STREDNÁ PRIEMYSELNÁ ŠKOLA ELEKTROTECHNICKÁ

**Zabezpečenie zariadení na sieti**

**Maxim Frühwald**

2024

Obsah

Obsah 2

Anotácia 3

1 Stratégie v zabezpečnení 4

2 Čo je to firewall 5

2.1.1 Prvé generácie (80. a 90. roky) 6

2.1.2 Vývoj v 90. rokoch 6

2.1.3 Firewally s aplikačnou podporou 6

2.1.4 Moderné firewally 6

2.2 Aplikačný firewall 7

3 Šifrovaný prenos dát 8

3.1 Ako a kde funguje 8

4 Tvorba Produktu 10

4.1 Obsah produktu 11

4.1.1 Antivírus 11

4.1.2 Firewall 12

4.1.3 VPN 13

5 Záver 15

Zoznam použitej literatúry 3

Anotácia

V dnešnej digitálnej ére, kedy je konektivita a využívanie sietí neoddeliteľnou súčasťou našich životov, je zabezpečenie našich zariadení na sieti kľúčovým aspektom pre ochranu citlivých údajov a zachovanie kybernetickej bezpečnosti. V tejto práci sa budem venovať problematike zabezpečenia zariadení na sieti, s dôrazom na tri kľúčové oblasti: firewall, antivírusovú ochranu a šifrovanie dát. V rámci tejto práce preskúmam princípy, technológie a implementáciu týchto bezpečnostných opatrení, ako aj ich význam a vplyv na ochranu našich zariadení a sietí pred kybernetickými hrozbami. Cieľom bude poskytnúť môj pohľad na problematiku zabezpečenia zariadení na sieti a zvýšiť povedomie o dôležitosti kybernetickej bezpečnosti v dnešnej digitalizovanej spoločnosti.

**Annotation**

In today's digital era, where connectivity and networking are an integral part of our lives, securing our networked devices is a key aspect of protecting sensitive data and maintaining cyber security. In this work, I will focus on the issue of securing devices on the network, with an emphasis on three key areas: firewall, antivirus protection and data encryption. As part of this work, I will examine the principles, technologies and implementation of these security measures, as well as their importance and impact on protecting our devices and networks from cyber threats. The goal will be to provide my perspective on the issue of securing devices on the network and raise awareness of the importance of cyber security in today's digitalized society.

1. Stratégie v zabezpečnení

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, umelé 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:

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.

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.

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.

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:

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.

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.

Virtuálne súkromné siete (VPN): Niektoré sieťové firewally majú schopnosť vytvárať VPN tunely, ktoré umožňujú bezpečnú komunikáciu medzi vzdialenými sieťami alebo zariadeniami cez verejný internet.

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.

* 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.

1. Šifrovaný prenos dát

Šifrovaný prenos dát cez sieť je kľúčovou technikou na zabezpečenie súkromia a bezpečnosti pri prenose citlivých informácií cez verejné siete, ako je internet. Táto metóda spočíva vo transformácii jasne čitateľného textu (tzv. plaintext) do nečitateľnej formy (tzv. ciphertext) pomocou šifrovacieho algoritmu a kľúča. Šifrovaný prenos dát je kľúčový pre ochranu citlivých informácií pred neoprávneným prístupom a útokmi tretích strán. Pomáha zabezpečiť, že iba autorizované osoby sú schopné prečítať a interpretovať prenášané dáta, čím sa minimalizuje riziko úniku informácií a krádeže dát.

Typy šifrovania:

Existuje niekoľko rôznych spôsobov šifrovania dát, vrátane symetrického a asymetrického šifrovania. Symetrické šifrovanie využíva rovnaký kľúč na šifrovanie a dešifrovanie dát, zatiaľ čo asymetrické šifrovanie používa dva rôzne kľúče - verejný a súkromný.

V súčasnosti je šifrovaný prenos dát neoddeliteľnou súčasťou kybernetickej bezpečnosti a je využívaný vo viacerých oblastiach, vrátane online bankovníctva, e-commerce, komunikácie a cloudových služieb. Zabezpečuje dôvernosť, autenticitu a integritu dát v prostredí sietí, kde je bezpečnosť kľúčovou prioritou.

* 1. Ako a kde funguje

Šifrovanie je proces konverzie čitateľného textu (plaintext) na nečitateľnú formu (ciphertext) pomocou šifrovacieho algoritmu a kľúča. Tento proces zabezpečuje, že aj keby sa neoprávnená osoba zmocnila prenášaných dát, nebola by schopná ich interpretovať bez znalosti dešifrovacieho kľúča. Dešifrovanie je naopak proces konverzie nečitateľného ciphertextu späť na pôvodný plaintext pomocou dešifrovacieho kľúča.

. Symetrické a Asymetrické Šifrovanie:

Symetrické Šifrovanie: Pri symetrickom šifrovaní je rovnaký kľúč použitý na šifrovanie aj dešifrovanie dát. Tento kľúč musí byť zdieľaný medzi odosielateľom a prijímateľom, čo môže predstavovať bezpečnostné riziko pri distribúcii kľúča.

Asymetrické Šifrovanie: Asymetrické šifrovanie používa dva rôzne kľúče - verejný a súkromný. Verejný kľúč je použitý na šifrovanie dát a je voľne dostupný každému, zatiaľ čo súkromný kľúč je použitý na dešifrovanie dát a je známy len prijímateľovi.

Použitie Šifrovaného Prenosu Dát:

Šifrovaný prenos dát je široko využívaný v rôznych oblastiach, vrátane:

Online Bankovníctvo: Zabezpečuje bezpečný prenos finančných informácií medzi bankou a klientom.

E-commerce: Zabezpečuje bezpečné transakcie a ochranu údajov zákazníkov pri online nákupe.

Komunikácia: Zabezpečuje súkromie a bezpečnosť pri komunikácii cez e-maily, správy a hlasové hovory.

Cloudové Služby: Zabezpečuje dôvernosť a ochranu dát uložených v cloude pred neoprávneným prístupom.

Šifrovaný prenos dát je nevyhnutnou súčasťou kybernetickej bezpečnosti v súčasnom digitálnom svete. Poskytuje dôvernosť, autenticitu a integritu dát pri ich prenose cez verejné siete, čím sa minimalizuje riziko úniku citlivých informácií a krádeže dát. Zabezpečuje bezpečnú komunikáciu a prevádzku digitálnych služieb, čo je kľúčové pre ochranu osobných údajov a bezpečnosť online prostredia.

1. Tvorba Produktu

Pri tvorbe plagátu o Zabezpečení zariadení na sieti som sa rozhodol použiť program Figma, ktorý mi poskytol robustné nástroje na tvorbu moderného a príťažlivého dizajnu. Mojim cieľom bolo vytvoriť plagát, ktorý by jasne a efektívne komunikoval dôležité informácie o zabezpečení zariadení pripojených na internet, a zároveň pôsobil atraktívne a profesionálne. Pri výbere pozadia som sa rozhodol pre modernú a technologickú textúru, ktorá by evokovala dynamiku v oblasti kybernetickej bezpečnosti. Farebná paleta pozadia pozostáva z odtieňov modrej, čo pridáva plagátu dojem dôvery a bezpečnosti. Pre vizuálnu ilustráciu dôležitých prvkov zabezpečenia sme zvolili príjemné obrázky, ktoré sú tematicky súvisiace. Medzi nich patria symbolické štíty a zariadenia. Tieto obrázky nielenže jasne komunikujú hlavné myšlienky plagátu o zabezpečení, ale tiež pridávajú celkovú vizuálnu atraktivitu a zaujímavosť. Pri výbere fontu sme sa rozhodli pre moderný a ľahko čitateľný font, ako je napríklad "JetBrains Mono" alebo "Helvetica". Tieto fonty sú vhodné pre digitálne projekty a poskytujú dobrú čitateľnosť aj pri menších veľkostiach písma. Hlavné nadpisy a tituly sú písané väčším písmom, aby pritiahli pozornosť a zdôraznili kľúčové body plagátu. Ostatné informácie a podrobnosti sú potom komunikované prostredníctvom QR kódu, čo umožňuje používateľom získať ďalšie informácie, keď ich naskenujú pomocou svojich zariadení. Tento prístup umožňuje udržať plagát prehľadný a zároveň poskytuje príležitosť na hlbší pohľad na tému prostredníctvom digitálnych médií. Obrázok, na ktorom je text, snímka obrazovky, softvér, multimediálny softvér

Automaticky generovaný popis

Obrázok 1 Program Figma Zdroj: Autor práce

* 1. Obsah produktu
     1. Antivírus

Antivírusový softvér je komplexný nástroj na ochranu počítačových systémov pred škodlivým softvérom. Jeho primárnym cieľom je identifikovať, blokovať a eliminovať rôzne formy malware, vrátane vírusov, červov, trojanov, adware a spyware.

Graf 1 Zdroj: Autor Práce

Fungovanie:

Skenovanie a Detekcia: Antivírusový softvér vykonáva systematické skenovanie systému, aby identifikoval potenciálne hrozby. Používa viacero techník, vrátane statického skenovania súborových podpisov, heuristického skenovania na základe behaviorálnych vzorov a analýzy správania programov.

Heuristická Analýza: Táto metóda umožňuje antivírusovému softvéru odhaliť nové, ešte neznáme hrozby na základe ich behaviorálnych charakteristík a spôsobu fungovania.

Karanténa a Odstránenie: Po identifikácii škodlivého softvéru sa infikované súbory alebo procesy izolujú a umiestnia do karantény, aby sa zabránilo šíreniu infekcie. Potom sa vykonáva proces odstránenia alebo dezinfekcie, ktorý zahŕňa opravu poškodených súborov alebo ich úplné odstránenie z systému.

Dôležitosť a Prevencia:

Antivírusový softvér je kritickým prvkom bezpečnostnej stratégie pre organizácie aj jednotlivcov. Pomáha minimalizovať riziko straty dát, poškodenia systémov a krádeže citlivých informácií. Okrem toho je dôležité pravidelne aktualizovať softvér, aby sa zabezpečila ochrana pred najnovšími hrozbami.

* + 1. Firewall

Firewall je základným prvkom bezpečnostnej infraštruktúry, ktorý slúži na ochranu počítačových sietí pred neoprávneným prístupom a nežiaducim prevádzkovým tokom. Jeho hlavnou úlohou je sledovať, filtrovať a riadiť tok dát medzi rôznymi časťami siete, aby sa zabránilo prístupu neautorizovaných používateľov a škodlivého softvéru.

Funkcia:

Filtrovanie Paketov: Firewall monitoruje všetky sieťové pakety, ktoré vstupujú a opúšťajú sieť, a rozhoduje, či ich povoliť alebo blokovať na základe preddefinovaných pravidiel. Tieto pravidlá môžu zahŕňať povolenie prístupu len z určitých IP adries, portov alebo typov dát.

Blokovanie Neautorizovaného Prístupu: Firewall aktívne odmietne prístup k sieťovým zdrojom, ktoré nie sú oprávnené alebo autentifikované. Tým sa minimalizuje riziko neoprávneného prístupu a zneužitia kritickej infraštruktúry.

Detekcia a Blokovanie Útokov: Niektoré firewally majú funkcie detekcie útokov, ktoré sledujú sieťovú prevádzku na hľadanie anomálií alebo podpisov útokov. Ak je zistená nebezpečná aktivita, firewall ju automaticky blokuje alebo upozorňuje na ňu administrátora.

Dôležitosť:

Firewall je nevyhnutným prvkom pre zabezpečenie sietí pred vonkajšími hrozbami, ako sú hackerské útoky, malvéry a úniky dát. Zabraňuje neoprávnenému prístupu k dátam a chráni citlivé informácie pred zneužitím. Bez firewallu by boli siete vystavené riziku útokov a závažných bezpečnostných incidentov.

Prevencia a Aktualizácia:

Je dôležité pravidelne aktualizovať a spravovať firewall, aby sa zabezpečilo, že je schopný detegovať a blokovať najnovšie hrozby. Okrem toho je potrebné pravidelne revízovať a aktualizovať bezpečnostné politiky a pravidlá firewallu podľa zmien v sieti a hrozbách.

* + 1. VPN

Virtuálna privátna sieť (VPN) je technológia, ktorá umožňuje vytváranie bezpečného a šifrovaného spojenia medzi vzdialenými zariadeniami cez verejnú sieť, ako je internet. VPN poskytuje užívateľom možnosť prenášať dáta cez nezabezpečené siete, akoby boli pripojené priamo do siete s fyzickou privátnou linkou. Hlavným cieľom VPN je zabezpečiť súkromie a bezpečnosť užívateľských dát, predovšetkým v prípade, že sa pohybujú cez verejné, nezabezpečené siete.

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

Automaticky generovaný popis

Obrázok 2 Demonštrácia funkcie VPN Autor: Hostinger Tutorials Zdroj: [www.hostinger.com](http://www.hostinger.com)

Ako funguje VPN?

VPN funguje pomocou kombinácie šifrovania, tunelovania a autentifikácie na zabezpečenie komunikácie medzi zariadeniami. Tu je stručný pohľad na jeho fungovanie:

Šifrovanie dát: Pri použití VPN sú všetky prenášané dáta šifrované, čím sa zabezpečuje ich bezpečná preprava cez verejné siete. Šifrovanie zabraňuje neoprávnenému sledovaniu alebo úprave dát počas ich prenosu.

Tunelovanie: VPN vytvára tzv. "virtuálny tunel" medzi používateľským zariadením a cieľovou sieťou. Tento tunel izoluje užívateľskú prevádzku od verejnej siete, čím zabezpečuje, že prenášané dáta nie sú vystavené vonkajším hrozbám.

Autentifikácia: Pred pripojením k VPN serveru musí užívateľ prejsť procesom autentifikácie, ktorý zahŕňa overenie svojej identity pomocou užívateľského mena a hesla, certifikátu alebo iných metód autentifikácie. Tým sa zabezpečuje, že iba oprávnení používatelia majú prístup k VPN.

V kombinácii tieto mechanizmy umožňujú VPN poskytovať bezpečné a súkromné pripojenie k internetu a iným sietiam, čo je veľmi užitočné pre ochranu osobných údajov, anonymitu a obchádzanie geografických obmedzení.

1. Záver

Štúdium problematiky zabezpečenia zariadení na sieti ma prenikavý pohľad do sveta kybernetickej bezpečnosti. Zistil som, že bezpečnosť mojich zariadení je kľúčovou prioritou, a tri základné nástroje - firewall, antivírusová ochrana a šifrovanie dát - sú základom pre ochranu citlivých údajov. Použitím týchto technológií som si uvedomil, že môžem aktívne prispievať k zabezpečeniu mojich digitálnych aktív. Správne nastavený firewall, aktuálny antivírusový softvér a použitie šifrovania dát mi poskytujú istotu, že moje dáta sú chránené pred rôznymi formami kybernetických hrozieb. Aj keď digitálny svet prináša nové výzvy a hrozby, som presvedčený, že s vhodnými bezpečnostnými opatreniami a neustálou odbornou prípravou môžeme minimalizovať riziká a zabezpečiť bezpečné digitálne prostredie pre seba a našich blízkych. Bezpečnosť mojich zariadení na sieti je neustály proces, do ktorého som pripravený investovať čas a úsilie, aby som ochránil moje digitálne aktíva a zachoval svoje súkromie.

Zoznam použitej literatúry

1. Wikipedia contributors. Firewall (computing). In: Wikipedia: The Free Encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2022-01-30, [cit. 2024-04-21]. Dostupné na internete: <https://en.wikipedia.org/wiki/Firewall\_(computing)>
2. ESET. Firewall ochrana [online]. Bratislava: ESET, [cit. 2024-04-21]. Dostupné na internete: <<https://www.eset.com/sk/firewall-ochrana/>>
3. Správa Sietí. Firewall [online]. [cit. 2024-04-21]. Dostupné na internete: <<https://www.sprava-site.eu/firewall/>>
4. ESET. Antivírus [online]. [cit. 2024-04-21]. Dostupné na internete: <https://www.eset.com/sk/antivirus/>
5. National Cyber Security Centre. What is an antivirus product? [online]. [cit. 2024-04-21]. Dostupné na internete: <<https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product>>
6. Check Point Software Technologies. What is Firewall? [online]. [cit. 2024-04-21]. Dostupné na internete: <https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/>