečnostnými funkciami, ako sú antivírové programy, systémy detekcie útokov (IDS/IPS) a filtre pre obsah internetu. V súčasnosti sú firewally neoddeliteľnou súčasťou zabezpečenia siete a sú nasadené vo všetkých druhoch prostredí, od domácich sietí po veľké korporátne siete a poskytujú kritickú ochranu pred mnohými hrozbami z internetu. Ich funkcie a schopnosti sa neustále vyvíjajú, aby dokázali zvládnuť nové a sofistikovanejšie hrozby.

* 1. Sieťový firewall

Sieťový firewall, známy aj ako rozhranie, je bezpečnostné zariadenie alebo softvér, ktorý funguje na úrovni sieťovej vrstvy OSI modelu (Open Systems Interconnection). Jeho hlavnou úlohou je chrániť sieť pred neoprávnenými prístupmi a škodlivými útokmi, kontrolujúc tok dát medzi internými a externými časťami siete a medzi sieťou a vonkajším prostredím, ako je internet.

Funkcie sieťového firewallu zahŕňajú:

1. Filtrovanie paketov: Firewall analyzuje pakety údajov prichádzajúce do siete a rozhoduje, či ich povoliť alebo zablokovať na základe preddefinovaných pravidiel. Tieto pravidlá môžu zahŕňať informácie o zdrojových a cieľových IP adresách, portoch a používaných protokoloch.
2. Stateful Inspection: Táto technika umožňuje firewallu sledovať stav sieťovej komunikácie a vytvárať dynamické pravidlá na základe kontextuálnych informácií o spojeniach. To umožňuje firewallu robiť rozhodnutia na základe stavu spojenia a nielen na základe jednotlivých paketov.
3. Virtuálne súkromné siete (VPN): Niektoré sieťové firewally majú schopnosť vytvárať VPN tunely, ktoré umožňujú bezpečnú komunikáciu medzi vzdialenými sieťami alebo zariadeniami cez verejný internet.
4. NAT (Network Address Translation): Firewall môže vykonávať funkciu NAT, ktorá prekladá interné IP adresy na verejné IP adresy a umožňuje viacerým zariadeniam v sieti komunikovať so zariadeniami mimo siete cez jedinú verejnú IP adresu.
5. Logging a správa udalostí: Firewall môže zaznamenávať informácie o sieťovej prevádzke a udalostiach, ako sú pokusy o neoprávnený prístup alebo pokusy o útoky, čo pomáha administrátorom sledovať a analyzovať bezpečnostné incidenty.

Sieťový firewall môže byť implementovaný ako hardvérové zariadenie alebo softvérové riešenie na serveri alebo osobnom počítači. Jeho konfigurácia sa zvyčajne riadi súborom pravidiel, ktoré administrátor nastavuje podľa potrieb a požiadaviek siete. Je to kľúčový prvok v ochrane siete pred rôznymi hrozbami a neoprávnenými prístupmi.

* 1. Aplikačný firewall

Aplikačný firewall, známy tiež ako firewall na aplikačnej úrovni alebo aplikačná brána, je výkonný bezpečnostný nástroj, ktorý poskytuje komplexnú ochranu pred škodlivým softvérom a neoprávnenými prístupmi v sieťach. Jeho účelom je monitorovať, filtrovať a riadiť tok dát, ktoré prechádzajú cez sieť, s dôrazom na aplikačnú vrstvu OSI modelu, čím poskytuje úroveň kontroly a zabezpečenia, ktorá je zložitejšia a sofistikovanejšia ako u tradičných sieťových firewallov. Jedným z hlavných prvkov aplikačného firewallu je aplikačná kontrola, ktorá umožňuje sledovať a identifikovať špecifické aplikácie a protokoly v sieťovej komunikácii. Táto schopnosť umožňuje firewallu efektívne rozhodovať o tom, ktoré aplikácie sú povolené a ktoré sú zablokované na základe definovaných pravidiel a politík zabezpečenia.

Okrem toho aplikačný firewall poskytuje filtrovanie obsahu, čo znamená, že môže analyzovať obsah dát a identifikovať škodlivý obsah, ako sú malvéry, phishingové pokusy, alebo nevhodný obsah, a následne ho zablokovať alebo upozorniť administrátora na možnú hrozbu. Táto funkcia je zvlášť dôležitá v prípade webstránok a aplikácií, ktoré sú vystavené riziku útokov z internetu.

Ďalšou dôležitou funkciou aplikačného firewallu je schopnosť protokolovania a správy udalostí. Firewall dokáže zaznamenávať udalosti a spravovať ich, čo umožňuje administrátorom sledovať sieťovú prevádzku, identifikovať potenciálne hrozby a reagovať na ne včas. Táto viditeľnosť a možnosť analýzy udalostí je kľúčová pre účinnú ochranu siete a prevenciu bezpečnostných incidentov.

Ďalej, aplikačný firewall môže poskytovať aj funkcie na prevenciu útokov, ako sú SQL injection útoky, XSS (cross-site scripting) útoky a ďalšie. Tieto funkcie pomáhajú chrániť webové aplikácie a serverové zdroje pred zneužitím a zraniteľnosťami, čo prispieva k celkovej bezpečnosti siete a aplikácií.

Celkovo je aplikačný firewall kľúčovým prvkom v moderných sieťových infraštruktúrach, ktorý pomáha organizáciám dosiahnuť vyššiu úroveň zabezpečenia a ochrany pred rôznymi hrozbami a útokmi. Jeho pokročilé funkcie a schopnosti poskytujú kontrolu nad sieťovou prevádzkou a umožňujú efektívnu detekciu a prevenciu bezpečnostných hrozieb.

* 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>