VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

Izboljšanje varnosti omrežja malih podjetij z ekosistemom Raspberry Pi

Kandidatka: Lea Rutnik

Vrsta študija: študentka izrednega študija

Študijski program: Informatika

Mentor predavatelj: mag. Dušan Brglez

Mentor v podjetju: Gregor Srdić univ. dipl. inž. rač. in inf.

Lektor: Nina Balažek, mag. angl. in mag. prof. slov.

Maribor, 2024

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisana Lea Rutnik, sem avtorica diplomskega dela z naslovom Izboljšanje varnosti omrežja malih podjetij z ekosistemom Raspberry Pi, ki sem ga napisala pod mentorstvom mag. Dušana Brgleza.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbela, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Maribor, september, 2024 Podpis študenta:

ZAHVALA

Zahvaljujem se svoji družini, partnerju, Mitji, Gregorju in predavatelju g. Dušanu Brglezu, brez katerih mi naloga ne bi uspela.

POVZETEK

V diplomskem delu je bila raziskana uporaba mikroračunalnika Raspberry Pi za izboljšanje varnosti v manjših podjetjih. Proučen je bil operacijski sistem Linux, ki poganja Raspberry Pi, in cenovno ugodne rešitve, ki so dostopne podjetjem z usposobljenim osebjem ali zunanjo IT podporo. V okviru raziskave je bil nameščen Pi-hole, ki je omogočil nadzor nad omrežjem, blokiranje zlonamernih domen in oglasov. Pi-hole je bil ključnega pomena pri izboljšanju učinkovitosti DNS poizvedb, kar je povečalo varnost omrežja in izboljšalo uporabniško izkušnjo zaposlenih. Ob tem se je zmanjšalo tveganje za okužbo z virusi in napade zlonamerne programske opreme, kar je vodilo k boljši zaščiti podatkov v podjetju. Zaposlenim je bil omogočen varen dostop do omrežja tudi zunaj podjetja z vzpostavitvijo VPN strežnika. Za to je bila uporabljena platforma WireGuard in OpenVPN. Varna povezava z uporabo VPN je bila ključna za zaščito občutljivih informacij in je zaposlenim omogočila dostop do virov podjetja za delo od doma. Varna povezava dostop omogoča tudi zunaj meja Slovenije, če je službena naprava povezana v aktivno internetno povezavo. Pri implementaciji rešitev je prišlo do različnih tehničnih izzivov, zlasti pri uporabi statičnega IP naslova, kar je zahtevalo dodatno konfiguracijo in podaljšalo potreben čas nastavitve. Za zbiranje podatkov o stanju mikroračunalnika in sistema Linux je bila uporabljena Docker platforma in sistem kontejnerizacije. Ta pristop je omogočil večji nadzor in stabilnost nad celotnim sistemom. Periodično so se v ozadju izvajali testi na področju hitrosti povezave, ki so bili nato z grafi prikazani s pomočjo spletnega vmesnika Speedtest Tracker. Z uporabo Grafane in Prometheusa v Dockerju je bila prikazana poraba pomnilnika, obremenitev in temperatura CPU-ja, uporaba diska in Pi-hole varnostne metrike. Konfiguracija in nadzor sistema sta bila izvedena skozi terminal s pomočjo orodij, kot so Putty, WinSCP, Notepad++. Podatki so bili vizualizirani v spletnem brskalniku Chrome. Ta pristop je omogočil enostavno upravljanje z različnimi komponentami sistema in zagotavljanje preglednosti podatkov. Za raziskavo hipotez in doseganje ciljev je bila uporabljena kombinacija kvantitativnih in kvalitativnih metod. Kvantitativni podatki so zajemali rezultate hitrostnih testov in analize delovanja sistema, medtem ko so kvalitativni podatki izhajali iz izkušenj z implementacijo in konfiguracijo skozi diplomsko delo.

Ključne besede: Raspberry Pi, VPN, Pi-hole, blokiranje oglasov, Docker.

ABSTRACT

Improving the Security of the Small Business Network with the Raspberry Pi Ecosystem

The thesis explored the use of the Raspberry Pi microcomputer to enhance security in small businesses. The Linux operating system that runs on the Raspberry Pi was examined, along with cost-effective solutions available to companies with skilled staff or external IT support. As part of the research, Pi-hole was installed, enabling network monitoring, blocking of malicious domains, and ads. Pi-hole played a crucial role in improving the efficiency of DNS queries, which increased network security and enhanced the user experience for employees. This also reduced the risk of virus infections and malware attacks, leading to better data protection within the company. Employees were provided with secure access to the network from outside the company through the setup of a VPN server. The platforms used for this were WireGuard and OpenVPN. A secure connection using VPN was crucial for protecting sensitive information and allowed employees to access company resources while working from home. The secure connection also enabled access outside Slovenia's borders if the work device was connected to an active internet connection. The implementation of these solutions encountered various technical challenges, particularly with the use of a static IP address, which required additional configuration and extended the setup time. The Docker platform and containerization system were used to collect data on the status of the microcomputer and the Linux system. This approach provided greater control and stability over the entire system. Periodic connection speed tests were run in the background and displayed through graphs using the Speedtest Tracker web interface. By using Grafana and Prometheus within Docker, memory usage, CPU load and temperature, disk usage, and Pi-hole security metrics were displayed. The system configuration and monitoring were performed through the terminal using tools such as Putty, WinSCP, and Notepad++. Data was visualized in the Chrome web browser. This approach allowed easy management of various system components and ensured data transparency. A combination of quantitative and qualitative methods was used to investigate the hypotheses and achieve the objectives. Quantitative data included the results of speed tests and system performance analysis, while qualitative data were derived from the experiences with implementation and configuration throughout the thesis.

Keywords: Raspberry Pi, VPN, Pi-hole, Ads blocking, Docker.

KAZALO VSEBINE

1 UVOD 11

1.1 Opis področja in opredelitev problema 11

1.2 Namen, cilji in osnovne trditve 12

1.3 Predpostavke in omejitve 13

1.4 Uporabljene raziskovalne metode 13

2 PREDSTAVITEV RASPBERRY PI 14

2.1 Izbira modela in potrebnih zunanjih naprav 14

2.2 Namestitev operacijskega sistema Linux 16

2.3 Konfiguracija osnovnih zahtev 17

3 KONFIGURACIJA PI-HOLE ZA BLOKIRANJE OGLASOV V OMREŽJU 19

3.1 Postopek namestitve in nastavitve 19

3.2 Prednosti in omejitve Pi-hole 20

3.3 Nastavitve DNS 22

4 IMPLEMENTACIJA VPN ZA VAREN ODDALJEN DOSTOP 24

4.1 Uvod v navidezna zasebna omrežja 24

4.2 Izbira programske opreme VPN 24

4.2.1 OpenVPN 25

4.2.2 WireGuard 26

4.3 Konfiguracija VPN za šifrirane povezave 27

5 VLOGA DOCKERJA PRI INTEGRACIJI VELEPODATKOV 32

5.1 Pregled Dockerja in njegove prednosti 32

5.2 Primeri uporabe Dockerja v okolju z veliko podatki 32

5.3 Integracija Dockerja 33

6 PRAKTIČNI PRIMER: VARNOST OMREŽJA MALIH PODJETIJ DO 5 RAČUNALNIKOV 35

6.1 Opis omrežne infrastrukture 35

6.2 Strategija uvajanja za integracijo z Raspberry Pi, Pi-hole, VPN in Docker 36

6.3 Ocena učinkovitosti 37

6.4 Analiza praktičnih omejitev 37

7 IZZIVI IN OMEJITVE 38

8 SKLEP 40

9 LITERATURA IN VIRI 45

KAZALO SLIK

SLIKA 1: RASPBERRY PI 5 15

SLIKA 2: RASPBERRY PI OHIŠJE 15

SLIKA 3: RASPBERRY PI IMAGER 17

Seznam uporabljenih kratic

KRATICA	Angleški zapis	Slovenski zapis
Apache NiFi	Apache Niagara Files	Apache Niagara datoteke
ARM	Advanced RISC Machine	Napredni RISC stroj
CA	Certificate Authority	Overitelj potrdil
CI/CD	Continuous Integration and Continuous Delivery	Neprekinjena integracija in neprekinjena dostava
CLS	Clear screen	Čisti zaslon
CPU	Central Processing Unit	Centralna procesna enota
DHCP	Dynamic Host Configuration Protocol	Omrežni protokol za dinamično nastavitev gostitelja
DNS	Domain Name System/Server/Service	Sistem domenskih imen
DNSSEC	Domain Name System Security Extensions	Varnostne razširitve sistema domenskih imen
DSI	Delivered Source Instruction	Dostavljena navodila za vir
Easy-RSA	Rivest–Shamir–Adleman Public-key cryptosystem	Rivest – Shamir – Adleman šifriranje z javnim ključem
ELK	Elasticsearch, Logstash and Kibana	Elasticsearch, Logstash, in Kibana
ETH0	Ethernet Interface 0	Ethernet vmesnik 0
ETL	Extract, transform, load	Izvleči, transformirati, naložiti
GPIO	General-purpose input/output	Splošni vhodi in izhodi

HDMI	High-Definition Multimedia Interface	Multimedijski vmesnik visoke ločljivosti
HTTPS	Hypertext Transfer Protocol Secure	Šifrirana varna povezava za prenos informacij na spletu
IoT	Internet of Things	Internet stvari
IP	Internet Protocol Address	Naslov internetnega protokola
IPV4	Internet Protocol version 4	Internetni protokol 4
IPV6	Internet Protocol version 6	Internetni protokol 6
LAN	Local area network	Lokalno omrežje
LCP	Link Control Protocol	Protokol za nadzor naprave
MICRO SD	Micro Secure Digital Card	Izmenljiva pomnilniška kartica
RAM	Random access memory	Pomnilnik z naključnim dostopom
SSD	Solid State Drive	Hitri diskovni negibljivi disk
SSH	Secure Shell	Varna šifrirana povezava za upravljanje računalnika na daljavo
SSL	Secure Sockets Layer	Vzpostavitev varne povezave
TCP	Transmission Control Protocol	Protokol za nadzor prenosa
TLS	Transport Layer Security	Varnost transportne plasti
TTFB	Time to first byte	Čas do prvega bajta
UDP	User Datagram Protocol	Nepovezani protokol za prenašanje paketov

UFW	Uncomplicated Firewall	Nezapleten požarni zid
USB	Universal serial bus	Univerzalno serijsko vodilo
VPN	Virtual Private Network	Navidezna zasebna omrežja

1 UVOD

V dobi nenehno naraščajoče digitalizacije je vprašanje kibernetske varnosti v ospredju kot ključni dejavnik za varno poslovanje, še posebej v manjših podjetjih, kjer so viri (angl. *resources*) omejeni. V diplomskem delu smo raziskali, kako lahko z majhnim, a izjemno zmogljivim mikroračunalnikom Raspberry Pi ustvarimo celovito varnostno rešitev za upravljanje omrežij. To smo dosegli z uporabo Pi-hole, orodja za blokiranje oglasov in filtriranje spletnega prometa, ki dodatno zaščiti naše omrežje. Nastavili smo tudi VPN povezavo, ki zaposlenim omogoča varen dostop do notranjih virov podjetja kjerkoli na svetu. S tem smo dosegli, da zaupni podatki ostanejo znotraj podjetja, obenem pa smo zmanjšali možnosti zunanjih vdorov. Testirali smo več hipotez, med drugim tudi to, da uporaba Pi-hole izboljša varnost in učinkovitost omrežja. Preverjali smo zmogljivost mikroračunalnika med različnimi obremenitvami ter ocenili odzivnost naprave. Z raziskavo hipotez smo prispevali k boljšemu razumevanju, kako lahko z omejenimi viri dosežemo visoko raven varnosti v sodobnem poslovnem svetu.

1.1 Opis področja in opredelitev problema

Obravnavana tema zajema različne kategorije iz obdobja študija, in sicer z vidika kibernetske varnosti, omrežne administracije in sistemske arhitekture. Izbrano področje nas zanima, saj se zavedamo pomena varovanja občutljivih podatkov in zaščite digitalne zasebnosti v vse bolj digitalizirani družbi. Z diplomskim delom bi radi razširili znanje s področja Linux-a, omrežnih protokolov in varnostne konfiguracije. Izbira teme temelji na želji po poglabljanju znanja na področju kibernetske varnosti ali omrežnega inženiringa.

V dobi, ki jo zaznamujejo napredna tehnologija in razširjene spletne grožnje, je varovanje zasebnosti postalo najpomembnejše. Namen študije je raziskati ter prikazati, kako lahko kombinirana uporaba Raspberry Pi, Pi-hole in VPN okrepi varnost malih podjetij in zmanjša tveganja, povezana s spletom. V razvijajočem se okolju velikih podatkov, kjer se ustvarjajo in analizirajo ogromne količine podatkov, postaja razumevanje in uporaba teh tehnologij še bolj ključna.

1.2 Namen, cilji in osnovne trditve

Cilji diplomskega dela so:

- Poglobiti razumevanje Raspberry Pi kot širše vsestranske platforme za implementacijo različnih varnostnih razširitev omrežja.
- Raziskati funkcionalnosti in konfiguracijo Pi-hole za blokiranje oglasov v celotnem omrežju in upravljanje DNS.
- Razumeti načela in protokole, ki so potrebni za varno vzpostavitev navideznih zasebnih omrežij (VPN) in kakšno vlogo imajo pri izboljšanju varnosti omrežja.
- Izboljšati splošno znanje o Linux administraciji.

Namen diplomskega dela:

- Oceniti vpliv Pi-hole na zmogljivost omrežja s strani uporabnika v podjetju.
- Oceniti varnostne prednosti in možne pomanjkljivosti ob integraciji z VPN, zlasti na primerih zasebnosti podatkov, zaupnosti in varnega oddaljenega dostopa.
- Prikazati, kako spremljati in analizirati omrežni promet z DNS poizvedbami.
- Predstaviti Docker in uporabnost te platforme.
- Raziskati vpliv velikih podatkov na varnost v majhnih podjetjih.

Hipoteze:

Hipoteza 1: Omrežja zaščitena s Pi-hole imajo izboljšano varnost v primerjavi s tistimi, ki se zanašajo izključno na tradicionalne protivirusne programe.

Hipoteza 2: Raspberry Pi je učinkovita naprava za uporabo v podjetjih.

Hipoteza 3: Omrežja, ki uporabljajo Pi-hole, imajo izboljšano hitrost internetne povezave v primerjavi s tistimi brez.

Hipoteza 4: Učinkovitost varnostnih rešitev se izboljšuje z večanjem omrežnega prometa in velikih količin podatkov.

Hipoteza 5: Docker izboljšuje razširljivost in prilagodljivost omrežnih varnostnih rešitev, kar omogoča lažjo uvedbo in upravljanje varnosti.

Hipoteza 6: Integracija Pi-hole, VPN in Docker na Raspberry Pi ponuja zadostno rešitev za varnost omrežja za mala podjetja.

Hipoteza 7: Predlagane varnostne rešitve v diplomskem delu predstavljajo učinkovite in cenovno dostopne alternative za mala podjetja v primerjavi s tradicionalnimi metodami.

1.3 Predpostavke in omejitve

Predpostavljamo, da bodo raziskovalne metode potekale brez zapletov, z manjšimi omejitvami. Omejitve se lahko pojavijo pri zbiranju in razpoložljivosti podatkov, saj so nekateri podatki lahko zaščiteni ali omejeni. V primeru manjše razpoložljivosti računalniške opreme za eksperimentalno testiranje bi to lahko zožilo obseg raziskave.

1.4 Uporabljene raziskovalne metode

Za opredelitev raziskovalnih metod so bile uporabljene tri metodologije.

Kvantitativna metodologija, ki vključuje zbiranje numeričnih podatkov o različnih meritvah zmogljivosti, kot so prepustnost, zakasnitev, uporaba virov in varnostna učinkovitost ob različnih prometnih obremenitvah in v okolju velikih podatkov. Kvantitativna analiza je omogočila objektivno merjenje in primerjavo uspešnosti rešitve ter zagotavljala dragocen vpogled v razširjenost in učinkovitost.

Kvalitativna metodologija je vključevala študije primerov iz resničnega sveta, ki omogočajo podroben vpogled v praktično izvajanje, uspehe in izzive podjetij ter izkušnje, ki so jih podjetja pridobila z integracijo Raspberry Pi, Pi-hole in VPN. Z uporabo te metode smo pridobili podatke, ki jih ni mogoče zajeti s kvantitativno metodo, in sicer so to tehnične omejitve, uporabniške izkušnje in organizacijska dinamika znotraj podjetij.

Eksperimentalno testiranje je potekalo z izvajanjem nadzorovanih poskusov za simulacijo naraščajočih prometnih obremenitev in okolij z veliko podatki, hkrati pa se je spremljalo meritve učinkovitosti rešitev v nadzorovanem okolju, kar omogoča sistematično opazovanje in merjenje varnosti in zaščite v različnih pogojih.

Omenjeni pristopi omogočajo celostno razumevanje raziskovalne teme, kar povečalo verodostojnost teme in hipotez.

2 PREDSTAVITEV RASPBERRY PI

Raspberry Pi je mikroračunalnik v velikosti kreditne kartice. To je serija majhnih cenovno dostopnih računalnikov, ki vsebujejo samo eno ploščo. Razviti in namenjeni so bili za namene poučevanja osnov računalništva in programiranja. Matične plošče so običajno opremljene s procesorjem ARM, pomnilnikom RAM in raznimi priključki, kot so USB, HDMI izhod in priključki GPIO, ki služijo za povezovanje z zunanjimi napravami in senzorji, ob tem pa nudijo podporo za različne operacijske sisteme in ne samo za Linux distribucijo. Raspberry Pi se lahko uporablja za številne projekte, kot so medijski centri, starejše (angl. *retro*) igralne konzole, sistemi za avtomatizacijo doma, video nadzor, robotiko in naprave IoT, ki so vedno bolj priljubljene.

(Team, 2024)

2.1 Izbira modela in potrebnih zunanjih naprav

Za potrebe diplomskega dela smo izbrali v tem trenutku najnovejši Raspberry Pi 5 s 4 Gb rama. Izbrani model Raspberry Pi 5 nudi izboljšano zmogljivost in hitrost v primerjavi s prejšnjimi generacijami, kar je ključno za izvedbo različnih varnostnih rešitev v omrežju malih podjetij. Integracija M.2 SSD omogoča hitrejši prenos podatkov in hitrejši zagon naprave, kar je pomembno za tekoče delovanje storitev. To je model z dva do trikrat večjo hitrostjo kot prejšnja generacija. Ima dva 3.0 USB vhoda, ki omogočata še hitrejši prenos podatkov. Priključke za kamere in DSI zaslone se lahko zamenja po željah uporabnika, saj sta dva priklopa lahko popolnoma enaka. Kot smo že omenili, je model hitrejši zaradi svojega štirijedrnega procesorja Broadcom BCM2712 Arm Cortex A76 s frekvenco 2,4 GHz. Posebnost je priklop M.2 SSD diska, kar omogoča še hitrejši prenos podatkov in izjemno hiter zagon naprave.

(Raspberry Pi, 2024)

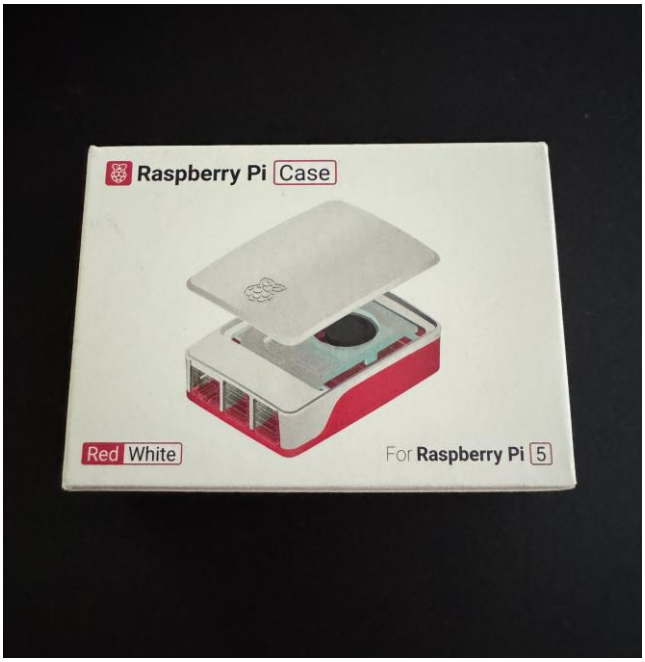
Med obvezno strojno opremo smo vključili 27 W original polnilec, ki zagotavlja stabilno napajanje, kabel Micro HDMI D za povezavo z zaslonom in Micro SD 128 GB kartico, ki je služila kot primarni pomnilnik. Ker se zavedamo, da lahko pride do poškodb in kako pomembno je vzdrževanje optimalne temperature delovanja, smo Raspberry Pi opremili še z dodatnim ventilatorjem in ohišjem. Poleg obveznih komponent smo vključili še nekaj dodatnih zunanjih naprav, ki omogočajo lažje in nemoteno delovanje, to so miška, tipkovnica in zaslon. Z vso

skupno integracijo smo ustvarili celovito računalniško okolje, potrebno za izdelavo diplomskega dela.



Slika 1: Raspberry Pi 5

Vir: (Lastni vir)



Slika 2: Raspberry Pi ohišje

Vir: (Lasten vir)

2.2 Namestitev operacijskega sistema Linux

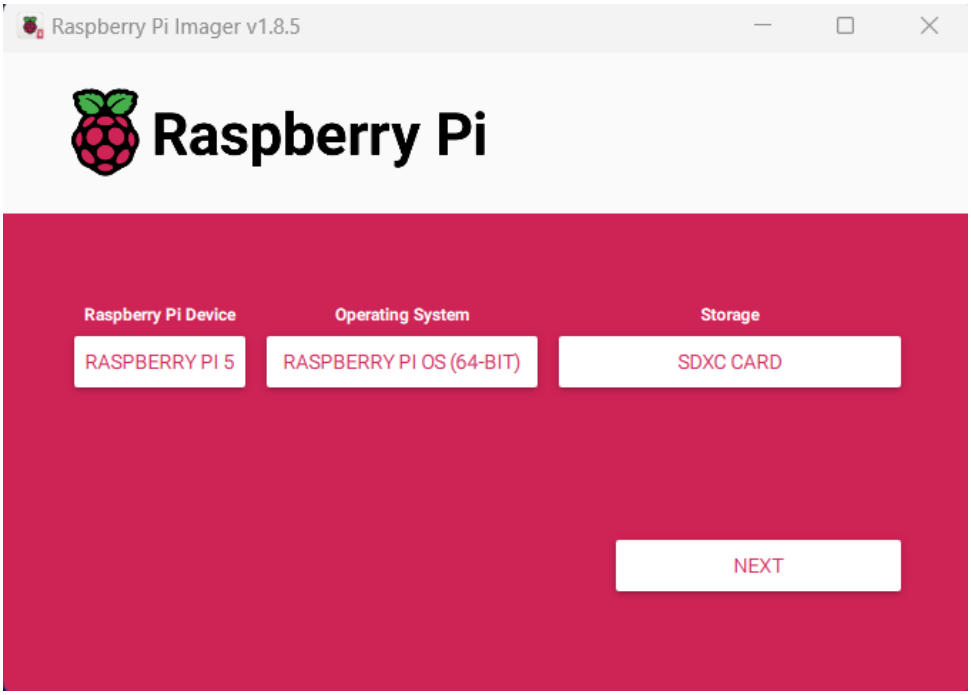
Po tehtnem premisleku, katera distribucija bo več doprinesla k vzpostavitvi potrebne infrastrukture, smo izbirali med Ubuntu Server in Raspberry Pi OS. Na koncu smo izbrali Raspberry Pi OS. Na to odločitev je vplival predvsem operacijski sistem Debian zaradi svoje stabilnosti in varnosti v strežniškem okolju. Prav tako je sistem posebej optimiziran za strojno opremo, ki jo uporabljamo in zagotavlja izboljšano zmogljivost in združljivost z napravami.

Raspberry Pi je uporabniku prijazen vmesnik, kar pomeni, da ga lahko uporabljajo vsi, ne glede na znanje. Za tem stoji velika podporna skupnost, ki je lahko v zelo veliko pomoč pri odpravljanju težav in optimizaciji. Čeprav Ubuntu Server ponuja zelo obsežno dokumentacijo za naprednejše uporabnike, se zanj nismo odločili. Izbrali smo primernejšo distribucijo glede na potrebe zagotavljanja zanesljivega delovanja obravnavanih storitev v diplomskem delu.

Za namestitev Raspberry Pi OS smo uporabili Raspberry Pi Imager na zunanjem računalniku, ki omogoča enostavno namestitev operacijskega sistema na Micro SD kartico. Postopek je naslednji:

- namestitev najnovejše verzije Raspberry Pi Imager na zunanji računalnik;
- v zunanji računalnik vstavimo SD kartico;
- izberemo napravo (angl. *device*), operacijski sistem in pomnilniški medij;
- na to se začne postopek zapisovanja na SD kartico, program nas ob koncu z zvokom obvesti, da je zapis uspešno zaključen;
- operacijski sistem je pripravljen na nadaljnjo konfiguracijo.

(Getting started with your Raspberry Pi, 2024)



Slika 3: Raspberry Pi Imager

Vir: (Lastni vir)

2.3 Konfiguracija osnovnih zahtev

Po nameščenem operacijskem sistemu je sledil naslednji korak za potrebno konfiguracijo. Treba je bilo vzpostaviti omrežje, zaščititi sistem in namestiti potrebne pakete.

Konfiguracija omrežja:

1. Statični IP – treba je imeti fiksno dodeljen naslov v lokalnem omrežju, za dostop do storitev, ki se izvajajo na strežniku.

Treba je urediti dhcpcd.conf datoteko, kar naredimo z ukazom:

- sudo nano /etc/dhcpcd.conf

V datoteko dodamo potrebno konfiguracijo.

- interface eth0
- static ip_address=192.168.x.xx/xx
- static routers=192.168.x.x
- static domain_name_servers=192.168.x.x

Omenjeni podatki so ustvarjeni za potrebe diplomskega dela in se lahko razlikujejo glede na omrežje v poslovnih ali domačih prostorih.

2. Konfiguracija imena gostitelja (angl. *Hostname*) nam pomaga pri prepoznavanju naše naprave v omrežju. To zagotovimo z ukazom v spodnjih dveh vrsticah.

- sudo nano /etc/hostname
- sudo nano /etc/hosts

Varnost sistema:

1. Treba je skrbeti za pravočasno najnovejšo (angl. *up-to-date*) nadgradnjo in posodobitev sistema.

To zagotovimo z ukazi v spodnjih dveh vrsticah. Prva nam prikaže pakete, ki so na voljo za namestitev. S kodo v drugi vrstici pakete namestimo.

- sudo apt update
- sudo apt upgrade -y

2. Konfiguracija požarnega zidu (angl. *Firewall*)

- sudo apt install ufw
- sudo ufw allow ssh
- sudo ufw enable

3. Konfiguracija SSH

V terminal zapišemo naslednji ukaz: sudo nano /etc/ssh/sshd_config

Ko se datoteka odpre, spremenimo številko vrat (angl. *port*) in onemogočimo root vpis (angl. *login*).

4. Namestitev dodatnih programov

- Namestitev spletnega (angl. *web*) serverja: sudo apt install nginx
- Namestitev podatkovne baze: sudo apt install postgresql

S konfiguracijo osnovnih zahtev smo poskrbeli za varen strežnik, ki je sposoben izvajati ukaze za potrebe diplomskega dela.

(Getting started with your Raspberry Pi, 2024)

3 KONFIGURACIJA PI-HOLE ZA BLOKIRANJE OGLASOV V OMREŽJU

V današnji digitalni dobi so spletni oglasi postali nekaj vsakdanjega, saj so vselej prisotni in s tem posegajo globoko v uporabniško izkušnjo, kar predstavlja veliko varnostnih tveganj. Da bi to ublažili na ravni omrežja, smo se odločili za programsko opremo Pi-hole, ki nam bo služila za blokiranje oglasov v omrežju znotraj podjetja. Z blokiranjem neželene vsebine se bo izboljšala hitrost interneta ter nudila potrebna zaščita pred zlonamernimi domenami. Z DNS poizvedbami se zaščiti naprave pred neželeno vsebino, in sicer brez nalaganja dodatne programske opreme (angl. *software*) na računalnike.

Prednosti so:

- enostavna namestitev;
- blokiranje vsebine ni omejeno le na spletne brskalnike, temveč deluje tudi na pametnih televizorjih in mobilnih aplikacijah;
- pospeši občutek hitrejšega brskanja s pred pomnjenjem DNS poizvedb;
- deluje gladko z minimalnimi zahtevami programske in strojne opreme;
- zelo odzivna nadzorna plošča spletnega vmesnika za pregled in nadzor Pi-hole;
- je zelo vsestranski, saj dodatno deluje tudi kot strežnik DHCP, kar zagotavlja še večjo zaščito za naše naprave;
- zmožnost obdelave več kot milijon poizvedb, kadar je nameščena na strežniški strojni opremi;
- oglasi se blokirajo preko protokola IPv4 in IPv6.

(Warner, 2024)

3.1 Postopek namestitve in nastavitve

Kot smo omenili že v prejšnji točki, je namestitev Pi-hole programske opreme enostaven postopek, vendar je treba biti zelo pozoren pri nastavitvah in podrobnostih.

Proces namestitve se začne s prenosom in namestitvijo:

- sudo curl -sSL https://install.pi-hole.net | bash

V primeru, da nam računalnik javi napako "Script called with non-root privileges", prenesemo in zaženemo skripto kot root uporabnik.

S spodnjim ukazom prenesemo skripto:

- wget -O basic-install.sh https://install.pi-hole.net

Zaženemo namestitev kot root uporabnik:

- sudo bash basic-install.sh

Med namestitvijo je treba konfigurirati:

- izbrati pravilni vmesnik; v našem primeru je to eth0, saj uporabljamo žično povezavo;
- izberemo ponudnika DNS;
- izbrati je treba seznam blokiranih domen (angl. *Block List*), ki ga želimo uporabiti;
- izberemo protokole IPv4 in IPv6;
- uporabimo trenutne omrežne nastavitve, saj smo že v predhodni konfiguraciji Raspberry Pi nastavili statični IP;
- namestitev spletnega vmesnika za nadzor in spremljanje prometa.

Po namestitvi do vmesnika dostopamo na spletu.

(Pi-hole, 2024)

3.2 Prednosti in omejitve Pi-hole

Prednosti:

1. Blokiranje oglasov v celotnem sistemu

Nadzor je popolnoma centraliziran po konfiguraciji, saj Pi-hole blokira oglase na vseh napravah, ki so povezane v omrežju, tudi v napravah, kjer ne moremo namestiti drugačnih aplikacij, ki blokirajo oglase. To so igralne konzole in pametni televizorji. Deluje na vseh napravah ne glede na operacijski sistem ali brskalnik.

2. Zmanjšana pasovna širina in hitrejše brskanje

Pi-hole oglase blokira še preden pridejo do naše naprave. S tem zmanjša količino podatkov, ki jih je treba prenesti, da končni uporabnik vidi spletno stran. To za nas pomeni, hitrejše nalaganje spletnih strani in manjša poraba pasovne širine.

3. Napravam v omrežju blokira sledenje

Blokira domene, ki so znane po sledenju uporabnika in pripomore k izboljšanju zasebnosti. Vsak uporabnik lahko posebej zase doda še dodatne sezname blokiranih domen za dodatno izboljšano varnost in zasebnost na spletu.

4. Enostavna uporaba spletnega vmesnika

Je uporabniku zelo prijazen vmesnik. Blokirane domene se lahko spremlja, nadzoruje in ureja. Ogleda se lahko statistika točno za določeno obdobje.

5. Odprtokoden sistem

Pi-hole je odprtokoden, kar pomeni, da ima veliko podporno skupnost, ki prispeva k razvoju, zagotavlja posodobitve in vtičnike ter nudi podporo. Uporabniki lahko svojo programsko opremo razširijo in spreminjajo glede na lastne zahteve.

(Block ads at home with Pi-hole, 2024)

Omejitve:

1. Kompleksnost namestitve

Od uporabnika se zahteva določena raven znanja, predvsem znanje o konfiguraciji omrežja in nastavitev DNS. Naprava, na katero je nameščen Pi-hole, mora biti vedno vklopljena. V tem primeru je koristen Raspberry Pi ali majhen strežnik.

2. Ni popolna zamenjava za blokiranje oglasov v brskalniku

Vseh oglasov ni mogoče blokirati. Problem so oglasi, ki se prikazujejo z iste domene kot vsebina. Teh domen Pi-hole ne more blokirati, ne da bi se istočasno blokirala še vsebina. Za razliko od zaviralcev oglasov (angl. *Ad block*), ki temeljijo na brskalniku, Pi-hole ne more odstraniti praznih mest, ki jih pustijo blokirani oglasi.

3. Lahko blokira preveč

Lahko se zgodi, da aplikacija blokira legitimno stran. Do tega pride, ko imajo oglasi ali storitve sledenja enako domeno kot stran, ki jo želimo obiskati. V takem primeru ročno popravimo domeno na seznam dovoljenih. Redno je treba posodabljati sezname blokiranih in dovoljenih domen, da se omogoči pravilno delovanje.

4. Blokiranje z uporabo DNS je omejeno

Pi-hole ne prestreže HTTPS protokola, saj ne more pregledati šifriranega prometa. S tem se omeji njegova zmožnost blokiranja oglasov, ki so prikazani s protokolom HTTPS, razen v primeru, ko je domena v celoti blokirana. Oglasov, ki za prikaz uporabljajo kodirane IP naslove ali kako drugače skrijejo IP, se v aplikacijah ne more blokirati. V primeru izpada Pi-hole naprave v omrežju izgubijo DNS zapise, kar lahko povzroči težave s povezljivostjo, zato se mora narediti rezervna kopija DNS.

5. Brez nadzora za specifičnega uporabnika

Nastavljena pravila za blokiranje vsebine veljajo za vse uporabnike v omrežju enako. Naprav se ne more konfigurirati in prilagoditi za potrebe vsakega uporabnika posebej.

(Community, 2024)

3.3 Nastavitve DNS

Nastavitve DNS so ključnega pomena za učinkovito delovanje Pi-hole.

1. Predhodni (angl. *upstream*) DNS serverji

So zunanji strežniki Pi-hole poizvedb, ko domena ni shranjena v predpomnilniku ali na seznamu blokiranih. Izberemo lahko javne strežnike DNS, kot so Google DNS, OpenDNS, Cloudflare ali izberemo strežnik po meri.

2. Pogojevanje posredovanja podatkov

Pogojevanje posredovanja podatkov naši napravi omogoča, da uspešno pridobi imena lokalnih omrežij, ki jih upravlja drugi DNS strežnik. To je lahko tudi kakšen usmerjevalnik, ki ima drugačno konfiguracijo.

3. Poslušanje vmesnika

Določa, kateri omrežni vmesniki Pi-hole nadzorujejo DNS poizvedbe. Konfigurira se lahko:

- poslušanje le enega določenega vmesnika;
- poslušanje vseh vmesnikov, dovoli se le izjeme;
- poslušanje vseh vmesnikov, poizvedbe so dovoljene le znotraj lokalnega omrežja.

4. DNS varnostni dodatek DNSSEC

Dodaja stopnjo varnosti s preverjanem DNS, da se zagotovi pristnost, celovitost in zaščita pred napadi. S to nastavitvijo izboljšamo varnost, vendar podaljšamo čas vračanja poizvedb.

5. Konfiguracija DNS

- prijavimo se v spletni vmesnik usmerjevalnika;
- pod nastavitvami DNS nastavimo Pi-hole kot primarni strežnik;
- za redundanco nastavimo še sekundarni DNS server;
- spremembe shranimo in ponovno zaženemo naš usmerjevalnik.

Po uspešni konfiguraciji preverimo delovanje Pi-hole in počistimo predpomnilnik DNS.

Windows ukaz: ipconfig/flushdns

Linux ukaz: sudo systemd-resolve –flush-caches

(Faq-bot, 2024)

4 IMPLEMENTACIJA VPN ZA VAREN ODDALJEN DOSTOP

4.1 Uvod v navidezna zasebna omrežja

Navidezna zasebna omrežja nam omogočajo varen dostop do zasebnih omrežij preko javnih internetnih povezav. VPN-ji se v podjetjih uporabljajo za zaščito občutljivih podatkov, ohranjanje zasebnosti in dostop do omejene vsebine. S prikrivanjem uporabnikovega naslova IP in šifriranjem internetnega prometa lahko VPN prepreči nepooblaščen dostop in zaščiti podatke pred napadi hekerjev ali drugih zlonamernih subjektov.

Uporaba VPN ima več ključnih prednosti:

- Varnost: Povezava VPN šifrira podatke, kar nepooblaščenim osebam otežuje dostop do občutljivih informacij.
- Zasebnost: Z maskiranjem uporabnikovega naslova IP VPN-ji pomagajo ohranjati anonimnost in varujejo zasebnost.
- Dostop do omejene vsebine: VPN-ji lahko zaobidejo geografske omejitve in uporabnikom omogočijo dostop do vsebin, ki je morda blokirana v njihovi regiji.

Pi-hole napravo za blokiranje oglasov smo uporabili v konfiguraciji z VPN, kar nam je omogočilo varen oddaljen dostop do omrežja, kjer je nameščen Pi-hole. Nastavljeni filtri so tako učinkoviti ne glede na lokacijo uporabnika.

(What is a VPN, 2024)

4.2 Izbira programske opreme VPN

Izbira prave programske opreme VPN je ključnega pomena za zagotavljanje varnih, zanesljivih in učinkovitih omrežnih povezav. Pri izbiri VPN-ja je treba upoštevati različne dejavnike, vključno s stopnjo varnosti, enostavnostjo uporabe, združljivostjo z različnimi napravami in stroški. Programsko opremo VPN lahko na splošno razvrstimo v dve kategoriji, in sicer VPN-ji, ki temeljijo na ponudnikih storitev in VPN-ji z lastnim gostovanjem.

VPN-ji, ki temeljijo na ponudnikih storitev:

- To so storitve VPN, ki jih zagotavljajo podjetja tretjih oseb. Uporabnikom pogosto ponudijo uporabniku prijazne vmesnike z rednimi posodobitvami in dobro podporo strankam. So

idealni za uporabnike, ki imajo raje udobje in ne želijo obravnavati tehničnih vidikov delovanja VPN.

- Ni vpliva na hitrost širokopasovne povezave z VPN.

Samostojni VPN:

- Tukaj morajo uporabniki sami nastaviti in vzdrževati lastne VPN strežnike. Ta možnost ponuja večji nadzor in prilagajanje konfiguracije po lastnih potrebah podjetja. Od nas zahteva več tehničnega znanja in vloženega truda. Primerno je za podjetja, ki potrebujejo posebne konfiguracije ali imajo stroge zahteve glede zasebnosti in varnosti.

Pri izbiri je treba oceniti:

- Poiskati je treba močno šifriranje, uporabiti varne protokole in politiko brez zapisovanja dnevnikov.
- Upoštevati je treba hitrosti in zanesljivosti povezav VPN.
- Prepričati se moramo, da izbran VPN podpira vse naprave in operacijske sisteme, ki jih v podjetju uporabljamo.
- Treba je oceniti cenovne načrte in preveriti ali ustrezajo našemu proračunu.

Za zagotovitev oddaljenega dostopa do omrežja podjetja sta bili izvedeni dve rešitvi VPN: OpenVPN in WireGuard. Oba ponujata močno šifriranje in varen dostop.

(Hosted VPN Solutions & Service, 2024)

4.2.1 OpenVPN

OpenVPN je priljubljen odprtokodni protokol VPN, znan po svoji robustni varnosti in prilagodljivosti. Za izmenjavo ključev uporablja SSL/TLS in lahko zaobide požarne zidove in prevajalnike omrežnih naslovov. OpenVPN podpira različne algoritme šifriranja, ki zagotavljajo varen prenos podatkov.

Značilnosti OpenVPN:

- Uporablja močne standarde šifriranja in zagotavlja zaščito pred različnimi vrstami kibernetskih napadov.

- Deluje lahko na vseh vratih preko UDP ali TCP, zaradi česar je zelo prilagodljiv različnim omrežnim okoljem.
- Ker je odprtokoden, ga skupnost razvijalcev nenehno pregleduje in posodablja, kar povečuje njegovo zanesljivost in varnost.

OpenVPN je bil nameščen na Raspberry Pi zaradi svojih robustnih varnostnih funkcij in široke združljivosti. Strežnik je bil konfiguriran z varnimi šifrirnimi protokoli in šiframi, ki zagotavljajo visoko raven zaščite podatkov. Prilagodljivost OpenVPN je omogočila obsežno prilagajanje varnostnih nastavitev, kot so preverjanje pristnosti na podlagi potrdil in posebna uporabniška dovoljenja.

Konfiguracija odjemalca: Za vsakega zaposlenega so bili ustvarjeni posamezni profili odjemalcev VPN, ki jim omogočajo varen dostop do pisarniškega omrežja z različnih lokacij. Ti profili, vključno s potrebnimi potrdili in konfiguracijskimi datotekami, so bili varno razdeljeni zaposlenim. Uporabljajo se lahko na prenosnih računalnikih in pametnih telefonih, kar zagotavlja brezhibno povezljivost.

(OpenVPN, 2024)

4.2.2 WireGuard

WireGuard je sodoben VPN protokol zasnovan tako, da je hitrejši in učinkovitejši od tradicionalnih protokolov VPN, kot je OpenVPN. Uporablja najsodobnejšo kriptografijo za zagotavljanje vrhunske varnosti in zmogljivosti. WireGuard je znan po svoji preprostosti, enostavnosti konfiguracije in minimalni kodni bazi, kar zmanjšuje površino napada in možnost ranljivosti.

Ključne lastnosti protokola WireGuard:

- Ponuja hitrejše povezave in nižjo zakasnitev v primerjavi z drugimi protokoli VPN.
- Enostavna konfiguracija in upravljanje z minimalistično kodno bazo, ki izboljšuje varnost.
- Na voljo je za različne operacijske sisteme, vključno z Windows, macOS, Linux, iOS in Android.

Postopek konfiguracije je vključeval nastavitev strežnika z javnimi in zasebnimi ključi ter opredelitev omrežnega vmesnika za WireGuard.

Konfiguracija odjemalca: Podobno kot pri OpenVPN so bili za vsakega zaposlenega ustvarjeni profili odjemalcev za WireGuard. Ti profili so vključevali potrebne ključe in konfiguracijske nastavitve, ki so varno porazdeljene, da se zagotovi pravilna nastavitev. Konfiguracija WireGuard je omogočila enostavno uvedbo in hitro vzpostavitev povezave. Odjemalska programska oprema za WireGuard, ki je na voljo na več platformah, je zaposlenim omogočila, da se brez težav povežejo s pisarniškim omrežjem iz svojih naprav.

(Pi-hole documentation, 2024)

4.3 Konfiguracija VPN za šifrirane povezave

Konfiguriranje VPN-ja za zagotavljanje šifriranih povezav je bistvenega pomena za ohranjanje varnosti in zasebnosti podatkov. Različni protokoli VPN ponujajo različne ravni šifriranja in zmogljivosti, razumevanje teh protokolov pa je ključnega pomena za optimalno konfiguracijo VPN.

Konfiguracija in nastavitve OpenVPN. Je zelo nastavljiv in ga je mogoče nastaviti tako, da zagotavlja močno šifriranje in varne povezave. Postopek običajno vključuje namestitev programske opreme OpenVPN, ustvarjanje certifikatov strežnika in odjemalca ter konfiguriranje nastavitev strežnika in odjemalca OpenVPN.

1. Namestitev paketa OpenVPN.

- sudo apt install openvpn -y

2. Prenesemo in namestimo certifikate.

- sudo apt install easy-rsa -y

3. Ustvarimo direktorij za Easy-RSA in se prestavimo v ta direktorij.

- make-cadir ~/openvpn-ca
- cd ~/openvpn-ca

4. Odpremo datoteko vars in nastavimo lokalne spremenljivke.

- nano vars

    set_var EASYRSA_REQ_COUNTRY "YourCountry"

    set_var EASYRSA_REQ_PROVINCE "YourProvince"

    set_var EASYRSA_REQ_CITY "YourCity"

set_var EASYRSA_REQ_ORG "YourOrganization"

set_var EASYRSA_REQ_EMAIL "YourEmail"

set_var EASYRSA_REQ_OU "YourOrganizationalUnit"

5. Zgradimo CA in nastavimo geslo za CA.

- source ./vars
- ./easyrsa clean-all
- ./easyrsa build-ca

6. Generiramo certifikat za server in ključ.

- ./easyrsa build-server-full server nopass

7. Generiramo certifikat za klienta in ključ.

- ./easyrsa build-client-full client1 nopass

8. Generiramo Diffie-Hellman parametre.

- ./easyrsa gen-dh

9. Konfiguriramo OPenVPN in prestavimo potrebne datoteke.

- sudo mkdir /etc/openvpn
- sudo cp ~/openvpn-ca/pki/ca.crt /etc/openvpn/
- sudo cp ~/openvpn-ca/pki/issued/server.crt /etc/openvpn/
- sudo cp ~/openvpn-ca/pki/private/server.key /etc/openvpn/
- sudo cp ~/openvpn-ca/pki/dh.pem /etc/openvpn/

10. Ustvarimo datoteko s server konfiguracijo in vnesemo podatke.

- sudo nano /etc/openvpn/server.conf

port 1194

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh.pem

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

status openvpn-status.log

verb 3

11. Omogočimo posredovanje IP.

- sudo nano /etc/sysctl.conf
- odkomentiramo vrstico net.ipv4.ip_forward=1

12. Dovolimo prenos podatkov preko VPN.

- sudo ufw allow 1194/udp

13. Dodamo pravilo za prenos podatkov.

- sudo nano /etc/ufw/before.rules

*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -s 10.8.0.0/8 -o eth0 -j MASQUERADE

COMMIT

14. Omogočimo UFW.

- sudo ufw enable

15. Zaženemo in omogočimo OpenVPN.

- sudo systemctl start openvpn@server
- sudo systemctl enable openvpn@server

16. Konfiguracija klienta.

Na računalnik od klienta prenesemo datoteke ca.crt, client1.crt in client1.key. Potem pa ustvarimo datoteko client.ovpn in vanjo zapišemo:

client

dev tun

proto udp

my_raspberry_pi_IP 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

cert client1.crt

key client1.key

cipher AES-256-CBC

verb 3

(OpenVPN, 2024)

Konfiguracija in namestitev programske opreme WireGuard vključuje generiranje parov ključev in nastavitev konfiguracijskih datotek za strežnik in odjemalce.

1. Namestimo paket.

- sudo apt install wireguard -y

2. Generiramo zasebne in javne ključe strežnika in klienta.

- umask 077
- wg genkey | tee server_private.key | wg pubkey > server_public.key

- wg genkey | tee client_private.key | wg pubkey > client_public.key

3. Konfiguriramo WireGuard.

- sudo nano /etc/wireguard/wg0.conf

  [Interface]

  PrivateKey = [server_private_key]

  Address = 10.0.0.1/24

  ListenPort = 51820

  [Peer]

  PublicKey = [client_public_key]

  AllowedIPs = 10.0.0.2/32

4. Omogočimo IP posredovanje na enak način, kot smo to naredili pri OpenVPN in zaženemo ter omogočimo WireGuard ob zagonu naprave.

- sudo wg-quick up wg0
- sudo systemctl enable wg-quick@wg0

5. Konfiguracija klienta.

- nano wg0-client.conf

  [Interface]

  PrivateKey = [client_private_key]

  Address = 10.0.0.2/24

  [Peer]

  PublicKey = [server_public_key]

  Endpoint = your_server_ip:51820

  AllowedIPs = 0.0.0.0/0

6. Zaženemo WireGuard vmesnik pri klientu.

- sudo wg-quick up wg0-client

  (WireGuard, 2024)

5 VLOGA DOCKERJA PRI INTEGRACIJI VELEPODATKOV

5.1 Pregled Dockerja in njegove prednosti

Docker je platforma, ki uporablja tehnologijo kontejnerizacije za avtomatizacijo uvajanja, zagona in upravljanja aplikacij. Za razliko od tradicionalne virtualizacije, kjer vsaka aplikacija deluje na svojem virtualnem stroju z lastnim operacijskim sistemom, imajo Docker kontejnerji enako jedro operacijskega sistema, zaradi česar so lažji in učinkovitejši.

Ključne prednosti uporabe Dockerja so:

- Kontejnerji se lahko izvajajo v katerem koli sistemu, ki podpira Docker. To omogoča enostavno premikanje aplikacij med okolji, na primer iz razvoja v produkcijo.
- Kontejnerji so lažji od tradicionalnih navideznih strojev, saj imajo enako jedro operacijskega sistema, kar vodi do hitrejšega zagona in manjše porabe virov.
- Vsak kontejner deluje ločeno od drugih, kar zagotavlja, da aplikacije ne motijo ena druge. S tem se izboljša varnost in stabilnost.
- Docker omogoča enostavno prilagajanje aplikacij, po potrebi tudi z dodajanjem več kontejnerjev.
- Zagotavlja, da aplikacije delujejo dosledno v različnih okoljih, kar zmanjšuje težavo »ne deluje na mojem računalniku«.

(Docker Docs, 2024)

5.2 Primeri uporabe Dockerja v okolju z veliko podatki

Docker se veliko uporablja v podatkovno bogatih okoljih za racionalizacijo procesov, povečanje učinkovitosti in izboljšanje razširljivosti.

1. Cevovod (angl. *pipeline*) za obdelavo podatkov

- ETL procesi: Docker olajša postopke ekstrakcije, transformacije in nalaganja s kontejnerizacijo vsakega koraka. To zagotavlja nemoteno orkestracijo in izvajanje nalog obdelave podatkov, kar zagotavlja dosledno in izolirano okolje za ravnanje z velikimi podatki.

- Apache spark: Uvajanje Apache Sparka v Docker kontejnerje poenostavlja uvajanje in upravljanje ogrodij za obdelavo velikih podatkov. Omogoča dosledne konfiguracije v različnih okoljih, zaradi česar je idealen za zapletene naloge analize podatkov.

2. Strojno učenje in umetna inteligenca

- Kontejnerji standardizirajo okolje usposabljanja za modele strojnega učenja in zagotavljajo doslednost na različnih stopnjah razvoja. To omogoča nemoten prehod iz razvoja v proizvodnjo. Modele je mogoče zapakirati v kontejnerje, zaradi česar so prenosni in lažji za upravljanje, posodabljanje in prilagajanje.

(Landscape, 2024)

3. Upravljanje in shranjevanje podatkov

- Podatkovni kontejnerji: Zagon podatkovnih zbirk podatkov, kot so MySQL, PostgreSQL in NoSQL, pomaga vzdrževati izolirana in dosledna okolja zbirk podatkov. Ta nastavitev poenostavi postopke varnostnega kopiranja, obnovitve in selitve.
- Rešitve za shranjevanje velikih podatkov: Tehnologiji, kot sta Hadoop in Cassandra, je mogoče uporabiti v Docker kontejnerjih za učinkovito pridobivanje in shranjevanje podatkov v velikem obsegu. To zagotavlja prilagodljivost in razširljivost za povečanje virov glede na povpraševanje.

4. Integracija podatkov in analitika

- Integracijske platforme: Orodja, kot je Apache NiFi, se lahko uporabijo v kontejnerjih za avtomatizacijo podatkov. Platforme je mogoče enostavno uvesti in razširiti, kar zagotavlja prilagodljivost pri upravljanju podatkov in obdelavi delovnih tokov.
- Prenos podatkov v realnem času: Orodja, kot je Apache Kafka, se uporabijo za prenos podatkov in analitiko.

(How to Use Docker For Big Data Processing?, 2024)

5.3 Integracija Dockerja

Integracija Dockerja vključuje več ključnih korakov.

1. Namestitev Dockerja in zagon

- sudo apt install docker.io -y

- sudo systemctl start docker
- sudo systemctl enable docker

2. Kontejneriziranje aplikacij

Ustvarimo Dockerfile

```
FROM python:3.8-slim

WORKDIR /app

COPY . /app

RUN pip install -r requirements.txt

CMD ["python", "app.py"]
```

Ustvarimo sliko.

- docker build -t myapp:latest.
- docker tag myapp:latest myusername/myapp:latest
- docker push myusername/myapp:latest

3. Orkestracija in management

Docker compose uporabimo za definiranje in upravljanje aplikacij, ki imajo več kontejnerjev. Določimo, kako različni kontejnerji med seboj delujejo.

Zaženemo aplikacijo.

- docker-compose up

4. Neprekinjena integracija in neprekinjeno uvajanje (CI/CD)

Docker se integrira v cevovode za avtomatizacijo gradnje, testiranja in uvajanja kontejnerskih aplikacij. Pomagamo si lahko z orodji, kot so Gitlab CI, Jetkins in GitHub Action, ki nam te procese poenostavijo.

5. Implementacija orodij, kot sta Prometheus in Grafana, za spremljanje stanja in zmogljivosti zabojnikov. Za združevanje in analizo dnevnikov (log zapisov) uporabimo ELK Stack, ki je sestavljen iz Elasticsearca, Logstasha in Kibana.
6. Pravilna konfiguracija omrežne politike in uporaba orodij, kot je Docker omrežje (angl. *network*), da lahko izoliramo in zaščitimo komunikacijo kontejnerjev.

Z integracijo Dockerja lahko organizacije dosežejo večjo prilagodljivost, razširljivost in učinkovitost pri upravljanju svojih okolij velikih podatkov, kar na koncu vodi do izboljšane učinkovitosti delovanja in produktivnosti.

(Docker Docs, 2024)

6 PRAKTIČNI PRIMER: VARNOST OMREŽJA MALIH PODJETIJ DO 5 RAČUNALNIKOV

6.1 Opis omrežne infrastrukture

Omrežje za mala podjetja je sestavljeno iz petih medsebojno povezanih računalnikov, pametnih telefonov in tiskalnika v pisarni. Omrežno infrastrukturo sestavlja preprosta in varna mešanica potrošniških in odprtokodnih tehnologij. Brezžični usmerjevalnik tvori jedro omrežja in zagotavlja žični in brezžični dostop do vseh naprav. Raspberry Pi je tisto, kar naredi omrežje varno in hkrati obvladljivo. Povezan je z omrežjem preko Etherneta in konfiguriran za izvajanje več storitev:

Pi-hole: Ta del programske opreme deluje na Raspberry Pi in blokira oglase pri vseh napravah v istem omrežju. Pi-hole zajame in filtrira poizvedbe DNS, iz katere koli naprave v omrežju in blokira zahteve za vse znane domene, ki smo jih nastavili za prikazovanje oglasov. Onemogočili smo dostop tudi do družbenih medijev in socialnih mest, kot so Facebook, Facebook Messenger, Instagram, Gmail, X, TikTok, WhatsApp in Snapchat. To zmanjša neželene oglase in potencialno sledenje za veliko čistejšo in varnejšo izkušnjo brskanja za vse uporabnike.

VPN: Raspberry Pi je konfiguriran za zagotavljanje strežniških zmogljivosti VPN. To omogoča varno prijavo zaposlenih v pisarniško omrežje od doma ali od drugod. To še dodatno postavi šifriran tunel za podatke, da med postopkom prenosa ni mogoče prestreči občutljivih informacij.

Docker: Uporablja se za upravljanje in izolacijo različnih storitev. Podjetje lahko brez konfliktov zažene več aplikacij hkrati, saj je vsaka aplikacija v svojem kontejnerju neodvisna od drugih. Lahko bi uporabili tudi Pi-hole znotraj kontejnerja, da bi poenostavili posodobitve in varnostne popravke, vendar smo se odločili, da bo Pi-hole samostojen del Raspberry Pi.

Infrastruktura omrežja vključuje standardne potrošniške omrežne naprave. To so stikala (angl. *switch*), tiskalnik in dva usmerjevalnika, primarni je vezan neposredno na modem, ki smo ga

prejeli od ponudnika storitev. Naloga modema je, da ves internetni promet prenese do našega primarnega usmerjevalnika, ki nato povezavo spremeni v LAN linijo, ki jo uporabljamo znotraj podjetja. Omrežni tiskalnik je povezan znotraj omrežja in je zato dostopen vsem napravam, ki se nahajajo v isti mreži.

6.2 Strategija uvajanja za integracijo z Raspberry Pi, Pi-hole, VPN in Docker

V strategiji uvajanja smo dobro premislili, kako zaščititi omrežje v malem podjetju, kjer je cilj priti do ugodnih rešitev s čim manjšimi stroški. Navedli smo ključne komponente in ustrezne postopke uvajanja.

Konfiguracija Raspberry Pi: Za strojno opremo smo izbrali Raspberry Pi 5, saj ima dovolj močan procesor in dovolj velik RAM za naše potrebe. Zaščiten je z originalnim ohišjem. Nameščen je operacijski sistem Raspberry Pi OS na microSD kartici. To je lahek operacijski sistem, ki temelji na Linuxu in je optimiziran za našo strojno opremo.

Konfiguracija Pi-hole: Določili smo statični IP zaradi doslednega dostopa do naprave. IP naslov naprave smo morali tudi nastaviti v konfiguraciji usmerjevalnika kot prvi DNS strežnik. Za namestitev Pi-hole smo uporabili namestitveno skripto, aplikacija je bila nameščena za blokiranje oglasov in zlonamernih domen ter za izboljšanje varnosti.

Konfiguracija VPN: Dvojna implementacija OpenVPN in WireGuard je zagotovila, da je podjetje lahko izkoristilo prednosti obeh tehnologij in zagotovilo varne, zanesljive in učinkovite možnosti oddaljenega dostopa za vse zaposlene.

Docker integracija: Namestitev Dockerja na Raspberry Pi je bila narejena, da bi imeli sistem, kjer bi lahko vse potrebne storitve enostavno uporabljali v izoliranih kontejnerjih. Na ta način se bo vsaka storitev izvajala neodvisno, s čimer se bodo zmanjšali morebitni konflikti in varnostna vprašanja.

Testiranje in preverjanje: Izvedeno je bilo obsežno testiranje, da bi zagotovili stabilnost sistema in varnost. Pred tem smo zagotovili, da je Pi-hole pravilno blokiral oglase, da je bil pravilno omogočen na usmerjevalniku kot prvotni DNS in da so tudi VPN klienti bili vidni in zaščiteni znotraj Pi-hole nastavitev. Na sistemski ravni smo vzpostavili neprestano spremljanje in beleženje, da bi se spremljala uspešnost in da bi lažje sledili napakam v omrežju.

6.3 *Ocena učinkovitosti*

Ugotovili smo, da so izvedeni ukrepi za varnost omrežja uspešni v nekaterih ključnih vidikih.

Blokiranje oglasov in sledilcev na spletu: Občutno se je zmanjšalo število oglasov, prikazanih na vseh napravah, povezanih v omrežju. Ta korak je bil izjemen pri izboljšanju uporabniške izkušnje in zmanjšanju izpostavljenosti zlonamernim oglasom in sledilcem.

Varen oddaljeni dostop: Nastavitev VPN zaposlenim omogoča varen dostop do omrežja z oddaljenih lokacij. To je še posebej pomembno pri dostopu do občutljivih dokumentov in notranjih virov, hkrati pa zagotavlja, da podatki ostanejo zasebni s pomočjo šifriranih povezav.

Upravljanje omrežja in razširljivost: Z uporabo Dockerja številne storitve lažje upravljamo. To pomeni, da se postopki posodabljanja in vzdrževanja lažje izvajajo brez večjih izpadov ali večjih varnostnih groženj. Nastavitve se da tudi enostavno razširiti, če bodo v prihodnosti potrebne dodatne ali druge storitve.

6.4 *Analiza praktičnih omejitev*

Čeprav so se varnostni ukrepi izkazali za razmeroma učinkovite, obstajajo nekatere praktične omejitve in izzivi:

Omejitev stojne opreme: Raspberry Pi je odličen, vendar ima nekoliko manjšo procesorsko moč in pomnilnik v primerjavi z namenskimi strežniki, zato lahko v primeru izvajanja več storitev naenkrat vpliva na samoučinkovitost naprave.

Hitrost omrežja: Hitrost interneta je lahko ovirana ob prevelikem številu povezanih naprav v VPN. Čeprav je zelo majhna zakasnitev, postopek šifriranja vpliva na zmogljivost interneta, zlasti pri večjem prenosu podatkov.

Vzdrževanje in posodobitve: Posodabljanje sistema z najnovejšimi varnostnimi popravki ohranja računalniško opremo robustno in manj ranljivo za grožnje. Redni pregledi in morebitne nadgradnje obstoječega sistema glede na potrebe podjetja. Zanemarjanje teh posodobitev lahko privede do ranljivosti in zmanjšane učinkovitosti. Ročno vzdrževanje je lahko veliko breme, zlasti za mala podjetja brez namenske podpore IT.

Zavedanje uporabnikov: Zagotavljanje, da zaposleni pravilno uporabljajo VPN in se držijo varnostnih protokolov je bistvenega pomena. Zloraba ali neuspeh vklopa VPN med delom na daljavo lahko omrežje izpostavi morebitnim grožnjam. Dosledno doseganje skladnosti uporabnikov je lahko zahtevno in zahteva jasno komunikacijo in usposabljanje.

7 IZZIVI IN OMEJITVE

Implementacija rešitev za omrežno varnost z uporabo Raspberry Pi, Pi-hole, VPN in Docker v okolju majhnega podjetja predstavlja več izzivov in omejitev, ki lahko vplivajo na splošno učinkovitost in stabilnost nastavitve. Opredeljeni so bili naslednji ključni izzivi in omejitve:

1. Procesorska moč in pomnilnik

Raspberry Pi je vsestranska, cenovno učinkovita in dostopna naprava, vendar ima omejene zmogljivosti obdelave. Ta omejitev lahko povzroči težave z zmogljivostjo, zlasti pri hkratnem izvajanju več storitev, kot sta Pi-hole in VPN. Omejeni viri strojne opreme lahko ob veliki uporabi omrežja postanejo obremenjeni, kar lahko poslabša uporabniško izkušnjo.

2. Pasovna širina in zakasnitev

Uporaba Pi-hole za filtriranje DNS in VPN za varen oddaljeni dostop lahko uvede dodatno zakasnitev in vpliva na razpoložljivo pasovno širino. Postopek filtriranja v Pi-hole lahko povzroči zamude pri reševanju DNS, medtem ko lahko stroški šifriranja iz VPN dodatno vplivajo na delovanje omrežja, zlasti za aplikacije, ki zahtevajo pasovno širino.

3. Nepravilna konfiguracija omrežja

Pravilna konfiguracija omrežja je bistvenega pomena za nemoteno delovanje storitev VPN in Pi-hole. Omejitev izhaja iz nezadostnega znanja o konfiguraciji ali pomanjkanja nadzora nad obstoječo postavitvijo omrežja. Na primer, če modem, ki ga zagotavlja ponudnik internetnih storitev, ni nastavljen na način mostu (angl. *bridge*), lahko to povzroči obstoj dveh lokalnih omrežij (LAN) znotraj ene internetne povezave. Ta napačna konfiguracija lahko prepreči pravilno usmerjanje, kar povzroči okvaro VPN. Primer te težave se je pojavil v začetni fazi uvajanja, ko ponudnik interneta ni nastavil modema v način mostu, kar je otežilo nastavitev VPN. (Fitzpatrick, 2024)

4. Izzivi konfiguracije WireGuard VPN

Nastavitev in pravilno konfiguriranje VPN-ja, kot je WireGuard, zahteva tehnično strokovno znanje. Težave, kot so nepravilna pravila požarnega zidu, napačno konfigurirane usmerjevalne tabele ali napake pri upravljanju ključev, lahko povzročijo nedelovanje omrežja VPN. Med začetno uvedbo so napake pri konfiguraciji povzročile nedelujoč VPN, kar je zahtevalo dodatno odpravljanje težav in prilagoditve.

5. Varnostni pomisleki

Medtem ko uporabljene rešitve povečujejo varnost, te niso popolna zaščita. Pi-hole zagotavlja filtriranje in blokiranje oglasov na ravni DNS, vendar ne nadomešča celovitih varnostnih ukrepov, kot so požarni zidovi, varnostne rešitve za končne točke in sisteme za zaznavanje vdorov. VPN-ji varujejo podatke med prenosom, vendar ne obravnavajo notranjih omrežnih groženj.

6. Razširljivost in vzdrževanje

Trenutna infrastruktura je primerna za manjšo uporabo, vendar ima omejeno razširljivost. Ker podjetje raste in se omrežni promet povečuje, lahko obstoječa nastavitev strojne opreme postane nezadostna. Razširitev infrastrukture bi zahtevala nadgradnjo na robustnejšo strojno opremo ali ponovno konfiguracijo omrežja, kar bi lahko zahtevalo precejšnje časovne in finančne naložbe.

7. Tehnični izzivi

Uvajanje in vzdrževanje varnostnih nastavitev, ki temeljijo na Raspberry Pi, zahteva veliko znanja o Linuxu, omrežju in varnostnih protokolih. Malim podjetjem se nastavitve lahko zdijo zahtevne, kar lahko povzroči napačne konfiguracije ali premajhno izkoriščenost sistema. Usposabljanje ali neprestana podpora sta potrebni, vendar lahko zahtevata veliko sredstev.

8. Vpliv velikih podatkov

Orodja za nadzor omrežja ustvarjajo velike količine podatkov, zlasti v dnevnikih poizvedb DNS. Upravljanje in analiza teh podatkov je lahko zapletena in zahteva ustrezna orodja in strokovno znanje. Za mala podjetja lahko stroški obdelave in interpretacije teh podatkov predstavljajo velik izziv, ki zahteva dodatne naložbe v rešitve za upravljanje podatkov.

Medtem ko integracija Raspberry Pi, Pi-hole, VPN in Docker ponuja stroškovno učinkovito in prilagodljivo rešitev za varnost omrežja, je treba obravnavati več izzivov in omejitev. Ti vključujejo omejitve strojne opreme, pravilno konfiguracijo omrežja, vprašanja razširljivosti in potrebo po tehničnem strokovnem znanju. Poleg tega sta neprestano vzdrževanje in zagotavljanje skladnosti uporabnikov ključnega pomena za uspešno in varno delovanje omrežja.

8 SKLEP

Diplomsko delo se osredotoča na raziskavo možnosti uporabe Raspberry Pi ekosistema kot ključnega elementa za izboljšanje varnosti in upravljanja omrežij v malih podjetjih. Z analizo različnih tehnologij in rešitev, vključno z uporabo Pi-hole, VPN, Docker kontejnerjev in spletnim vmesnikom Grafana, smo pridobili dragocen vpogled v zmogljivosti in omejitve te majhne, a zmogljive naprave.

Hipoteza 1 je proučevala vpliv Pi-hole na blokiranje neželenih domen in izboljšanje varnosti omrežja. Primerjava je pokazala, da Pi-hole dnevno blokira okoli šest tisoč oglasov, kar predstavlja približno 10,71 % vseh poizvedb. Iz grafa so razvidne najpogosteje blokirane domene: mask.icloud.com, mask-h2.icloud.com, q.live.com, static.doubleclick.net, www.googletagmanager.com in googleads.g.doubleclick.net.

Testiranje zaščite pred zlonamerno programsko opremo (angl. *malware*), lažnim pretvarjanjem (angl. *phishing*) in pretvezo (angl. *scam*) spletnih strani smo preverili na dva načina, in sicer s pomočjo spletne strani (https://www.amtso.org/), kjer smo preveri, kako hitro Microsoft Defender zazna zlonamerno opremo, ko deluje samostojno brez uporabe Pi-hole, ki to spletno stran blokira in svetuje, da obisk te strani ni varen. Izvedli smo simulirane napade ugrabitev DNS (angl. *DNS hijacking*) in ponarejanje DNS (angl. *DNS spoofing*), s čimer smo preverili, kako Pi-hole blokira napade. Nato smo primerjali hitrost nalaganja spletnih strani. Teste smo izvedli na spletni strani https://www.webpagetest.org/. Testi so pokazali, da Pi-hole rahlo vpliva na nekatere metrike zmogljivosti spletne strani. Čas do prvega bajta (TTFB) se je nekoliko povečal, in sicer iz 1,505 s na 1,518 s, kar nakazuje na manjšo zamudo zaradi dodatnega DNS, ki gre skozi Pi-hole. Prav tako se je začetek prikaza strani povečal iz 4,000 s na 4,200 s, kar kaže na majhno zamudo pri prikazu prve vsebine. Kljub tem zamudam je izboljšava vidna pri vsebinski sliki (LCP), kjer se je čas zmanjšal iz 5,381 s na 5,307 s, kar nakazuje, da Pi-hole učinkovito blokira vsebino, ki bi sicer upočasnila prikaz strani. Premik postavitve (CLS) je bil skoraj nespremenjen, kar nam pove, da Pi-hole ne vpliva na stabilnost postavitve strani pred nalaganjem. Prav tako uporabniška interakcija ostaja nespremenjena, torej Pi-hole v resničnih pogojih nima bistvenega negativnega vpliva na uporabniško izkušnjo.

Hipoteza 2 je primerjala zmogljivost dveh spletnih strežnikov, Nginx in Lighttpd na Raspberry Pi. Za oceno zmogljivosti smo izvedli preizkus referenčnih vrednosti (angl. *benchmarks test*). Uporabili in primerjali smo dva spletna strežnika, Nginx in Lighttpd. Testi so bili izvedeni na

enaki napravi, z enakimi parametri, kar omogoča neposredno primerjavo med obema strežnikoma.

Nginx je bil konfiguriran za poslušanje na portu 8080. Nginx je uspel obdelati približno 16,457 zahtevkov na sekundo. Povprečen čas obdelave ene zahteve je bil 0,608 ms, prenosna hitrost je dosegla 13,628.77 KB/sec.

Lighttpd je bil nastavljen na portu 80, kjer je prav tako uspešno obdeloval vse zahteve. Dosegel je hitrost obdelave 16,424 zahtevkov na sekundo. Povprečen čas obdelave je bil 0,609 ms, prenosna hitrost je znašala 7,923.62 KB/sec.

Primerjava je pokazala, da sta oba strežnika delovala zelo dobro, saj sta na sekundo obravnavala približno 16.400 zahtev. Ob tem je je strežnik Nginx pokazal nekaj prednosti, saj je dosegel višjo hitrost prenosa podatkov kot Lighttpd, kar lahko pomeni, da je Nginx bolj optimiziran za prenos večjih količin podatkov.

Pi-hole je konfiguriran, da deluje kot požarni zid, ki uporablja iptables za filtriranje zlonamernega prometa. Nameščen je VPN Server z Wireguard aplikacijo, ki omogoča varen dostop do omrežja, ko smo zunaj pisarne. S programom Sirocato, ki teče v ozadju, spremljamo sumljive dejavnosti in morebitne vdore, s tem pa smo dodali tudi dodatno plast varnosti. Na podlagi izvedenih testov lahko potrdimo, da je Raspberry Pi učinkovita naprava za uporabo v podjetjih, saj z lahkoto podpira dva različna spletna strežnika s skoraj identično zmogljivostjo. Glede na rezultate je Raspberry Pi sposoben zadovoljiti potrebe manjših podjetij, ki potrebujejo zanesljivo spletno strežniško okolje ter več kot osnovno obrambo pred morebitnimi grožnjami. Ta ugotovitev potrjuje hipotezo, da je Raspberry Pi primerna naprava za uporabo v podjetniških okoljih, kjer so potrebe po spletnem strežniku zmerne, vendar zahtevajo zanesljivost in učinkovitost z visoko stopnjo varnosti.

Hipoteza 3 je obravnavala vpliv Pi-hole na hitrost internetne povezave. Testi so se izvajali en teden, da se je preverila hitrost povezave. Za namene testiranja smo uporabili Speedtest Tracker, ki smo ga namestili v Docker kontejner. Z uporabo Pi-hole je bila povprečna hitrost prenosa (angl. *download speed*) 815.95 Mbps, hitrost nalaganja (angl. *upload speed*) je bila 111.42 Mbps in zakasnitev (angl. *latency*) je bila 10.93 ms.

Brez uporabe Pi-hole je povprečna hitrost prenosa (angl. *download speed*) 837.98 Mbps, hitrost nalaganja (angl. *upload speed*) je 99.71 Mbps in zakasnitev (angl. *latency*) je 12.16 ms.

Iz tega lahko ugotovimo, da je povprečna hitrost nižja, ko ne uporabljamo Pi-hole, vendar je zaradi uporabe DNS hitrost večja, ko ne uporabljamo Pi-hole. Ugotovitve kažejo, da je hitrost nalaganja nekoliko počasnejša ob uporabi Pi-hole in DNS filtriranje učinkovito deluje, saj je odzivni čas hitrejši, kar za uporabnika pomeni hitrejše nalaganje strani in manj zakasnitev. To hipotezo smo zavrnili, saj ne vidimo pozitivnih vplivov na hitrost internetne povezave z uporabo Pi-hole.

Hipoteza 4 je raziskovala, ali povečanje omrežnega prometa izboljša učinkovitost varnostnih rešitev. Varnostni sistemi, ki jih uporabljamo za zaznavanje vdorov in zlonamernih napadov, so namenjeni predvsem za spremljanje in analizo omrežnega prometa in zaznavanje groženj. Menimo, da povečanje prometa ne naredi varnostnih rešitev bolj robustnih in učinkovitejših, temveč je mogoča preobremenitev varnostnega sistema. Napačna konfiguracija lahko vodi do mrtvih kotov oziroma lukenj v varnostnih sistemih. Ob tem pa ne smemo pozabiti, da nam ravno velika količina podatkov nudi podrobno analizo, kako povečati varnostne rešitve, pri katerih so bile zaznane napake. Visokokakovostni ustrezni podatki, ki natančno odražajo vedenje omrežja in vzorce groženj, so ključnega pomena za učinkovito analizo varnosti. Da bi zagotovili učinkovite varnostne rešitve ob povečanem omrežnem prometu velikih podatkov, je treba vključiti razširitev v oblaku. Neustrezna infrastruktura ob veliki količini podatkov in prometu lahko povzroči tako imenovana »ozka grla« v zmogljivosti, kar nam zmanjša učinkovitost varnostnih rešitev. To hipotezo smo zavrnili, saj nam velike količine podatkov in večji internetni promet veliko informacij za analizo zagotovijo vnaprej, vendar nam ne zagotovijo večje varnosti. Tukaj je pomembnejša razširljivost sistemov in kakovost podatkov za analizo.

Hipoteza 5 je proučevala vpliv Dockerja na razširljivost in prilagodljivost omrežnih varnostnih rešitev. Izvedli smo različne teste. Najprej smo uvozili podatke v Grafano, ki nam je prikazala porabo CPU-ja, porabo pomnilnika in omrežni promet. Meritve so pokazale, da lahko Docker učinkovito porazdeli obremenitve med različnimi kontejnerji. Grafi so pokazali, da dodajanje kontejnerjev ne porabi vseh virov, kar podpira hipotezo, da Docker izboljša razširljivost. Ob Grafani smo za prikaz podatkov v Docker želeli namestiti tudi ElasticSearch, in sicer skupaj s Kibano. Naleteli smo na težave, saj se je sistem porušil in bil neodziven tako dolgo, dokler nismo naprave fizično izklopili iz elektrike. Ker aplikacija zahteva preveč virov na naši strojni opremi, smo jo morali odstraniti, saj so bile vidne motnje na omrežju in napravi. Povečana je bila preobremenitev, pregrevanje in tudi glasnost naprave. Razširljivost Dockerja je v veliki meri odvisna od razpoložljivosti strojne opreme. Podatki, pridobljeni iz Grafane, so pokazali,

da sistem ni zdržal obremenitve ob zagonu kontejnerjev, saj vsi potrebujejo veliko količino virov in pomnilnika za delovanje. Testirali smo tudi poslani in prejeti promet v kontejnerjih. Največ aktivnosti je bilo vidnih v kontejnerju ElasticSearch in Kibana, ki nista samo zavzela veliko CPU-ja in pomnilnika, temveč sta tudi obremenila omrežje in povzročila nedelovanje omrežja in izpade. Hipotezo smo zavrnili na podlagi naših testov, z našo strojno opremo. V primeru izboljšane strojne opreme, ki ponuja več virov, predvsem glede pomnilnika in zmogljivosti CPU-ja, bi testi lahko pokazali popolnoma drugačne rezultate.

Hipoteza 6 je obravnavala zmogljivost Raspberry Pi pri večjih obremenitvah. Raspberrry Pi je zmogljiv, cenovno zelo ugoden, vendar zna povzročati težave pri večji obremenitvi internetnega prometa, kar je lahko ovira za večja podjetja. Konfiguracija in vzdrževanje Dockerja, Pi-hole in VPN zahteva tehnično znanje. Treba je imeti zaposlenega za vzdrževanje na področju IT ali poiskati pomoč zunaj podjetja. V podjetju sta potrebna vsaj dva računalnika, saj je treba imeti tudi kopijo, v primeru, da eden odpove, saj s tem preprečimo izgubo podatkov. To hipotezo smo glede na raziskave in z iskanjem podatkov, pridobljenih iz spleta in lastnimi testi, potrdili. Še vedno menimo, da si manjše podjetje do maksimalno pet računalnikov to lahko privošči, še posebej, če gre za IT podjetje. Če je v podjetju potreba po večjem številu virov, naša naprava ne bo več priporočljiva za uporabo. Kljub možni nadgradnji ne bo dovolj zmogljiva za zahtevnejše naloge.

Hipoteza 7 je raziskovala uporabo Raspberry Pi kot cenovno ugodno rešitev za mala podjetja. Mala podjetja zaradi omejenega proračuna pogosto iščejo rešitve v odprtokodnih platformah in v cenovno ugodnejših, a učinkovitih rešitvah, kot je v našem primeru Raspberry Pi, vsestranski mikroračunalnik. Na podlagi raziskav in testov smo ugotovili, da Raspberry Pi ponuja nekaj pomembnih prednosti, vendar ne predstavlja popolne alternative za zagotavljanje celovite varnosti v podjetju. Hipotezo smo zavrnili, saj se Raspberry Pi bolje obnese pri nalogah, kot so blokiranje oglasov, izmenjava datotek in nadzor nad sistemi, ne pa kot temeljna varnostna rešitev.

Celotno diplomsko delo je prispevalo k boljšemu razumevanju uporabe Raspberry Pi in povezanih tehnologij v malih podjetjih. Kljub določenim omejitvam naprave, predvsem v smislu zmogljivosti pri visokih obremenitvah, se je Raspberry Pi izkazal za učinkovito in cenovno ugodno rešitev za specifične varnostne naloge. Zastavljeni cilji so bili doseženi, pri čemer so se VPN povezave, Pi-hole in Docker kontejnerji izkazali za uporabne pri zagotavljanju osnovne varnosti in upravljanju omrežja. Pomemben vidik diplomskega dela je pridobitev praktičnih izkušenj pri konfiguraciji in upravljanju varnostnih rešitev, kar poudarja pomen

strokovnega znanja pri vzdrževanju in upravljanju omrežij v podjetjih. V nalogi smo izpostavili potrebo po morebitnih nadgradnjah strojne opreme ali optimizaciji programske opreme, da bi Raspberry Pi lahko še naprej služil kot učinkovita rešitev v različnih poslovnih scenarijih. Nadaljnje raziskave bi se lahko osredotočile na optimizacijo teh rešitev za bolj zahtevne poslovne aplikacije kot tudi na proučevanje možnosti uporabe Raspberry Pi v večjih podjetjih, z večjo stopnjo obremenitve. Prav tako bi bilo koristno raziskati, kako bi nadgradnja strojne opreme ali implementacija dodatnih varnostnih protokolov lahko še dodatno izboljšali varnost in zmogljivost.

9 LITERATURA IN VIRI

Block ads at home with Pi-hole. (06. Junij 2024). Pridobljeno iz Raspberry Pi: https://www.raspberrypi.com/tutorials/running-pi-hole-on-a-raspberry-pi/

Community, L. (30. Julij 2024). *What are the benefits and drawbacks of using Pi-hole as a DNS blackhole for your network*. Pridobljeno iz LinkedIn: https://www.linkedin.com/advice/0/what-benefits-drawbacks-using-pi-hole-dns

Docker Docs. (15. Julij 2024). Pridobljeno iz Install Docker Desktop on Linux: https://docs.docker.com/desktop/install/linux-install/

Docker Docs. (15. Julij 2024). Pridobljeno iz Docker overview: https://docs.docker.com/guides/docker-overview/

Faq-bot. (02. Junij 2024). *How do I configure my devices to use Pi-hole as their DNS server*. Pridobljeno iz Pi-hole: https://discourse.pi-hole.net/t/how-do-i-configure-my-devices-to-use-pi-hole-as-their-dns-server/245

Fitzpatrick, J. (20. Julij 2024). *How to Geek*. Pridobljeno iz What Is Bridge Mode on a Router, and Why Should You Use It: https://www.howtogeek.com/867942/what-is-router-bridge-mode/

Getting started with your Raspberry Pi. (11. Junij 2024). Pridobljeno iz Raspberry Pi Documentation: https://www.raspberrypi.com/documentation/computers/getting-started.html

Hosted VPN Solutions & Service. (13. Avgust 2024). Pridobljeno iz Perimeter 81: https://www.perimeter81.com/resources/hosted-vpn-service

How to Use Docker For Big Data Processing? (22. Julij 2024). Pridobljeno iz Geeks For Geeks: https://www.geeksforgeeks.org/how-to-use-docker-for-big-data-processing/

Landscape, B. D. (18. Julij 2024). *Big Data with Docker*. Pridobljeno iz Medium: https://medium.com/@big_data_landscape/the-ultimate-guide-of-docker-b3f2752f488b

OpenVPN. (15. Julij 2024). Pridobljeno iz Get & Install Access Server on Linux | OpenVPN: https://openvpn.net/as-docs/get---install-for-linux.html

Pi-hole. (30. maj 2024). Pridobljeno iz Pi-hole Network-wide Ad Blocking: https://pi-hole.net/

Pi-hole documentation. (10. junij 2024). Pridobljeno iz Overview: https://docs.pi-hole.net/guides/vpn/wireguard/overview/

Raspberry Pi. (23. April 2024). Pridobljeno iz Raspberry Pi: https://www.raspberrypi.com/products/raspberry-pi-5/

Team, D. (20. Avgust 2024). *Digiteum Sp. z o.o.* Pridobljeno iz Digiteum: https://www.digiteum.com/raspberry-pi-for-small-business/

Warner, A. (30. Maj 2024). *Github*. Pridobljeno iz Spletno mesto Github: https://github.com/pi-hole/pi-hole/#one-step-automated-install

What is a VPN. (Julij. 28 2024). Pridobljeno iz NordVPN: https://nordvpn.com/what-is-a-vpn/

WireGuard. (16. Julij 2024). Pridobljeno iz WireGuard: https://www.wireguard.com/install/