Oskari Saari

VERKKOSIVUN PALVELIMEN TIETOTURVA
CASE: RASPBERRY PI

Opinnäytetyö
Viestintä

2017

Kaakkois-Suomen
ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Oskari Saari	Medianomi (AMK)	Huhtikuu 2016
Opinnäytetyön nimi Verkkosivun palvelimen tietoturva case: Raspberry Pi		37 sivua
Toimeksiantaja Deltagon Group Oy		
Ohjaaja Marko Siitonen		

Tiivistelmä

Opinnäytetyö käsittelee verkkosivujen palvelimien tietoturvaa. Työssä käsitellään tapaustutkimuksena Raspberry Pi-tietokoneen valmistamista tietoturvalliseksi palvelimeksi. Työn tavoite on olla katsaus tietoturvaan ja Linux-palvelimien perusteisiin ja käytäntöihin.

Työn ensimmäisessä osiossa käsitellään tietoturvan perusteita ja käytäntöjä. Tämän tarkoituksena on olla suuntaa antava ohje tietoturvaratkaisujen arvostelua varten. Osiossa annetaan myös taustakatsaus palvelimista ja Raspberry Pi-tietokoneesta. Osion loppupuolella käsitellään yleisimpiä hyökkäyksiä, joita voi ilmetä staattisen verkkosivun palvelimella.

Toisessa osiossa tutkitaan käytännön esimerkein Raspberry Pi palvelimen käyttöönottoa tietoturvalliseksi verkkosivun palvelimeksi. Osiossa tutkitaan tärkeimmät tarvittavat ratkaisut turvallisen palvelimen asennukseen. Tietoturvaratkaisujen ohessa selitetään, milloin ja mitä uhkia vastaan ne ovat tarpeellisia. Osion loppupuolella tehdään tietoturvan tulevaisuudennäkymistä päättelyitä ja tutkitaan mahdollisia tulevaisuudessa tarvittavia toimenpiteitä liittyen Raspberry Pi palvelimen tietoturvaan.

Raspberry Pi tietokone valittiin tutkimuskohteeksi sen lähestyttävyyden ja helppokäyttöisyytensä tähden. Laite on sopiva lähtökohta tietokoneista ja palvelimista kiinnostuneille harrastelijoille ja opiskelijoille. Kaikkia tietoturvaratkaisuja kokeiltiin käytännössä Raspberry Pi palvelimella. Tarvittaessa tarkistettiin käytännössä tietoturvaratkaisujen eheys ja vaihtoehtoiset ratkaisut. Pi:n käyttöjärjestelmänä käytettiin laitteen suosituinta käyttöjärjestelmää Raspbiania. Palvelimella hostattu verkkosivu oli yksinkertainen staattinen html dokumentti.

Tutkimuksessa selvisi, että Pi:llä on suositeltavaa hyödyntää muutamia ylimääräisiä Raspberry Pi:n käyttötapaukseen liittyviä tietoturvaratkaisuja. Nämä toimenpiteet eivät välttämättä ole tarpeellisia etäpalvelimella. Suositeltavaa on myös hyödyntää etäpalvelimilla käytettyjä standardi tietoturvaratkaisuja.

Asiasanat

palvelin, linux, verkkosivu, tietoturva, raspberry pi

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Oskari Saari	Bachelor of Culture and Arts	April 2016

Thesis Title

Server-side Security of Websites
case: Raspberry Pi

37 pages

Commissioned by

Deltagon Group Oy

Supervisor

Marko Siitonen

Abstract

The subject of the thesis is server-side security of websites. The case study included in the study consists of preparing a Raspberry Pi-computer into a secure webserver. The objective of the study is to serve as an introduction to Linux server security basics.

The first section of the study covers the basis of information security. The purpose of the section is to give a basic understanding of the subject, which can be applied in critical assessment of information security methods and tools. The section also covers some background information about servers and Raspberry Pi in general. The section also discusses some of the most prominent attacks that might occur on a static website's server.

The second section consists of a practical look at preparing Raspberry Pi into a secure webserver. The section covers the mission critical steps to establishing a secure installation of a webserver. An explanation of when and why a solution is needed is provided regarding each security measure. The latter part of the section discusses possible security measures required in the near future regarding webserver security of a Raspberry Pi server.

Raspberry Pi computer was selected as a case study because of its ease of use and accessibility. The computer is an affordable starting point for students who are interested in computers and servers. All the security measures were tested on a live Raspberry Pi server. When required, each security measure's integrity and alternatives were tested in practice. The selected operating system was Raspberry Pi's favored system, Raspbian. The website hosted on the server was a simple static html document.

The study concluded that some extra security measures are required in using a Raspberry Pi as a home server. Some security solutions that wouldn't be necessary in a remote server are recommended in addition to standard server security practices.

Keywords

server, security, website, linux, raspberry pi

SISÄLLYS

SANASTO

Palvelin: Verkon kautta tai tietokoneen sisäisesti sisältöä ja palveluja tarjoava järjestelmä. Koostuu järjestelmästä ja palvelinohjelmistosta.
Komentojono: Tekstipohjainen käyttöliittymä tietokoneen käyttöön, jonka kautta syötetään komentoja toimintojen suorittamiseksi.
Linux-jakelu: Linux-käyttöjärjestelmä, joka koostuu yleensä ohjelmistokokoelmasta, Linux-ytimestä ja paketinhallintajärjestelmästä.
Hostaus: Verkkosivun ylläpito palvelimella.
Staattinen verkkosivu: Verkkosivu, jonka sisältö riippuu verkkosivun HTML-dokumentista. Verkkosivun sisältöä muokataan vain muokkaamalla HTML-dokumenttia ja siihen linkitettyjä tiedostoja.
Dynaaminen verkkosivu: Verkkosivu, jonka sisältöä hallitaan palvelimenpuoleisella käsittelyllä. Voi käsitellä verkkosivun käyttäjien syöttämää dataa.
Operaattori: Tässä opinnäytetyössä viitataan operaattorilla teleoperaattoreihin. Hoitaa tietoliikenteen välitystä yhteyden tilaajien välillä.
Webhotelli: Palvelu, joka vuokraa levytilaa ja työkaluja asiakkaille verkkosivujen ja palveluiden ylläpitoa varten.
Haavoittuvuus: Tietoturva-aukko.
”sudo” -komento: Komento, jolla Linux-järjestelmillä tavalliset käyttäjät suorittavat pääkäyttäjän oikeuksilla komentoja.
IP-osoite: Laitteelle osoitettu osoite, josta laitteeseen voidaan muodostaa yhteys verkossa.
Protokolla: Määrittelee kuinka, milloin ja miten tietokoneen on tarkoitus toimia ja vastata kun sille osoitetaan pyyntö.
Kryptaus: Viestien tai tiedon sisällön salaus salausalgoritmeillä sellaiseen muotoon, jota ei voi lukea ilman salausavainta.

1 JOHDANTO

Internet on kehittynyt muutaman vuosikymmenen aikana valtavaksi maailmanlaajuiseksi ilmiöksi. Jokaisen meidän taskussamme on jatkuvasti ulottuvilla pieni tietokone, joka on portti tähän maailmaan. Työssä ja vapaa-ajalla, olemme yhteydessä sen kautta ystäviimme, uutisiin ja työkaluihin. Nykymaailmassa kaikki ovat jonkinlaisessa riippuvuussuhteessa tämän verkon kanssa joko suorasti tai epäsuorasti.

Tällaisen työkalun ollessa meidän jokapäiväisessä käytössä, on erittäin tärkeää pitää siitä huolta. Me lähetämme kaikenlaista dataa internetin välityksellä. Oli tämä data sitten kuvia, käyttäjätietoja tai luottamuksellisia asiakirjoja, emme halua sen joutuvan vääriin käsiin. Tietojen käsitteleminen turvallisesti on sekä käyttäjän että verkkosivun kehittäjien vastuulla. Käyttäjä saa toki käsitellä tietojaan oman makunsa mukaan, mutta kehittäjille lankeaa kokonaisvastuu kaikkien verkkosivun käyttäjien tiedoista.

Kuka vain pystyy nykyään pienellä harrastuneisuudella laittamaan internettiin pystyyn oman osoitteensa. Tietokoneiden kehitystahdin ansiosta tarpeeksi tehokkaan verkkosivun palvelimen omistaminen on nykyään erittäin edullista. Yhtenä edullisimmista nykyaikaisista ratkaisuista on pienen pankkikortin kokoisen Raspberry Pi-tietokoneen asentaminen palvelimeksi. Ongelmana aloittelevan palvelimen ylläpitäjän pystyttämässä palvelimessa on usein huomiotta jäävät tietoturvariskit. Vaikka verkkosivu ei käsittelisi minkäänlaisia käyttäjätietoja, huonosti turvattu Raspberry Pi-palvelin on uhaksi palvelimenhaltijalle, tuleville sivun käyttäjille ja muille palvelimeen liittymättömille osapuolille.

Nykyaikaisten tietokoneiden monimutkaisuuden tähden on jokaisessa laitteessa tietoturvariski, oli se sitten ihmisen tulosta tai luonnonvoimien aiheuttamaa. Palvelimen saa kuitenkin muutamalla toimenpiteellä muodostettua huomattavasti tietoturvallisemmaksi. Monimutkaisen verkkosivun tietoturvaaminen on monivaiheinen ja vaikea prosessi, mutta yksinkertaisen verkkosivun voi muutamalla tehokkaalla nykyaikaisella ratkaisulla tehdä helposti paljon turvallisemmaksi.

2 TUTKIMUKSEN TAUSTAA

Tämä opinnäytetyö käsittelee verkkosivujen Linux-palvelimien nykyaikaisia tietoturvaratkaisuja. Tapaustutkimuksena käsitellään Raspberry Pi-tietokoneen asennusta tietoturvalliseksi verkkosivun palvelimeksi. Opinnäytetyön tavoitteena on valaista tietoturvaan tutustuvalle Linux-palvelimien tietoturvakäytäntöjä ja ratkaisuja.

Raspberry Pi-tietokone on sopiva lähtökohta ensimmäisen palvelimen valmistelua varten. Raspberry Pi on piirilevyn kokoinen tietokone, joka maksaa korkeintaan muutaman kymmenen euron verran. Hintansa tähden tietokone on sopiva lähtökohta harrastelijalle, joka haluaa turvallisen ja hallitun harjoitteluympäristön Linux-palvelimien tutkimiseen.

Työ keskittyy Raspberry Pi:n suosituimman käyttöjärjestelmän, Raspbianin, tietoturvaamiseen. Opinnäytetyössä käsitellyt työkalut ja ohjelmistot pitäisivät toimia myös monilla muilla Linux käyttöjärjestelmillä miltei, ellei täsmälleen samalla tavalla. Raspbian on tehty Debian käyttöjärjestelmän pohjalta, ja molemmat toimivat käytännössä miltei identtisesti. Myös Debianin pohjalta kehitetty Ubuntu-käyttöjärjestelmä pitäisi olla suoraan yhteensopiva opinnäytetyössä käytettyjen ohjelmien asetuksien ja toiminnallisuuden kanssa.

Opinnäytetyössä selvitetään lukijalle jokaisen tietoturvaratkaisun tarpeellisuus. Pyrkimyksenä on kehittää lukijalle selkeä ymmärrys ohjelmien ja toimintojen käytöstä palvelimen tietoturvan asiayhteydessä. Lisäksi tavoitteena on selvittää mahdolliset uhkatekijät, jotka saattavat käyttää hyväkseen työkaluista aiheutuvia tietoturva-aukkoja. Työssä käsitellään myös tärkeimpiä tietoturvan perusteita ja käytäntöjä yleisesti ja Linux-palvelimeen liittyen.

Opinnäytetyön Raspberry Pi tapaustutkimuksessa tavoitteena on toistaa tietoturvaratkaisut käytännössä. Pyrkimys on tutkia ratkaisujen tehokkuutta ja selvittää tarvittaessa vaihtoehtoisia ratkaisuja. Tutkimuksen tavoitteena on olla riittävä lähtökohta Linux-palvelimien perustietoturvaan ja käyttöön. Opinnäytetyön pääkohderyhmänä on Linux-tietokoneiden perustoiminnallisuuden ja komentojonon yleisimpien komentojen hallitsevat aloittelevat tietokoneharrastelijat ja -opiskelijat.

3 TYÖN POHJUSTUS

Ennen palvelimen käyttöönottoa on suositeltavaa tietää perustietoja ja käytäntöjä liittyen palvelimiin ja tietoturvaan. Tietämällä tietoturvakäytännöt ja syyt ratkaisuihin, voi palvelimen ylläpitäjä tehdä informoituja päätöksiä palvelimen asennuksessa. Kaikki Linux-palvelimien tietoturvaratkaisut perustuvat näihin käytäntöihin. Tietämällä ratkaisut ja niiden käyttötilanteet, voi käyttäjä päättää tarvitaanko tietoturvaratkaisua lainkaan, vai tuleeko se ottaa käyttöön toisessa muodossa.

3.1 Verkkosivujen palvelimet

Verkkotuotanto on tullut lähivuosina kasvavissa määrin suurempaan rooliin. Jokapäiväisessä käytössä olevat suuret verkkosovellukset kuten Netflix, Facebook, Airbnb ja Uber ovat kasvattaneet kiinnostuksen verkkotuotantoon monien startup-yrityksien muodossa. Tämä kiinnostus on muun muassa ilmentynyt Slush startup-tapahtuman suosion kasvussa. Näiden startup-yrityksien sovelluksien rajapintana on joko älypuhelimen appi tai verkkosivusto. Tämä rajapinta on yhteydessä yleensä jonkinlaiseen palvelimeen, jossa käsitellään kaikkien käyttäjien toiminnot ja lähettämä data.

Tällä palvelimella useimmiten on käytössä Unix pohjainen käyttöjärjestelmä. Unix-käyttöjärjestelmiin kuuluvat muun muassa käyttöjärjestelmät, kuten Applen macOS, Sun Microsystemsin Solaris ja kaikki eri variaatiot Linux-käyttöjärjestelmistä. Nämä Unix-palvelimet kattavat tällä hetkellä 26. helmikuuta 2017 66.6 % kaikista verkkosivujen palvelimista (Usage of operating systems for websites 2017). Kaiken kaikkiaan verkkosivujen palvelimista 37.1 % on Linux-palvelimia. Näiden Linux palvelimien variaatioista suosituimmat ovat Ubuntu, Debian ja CentOS. (Usage statistics and market share of Linux for websites 2017.)

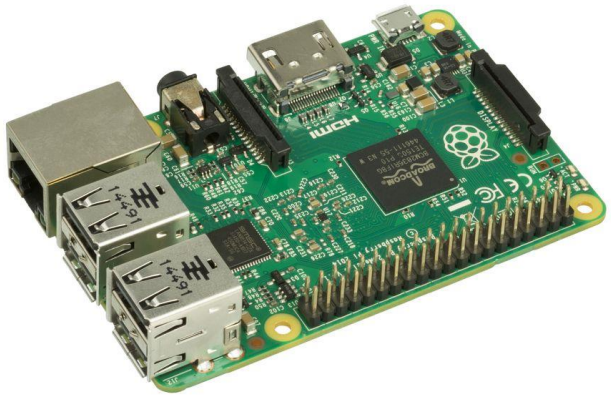
Debianin pohjalta on kehitetty Raspberry Pi-tietokoneen suosituin käyttöjärjestelmä Raspbian. Vaikka Pi:lle voi asentaa melkein minkä tahansa Unix-pohjaisen käyttöjärjestelmän, on suositeltavaa asentaa käyttöjärjestelmä, joka on kevyt ja optimoitu Raspberry Pi:lle. Pi on pieni piirilevyn kokoinen tietokone, ja

laitteen suorituskyky pitäytyy samassa suhteessa kuin sen koko. Raspbian-käyttöjärjestelmä ottaa huomioon laitteen suorituskyvyn ja tarjoaa tiiviin Linux-paketin, jolla pystyy tekemään käytännössä kaikkia tietokoneen perustoimintoja verkkoselaimen käytöstä videoiden katsomiseen.

Jotta Raspberry Pi-tietokoneesta saisi muodostettua tehokkaan ja tietoturvallisen verkkosivun palvelimen, on suositeltavaa olla käyttämättä käyttöjärjestelmän graafista käyttöliittymää resurssien säästämiseksi. Miltei kaikki palvelimen ylläpidon työkalut ovat käytettävissä vain komentojonossa. Usein palvelimien ylläpitäjät tähtäävät pitämään palvelimen ohjelmiston mahdollisimman minimaalisena tietoturvasyistä. Tästä syystä Linux-palvelimissa on harvemmin ollenkaan graafista käyttöliittymää käytössä.

3.2 Raspberry Pi-tietokone

Raspberry Pi on Raspberry Pi Foundationin kehittelemä tuote. Ensisijaisena järjestön tavoitteena on edistää tuntemusta digitaalisesta maailmasta ja tuottaa edullisia työkaluja tämän tavoitteen saavuttamiseksi. Pi-tietokoneet ovat täten erinomainen ratkaisu opiskelijoille ja harrastelijoille tietokoneisiin syventymistä varten. Pi-tietokoneet ovat keränneet ympärillensä suuren yhteisön kehittäjiä ja tietokoneharrastelijoita.



Kuva 1. Raspberry Pi-tietokone

Pi-laitteet ovat kehittyneet esineiden internetin (engl. Internet of things) suosituimpien työkalujen joukkoon monesta syystä. Raspberry Pi on hinta-laatusuhteensa ansiosta sopiva ratkaisu tietokoneharrastelijoille. Hinnoittelunsa tähden laite on turvallista asettaa sen äärirajoille ja korvata uudella Pi:llä tarvittaessa. Pi tietokone käyttää mallista riippuen todella vähän virtaa, ja edullisimpia

Raspberry Pi Zero-malleja voi jopa pitää käynnissä pelkällä USB portista saadulla vähäisellä virransyötöllä.

Kokonsa tähden Pi sopii hyvin moniin eri tarkoituksiin. Monet käyttävät Pi-laitteita harrastusprojektiensa ytimenä, joista yleisiä ovat muun muassa retropelikoneet, mediakeskukset ja äänentoistolaitteet. Kaiken lisäksi Pi:n laitteistossa ei ole ollenkaan liikkuvia osia, joten se on täysin hiljainen ja täten sopiva laite olemaan jatkuvasti käynnissä myös kotiolosuhteissa. (http://www.zdnet.com/article/raspberry-pi-11-reasons-why-its-the-perfect-small-server/)

Palvelimeksi Pi on kustannustehokas ratkaisu. Vaikka verkkosivun palvelimen voi saada nykyään ilmaiseksi yksinkertaisille staattisille verkkosivuille, yhtään dynaamisempien verkkosivujen palvelimista joutuu kuitenkin maksamaan kohtuullisia kuukausittaisia hintoja. Joka tapauksessa näitä palveluita käyttäessä käyttäjä joutuu sietämään rajoitettua palvelimenhallintaa ja ominaisuuksien puutetta.

Raspberry Pi:lle pystyy palvelimenhaltija kehittämään melkein minkälaisen vaan verkkosivun. Raspbianilla voi käyttää verkkosivun palvelimenpuoleisena ohjelmointikielenä kaikkia kieliä mitä muissakin Linux käyttöjärjestelmissä voi käyttää. Kuitenkin mitä massiivisemmaksi verkkosovellusta kehitetään, sitä huonompi vaihtoehto Raspberry Pi on sovellukselle. Intensiiviset operaatiot tai suuret sovellusten tietokannat kannattaa pitää pienenä ottaen huomioon Pi:n suorituskyky.

Muutaman satunnaisen käyttäjän verkkosovellusta pystyy Pi vielä käsittelemään, mutta jos tavoitteena on saada laajempaa käyttäjäkuntaa verkkosivulle, Raspberry Pi luonnollisesti ei ole optimaalinen ratkaisu. Hostaus- ja pilvipalvelut ovat yleensä suunniteltu skaalautumaan paremmin kävijämäärän mukaan ja tarvittaessa palvelimen kaistaa ja tehoa pystyy parantamaan helposti siirtymällä sopivampaan hostauspakettiin. Raspberry Pi on verkkosivun palvelimena kuitenkin riittävä sivuille, joilla ei ole jatkuvaa kävijäkuntaa tai muuta intensiivistä prosessointia, kuten portfoliosivuissa, yksinkertaisissa yrityksien aloitussivuissa tai kevyissä verkkosovelluksissa.

3.3 Tietoturvan käytännöt

Helpoin mahdollinen keino laittaa verkkosivu näkyville ulkomaailmalle on asentaa palvelimelle palvelinohjelmisto, kuten Apache tai Nginx, ja siirtää verkkosivun tiedostot palvelinohjelmiston verkkosivun oletuskansioon. Jos reititin ei ole palvelimen edessä estämässä ulkopuolista liikennettä yhdistämästä palvelimeen, on verkkosivu nyt tavoitettavissa mistä tahansa maailman kolkasta palvelimen IP-osoitteesta.

Palvelin on kuitenkin vielä täynnä tietoturvariskejä. Internetissä virukset leviävät joskus automaattisesti koneesta toiseen. Hakkerit yrittävät murtautua palvelimille haasteen, maineen ja rahan vuoksi. Rikollisryhmät saalistavat lunnaita takavarikoimalla tietokantoja. Nämä hyökkäykset kohdistuvat niin suuriin yhtiöihin, kuin myös pieniin palvelimiin.

Monien tekijöiden tähden palvelimen tietoturvaa on miltei mahdotonta taata. Täydellisen turvallinen järjestelmä olisi sellainen, joka tekee täsmälleen sen, mitä se on suunniteltu tekemään eikä yhtään sen enempää. Tarpeeksi monimutkaisissa järjestelmissä on kuitenkin mahdotonta määrittää järjestelmältä toivottua käytöstä. (Zalewski 2011, 10.) Tietoturvaa varten ei olla kehitetty varmoja ratkaisuja, mutta muutamat tehokkaat kokemuksen tuloksena kehitetyt toimintamallit ovat vakiintuneet tietoturvan vankaksi perustaksi. Tehokkaimpia lähestymistapoja tietoturvaan on rakentaa turvaratkaisut kerroksittain. Mitä enemmän tietoturvakerroksia on käytössä, sitä vaikeammaksi hyökkääjän työ käy.

Monien tietoturva-ammattilaisten yleisesti hyväksymä tietoturvamalli on nimeltään CIA (Confidentiality, Integrity and Availability). Tämä malli jakautuu kolmeen osioon. Ensimmäinen osio, luottamuksellisuus, tarkoittaa että tiedon käsittely on mahdollista vain käyttäjille, joilla on tietoon oikeudet. Eheys tarkoittaa, että tietoa ei saa muokata virheelliseksi tai vääräksi. Saatavuus tarkoittaa, että tieto tulee olla saatavilla käyttäjille silloin kun tarpeellista. Näitä periaatteita toteutetaan käytännössä toisella kolmen vaiheen järjestelmällä. (Red Hat Enterprise Linux 4 - Security Guide 2008.)

3.3.1 Tunnistaminen

Ensimmäinen vaihe on käyttäjän tunnistaminen. Käyttäjän tunnisteen päättämisen tulee riippua siitä, kuinka laaja-alaisessa järjestelmässä sitä käytetään. Riippuen onko kyseessä esimerkiksi maailmanlaajuinen verkkopalvelu tai paikallinen yritys, tunnistuksen muoto vaihtelee. Ainutlaatuisella tunnuksella pyritään muodostamaan käyttäjille vastuuvelvollisuus ja kulunvalvonta. Oskari Saari nimiselle käyttäjälle tunniste voi olla vaikka osaari pienemmässä yrityksessä, tai isommissa organisaatioissa, oskari.saari. (Chirillo & Danielyan 2005, 6.)

Käytännössä Linux palvelimissa tunnisteet ovat käyttäjien käyttäjänimet. Raspberry Pi palvelimella ei luultavasti kannata edes päästää hirveästi käyttäjiä sisään koneen suorituskyvyn tähden. Palvelimella, joka on yksittäisen henkilön käytössä, ei hirveästi väliä käyttäjänimen valinnassa. Kuitenkin turvallinen käyttäjänimi palvelimella on suositeltavaa olla joku muu kuin oletuskäyttäjät kuten Raspberry Pi:n ”pi”-käyttäjä. Lisäksi, mitä vähemmän käyttäjiä on palvelimella, sitä turvallisempi se on.

3.3.2 Todentaminen

Seuraava vaihe on käyttäjän todentaminen. Käyttäjältä vaaditaan jonkinlaista tietoa, jolla pystytään todistamaan, että käyttäjä on todella kuka hän väittää olevansa. Tämä voidaan suorittaa kolmella eri keinolla: ”mitä sinä tiedät”, ”mitä sinulla on” ja ”mitä sinä olet”. ”Mitä sinä tiedät” tarkoittaa, että käyttäjältä kysytään yleensä jonkinlainen PIN-koodi tai salasana. ”Mitä sinulla on” tarkoittaa jonkinlaista tunnistetta, jonka vain sinä omistat, kuten vaikka kertakäyttösalasanasovellukset (OTP), sirukortti tai USB tunnistuslaite. Viimeinen tapa on ”mitä sinä olet”, joka tarkoittaa käytännössä yleensä biometristä tunnistautumista. Biometrinen tunnistautuminen voidaan muun muassa tehdä käyttäen silmän iiristä tai sormenjälkeä. (Chirillo & Danielyan 2005, 7.)

Todentaminen Linux-palvelimella yleensä suoritetaan käyttäjän kirjautuessa käyttämällä tavallista salasanaa. Tämä on oletuskeino, mutta muita turvallisempia vaihtoehtoja on esim. SSH-avainparitiedostojen muodostaminen todennuskeinoksi. SSH-avainparien käyttö vaatii salasanan avaimen salauksen

purkamiseksi, joten tässä todennuskeinossa yhdistyy todennuskeinot ”mitä sinä tiedät” ja ”mitä sinulla on”.

3.3.3 Valtuutus

Viimeinen vaihe prosessissa on käyttäjän valtuutus. Käyttäjän tunnistauduttua järjestelmään, annetaan edeltävän tunnistautumisen mukaisia oikeuksia hallinnoida järjestelmää. Nämä oikeudet annetaan sen mukaan, mitä järjestelmän ylläpitäjä on luovuttanut kyseiselle käyttäjälle käyttäjän luonnin yhteydessä tai lisännyt jälkeenpäin.

Nämä mainitut kolme vaihetta ovat tehokas tapa käyttäjien vahvistamiseen ja vastuuvelvollisuuden muodostamiseen. Käyttäjien asettaminen vastuuseen teoistaan on yksi tärkeimpiä tietoturvaratkaisuja palvelimella. Järjestelmää ei voi pitää turvallisena, jos käyttäjiä ei aseteta vastuuseen teoistaan. Käyttäjien seuraus usein toteutetaan lokitiedostoilla ja jäljitysketjuilla (engl. audit trail). Ilman tällaista vastuuvelvollisuutta ei pysty tietämään mitä on tapahtunut ja mitä ei ole tapahtunut palvelimella tietoturvamurron tapahtuessa. (Chirillo & Danielyan 2005, 9.)

Yleisin keino asettaa käyttäjät vastuuseen teoistaan ovat lokitiedostot. Linux palvelimella on monia eri lokitiedostoja valmiiksi, joihin eri ohjelmat ja toiminnot tallentavat tapahtumia. Nämä tiedostot sijaitsevat Raspbian-käyttöjärjestelmässä kansiossa /var/log/. Yksityiskohtainen lokijärjestelmä käyttäjien toimintojen tutkimiseen ovat käyttäjän komentojonolla suoritettujen komentojen historia. Käyttäjien vastuuseen asettamiseen on muitakin keinoja ja työkaluja, joita voi ottaa käyttöön tarpeen ja tietoturvatason vaatiessa.

3.4 Haavoittuvuudet

OWASP eli Open Web Application Security Project on verkkoyhteisö, jonne kerätään tietoa verkkosovellusten tietoturvasta. Tällä yhteisöllä on lista kymmenestä yleisimmästä verkkosovellushaavoittuvuuksiin liittyvistä tietoturvariskeistä. Vähintään tästä OWASP:n Top 10 haavoittuvuuksien listasta kannattaa olla perillä verkkosovellusta kehittäessä. Staattiseen verkkosivuun moni näistä haavoittuvuuksista ei vaikuta niin paljon, sillä moni haavoittuvuuksista liittyy

käyttäjien syöttämän datan käsittelyyn ja istunnonhallintaan. Muutamasta haavoittuvuudesta kannattaa olla kuitenkin tietoinen, oli kyseessä sitten staattinen verkkosivu tai ei. Nämä haavoittuvuudet usein liittyvät enemmän palvelimen käyttöjärjestelmän tietoturvaan kuin verkkosivuun itseensä.

Suurimmat palvelimen haavoittuvuudet ovat usein käyttäjänhallintaan liittyviä. Heikko palvelimen salasana on yksi tärkeimpiä huomioon otettavia riskejä. Raspberry Pi:n tapauksessa tämän on erityisen tärkeää ottaa huomioon, sillä Pi:n oletusasennuksessa ei automaattisesti tehdä uutta käyttäjää käyttöjärjestelmään. Jos palvelinta haluaa hallita etäältä, on etenkin suositeltavaa tehdä palvelimelle tunnistautuminen turvalliseksi. Verkossa heikosti turvattujen palvelimien käyttäjänhallintaan usein hyökätään ns. brute force ja sanakirjahyökkäyksillä.

Brute force -hyökkäyksellä pyritään kokeilemaan kaikkia mahdollisia merkkiyhdistelmiä kirjautuessa sisään palvelimelle. Brute force -hyökkäys on laaja-alainen, sillä se tarkastaa käytännössä kaikki mahdolliset kirjautumistunnukset ja keinot. Samalla tämä hyökkäystapa on erittäin hidas, joten se on käytännössä hyödyllinen vain murtaessa tunnuksia, jotka ovat lyhyitä. Usein tätä hyökkäystä vastaan turvaudutaan estämällä liian monen epäonnistuneen kirjautumisyrityksen jälkeen yhdistäminen palvelimeen.

Sanakirjahyökkäys on yleisempi hyökkäystapa pienempiä palvelimia vastaan. Palvelimella saattaa olla ohjelmistoa, joka on unohtunut konfiguroida kunnolla. Tätä vastaan sanakirjahyökkäystä usein hyödynnetään. Hyvänä käytännön esimerkkinä on MongoDB nimisen tietokantaohjelman haavoittuvuus. Oletusasetuksilla tietokantaan pystyi kirjautumaan sisään ilman salasanaa oletuskäyttäjänä. Monet olivat avanneet tietokannan suoraan verkosta saavutettavaksi, joka avasi monille hyökkääjille helpon tien tietokantojen takavarikointiin ja lunnasvaatimuksien tekemiseen. Tällaisiin tapauksiin hyökkääjät yleensä käyttävät botteja, jotka käyttävät valmiita salasanalistoja tai ”sanakirjoja” haavoittuvaisiin verkkopalveluihin kirjautumiseen. (Blocking Brute Force Attacks 2016.)

Samaan MongoDB tapaukseen liittyen, on erittäin tärkeää, että palvelimien ohjelmisto pidetään päivitettynä ja täten turvallisena. MongoDB:n oletusasetukset korjattiin nopeasti haavoittuvuuden löytymisen jälkeen. (Masters 2017.) Ohjelmistoissa on aina mahdollista, että ilmenee tietoturva-aukkoja päivityksien yhteydessä. Näitä varten tuotetaan jatkuvasti uusia korjaavia tietoturvapäivityksiä. Tämän takia palvelimen ohjelmistoa on suositeltavaa päivittää mahdollisimman usein ja mielellään heti kun tietoturvapäivitys ilmenee. Päivityksiä suositellaan myös ottamaan vastaan vain luotettavista lähteistä.

Nämä ovat muutamia tärkeimpiä tietoturvariskejä liittyen staattisen verkkosivun Raspberry Pi palvelimen tietoturvaan. Muista tietoturvariskeistä saa lisätietoa OWASP:n verkkosivuilta osoitteesta owasp.org. OWASP tarjoaa ratkaisuja ja muuta syvempää tietoa jokaiseen haavoittuvuuteen liittyen. Etenkin jos verkkosovellus käsittelee käyttäjän syöttämää dataa tai käyttäjätunnuksia, tulee kehittäjän olla perillä mahdollisista riskeistä ja turvakeinoista niiden käsittelyyn liittyen.

4 PALVELIMEN TIETOTURVA

Tässä kappaleessa käsitellään toimenpiteet Raspberry Pi-palvelimen tietoturvaamista varten. Tietoturvaa voi hioa loputtomiin ja uusia ratkaisuja tulee koko ajan lisää, joten tavoitteena tässä osiossa on selvittää vain tärkeimmät ratkaisut kotipalvelimen turvaamiseksi. Tavoite on tehdä tästä rajatusta katsauksesta hyvä lähtökohta Linux palvelimien tietoturvaan syventymiseen.

Käyttämäni laite on Raspberry Pi 3 model B. Käyttöjärjestelmänä laitteelle on asennettu Raspbian Jessie Lite. Tässä käyttöjärjestelmäversiossa ei ole ollenkaan graafista käyttöliittymää. Lisää tietoa Raspbianin asennuksesta saa osoitteesta raspberrypi.org. Palvelimella hostattu verkkosivu on yksinkertainen staattinen html dokumentti.

Ohjeita seuraavan on suositeltavaa osata käyttää yleisimpiä Linux-komentojonossa käytettyjä komentoja, kuten cd, ls, apt, rm, rmdir, mv ja muita vastaavia. Myös joku komentojonossa käytettävä tekstinmuokkaustyökalu on osattava ohjeiden seuraamista varten. Hyviä helppokäyttöisiä tekstieditoreja ovat

”nano” ja ”ne”. Nano on jo valmiiksi asennettu Raspbianiin ja on hyvä yksinkertainen vaihtoehto, mutta ne-editori saattaa olla parempi ja monipuolisempi vaihtoehto Windowsin tekstieditoreista pitäville.

Ohjeissa merkitään komentojen alku merkillä ”>”. Tiedostot ja hakemistot merkitään muodossa ”/hakemisto/tiedosto” ja ”/hakemisto1/hakemisto2/”. Kenoviivaan päättyvät viittaukset osoittavat viittauksen olevan hakemisto. Jos viittaus päättyy nimeen, on kyseessä tiedosto.

4.1 Käyttäjätilin luominen

Ennen kuin aloitetaan Raspberry Pi:n asentaminen palvelimeksi, on suositeltavaa jättää verkkokaapeli irti laitteesta. Toinen riittävä ratkaisu on estää reitittimessä verkkoosi suunnatut yhteydet reitittimen palomuurissa. Yleensä reitittimen oletusasetuksena on estää kaikki tällaiset yhteydet, mutta tämä on suotavaa tarkistaa joka tapauksessa. Tämä on suositeltava turvakeino ulkopuolisten yhteyksien estämiseksi oletusasetuksilla olevaan palvelimeen.

Aivan uuden Raspbian asennuksen ensimmäinen tietoturvatoimenpide on vaihtaa tietokoneen oletuskäyttäjä ”pi” pois käytöstä. Tämä on todella tärkeä askel tietoturvalliseen palvelinympäristön kehittämiseksi. Kun palvelin on saavutettavissa verkossa, siihen pystyy yhdistämään sekä tavalliset kävijät, että botit. Botit skannaavat jatkuvasti IPv4-osoitteita läpi, etsien haavoittuvuuksia palvelimissa ja verkkopalveluissa.

Hyvä esimerkki haavoittuvaisesta palvelimesta on Raspberry Pi, joka on oletusasetuksilla. Pi:n oletuskäyttäjä on ”pi”, jonka oletussalasana on ”raspberry”. Botit pyrkivät tätä tunnettua tunnuskombinaatiota käyttäen murtautua oletusasetuksilla oleviin palvelimiin. Periaatteessa riittäisi, että palvelimelta vaihdetaan käyttäjän salasana, mutta kun tietoturvallista palvelinta ollaan tekemässä, tähdätään muodostamaan mahdollisimman monta tietoturvakerrosta palvelimen suojaksi.

Tavallisesti Linux-jakeluissa uusi käyttäjä luodaan samalla kun käyttöjärjestelmä asennetaan levylle. Raspbian asennetaan kuitenkin vain kirjoittamalla

käyttöjärjestelmän järjestelmäkuvatiedosto microSD-kortille. Tässä prosessissa ei luoda käyttäjiä, päivitetä järjestelmää tai aseteta maakohtaisia tietoja käyttöjärjestelmälle. Nämä vaiheet voi suorittaa vasta järjestelmän ensimmäisen käynnistyksen jälkeen.

Ennen uuden käyttäjän lisäystä tarkistetaan ”pi” -käyttäjän ryhmät komennolla ”groups”. Raspbianin oletuskäyttäjän voi vaihtaa komennolla useradd. ”useradd” -komentoon lisätään muutamat parametrit uuden käyttäjän luomiseksi:

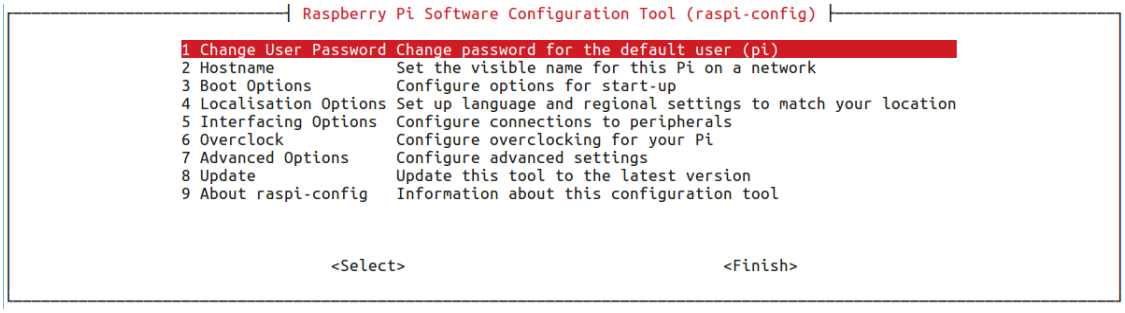
>sudo useradd -m -G ryhmät,tulee,tähän,tässä,muodossa käyttäjätunnus

”-m” parametrilla luodaan käyttäjälle suoraan oma kansio /home/ kansioon. ”-G” parametrin jälkeen listataan pilkuilla ryhmät, jotka tarkistettiin ”groups” -komennolla. Loppuun tulee uuden käyttäjän käyttäjätunnus.

Käytettävyyden tähden kannattaa lisätä uusi käyttäjä kaikkiin ryhmiin missä oletuskäyttäjäkin oli. Tarvittaessa käyttäjän ryhmiä voi kuitenkin hienosäätää tietoturvan parantamiseksi. Pi käyttäjällä on muun muassa oikeuksia ohjata piirilevyn GPIO-porttia ja muuta laitteistoa. Kun uusi käyttäjä on valmis ja oikeudet kunnossa, voi Pi:n oletuskäyttäjän poistaa komennolla ”sudo deluser --remove-all-files pi”. Tämä komento poistaa myös kaikki tiedostot ”pi” -käyttäjän /home/pi/ kansiosta, joten kannattaa ottaa säästettävät tiedostot ensin talteen. (Wilcox 2013.)

4.2 Palvelimen perusasetukset

Seuraava askel on korjata Raspberry Pi:n asetuksia. Raspbian käyttöjärjestelmän mukana tulee helppokäyttöinen työkalu Linuxin tärkeimpien asetuksien säätämiseen. Suorittamalla komennon ”sudo raspi-config” saa esiin työkalun käyttöliittymän.



Kuva 2. raspi-config käyttöliittymä.

Ensin kannattaa päivittää työkalu uusimpaan versioon käyttöliittymän kautta. Tämän jälkeen asetetaan palvelimen sijaintiasetukset oikein. ”Localisation options” -valikon alta voi vaihtaa muun muassa palvelimen esityskieltä, aikavyöhykettä ja wi-fi:n maakohtaisia asetuksia.

Hostname valikosta asetetaan palvelimelle oikea nimi. Palvelimen verkkotunnuksen voi laittaa tähän kohtaan muodossa ”verkkotunnus.tld”. Tämä lisää verkkotunnuksen /etc/hostname tiedostoon. Muutamat ohjelmat myös hyödyntävät nimeä asetuksissaan, kuten palvelinohjelmisto Apache.

Jos Raspbian on asennettu käyttöliittymän kanssa, voi sen ottaa myös pois käytöstä raspi-config käyttöliittymästä. ”Boot options” -valikon alta, kohdasta Desktop / CLI, voi päättää mihin palvelimen oletusnäkymän käynnistäessä. Poistamalla graafisen käyttöliittymän käytöstä, säästyy resursseja muille toiminnoille.

”Interfacing options” -valikon alta käynnistetään SSH. SSH:n avulla voi turvallisesti käyttää Pi:n komentojonoa muilta koneilta lähiverkossa tai tarvittaessa myös verkon ulkopuolelta. Periaatteessa turvallisin tapa käyttää Raspberry Pi palvelinta on kiinnittää siihen monitori ja näppäimistö ja tehdä kaikki työ niiden kautta. SSH on kuitenkin käytännöllinen työkalu, joka ei ole iso tietoturvariski, jos sen asetukset ovat asetettu oikein.

Viimeinen hyödyllinen asetus raspi-config:ssa on ”advanced options” -valikon alla ”memory split” -asetus. Koska palvelinta on suositeltavaa käyttää vain komentojonossa, meidän ei tarvitse uhrata paljon muistia näytönohjaimelle. Minimivaihtoehto 16 mb on riittävä muistimäärä. Tämän jälkeen voi poistua raspi-config valikosta ja käynnistää palvelimen uusiksi. (Wilcox 2013.)

4.3 SSH-yhteys

Kun palvelin on saavutettavissa ja asetukset ovat kohdillaan, tehdään Raspberry Pi tietokoneeseen turvallinen etäyhteys käyttämällä SSH-asiakasohjelmaa. SSH on protokolla, jonka avulla muodostetaan turvattu etäyhteys palvelimeen toisesta tietokoneesta. SSH-yhteyden kautta pystyy hallitsemaan palvelinta sen komentojono käyttöliittymän kautta. Tosin on myös mahdollista suorittaa graafisia sovelluksia palvelimella SSH-yhteyden välityksellä. SSH:n käyttäminen ei ole kotipalvelimella välttämätöntä, jos palvelin on kiinnitetty näyttöön. Tällainen suora käsittely on myös turvallisempi vaihtoehto SSH-yhteyteen verrattuna, mutta helppokäyttöisyyden ja turvallisuutensa tähden SSH on hyvä vaihtoehto.

SSH-yhteyden voi muodostaa kahden tietokoneen välille yhdistämällä millä vain tietokoneella kohde tietokoneen SSH-palvelimeen. Tähän palvelimeen yhdistetään asiakasohjelmalla kuten Windowsin Putty-ohjelmalla tai Linuxilla saman voi suorittaa oletuksena asennetulla OpenSSH-työkalukokoelman ”ssh” -komennolla komentojonossa. Todentaminen suoritetaan joko salasanalla tai avainpari todennuksella.

Salasanapohjaista todennusta voi käyttää suoraan Raspberry Pi palvelimella yhdistämällä SSH-asiakasohjelmalla osoitteeseen käyttäjänimi@192.168.x.x. IP-osoitteen kohdalle laitetaan Raspberry Pi:n sisäverkon kiinteä IP-osoite, tai jos palvelimeen otetaan ulkoverkosta yhteys voi käyttää joko ulkoverkon IP-osoitetta tai verkkosivun verkkotunnusta. Periaatteessa todennuksen ei tarvitse olla erityisen vahva sisäverkossa, sillä ulkopuoliset tietokoneet eivät pääse yhdistämään palvelimen SSH-porttiin reitittimen palomuurin lävitse. Jos on tarpeellista yhdistää palvelimeen ulkoverkosta, on kuitenkin erittäin suositeltavaa ottaa käyttöön avainpari todennuskeino sen turvallisuuden tähden.

Jos palvelimen SSH-portti on avattu ulkoverkosta saavutettavaksi, tulee portti lukemattomien murtoyritysten kohteeksi. Ulkoverkkoon avoimena oleviin SSH-portteihin tehdään jatkuvasti sisäänkirjautumisyrityksiä sanakirjahyökkäyksien muodossa. Tämän takia on tärkeää muuttaa ennen verkkoon yhdistämistä jär-

jestelmän käyttäjätili ja salasana. Myös samojen salasanojen ja käyttäjätunnusten käyttäminen monessa paikassa on riski, sillä internetissä salasanatietokantoja vuotaa verkkoon silloin tällöin ja oma käyttäjätilisi saattaa olla niiden mukana. Tämän takia avainparipohjainen tunnistautuminen on tehokas suojautumiskeino. Avainta on miltei mahdotonta arvata brute force-hyökkäyksillä ja vaikka avain vuotaisikin vääriin käsiin, täytyy sen salaus purkaa avainparia muodostaessa käytetyllä salasanalla. Avaintiedoston sisällön perusteella on myös mahdotonta päätellä mihin palvelimeen avain on tarkoitettu.

Avainparipohjainen tunnistautuminen onnistuu käyttämällä kahta avaintiedostoa: julkista avainta ja henkilökohtaista avainta. Avainparin voi muodostaa puttyn mukana tulevalla puttygen-ohjelmalla tai Linuxilla ssh-keygen komennolla. Julkinen avain siirretään palvelimelle ja henkilökohtainen pidetään yhdistävällä tietokoneella. Henkilökohtainen avain on käytännössä avain ja julkinen avain on lukko. Jos lukko aukeaa, eli saadaan oikea tieto ulos julkisesta avaimesta, on todentaminen onnistunut ja muodostetaan SSH-yhteys laitteiden välille. Muodostettu yhteys laitteiden välillä on salattu ja turvallinen.

SSH-palvelimen asetuksia ei tarvitse muuttaa paljon Raspberry Pi-palvelimessa. Pari asetusmuutosta parantaa kuitenkin jonkin verran palvelimen tietoturvaa. Tiedostossa /etc/ssh/sshd_config on kohta ”PermitRootLogin”, joka on suositeltavaa muuttaa. Asetus on oletuksena päällä, mutta palvelimissa on hyvä käytäntö poistaa mahdollisuus kirjautua suoraan käyttäjille, joilla on kaikki hallintaoikeudet järjestelmässä. Jos avainparipohjainen todennus riittää niin salasanalla kirjautumisen voi ottaa kokonaan pois käytöstä asettamalla tiedostossa ”PasswordAuthentication” -asetus pois päältä. (Champ 2014.)

Ulkopuolisen liikenteen salliminen SSH:n käyttämään porttiin 22 täytyy tehdä sekä palvelimen palomuurissa, että reittimessä. Reitittimessä täytyy avata sekä palomuuriin auki portti 22, että ohjata liikenne Raspberry Pi:n porttiin 22 reitittimen ”port forward” -valikossa. Joissakin reitittimissä riittää, että liikenne ohjataan porttiin ”port forward” -valikossa. Lisää tietoa tästä löytyy käytetyn reitittimen ohjekirjasta.

4.4 Palvelimen saavutettavuus

Tärkeä askel palvelimen asennuksessa on tehdä palvelimesta luotettava. Palvelimen olisi suotavaa olla aina saavutettavissa IP-osoitteestaan. Kotipalvelimen ongelma on, että IP-osoite voi muuttua milloin hyvänsä operaattoreiden osoitteenmuunnoksien tähden. IP-osoitteet pysyvät yleensä useampia kuukausia samana, joten osoitteen satunnaisen vaihtumisen ei pitäisi olla suuri haittatekijä. Tätä ongelmaa varten on kuitenkin muutama ratkaisu, jolla varmistetaan palvelimen jatkuva saavutettavuus. Tarvittaessa voi asettaa myös työkaluja käyttöön, jotka ilmoittavat ylläpitäjälle verkkosivun ollessa saavuttamattomissa. Yksi suosituimpia työkaluja tätä varten ovat googlen webmaster työkalut.

Verkkosivun IP-osoite pitää asettaa ensinnäkin kiinteäksi sisäverkossa. Kodin reititinkin voi vaihtaa palvelimen IP-osoitetta toisinaan. Reitittimen DHCP-asetuksissa, missä hallinnoidaan verkon jäsenille annettuja verkkoasetuksia, voi asettaa verkon jäsenille kiinteän IP-osoitteen. Tämä asetetaan osoittamalla IP-osoite tietokoneen MAC-osoitteeseen. MAC-osoitteen avulla reititin tunnistaa tietokoneet. MAC-osoitteen saa esiin Rasbperry Pi:n komentojonossa komennolla ”ifconfig”. Komennolla tulee esiin lista verkkosovittimien tietoja. MAC-osoitteen löytää kohdasta eth0, jos Pi on yhdistetty ethernet-kaapelilla, ja kohdasta wlan0, jos se on yhdistetty langattomasti.

Palvelin on nyt kiinteässä IP-osoitteessa sisäverkossa. Ulkoverkon IP-osoite on vaikeampi saada kiinteäksi. Monet operaattorit Suomessa ovat luopuneet kiinteiden IP-osoitteiden tarjoamisesta kuluttajille. Kiinteää IP-osoitetta ei kuitenkaan tarvitse käyttää, jos verkkotunnuksen nimipalvelu tarjoaa dynaamista nimipalvelujärjestelmää (dynamic DNS). Tämän asettamiseen löytyy yleensä ohje käytetyn nimipalvelun verkkosivuilta. Käytännössä toiminnon käyttöönotto onnistuu asettamalla verkkotunnukselle dynaaminen DNS päälle verkkotunnuksen DNS-asetuksissa. Seuraavaksi asetetaan dynaaminen DNS päälle palvelimella asentamalla suositeltu sovellus kuten DDClient. Asetukset DDClienttiin pitäisi löytyä nimipalvelun verkkosivuilta, jos dynaamisen IP-osoitteen asetus on mahdollista.

4.5 Palomuuri

Palvelimen edessä on yleensä valmiiksi jo reitittimen palomuuri, joka estää tulevia yhteyksiä. Kuitenkin palvelimella ei voi koskaan olla liikaa tietoturvaratkaisuja käytössä, joten on suositeltavaa asettaa palvelimelle myös palomuuri. Palomuuriohjelmana Raspberry Pi:llä on oletuksena iptables-ohjelma. Kyseinen ohjelma vaatii vähän ylimääräistä teknistä tietämystä. Sen sijaan aloittelevalle palvelimen ylläpitäjälle suositellaan UFW-palomuurisovellusta (uncomplicated firewall).

Kyseinen ohjelma ei ole asennettu valmiiksi Raspbianilla. Ohjelman voi asentaa komennolla ”sudo apt install ufw”. UFW otetaan käyttöön komennolla ”sudo ufw enable”. Tarvittavat portit, jotka täytyy avata verkkosivun palvelinta varten, ovat portit 80 ja 443 verkkosivulle ja 22 SSH-yhteyksille, jos on tarvetta hallinnoida palvelinta sisäverkon ulkopuolelta. Näitä varten ohjelma löytää Pi:ltä asetukset suoraan kyseiseltä palvelulta. Ne saadaan käyttöön suorittamalla komennot ”sudo ufw allow http”, ”sudo ufw allow https” ja ”sudo ufw allow ssh”. (Anicas 2015.)

Käytännössä tässä pisteessä palvelimen palomuuri on jo hyvällä mallilla. Palomuuria voi vielä hienosäätää poistamalla käytöstä oletusasetuksilla avatut IPv6 versiot porteista. Suomessa verkko-operaattorit eivät ole siirtyneet käyttämään laajasti IPv6-osoitteita, joten näiden porttien avaaminen ei ole tarpeellista vielä.

4.6 Fail2ban

Verkkoon avoimiin portteihin tulee jatkuvasti yhdistysyrityksiä. Näiden määrää voi hallita työkaluilla kuten fail2ban-ohejlmalla. Ohjelman voi asentaa komennolla ”sudo apt install fail2ban”. Fail2ban estää IP-osoitteen yhdistämästä palvelimeen, kun osoitteesta on tullut tarpeeksi epäonnistuneita yhdistysyrityksiä. Fail2ban lisää palomuuriin väliaikaisen säännön estääkseen hyökkääjän yhdistysyritykset oletusasetuksilla asetuksissa määritellyksi ajaksi. Ohjelma on jo oletusasetuksilla käytettävässä kunnossa, mutta lisää asetuksien säätöä voi tehdä tiedostossa ”/etc/fail2ban/jail.conf”.

Asetuksissa voi muuttaa muun muassa, kuinka monesta epäonnistuneesta kirjautumisyrityksestä seuraa yhdistämisenesto ja kuinka kauan esto kestää. Myös aikaa jonka ajalta kirjataan kirjautumisyritystä voi muuttaa. Nämä asetukset löytyvät kohdista maxretry, bantime ja findtime tiedoston alkupuolelta. Muut tiedoston asetukset alkavat olla vähän liian teknisiä yksinkertaiselle verkkosivun palvelimelle. Oletusasetuksilla pärjää pitkälle.

4.7 Palvelinohjelmisto

Palvelinohjelmistona Pi:llä ei ole asennettu oletuksena mitään. Kaksi suosituinta palvelinohjelmistovaihtoehtoa ovat Apache ja Nginx. Molemmat ovat erittäin hyviä vaihtoehtoja palvelinohjelmistoksi. Näillä ohjelmistoilla on kuitenkin muutamia näkemys- ja toiminnallisuuseroja palvelimen operoinnista ja hallinnasta.

Palvelinohjelmiston valinta riippuu siitä, minkälainen palvelin on käytössä ja mitä palvelimella hostataan. Raspberry Pi:n tapauksessa täytyy ottaa huomioon palvelimen suorituskyky ja muistikapasiteetti. Raspberry Pi 3:lla on keskusmuistia käytössä 1 GB, joka ei ole suuri määrä. Pienellä käyttäjäkunnalla Apache-palvelin saattaa vielä käyttää tasaisesti palvelimen keskusmuistia, mutta isommilla kävijämäärillä voidaan joutua hyödyntämään palvelimen swap-muistia, joka on hitaampaa ja saattaa hidastaa myös palvelimen toimintaa.

Apachen sijaan Nginx on sopivampi palvelinohjelmisto Raspberry Pi:lle. Nginx on tehokkaampi käsittelemään palvelimen pyyntöjä ja käyttää vähemmän keskusmuistia. Etenkin staattisia verkkosivuja varten Nginx on parempi vaihtoehto. Nginx uhraa monia toimintoja, jotka tekevät Apachesta joustavan ja helppokäyttöisen, mutta tarjoaa suorituskykyisen palvelinratkaisun, joka tarvittaessa pystyy kaikkeen mihin Apachekin. Nginx on myös koodipuolella vähemmän monimutkainen ohjelmisto kuin Apache, joka tekee siitä luotettavamman ja tietoturvallisemman. (Ellingwood 2015.)

Tässä tapauksessa käsittelemme yksinkertaisen staattisen verkkosivun jakamista Nginxillä. Nginxin voi asentaa suorittamalla komennon ”sudo apt install nginx”, jos ohjelmisto ei ole vielä asennettu. Nginx pystyy jo oletusasetuksilla

hostaamaan staattisia verkkosivuja. Lisäämällä verkkosivun tiedostot Nginx:n asetuksissa määriteltyyn kansioon /var/www/html/ saa staattisen verkkosivun näkymään palvelimen osoitteesta. Nginxin asetuksia tulee kuitenkin vielä hieman muokata palvelimen tietoturvan varmistamiseksi.

Palvelimen tietoturva-asetuksia konfiguroidessa pyritään piilottamaan mahdollisimman paljon tietoa palvelimesta mahdollisilta hyökkääjiltä. Mitä enemmän tietoa hyökkääjä saa palvelimesta ja palvelinohjelmistosta, sitä todennäköisemmin hyökkääjä löytää haavoittuvuuden palvelimen tietoturvasta. Esim. jos hyökkääjä tietää mikä käyttöjärjestelmä on kyseessä, voi hän käyttää tätä tietoa etsiessään tietoturva-aukkoja, joita on ilmennyt kyseisessä käyttöjärjestelmässä. Tätä samaa periaatetta kannattaa hyödyntää kaikkialla muuallakin palvelimessa. Mitä vähemmän hyökkääjä tietää palvelimesta sen parempi.

Nginx palvelinasetuksia voi muokata tiedostossa /etc/nginx/nginx.conf. Kohdassa ”Basic Settings” tiedoston alkupuolella on asetus ”server_tokens”. Tämä asetus poistaa ylimääräistä tietoa, joka näkyy jokaisessa http-pyynnössä. Tässä tapauksessa asetus poistaa palvelinohjelmiston versiotiedot kaikista pyynnöistä. (Ellingwood 2016.)

4.7.1 SSL

Verkkosivu on nyt saavutettavissa verkossa, mutta sivu ei ole vielä täysin turvattu sen käyttäjille. Jotta verkkosivu saataisiin mahdollisimman turvalliseksi käyttäjäkunnalle, on suositeltavaa käyttää SSL-sertifikaattia. SSL-sertifikaatti on varmenne siitä, että palvelin on varmasti sama palvelin kuin se väittää olevansa.

SSL-sertifikaatti asennetaan palvelimelle ja palvelinohjelmistoon muodostetut yhteydet turvataan sertifikaatin avulla tarkastamalla sertifikaatilla, että palvelin on todella sama palvelin kuin se väittää olevansa. Kun on varmistettu, että palvelin on luotettava, muodostetaan salattu yhteys palvelimen ja kävijän välille, jonka kautta palvelin lähettää dataa kävijälle ja kävijä palvelimelle.

Ilman tätä SSL-yhteyttä kävijä lähettäisi tietojaan palvelimelle täysin luettavassa muodossa. Jos kävijä on julkisessa Wi-Fi verkossa, voi joku muu tehdä

ns. mies välissä -hyökkäyksen (engl. man-in-the-middle attack), ja kaapata muiden verkon käyttäjien dataa esittämällä kohde verkkosivuja. Jos verkon jäsenien yhteys verkkosivuun ei ole suojattu SSL:n avulla, pystyy hyökkääjä lukemaan mm. jäsenien käyttäjätunnuksia ja salasanoja siinä muodossa kuin ne on kirjoitettu. SSL-yhteyden avulla nämä tunnukset olisivat kryptattu lukemattomaan muotoon heti kun tunnukset lähetetään tietokoneelta, aina kohdepalvelimelle asti.

Luotettavien sertifikaatin myöntäjien sertifikaatit olivat vielä pari vuotta sitten käytännössä kaikki maksullisia. Nykyään kuitenkin ilmaisia sertifikaatteja pystyy saamaan Let’s Encrypt -palvelusta. Let’s Encrypt tarjoaa ilmaisia kolmen kuukauden ajan kestäviä sertifikaatteja verkkotunnuspohjaisella tunnistuksella. Sertifikaatin hankkiminen on automatisoitu prosessi. Kuitenkin Nginx:llä sertifikaatin käyttöönotto on hieman kömpelömpää tällä hetkellä kuin muilla palvelinohjelmistoilla. SSL-sertifikaatin asennusprosessi ei ole yksinkertaisimmasta päästä, mutta SSL-yhteys verkkosivuilla on nykyään erittäin tärkeä osa turvallista palvelinta.

4.7.2 SSL-sertifikaatin asennus

Tällä hetkellä työkalu, jota käytetään sertifikaatin muodostamiseen ei ole virallisissa Raspbianin käyttämissä Debian 8 pakettivarastoissa. Tätä varten lisätään ylimääräinen pakettivarasto Raspbianiin. Lisäämällä /etc/apt/sources.list tiedostoon ”deb http://ftp.debian.org/debian jessie-backports main” uudelle riville, saa palvelimelle uudemmat paketit Debianin testiversioista. Pakettivaraston allekirjoitus pitää vielä lisätä palvelimelle seuraavilla komennoilla:

```
>gpg –keyserver pgpkeys.mit.edu –recv-key 8B48AD6246925553
>gpg -a –export 8B48AD6246925553 | sudo apt-key add –
>gpg –keyserver pgpkeys.mit.edu –recv-key 7638D0442B90D010
>gpg -a –export 7638D0442B90D010 | sudo apt-key add –
```

Ohjelman voi asentaa nyt päivittämällä pakettivaraston komennolla ”sudo apt update” ja asentamalla ohjelma komennolla ”sudo apt install certbot -t jessie-

backports”. Debian 9 version pohjalta kehitetyssä seuraavassa Raspbian päivityksessä ohjelman pitäisi olla saatavissa suoraan myös virallisesta pakettivarastosta suoraan asennuskomennolla.

Jotta Let’s Encrypt pystyisi muodostamaan sertifikaatin palvelimelle, tulee se sallia käsittelemään certbotin muodostamaa kansiota palvelimen verkkosivun hakemistossa. Verkkosivun palvelinasetuksia voi muokata tiedostossa /etc/nginx/sites-available/default. Tähän tiedostoon ”server” -lohkon sisälle lisätään seuraava:

```
location ~ /.well-known {
    allow all;
}
```

Kun tämä asetus on lisätty, voi palvelimen käynnistää uudelleen komennolla ”sudo systemctl restart nginx”. Nyt sertifikaatin voi asentaa palvelimelle. Sertifikaatin asennuksen voi suorittaa komennolla ”sudo certbot certonly”. Sertifikaatin asennusprosessi käynnistyy ja ensimmäisessä kysymyksessä pyydetään tunnistumistapaa. Tähän valitaan ensimmäinen vaihtoehto ”webroot”. Muut kysymykset asennuksessa ovat verkkosivuun liittyviä ja muita yleisiä tietoja palvelimenhaltijasta. Asennuksessa palvelimen webroot kansio on /var/www/html/. Sertifikaatin tietoturvan parantamiseksi on suositeltavaa suorittaa vielä seuraava komento:

```
>sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

Kun asennusprosessi on suoritettu loppuun, on palvelimella nyt sertifikaatti käytetylle verkkotunnukselle. Seuraavaksi lisätään vielä Nginxiin asetukset, jotta palvelin pystyisi käyttämään uutta sertifikaattia. Tehdään uusi tiedosto /etc/nginx/snippets/ssl-esimerkkisivu.com.conf. Tähän tiedostoon lisätään seuraavat asetukset:

```
ssl_certificate /etc/letsencrypt/live/esimerkkisivu.com/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/esimerkkisivu.com/privkey.pem;
```

“Esimerkkisivu.com” kohtaan lisätään käytetty verkkotunnus. Lisätään Nginxiin vielä muutamia SSL-asetuksia, jotka takaavat turvallisen yhteyden käyttäjän ja palvelimen välille. https://cipherli.st/ osoitteesta saa vahvat valmiit SSL-salaus-asetukset Nginx-palvelimelle ja muille palvelimille myös tarvittaessa. Näistä asetuksista kannattaa lukea vielä lisää, mutta suositeltavaa on jättää kohdan ” add_header Strict-Transport-Security” lopusta pois ”preload” -asetus. ”Strict-Transport-Security” -asetus pakottaa kävijät käyttämään verkkosivun https-osoitetta http-osoitteen sijasta. ”preload” -kohta säästää tämän asetuksen kävijöille selaimen välimuistiin. Selain pyrkii tämän takia yhdistämään pelkästään muistamaansa https-osoitteeseen, vaikka palvelimella ei olisikaan voimassa olevaa SSL-sertifikaattia tai verkkosivu olisi muutettu http-sivustoksi. (HTTP Strict Transport Security Cheat Sheet 2017.) Asetuksiin lisätään vielä loppuun generoitu dhparam-tiedosto ”ssl_dhparam /etc/ssl/certs/dhparam.pem;” -asetuksella.

Nämä asetukset lisätään uuteen tiedostoon nimeltään /etc/nginx/snippets/ssl-params.conf. Lopuksi Nginxin palvelinasetuksia muutetaan vielä hieman käyttämään SSL-sertifikaattia ja asetuksia muuttamalla /etc/nginx/sites-enables/default tiedosto seuraavaan muotoon:

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name esimerkkisivu.com www.esimerkkisivu.com;
    return 301 https://$server_name$request_uri;
    root /var/www/html;
}

server {
    listen 443 ssl default_server;
    listen [::]:443 ssl default_server;
    include snippets/ssl-esimerkkisivu.com.conf;
    include snippets/ssl-params.conf;
    root /var/www/html;
}
```

Esimerkkisivu.com kohtaan tulee jälleen oma verkkotunnus. Jos sertifikaattia muodostaessa käytettiin vain osoitetta muodossa ”esimerkkisivu.com”, riittää, että laitetaan server_name kohtaan vain tämä osoitemuoto. Lisäämme oletus palvelinlohkon lisäksi toisen lohkon SSL-yhteyttä varten. Vanhasta ylemmästä palvelinlohkosta ohjataan kaikki liikenne palvelimen https osoitteeseen, että kaikki palvelimelle muodostetut yhteydet olisivat SSL-yhteyksiä. Lisäämme myös SSL-asetukset ja sertifikaatin toiseen lohkoon ”include” -komennoilla.

Suorittamalla komennon ”sudo systemctl restart nginx” pitäisi palvelimelle tulla SSL-yhteys käyttöön. SSL-sertifikaatin automaattinen uusiminen aktivoidaan ” sudo certbot renew” -komennolla. Jos palvelinohjelmisto antaa virheilmoituksia missään asennuksen vaiheessa, kannattaa tarkistaa ”nginx -t” -komennolla virheilmoitukset ja käydä läpi asetustiedostoissa virheet. Oman kokemukseni mukaan SSL-yhteys ei välttämättä heti ala toimia palvelimella. Muutaman tunnin odotus saattaa auttaa mahdollisten yhdistysongelmien ilmetessä. Tämä saattaa johtua siitä, että verkkotunnus on osoitettu vasta vähän aikaa sitten laitteesi IP-osoitteeseen tai jostain muusta vastaavasta. (Ellingwood 2016.)

4.8 Lähitulevaisuuden tietoturva

Palvelimien tietoturva kehittyy jatkuvasti. Tietoturvaan liittyen on tulossa muutamia suurempiakin muutoksia lähivuosina. Jotkut näistä muutoksista tulee myös vaikuttamaan Raspberry Pi-kotipalvelimiin. Periaatteessa käyttämämme asetukset ja ratkaisut ovat riittävät tulevaisuudessakin, mutta on hyvä olla tietoinen muutoksista ja kehityksistä, joita voi hyödyntää tarpeen vaatiessa tai asentaessa uudelleen palvelinta.

4.8.1 HTTPS

Tähän mennessä sivut, jotka ovat pyytäneet käyttäjiltä käyttäjätunnuksia, salasanoja tai muuta henkilökohtaista tietoa, on näytetty selaimissa verkkosivuina kuten kaikki muutkin. Tietenkin HTTPS yhteyttä käyttävillä sivustoilla näkyy URL alueen vasemmalla puolella ”Secure” tai vihreä palkki ja muuta tekstiä osoittaen verkkosivun turvallisuuden.

Chrome 56 versiopäivityksessä sivustot, joilla pyydetään salasanoja tai luottokorttitietoja, ovat merkitty epäturvallisiksi URL-palkissa. Myös Firefox versiossa 52 kirjautumistietoja kirjoittaessa ilmestyy ilmoitus tekstikentän viereen ilmoittaen sivuston epäturvallisuudesta. Tämä on askel kohti tavoitetta merkitä kaikki verkkosivut, jotka eivät käytä HTTPS yhteyttä, epäturvallisiksi. Google on esittänyt ehdotuksen kaikille muille selaintarjoajille kyseisestä muutoksesta. (Marking HTTP As Non-Secure 2016; Schechter 2016.)

Palvelimen ylläpitäjälle tämä tarkoittaa SSL-sertifikaattien käyttöönottoa kaikilla verkkosivujen palvelimilla. Verkkosivut, jotka eivät käytä HTTPS yhteyttä merkitään loppujen lopuksi epäturvallisiksi, ja tämän lisäksi sivustojen sijainti hakukoneiden tuloksissa paranee, jos verkkosivulle pystytään muodostamaan HTTPS-yhteys. Tämä ei ole nykyään enää iso haaste palvelimenhaltijoille, sillä ilmaiset ja helppokäyttöiset sertifikaatti palvelut kuten Let’s Encrypt ja StartSSL ovat pienentäneet kynnystä ottaa SSL-sertifikaatti käyttöön.

4.8.2 IPv6

Jatkuvan kehityksen alla on myös siirtyminen vanhasta IPv4-protokollasta IPv6-protokollaan. Tämän siirtymisen takana on IPv4 IP-osoiteavaruuden loppuminen. Maailmassa on paljon laitteita, jotka kaikki tarvitsevat IPv4 osoitteen ja myös monia ns. varattuja IPv4 osoitteita, jotka eivät ole kuitenkaan käytössä. Näiden varattujen IPv4-osoitteiden jakoa verkko-operaattoreille ja muille tarvitseville on pyritty parantamaan työkaluilla, jotka parantavat IPv4 osoitteiden jakelua ja käyttöä. Osoiteavaruuden käyttöä on pystytty tehostamaan myös osoitteenmuunnostekniikoilla, joiden avulla moni laite hyödyntää samaa IP-osoitetta.

Kuitenkin tavoitteena on ennen pitkää siirtyä käyttämään IPv6-protokollaa laajemmin. IPv6-protokollaan siirtyminen tekee internetistä turvallisemman, sillä IPv6:ssa hyödynnetään yhteyksien salausta ja muita kehittyneempiä yhteyden ja viestien todentamistekniikoita oletuksena. IPv6-protokollan tullessa laajempaan käyttöön tulee kotipalvelimen haltijankin suorittaa muutamia toimenpiteitä käyttöönotossa.

IPv6-protokollan yhtenä tavoitteena on antaa jokaiselle laitteelle oma uniikki IP-osoite. IPv4:n kanssa hyödynnettyjä osoitteenmuunnostekniikoita ei enää käytetä IPv6-protokollan kanssa, joten reitittimessä ei tarvitse ohjata liikennettä oikeaan osoitteeseen sisäverkossa. Käytetyssä nimipalvelussa pitää ohjata IPv6-osoitteeseen myös liikenne, kuten ohjataan liikenne IPv4-osoitteeseenkin. Tämä tehdään käyttämällä verkkotunnuksen asetuksissa IPv6-osoitteille tarkoitettua AAAA-tietuetta IPv4:n A-tietueen lisäksi. Palvelinohjelmistot, kuten Nginx ja Apache, täytyy myös asettaa kuuntelemaan IPv6-osoitteeseen tulevaa liikennettä. (Rowe 2014.)

4.8.3 Raspbian päivitykset

Yksi tärkeimpiä tietoturvatoimenpiteitä on pitää palvelin päivitettynä. Palvelinohjelmistoihin ja muihin työkaluihin tulee jatkuvasti päivityksiä, jotka korjaavat tietoturva-aukkoja ja muita ongelmia. Jossain vaiheessa tulevaisuudessa Raspbianiin tulee kuitenkin suurempi ohjelmistopäivitys, jota ei pysty suorittamaan komennolla sudo apt upgrade.

Tämä tulee luultavasti muutaman kuukauden päästä Debian 9 version julkaisun jälkeen. Julkaisun ajankohtaa ei ole vielä varmistettu, mutta edellisten päivityksien julkaisujen mukaan Debian 9 päivityksen ajankohta on 2017 kesän paikkeilla. Raspbian päivitys tehdään Raspberry Pi:lle asentamalla koko käyttöjärjestelmä uudestaan microSD-kortille. Suoraa päivitysvaihtoehtoa uuteen versioon ei ollut ainakaan viimeisessä suuressa päivityksessä, mutta lisää tietoa päivityksestä saa Raspberry Pi:n kotisivuilta päivityksen julkaisun aikaan. Päivitys ei ole myöskään välttämätöntä tehdä heti, mutta ennen pitkää vanhaan Raspbian-versioon lopetetaan uusien tietoturvapäivityksien julkaiseminen. (Champ 2014.)

4.9 Yhteenveto

CIA-tietoturvamallin kaikki osat ilmenevät käytetyissä työkaluissa jossain muodossa. Käyttäjät luodaan käyttäen turvallisia asennuskeinoja ja käytetyt todennuskeinot ovat tarpeeksi turvallisia kotipalvelimelle. Yhteyksien estossa pyritään muodostamaan ympäristö, joka on saavutettavissa järjestelmän luvalli-

sille käyttäjille, mutta estetty muille. Laite- ja teknologiakohtaisesti hyödynnetään tarvittavia ratkaisuja turvallisen palvelimen kehittämiseksi, jolla hostattu verkkosivu on saavutettavissa kävijöille luotettavasti.

Tämä mahdollistetaan työkaluilla, jotka ovat luotettavia tietoturvaltaan sekä käytettävyydeltään. Käytetyt työkalut ovat kaikki avoimen lähdekoodin projekteja, joita on hiottu vuosien saatossa palvelinympäristöön sopiviksi. Kaikki ohjelmistot ovat jokapäiväisessä käytössä ympäri maailmaa ja uusien uhkien ilmetessä työkalut ottavat tarpeen mukaan uhkat huomioon tietoturvapäivityksien muodossa.

Nämä ohjelmistot riittävät tavallisen staattisen verkkosivun hallinnoimiseen, mutta jos tarkoituksena on jatkokehittää palvelinympäristöä tukemaan dynaamista verkkosisältöä, tulee ottaa huomioon monia muita asioita. Suurin uhka palvelimille on palvelimen käsittelemä verkkosivulta syötetty tieto. Myös hyödynnetyt ohjelmointikirjastot ja ohjelmistokehykset (engl. framework) saattavat lisätä verkkosovelluksiin haavoittuvuuksia. OWASP-yhteisö on hyvä lähde turvallisten verkkosovellusten kehitykseen.

Raspbian-käyttöjärjestelmän sijasta voi myös käyttää muita Linux-jakeluja. Suosittu vaihtoehtoinen Linux-jakelu palvelimille on esimerkiksi CentOS. CentOS on vakaa käyttöjärjestelmä, joka sopii hyvin pitkiä aikoja käynnissä oleville palvelimille. Vakautensa tähden CentOS:n ohjelmistopaketit saattavat olla toiminnallisuudeltaan jäljessä, mutta tietoturvapäivityksiä käyttöjärjestelmä saa ajallaan. Jakelu on kuitenkin monin tavoin erilainen verrattuna Raspbianiin, joten jotkut komennot ja hakemistorakenteet ovat hieman erilaisia.

Palvelimen jatkokehitykseen ja ylläpitoon digitalocean.com VPS-palvelun verkkosivu on erittäin hyvä lähde. Sivustolta löytyy melkein kaikille Linux käyttöjärjestelmille oma artikkelinsa työkalujen asennuksesta ja operoimisesta. Hyviä vaihtoehtoja palvelimen jatkokehitykselle ovat järjestelmän varmuuskopiointi ja auditointityökalut.

5 LOPPUSANAT

En odottanut saavani Raspberry Pi:stä hyvää verkkosivun palvelinta verrattaessa pilvi- ja hostingpalveluiden tarjoamiin palvelinratkaisuihin. Pi:n laitteiston tehot ovat heikohkot ja kotipalvelimen ylläpitäminen ei ole yhtä luotettavaa kuin muut palvelinvaihtoehdot. Kuitenkin kotipalvelimen käyttö mahdollistaa muutamia ylläpito- ja hallintakeinoja, joita etäpalvelimilla ei voi suorittaa. Tarvittaessa Pi:n käyttöjärjestelmän voi asentaa uusiksi helposti ja vaivattomasti sammuttamalla laite ja irrottamalla microSD-kortti. Pi:n voi kiinnittää monitoriin ja sitä voi hallita suoraan ilman verkkoyhteyttä. Raspbianin helppokäyttöisyys teki myös palvelimen käytöstä luotettavaa ja vaivatonta.

Asentamani palvelin on käynnissä vakaasti ja sen tietoturva tuntuu luotettavalta. Minun pilvipalvelimeeni tulee jatkuvasti bottien kirjautumistyrityksiä, mutta tässä kotipalvelimessa ei tule ollenkaan, sillä se on reitittimen palomuurin takana. Tavallaan tällainen kotipalvelin on siis turvallisempi vaihtoehto pilvipalveluiden palvelimiin verrattuna.

Nginx-palvelinohjelmiston asetuksien kanssa ilmeni varmaan eniten ongelmia. Pyrin olemaan tarkka tämän osion kanssa, sillä minulla Nginx-asetustiedostoissa ilmeni muutamia kirjoitusvirheitä ja muita ongelmia. SSL-yhteyden muodostamisessa ilmeni myös ongelmia, jotka katosivat kuitenkin loppujen lopuksi itsestään yön aikana. Ongelmia ilmeni myös vanhan reitittimeni asetuksien säädössä. Uudemmissa malleissa reitittimien käyttöliittymät ovat paljon selkeämpiä ja helppokäyttöisempiä.

Tietoturvan perusteista sain näkemystä tietoturvaan ja sen tärkeimpiin piirteisiin. Tietoturvaan yleisesti voisi kuitenkin sukeltaa paljon syvemminkin, mutta tämän projektin puitteissa tämä pintapuolinen katsaus oli mielestäni riittävä yksinkertaisen palvelimen asennusta ja turvaamista varten. Päämääränä oli kuitenkin palvelimen valmistaminen käytettäväksi ja turvalliseksi, ja hyvän pohjan muodostaminen jatkokehitystä varten.

Käyttämäni tietoturvaratkaisut ovat perustyökaluja, enkä käsittele tutkimuksessa paljon monimutkaisempia työkaluja ja toimenpiteitä. Tässäkin olisin voi-

nut sukeltaa syvemmälle, mutta staattiselle verkkosivulle nämä ratkaisut tuntuivat oikein riittäviltä. Aloittelevalle palvelimen ylläpitäjälle ratkaisut eivät ole välttämättä ilmiselviä, joten näen tämän ratkaisukoosteen arvokkaana tälle kohderyhmälle. Raspberry Pi on myös laitteena tähdätty tietokoneista kiinnostuneille, oli sitten kyseessä aloittelija tai kokeneempi käyttäjä. Raspberry Pi -säätiön tavoitteena on edistää tietotekniikan opetusta ja tietämystä, joten uskon tämän työn edistävän jossain suhteessa myös tätä kehitystyötä.

Suosittelen Raspberry Pi -tietokoneen käyttöön syventymistä kaikille. Itselleni laitteen hankkiminen ja tutkiminen on ollut erittäin kehittävä kokemus. Raspberry Pi kykenee niin paljon muuhunkin jokapäiväisistä tietokoneiden tehtävistä, aina koodaukseen ja kehitykseen. Tulevaisuudessa ohjelmoinnin, tietokonetaitojen ja tietoturvan arvokkuus tulee vain kasvamaan. Näiden taitojen kehittämiseen Raspberry Pi on sopiva laite ja tietoturvallisen kotipalvelimen asentaminen sopiva ensimmäinen haaste.

LÄHTEET

Anicas, M. 2015. UFW Essentials: Common Firewall Rules and Commands. DigitalOcean. Viitattu 21.3.2017. https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands.

Blocking Brute Force Attacks. 2016. OWASP. Viitattu 23.3.2017. https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks.

Champ, C. 2014. Linux server security best practices. Rackspace. Viitattu 1.4.2017. https://support.rackspace.com/how-to/linux-server-security-best-practices/.

Chirillo, J. & Danielyan, E. 2005. Sun Certified Security Administrator for Solaris 9 & 10 Study Guide. Yhdysvallat: McGraw Hill Professional.

Ellingwood, J. 2015. Apache vs Nginx: Practical Considerations. DigitalOcean. Viitattu 1.4.2017. https://www.digitalocean.com/community/tutorials/apache-vs-nginx-practical-considerations.

Ellingwood, J. 2016. How To Secure Nginx with Let's Encrypt on Debian 8. DigitalOcean. Viitattu 1.4.2017. https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-debian-8.

HTTP Strict Transport Security Cheat Sheet. 2017. OWASP. Viitattu 10.4.2017. https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Marking HTTP As Non-Secure. 2016. Chromium-projektin verkkosivu. Viitattu 2.4.2016. https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure.

Masters, G. 2017. MongoDB databases under attack worldwide. SC Media. Viitattu 23.3.2017. https://www.scmagazine.com/mongodb-databases-under-attack-worldwide/article/629601/.

Red Hat Enterprise Linux 4 - Security Guide. 2008. Red Hat. Viitattu 5.3.2017. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/ch-sgs-ov.html.

Rowe, W. 2014. IPv6 Guide for System Administrators. Anturis. Viitattu 2.4.2016. https://anturis.com/blog/ipv6-guide-for-system-administrators/.

Schechter, E. 2016. Moving towards a more secure web. Googlen tietoturvablogi. Viitattu 2.4.2016. https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html.

Usage of operating systems for websites. 2017. W3Techs. Viitattu 26.2.2017. https://w3techs.com/technologies/overview/operating_system/all.

Usage statistics and market share of Linux for websites. 2017. W3Techs. Viitattu 26.2.2017. https://w3techs.com/technologies/details/os-linux/all/all.

Wilcox, M. 2013. Setting up a (reasonably) secure home web-server with Raspberry Pi. Matt Wilcox:n kotisivu. Viitattu 5.3.2017. https://mattwilcox.net/web-development/setting-up-a-secure-home-web-server-with-raspberry-pi.

Zalewski, M. 2011. The Tangled Web. 1st edition. Yhdysvallat: No Starch Press.

KUVALUETTELO