Pk-yrityksen tietoturva-auditointi ja kybertur-vallisuuden parantaminen

Joonas Muhonen

2022 Laurea

Laurea-ammattikorkeakoulu

Pk-yrityksen tietoturva-auditointi ja kyberturvallisuuden parantaminen

Joonas Muhonen

Tietojenkäsittely

Opinnäytetyö

Toukokuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tietojenkäsittely (AMK)

Joonas Muhonen

Pk-yrityksen tietoturva-auditointi ja kyberturvallisuuden parantaminen

Vuosi 2022 Sivumäärä 73

Opinnäytetyön tavoitteena oli selvittää Uudellamaalla toimivan Pk-yrityksen tietoturvallisuuden nykytila, minkälaisia uhkia se kohtaa ja miten tehokkaasti suojausmekanismit toimivat. Työn tarkoitus on auttaa yritystä kehittämään ja tunnistamaan kyberturvallisuuteen liittyviä uhkia sekä valmiuksia. Työn toimeksiantajana on Selecore Oy, joka hallinnoi ja vuokraa palvelintilaa pienelle määrälle asiakkaita sekä ylläpitää omaa verkkokauppaa sivutoiminimellä.

Opinnäytetyö toteutettiin tapaustutkimuksena laadullisia menetelmiä käyttäen. Tietoperusta koostuu tieto- ja kyberturvallisuuteen liittyvästä kirjallisuudesta, tietoturva-auditoinnin menetelmistä sekä penetraatiotestauksesta. Tutkimuksen aikana tehdyt havainnot dokumentoitiin ja niistä laadittiin erillinen kooste, jotka luovutettiin yritykselle kommentoitaviksi. Työn tuloksista laadittiin kirjalliset raportit.

Tutkimuksen tulokset olivat pääosin positiivisia, eikä yrityksen tietoturvaratkaisuissa havaittu merkittäviä puutteita. Toiminnassaan se kohtaa päivittäisiä ulkoisia uhkia, jotka verkon suojausjärjestelmät kuitenkin kykenevät torjumaan. Yritykseen ei kohdistu välittömiä vakavia vaaroja tai uhkia. Toimeksiantajalle laadittuihin raportteihin sisällytettiin tarpeelliset kehitysehdotukset.

Työn lähtökohtana oli yrityksen halu selvittää oman tietoturvallisuuden nykytilaa. Oletusarvona oli, että sen tietojenkäsittely-ympäristössä havaitaan useita korjattavia kohteita. Työn lopputulos kuitenkin yllätti ja sai osakseen positiivista palautetta toimeksiantajalta. Tietoturva-auditointi todettiin tehokkaaksi ja tulokselliseksi menetelmäksi arvioidessa turvallisuustasoa.

Asiasanat: auditointi, tietoturva, penetraatiotestaus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's thesis

Joonas Muhonen

SME security auditing and improving cyber security

Year 2022 Pages 73

The aim of the thesis was to find out the current state of information security of an SME operating in Uusimaa, what kind of threats it faces and how effectively the security mechanisms work. The purpose of the work was to help the company develop and identify cyber security threats and capabilities. The work was commissioned by Selecore Oy, which manages and leases server space for a small number of customers and maintains its own online store under the side name.

The thesis was carried out as a case study using qualitative methods. The data base consisted of literature related to information and cyber security, information security auditing methods and penetration testing. The findings made during the investigation were documented and a separate summary was prepared and submitted to the company for comments. Written reports were prepared on the results of the work.

The results of the study were mainly positive, and no significant deficiencies were found in the company's security solutions. In its operations, it faced daily external threats which network security systems can however defend. Moreover, the company is not exposed to immediate serious hazards or threats. The necessary development proposals were included in the reports prepared for the client.

The starting point of the work was the company's desire to find out the current state of its own information security. It was assumed that several issues requiring repair would be found in its operating environment. However, the result of the work surprised and received positive feedback from the client. Security auditing was found to be an effective and efficient method for assessing the level of security.

Keywords: auditing, security, penetration testing

Sisällys

1 Johdanto

Tässä opinnäytetyössä tutkitaan Pk-yrityksen tieto- ja kyberturvallisuuden tasoa, selvitetään yrityksen kohtaamia yleisimpiä ja ajankohtaisimpia uhkia sekä yritetään tunnistaa tietoturvallisuuteen liittyviä puutteita erilaisten tutkimusmenetelmien avulla. Työn tulosten myötä haluttiin muodostaa kattava kokonaiskäsitys uhkien ja haavoittuvuuksien laaduista sekä tarjota kehitysehdotuksia niiltä suojautumiseksi. Tutkimus toteutettiin toimeksiantona verkko- ja pilvipalveluita tarjoavalle yritykselle.

Aiheen valintaan ovat vaikuttaneet tieto- ja kyberturvallisuuteen liittyvien uhkien nopea kasvu, digitaalisen toimintaympäristön kehittyminen sekä maailmanlaajuisten kriisien vaikutus yhteiskuntaamme. Tietoverkko- ja verkkoavusteisia rikoksia tehdään yhä kiihtyvällä tahdilla ja ne koskettavat niin yksittäisiä käyttäjiä, yhteisöjä, yrityksiä kuin valtion toimijoita. Tietoturvallisuuden toimivuus ja tehokkuus ovat liiketoiminnan jatkuvuuden kannalta ”elinehto”, joten toimijoiden tulee olla koko ajan varautuneita kyberturvallisuuteen liittyviä uhkia vastaan.

2 Työn lähtökohdat

Tieto- ja kyberturvallisuuteen liittyvät uhat ovat lisääntyneet huomattavasti viimeisen kymmenen vuoden aikana. Näiden vuosien saatossa käsityksemme tietotuvallisuuden vaaroista ja niiden torjuntaan tehtävistä investoinneista ovat muuttuneet merkittävästi. Organisaatiot ovat oppineet huomaamaan, että tietoturvallisuuteen on tärkeä panostaa jatkuvasti, jotta pystytään turvaamaan yrityksen kilpailukyky kaikissa olosuhteissa. Tietojen suojaamisen ja turvallisuuden laiminlyönti voivat johtaa mittaviin vahinkoihin ja pahimmassa tapauksessa liiketoiminnan lakkautumiseen.

Euroopan turvallisuustilanne muuttui merkittävästi 24.2.2022 Venäjän aloitettua laajamittaiset sotatoimet Ukrainassa. Venäjän julkilausuman mukaan tavoitteena on vaikuttaa Euroopan turvallisuusjärjestykseen. Hyökkäyksen myötä Ukrainassa käynnistyivät myös erilaiset kyberoperaatiot, joiden tarkoituksena on yleisen mielipiteen muuttaminen sekä yhteiskunnan toimintakyvyn lamauttaminen. Sotatoimet ovat myös vaikuttaneet Suomen Nato kannatuksen kasvuun, joka on sittemmin noteerattu naapurimaassamme. Tämä on kasvattanut merkittävästi myös Suomeen kohdistuvien kyberuhkien määrää. (Ajankohtaisselonteko turvallisuusympäristön muutoksesta 2022, 8-11.)

Valitettavasti nykyisistä ja tulevista uhkakuvista johtuen pelkästään vähimmäisvaatimukset täyttävät turvallisuustoimet eivät enää riitä, vaan yritysten on kehitettävä yleistä tietoturvallisuutta kaikilta osin. Opinnäyteyön aihe on erittäin ajankohtainen, sillä yritykset tulevat kohtaamaan yhä monipuolisempia hyökkäysmuotoja, joita syntyy muun muassa Euraasian sisäisen kilpailun kasvaessa, maailmalla vallitsevien jännitteiden ja kriisien kehittyessä sekä digitalisoitumisen myötä.

2.1 Kohdeorganisaatio

Työn toimeksiantajana on Uudellamaalla toimiva Selecore Oy, joka on perustettu vuonna 2018. Se hallinnoi ja vuokraa palvelintilaa pienelle määrälle asiakkaita sekä ylläpitää omaa verkkokauppaa sivutoiminimellä. Yritys työllistää muutamia henkilöitä, joista osa työskentelee markkinoinnin ja osa asiakaspalvelun puolella.

Selecore Oy hyödyntää toiminnassaan erilaisia pilvipalveluita, sovelluksia sekä ohjelmia. Palvelimen ja järjestelmien tietoturvan nykytaso on määritelty muutamia vuosia sitten ja niihin on tehty säännöllisesti ylläpitäviä ja parantavia toimia. Tietoturvallisuuden vastuuhenkilönä toimii yrityksen toimitusjohtaja.

Liiketoiminnan kasvun myötä, myös tietoturvallisuuteen liittyvät vaatimukset ovat kasvaneet. Yritys on varautunut muutoksiin tietoturvastrategian avulla, jonka toimesta se haluaa edelleen kehittää valmiutta tieto- ja kyberturvallisuuden suhteen sekä varautua erilaisten häiriötilanteiden varalta.

2.2 Työn tarkoitus ja tavoitteet

Tämän tutkimustyön tarkoituksena on tehdä yritykselle tietoturva-auditointi, jossa kartoitetaan tieto- ja kyberturvallisuuden nykytila. Työssä selvitetään miten tehokkaasti yrityksen käytössä olevien tietojärjestelmien suojausmenetelmät toimivat ja minkälaisia kyberuhkia ne kohtaavat. Työn avulla pyritään tarjoamaan yritykselle kehitysehdotuksia uhkien torjuntaan sekä kasvattamaan yrityksen tietoturvallisuuteen liittyen.

Tutkimuksen myötä esille tulleiden kehitysehdotuksen avulla yritys voi parantaa omaa tietoturvallisuuttaan ja siten tarjota asiakkailleen entistä turvallisempia verkkopalveluita. Lisäksi yritys voi edelleen kehittää tietoturvastrategiaansa ja parantaa liiketoiminnan jatkuvuuden suunnittelua. Työ myös tarjoaa valmiin pohjan mahdollisia uusintatarkastuksia varten.

2.3 Tutkimuskysymykset

Tutkimuskysymyksiä pidetään tutkimustyön lähtökohtana ja niiden avulla pyritään osoittamaan tutkimuksen tarpeellisuus sekä saatavilla olevan tiedon merkityksellisyys. Ne auttavat tutkijoita kohdentamaan tutkimustaan sekä ohjaamaan tutkimustyötä koko prosessin ajan.

(Vilkka 2021, luku 3.) Tutkimuskysymysten avulla voidaan myös välttää ylimääräistä ja turhaa työtä. Hyvin suunnitellut tutkimuskysymykset kaventavat aihetta ja sitovat prosessin eri vaiheet yhteen. Lisäksi niiden myötä lukija saa selkeän käsityksen siitä, mihin tutkimustyöllä on pyritty. (Kothari 2009, 21-22.) Tutkimuskysymykset koostuvat pääkysymyksestä sekä mahdollisista apukysymyksistä (Vilkka 2021, luku 3).

Tässä opinnäytetyössä tutkimuskysymykset liittyvät olennaisesti digitaalisen toimintaympäristön turvallisuuteen. Tutkimuksen keskiössä on kohteena olevan Selecore Oy:n tieto- ja kyberturvallisuuteen liittyvät epävarmuustekijät. Tutkimuksessa lähdettiin hakemaan vastausta pääkysymykseen: Mikä on Pk-yrityksen tieto- ja kyberturvallisuuden nykytila?

Pääkysymyksen lisäksi tutkimuksessa haettiin vastauksia kahteen apukysymykseen, jotka tukevat tutkimuksen tarkoitusta ja tavoitteita: Minkälaisia tieto- ja kyberturvallisuus uhkia Pk-yritys kohtaa? Miten Pk-yrityksen tieto- ja kyberturvallisuutta voidaan parantaa?

Apukysymysten avulla haluttiin syventämää tutkimuksen linjaa ja kartoittaa ongelman laajuutta. Apukysymysten tarkoituksena on tarjota uusia näkökulmia ja ratkaisuja pääkysymykseen liittyvään ongelmaan. Kysymyksen avulla pyritään selvittämään miten kyberturvallisuuteen liittyvät uhat vaikuttavat yrityksen toimintaan ja miten yritys voi parantaa kyberturvallisuuteen liittyvää suojautumistaan.

2.4 Työn rajaus

Opinnäytetyö toteutettiin toimeksiantajan tarpeiden ja toiveiden mukaisesti ja siinä rajattiin aiheen laajuudesta johtuen pois rakenteellinen turvallisuus, fyysisen aineiston säilyttämiseen liittyvä tietoturvallisuus, sisäiset uhat, hallinnollinen tietoturvallisuus sekä sosiaalisen manipulointiin liittyvät uhat. Kyseiset asiat ovat erillisiä kokonaisuuksia, eikä niiden käsittelyä katsottu tarkoituksenmukaiseksi tässä opinnäytetyössä. Tällä pyrittiin varmistamaan työn toteutuminen sekä kohtuullinen työmäärä tutkimustyölle asetettuihin tavoitteisiin nähden.

Aiheen rajaaminen ei kuitenkaan ollut yksinkertaista, sillä tieto- ja kyberturvallisuuteen liittyvät kokonaisuudet ovat usein varsin monisäikeisiä ja niiden teknilliset ulottuvuudet kytkeytyvät usein toisiinsa. Tässä tutkimuksessa pyritään keskittymään enemmän verkkoon sekä palvelimeen kohdistuviin uhkiin.

2.5 Sanasto

ACL	Access Control List on käyttöoikeuksien pääsylista
Brute Force	Väsytyshyökkäys, käytetään erilaisten tunnistetietojen murtamisessa.
DDoS	Distributed denial of service, hajautettu palvelunestohyökkäys.
FTP	File Transfer Protocol on tiedonsiirtoprotokolla.
Hyökkäysvektori	Reitti haavoittuvuuden hyödyntämiseen.
Hyökkäyspinta	Tietojärjestelmät, joihin voidaan kohdistaa hyökkäyksiä.
Koventaminen	Tietojärjestelmien turvallisuustason tehostaminen.
OWASP CRS	OWASP Core Rule Set on joukko uhkien havaitsemissääntöjä.
Pure-FTPd	Tiedonsiirron turvaamiseen räätälöity protokolla.
SLL	Secure Sockets Layer on Internet sovellusten välisen liikenteen salaamiseen käytetty protokolla.
SQL-Injection	SQL injekti on tietokantaan syötettävä haitallinen syöte.
SSH	Secure Shell on tietoliikenteen salaamiseen käytetty protokolla.
TLS	Transport Secure Layer on päivitetty versio SSL protokollasta.
WAF	Web Application Firewall on Web-sovellustason palomuuri.

3 Tietoturvallisuus

Tietoturvallisuus on osa liiketoiminnalle välttämätöntä yritysturvallisuutta. Sen tarkoituksena on suojata tietojen luottamuksellisuutta, eheyttä, saatavuutta ja estää luvattomia tahoja pääsemästä käsiksi yrityksen ja henkilöiden tietoihin. (Whitman & Mattord 2011, 41-42.) Tietoturva käsittää tietojen suojaamista varten tarvittavat työkalut, prosessit sekä toimintatavat. Toimivan tietoturvan avulla pyritään suojaamaan yrityksen toiminnan kannalta tärkeitä tietoja, häiriöiltä, luvattomalta pääsyltä ja käytöltä. Tavoitteena on varmistaa arkaluonteisien ja kriittisten tietojen koskemattomuus sekä luottamuksellisuus. (Peltier 2014, 2-3.)

Tietoturvallisuuteen kuuluvat yleinen tietoturvallisuus sekä tietotekninen tietoturvallisuus. Nämä puolestaan koostuvat useista eri tietoturvaan kuuluvista osa-alueista. Tietoturva käytänteen, periaatteet sekä tietoturvapolitiikka ovat tietoturvan peruskomponentteja. (Whit-

man & Mattord 2011, 8.) Tietoturvan perusta muodostuu niin sanotusta CIA mallista eli luottamuksellisuudesta, eheydestä ja saatavuudesta (eng. confidentiality, integrity, and availability). (Vacca 2009, 225.)

Luottamuksellisuuden periaatteena on, että vain oikeutetuilla henkilöillä on pääsy luottamukselliseen tietoon (Peltier 2014, 55). Tällä halutaan evätä oikeudeton pääsy ja siten suojata tietoa. Eheyden periaatteena on, että tiedot ovat säilytettyinä turvallisesti ja muuttumattomina. Sen tarkoituksena on estää, ettei tieto muutu vahingossa eikä tahallisesti. Saatavuuden periaatteella halutaan varmistaa, että tieto on niihin oikeutettujen henkilöiden saatavilla, eikä pääsyä estetä taikka rajoiteta kyseisiltä henkilöiltä. (Whitman & Mattord 2011, 13-14.)

Tietoturva on nopeasti kasvava ala, joka johtuu tietotekniikan huimasta kehitysvauhdista sekä niihin kohdistuvien uhkien lisääntymisestä (Peltier 2014, 8). Tyypillisiä yritysten tietoturvauhkia ovat tietomurrot, tietojenkalastelut sekä palvelunestohyökkäykset. Toteutuessaan nämä voivat merkittävästi vaikeuttaa yrityksen toimintaa, vahingoittaa mainetta ja lisätä kustannuksia. (Brooks, Grow, Craig, & Short 2018, 214.)

3.1 Kybertoimintaympäristö

Kybertoimintaympäristö on monimutkainen kokonaisuus ja sillä tarkoitetaan kyberfyysistä maailmaa, joka on vahvasti digitalisoitunut sekä verkottunut. Karkeasti voidaan todeta, että kybertoimintaympäristö koostuu tiedoista, käyttäjistä, verkoista, järjestelmistä, toiminnoista ja fyysisen maailman laitteista. Kyberfyysisessä maailmassa digitaalisuus vaikuttaa fyysiseen maailmaan ja fyysinen maailma digitaaliseen maailmaan. Kybertoimintaympäristössä voidaan tehdä toimenpiteitä reaaliajassa ympäri maailmaa, eikä ajalla tai fyysisellä sijainnilla ole merkitystä. (Limnell, Majewski & Salminen 2014, luku 1.)

Digitalisoituminen on tuonut merkittävää hyötyä niin yksilöille kuin maailmantaloudelle. Ympäristö on jatkuvassa muutoksessa yritysten keskittäessä palveluita sekä toimintoja tietoverkkoihin. Mitä enemmän tietoa on verkossa saatavilla, sitä enemmän haitallista kybertoimintaa harjoitetaan. (Communications Security Establishment 2021, 5.)

3.2 Kyberturvallisuus

Kyberturvallisuudessa on kyse järjestelmien ja tietojen suojaamisesta digitaalisessa toimintaympäristöstä vallitsevilta uhilta (Limnell ym. 2014, luku 1). Sen tavoitteena on tunnistaa ja ennaltaehkäistä kyberuhkien muodostamia riskejä sekä suojata järjestelmiä, verkkoja ja tekniikoita luvattomalta käytöltä, haittaohjelmilta sekä kyberhyökkäyksiltä. Se on varautumista kaikkeen tietojenkäsittely-ympäristön kielteisiin ja ei toivottuihin tapahtumiin. (Brooks ym. 2018, 10.) Suomen turvallisuuskomitean (2019) mukaan kyberturvallisuus on ennen kaikkea

yhteiskunnan kannalta kriittisten järjestelmien turvallisuuden ja toimivarmuuden turvaamista.

Kyberturvallisuus vaikuttaa niin kansallisella kuin kansainväliselläkin tasolla ja siksi se on osa Euroopan Unionin sisäisen turvallisuuden strategiaa (Sisäministeriö 2022). Kyberturvallisuuden vaikutus on kasvanut merkittävästi digitalisoitumisen ja tekniikan kehittymisen myötä. Kaikissa nykyaikaisissa järjestelmissä turvallisuus on niiden toiminnan kannalta välttämätöntä. (Limnell ym. 2014, luku 1).

4 Tietoturvariskien tunnistaminen

Tietoturvariskien tunnistaminen on osa kokonaisvaltaista riskienhallintaa ja siinä määritetään riskit, jotka toteutuessaan voivat estää järjestelmien toimivuuden tai muutoin vaarantaa yrityksen toimintaa. Tietoturvatiskien varhaisella tunnistamisella ja sitä seuraavilla toimenpiteillä voidaan estää ei toivottuja tapahtumia. (Ohje riskienhallinnasta 2017, 21.)

Ukrainan tilanne on korostanut entisestään ohjelmistojen sekä digitaalisten palveluiden hallinnan merkitystä. Alati kasvava komponenttipula heijastuu yhä voimakkaammin järjestelmien huoltoon sekä ylläpitoon. Viimeaikaisten tapahtumien myötä organisaatioihin kohdistuvien uhkien määrät ovat kasvaneet huomattavasti. On siis entistä tärkeämpää, että yritykset kykenevät tunnistamaan kyberympäristöön liittyviä riskejä sekä ymmärtävät niiden vaikutukset. (Ajankohtaisselonteko turvallisuusympäristön muutoksesta 2022, 32.)

4.1 Tietoturva-auditointi

Tietoturva-auditointi on prosessi, jossa tarkastellaan sekä arvioidaan yrityksen tietoturvallisuuden toimivuutta mahdollisimman kokonaisvaltaisesti. Tyypillisesti auditointi kohdistetaan johonkin tiettyyn järjestelmään tai prosessiin. Sen avulla arvioidaan kuinka tehokkaasti yrityksen eri turvallisuus- ja hallintajärjestelmät toimivat käytännön tasolla. (Halpert 2011, 16-17.) Tarkastelun myötä on mahdollista havaita järjestelmissä olevia puutteita ja haavoittuvuuksia. Lisäksi esille voi nousta yrityksen tietoturvapolitiikkaan liittyviä kehitystarpeita. Näin yritys voi parantaa tietoturvatasoaan ja siten vaikuttaa maineeseensa luotettavana toimijana. (Vacca 2009, 40.)

Karkeasti auditointi toteutetaan laatimalla huolellinen suunnitelma suoritettavasta arviointityöstä. Seuraavaksi tutustutaan kohteeseen ja saatavilla olevaan aineistoon. Tämän jälkeen auditointi tehdään kohteittain ja havainnot dokumentoidaan. Kerätystä aineistosta ja havainnoista laaditaan raportti, johon lisätään suositeltavat jatkotoimenpiteet. Auditointi on vuorovaikutteinen prosessi, jonka toteuttamiseen voidaan hyödyntää useita eri menetelmiä. (Katakri 2020, 109-111.)

Tietoturva-auditointi on järjestelmällinen mittaustapa, joka voidaan karkeasti jakaa kolmeen erilaiseen arviointitapaan, joista yritys voi valita omiin tarpeisiin parhaiten soveltuvimman menetelmän. Yleisimmät auditointitavat ovat yrityksen ulkoinen, sisäinen sekä vertaisauditointi. (Carter 2004, 56.) Ulkoisen auditoinnin suorittaa yrityksestä riippumattoman, ulkoinen ja luotettava taho. Kyseistä tapaa pidetään kattavimpana auditointimenetelmänä ja siinä perehdytään yrityksen tietoturva- politiikkaan, käytäntöihin, johtamiseen sekä järjestelmiin. Samalla saadaan kattava käsitys järjestelmiin ja prosesseihin liittyvistä puutteista sekä haavoittuvuuksista. Puolueettomuudesta johtuen ulkoista auditointia voidaan pitää erittäin luotettavana ja tehokkaana arviointitapana tarkastellessa yrityksen turvallisuuden toimivuutta. (Hiles 2013, 479-480.)

Sisäinen auditointi sopii parhaiten yrityksen tietoturvallisuuden hallintajärjestelmien toimivuuden arvioinnissa. Työ voidaan toteuttaa joko auditointiin perehtyneen ryhmän tai yksilöntoimesta. (Brewer 2021, 20.) Sisäisessä auditoinnissa muodostetaan kokonaiskuva yrityksen tietoturvallisuuden tasosta ja pyritään tunnistamaan turvallisuusjohtamiseen sekä tietoturvapolitiikkaan liittyviä ongelmia. (ISO 2015, 93-94.)

Vertaisauditoinnilla tarkoitetaan kahden eri yrityksen toisilleen toteuttamaa auditointia. Kyseisessä menettelyssä molempien yritysten auditoijat pyrkivät arvioimaan toistensa prosesseja sekä järjestelmien toimivuutta. Vertaisauditoinnin haasteena on muun muassa se, että yritysten toimintatapojen ja rakenteiden olisi hyvin samankaltaisia, jotta auditointi voidaan toteuttaa. (ISO 2015, 93-94.)

Auditointi yhdistetään erilaisiin laadullisiin sertifikaatteihin, sillä niiden avulla yritys voi osoittaa sitoutumistaan tietoturvallisuuteen liittyviä normien ja lakien noudattamisessa. Esimerkiksi ISO/IEC 27001/27002 sertifikaatit ovat kansainvälisiä standardeja tietoturvan hallinnassa. Kyseisten standardien suuntaviivoja hyödynnetään tietoturva-auditoinnissa, arvioimalla tietoturvaan liittyvien eri osa-alueiden heikkouksia sekä vahvuuksia. (Brewer 2021, 6.) Erityisesti pilvipalveluita ja palvelintilaa tarjoavien yritysten tulisi ottaa tietoturva-auditointi osaksi säännöllisesti suoritettavaa prosessia. Tällöin palveluiden loppukäyttäjät voivat varmistua siitä, palveluntarjoajat pitävät huolta tietoturva-asioista ja palvelualustat toimivat luotettavasti. (Halpert 2011, 34.)

4.2 Katakri

Katakri on viranomaisten ja yritysten käyttöön suunniteltu turvallisuuden auditoinnintyökalu, jota käytetään apuna kohdeorganisaation suojaustason määrittämisessä. Tarkemmin ottaen, sillä voidaan mitata, että kuinka organisaatio kykenee suojaamaan turvallisuusluokiteltua aineistoa. Katakrin taustalla on kansallinen turvallisuusauditointikriteeristö, jonka tarkoituksena on yhtenäistää eri turvallisuuden hallintaan käytettyjä menettelytapoja sekä tehostaa auditointia ja omavaraista valvontaa. (Katakri 2020, 5.)

Katakri koostuu useasta kokonaisuudesta, johon lukeutuvat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Jokaisessa kokonaisuudessa mitataan ja arvioidaan eri turvallisuustasoja aihealueittain. Turvallisuusjohtamiseen liittyvässä osiossa arvioidaan organisaation hallintajärjestelmien sekä henkilöstöturvan toteutumista tietoturvallisuuden näkökulmasta. Fyysinen turvallisuus koostuu turvallisuusluokiteltavan aineiston luottamuksellisuuden, saatavuuden ja eheyden turvaamiseen liittyvistä vaatimuksista. Tarkoituksena on, ettei asiattomilla ole pääsyä salassa pidettävään tietoon. Tekninen tietoturvallisuus on Katakrin viimeinen osa-alue ja se kattaa tietojenkäsittely-ympäristöön kuuluvien osien vaatimukset. Siihen sisältyvät tietoliikenne-, tietojärjestelmä-, tietoaineisto- sekä käyttöturvallisuus, jotka on edelleen jaettu omiin pienempiin osa-alueisiin. Aiheissa esitetään asetetut turvallisuusvaatimukset, jotka perustuvat lakeihin ja säädöksiin. Vaatimuksien täyttäviä toteutustapoja voi olla useita. (Katakri 2020, 5.)

4.3 Riskienhallinta

Riskienhallinta on yksi yritysturvallisuuden kulmakivistä ja se on välttämätöntä jokaiselle yritykselle, joka haluaa varautua erilaisiin negatiivisiin tapahtumiin liiketoiminnan jatkuvuuden varmistamiseksi (Gregory 2018, 198). Riskienhallinnalla tarkoitetaan tietoista riskien tunnistamista ja hallintaa. Niiden avulla voidaan vähentää tietoturvahäiriöitä, lieventää ei toivottujen tapahtumien vaikutuksia ja valmistautua kohtaamaan moninaisia uhkia. (Vacca 2009, 148.)

Riskienhallinnan toimivuuteen vaikuttavat yrityksen ylimmän johdon tuki sekä yrityksen kulttuurilliset tekijät turvallisuutta ja vastuullisuutta kohtaan. Riskienhallintaprosessi koostuu joukosta strukturoituja toimintoja, jotka mahdollistavat riskien tunnistamisen ja systemaattisen hallinnan. (Juvonen ym. 2014, 15–20.) Tietoriskien hallinnassa riskejä voidaan tunnistaa ja niiden vaikutuksia lieventää erilaisilla teknologisilla ratkaisuilla ja menetelmillä. Riskienhallinnan tulisi olla osana tietoturvastrategiaa, jotta yritys voi kohdistaa niukkoja resurssejaan merkittävimpien riskien minimoimiseen. Riskien tunnistaminen on erittäin tärkeää, sillä tunnistamattomat riskit voivat muodostaa merkittäviä uhkia yrityksen toiminnalle ja johtaa vakaviin taloudellisiin seuraamuksiin. (Gregory 2018, 200-201.)

Riskienhallintastrategian toteutuminen vaatii säännöllisiä toimia ja jatkuvaa kehitystä ympäristön ja olosuhteiden muuttuessa. Yrityksen ulkoiset ja sisäiset tekijät vaikuttavat riskienhallinnan viitekehyksen valintaan sekä toteutukseen. (Oriyano 2017, 27.) Yrityksen tarpeisiin parhaiten sopivimman viitekehyksen soveltaminen edellyttää aina syvällistä ymmärrystä yrityksen strategiasta, kulttuurista, rakenteista, taloudesta, riskinottohalusta ja riskinkantokyvystä. Kaikkia riskejä ei kuitenkaan voida poistaa eikä hallita, mutta niiden kanssa voidaan tasapainoilla tietyin edellytyksin. (Coso 2017, 2; Peltier 2014, 16.)

Tietoriskien hallinta on tasapainottelua liiketoiminnan mahdollisuuksien ja tietoturvaan liittyvien uhkien kanssa. Se on osittain laadullista työtä, sillä huomattavien vahinkotapahtumien

todennäköisyyttä ja todellisia kustannuksia on vaikea ennakoida. Riskienhallintaan on saatavilla erilaisia riskien arviointi- ja mittausmenetelmiä, joiden avulla yritys voi tunnistaa, ymmärtää ja hallita riskejä paremmin. Näiden laadullisten, että määrällisten tekniikoiden avulla yritys voi edistää liiketoimintaan liittyvien päätösten oikeasuuntaisuuden tekeminen. (Gregory 2018, 667; Peltier 2014, 161.)

4.4 Tietosuojalait

Euroopan unionin yleinen tietosuoja-asetus GDPR 2016/679 (General Data Protection Regulation) on EU maissa sovellettava yksityisyyttä ja tietosuojaa turvaava laki, joka astui voimaan keväällä 2018. Asetus velvoittaa kaikkia EU:n kansalaisten henkilötietoja käsitteleviä ja rekisteröiviä organisaatioita riippumatta niiden sijainnista tai siitä, missä tietoja käsitellään. Asetuksessa määritetään, kuinka henkilötietoja tulee käsitellä, velvoittamalla organisaatioita tietojenkäsittelyprosessin turvaamiseksi. (Yleinen tietoturva-asetus, 2016.)

Tietosuoja ovat vahvasti sidoksissa kyberturvallisuuteen ja niihin liittyviltä uhilta suojautumiseen. Tietosuoja-asetusten tarkoituksena on varmistaa asianmukaiset toimet tietoturvakäytäntöihin ja -ratkaisuihin liittyen. Asetuksilla pyritään tehostamaan yleistä tietoturvallisuusuutta ja yhdenmukaistamaan tietosuojaan liittyviä toimia. (Fitzgerald, 2019. 346-348.).

4.5 Penetraatiotestaus

Penetraatiotestauksessa eli murtotestauksessa on kyse simuloidusta hyökkäyksestä järjestelmää tai sen osaa kohtaan. Sen avulla pyritään selvittämään kohteen tietoturvantaso ja siinä piilevät heikkoudet (Van Eeckhoutte & Georgia 2014, 1). Testauksessa käytetään samoja tekniikoita, tietoja ja työkaluja, joita hakkerit käyttävät järjestelmien tietoturvaan liittyvien puutteiden ja haavoittuvuuksien paikantamiseen. Saatuja tuloksia voidaan hyödyntää organisaation tietoturvallisuuden parantamiseen ja siten uhkien minimoimiseen. (Oriyano 2017, 2.)

Yritykset voivat suorittaa penetraatiotestauksia omien osaajien avulla tai hyödyntäen ulkoisia tahoja. Tietoturvan testaaminen vie kuitenkin runsaasti aikaa ja niiden suorittamiseen vaaditaan osaavaa henkilöstöä. Tästä syystä monet yritykset turvautuvat usein kalliiden konsultaatioyritysten palveluihin. Yritysten tulisikin säännöllisesti suorittaa penetraatiotestauksia, sillä hyvin suunniteltu ja toteutettu testaus on yksi parhaimmista kyberturvallisuustason mittareista. (Vacca 2009, 370.)

Penetraatiotestaus tulee suunnitella huolella valituista testausmenetelmistä riippumatta. Testaus on mahdollista toteuttaa sisäisesti tai ulkoisesti ja se voidaan kohdistaa mihin tahansa järjestelmään. Hyökkäys koostuu kolmesta eri vaiheesta eli tiedustelusta, aktiivisesta hyökkäyksestä sekä jälkihyökkäyksestä. (Vacca 2009, 370-373.) Kuviossa 1 on kuvattu penetraatiotestauksen vaiheet.

Kuvio 1: Penetraatiotestauksen vaiheet (Vacca 2009, 373).

Tiedusteluvaiheessa kohteesta pyritään keräämään tietoja passiivisilla sekä aktiivisilla tiedonkeruumenetelmillä. Passiivisessa tiedustelussa tutkitaan avoimia lähteitä, kun taas aktiivisessa tiedustelussa ollaan suorassa kontaktissa kohteen kanssa ja suoritetaan erilasia haavoittuvuus- ja porttiskannauksia. Molemmissa tiedustelumuodoissa tavoitteena on kartoittaa hyökkäyspintaa sopivien hyökkäysvektorien määrittelemiseksi. (Oriyano 2017, 73) Hyökkäysvaiheessa pyritään murtautumaan järjestelmään sisälle soveltuvia työkaluja käyttäen. Jälkihyökkäyksessä arvioidaan hyökkäyksen jatkamisen tarpeellisuutta ja kerätään testauksen myötä saatua tietoa. (Vacca 2009, 373.)

5 Tieto- ja kyberuhat

Tieto- ja kyberuhalla tarkoitetaan sellaista uhkaa, joka toteutuessaan vaarantaisi tärkeiden järjestelmien toimivuuden, tiedon saatavuuden tai luotettavuuden. Kyberturvallisuuteen liittyvät uhat kehittyvät jatkuvasti ja uudet ilmiöt muodostavat entistä suurempia haasteita turvallisuuden ylläpitämisessä. Yritykset joutuvat toistuvasti kehittämään tietoturvapolitiikkaansa ja etsimään toiminnan tueksi uusia tietoturvaratkaisuja. Monesti tarvitaan useiden eri menetelmien yhdistelmiä, jotta voidaan torjua jo olemassa olevia kyberuhkia. (Brooks ym. 2018, 14-15.) Yritysturvallisuuteen liittyvät tieto- ja kyberuhat voidaan jakaa sisäisiin ja ulkoisiin tekijöihin. Sisäisen uhan muodostavat yrityksen henkilökunta, kun taas ulkoiset uhat aiheutuvat organisaation ulkopuolisista tekijöistä. (Bosworth, Kabay, & Whyne 2014, luku 13.1.)

Karkeasti kyberuhat voidaan jakaa kyberrikollisuuteen, kyberterrorismiin, kybersoperaatioihin, kybervandalismiin sekä kybervakoiluun (Puolustusvoimat 2013, 18). Kyberrikollisuus on tietojärjestelmiä ja tietoverkkoja hyödyntävää toimintaa, jonka kohteina voivat olla yritykset, kansalaiset tai valtiolliset toimijat. Kyberterrorismilla tarkoitetaan tietoverkkojen avulla toteutettua terrorismia tai sen uhkaa. Sen avulla pyritään aiheuttamaan pelkoa ja taloudellisia vahinkoja. Hyökkäyksen kohteena ovat usein kriittinen infrastruktuuri ja informaatiojärjestelmät. Kybersoperaatiot liittyy vahvasti maanpuolustukseen ja sotilasoperaatioihin. Kyberoperaatiot tunnetaan myös terminä kybersodankäynti. Sen kohteina ovat informaatiokanavat, järjestelmät ja kriittinen infrastruktuuri. Kybervandalismilla tarkoitetaan yleisesti hakkerointia sekä haktivismia. Toiminta voi kohdistua mihin tahansa yhteiskunnan tasoon ja se on

usein vahingontekoon tai näkyvyyteen pyrkivää toimintaa. Kybervandalismin taustalla on tarkoitukselliset tai aatteelliset syyt. Kybervakoilun avulla pyritään hankkimaan sellaista tietoa, jota muutoin ei ole saatavilla. Yleensä tieto on arkaluonteista ja mahdollisesti turvaluokiteltua. Salaisten tietojen hankinnan kohteina voivat olla yritykset sekä valtiolliset toimijat. (Kyberuhkien viisitasoinen malli 2022; Limnell ym. 2014. luku 2;)

Merkittävä uhka yrityksen tietoturvallisuudelle muodostuu sen entisistä ja nykyisistä työntekijöistä sekä vierailijoista. Työntekijät voivat olla uhkatekijöitä, sillä heillä on usein lähes rajaton pääsy yrityksen toiminnalle tärkeisiin tietoihin ja järjestelmiin. (Vacca 2009, 596.) Tämän takia yksittäinen virhe voi muodostaa vakavan uhan tiedon eheydelle, luottamukselle tai saatavuudelle. Tällaiset uhan konkretisoituvat usein henkilökunnan osaamattomuuden, kokemattomuuden tai väärien oletusten myötä. (Bosworth 2014, luku 13.2.) Tyypillisesi henkilökunnan tekemät virheet johtuvat huolimattomasta toiminnasta kuten turvaluokiteltujen tietojen suojaamattomasta tai epäasiallisesta käytöstä ja säilyttämisestä. Myös laitteistojen ja ohjelmien asiaton käyttö sekä tunnusten ja kulkuavaimien huolimaton hallinta muodostavat konkreettisen uhan yritysturvallisuudelle. Tahallinen toiminta on yksi vakavimmista sisäisistä uhista, sillä työntekijä on usein motivoitunut ja tietää miten suojaukset sekä tietoturvakäytänteet yrityksessä toimivat. (Whitman & Mattord 2011, 501-502; Vacca 2009, 474.)

5.1 Hakkerit ja krakkerit

Hakkerien motiivien ymmärtäminen voi auttaa hyökkäyksien laajuuden sekä mahdollisten hyökkäysvektoreiden tunnistamisessa. Hakkerin tavoitteet sekä taidot määrittävät, että onko kyseessä erimerkiksi hakkeri vai krakkeri. (Oryano 2017, 1-3.) Valkohattu ja harmaahattu hakkerit pyrkivät hyödyntämään verkossa olevien laitteiden ja järjestelmien tietoturva-aukkoja sekä heikkouksia, mutta eivät lähtökohtaisesti pyri tekemään mitään laitonta, vaan ilmoittavat tekemistään havainnoista järjestelmien ylläpitäjälle. (Brooks ym. 2018, 224.)

Krakkerit eli mustahattu hakkerit ovat henkilöitä, jotka pyrkivät murtautumaan järjestelmän sisälle erilaisia menetelmiä käyttäen tarkoituksenaan aiheuttaa vahinkoa joko suoraan tai epäsuoraan. Uhka muodostuu siitä, että krakkeri varastaa tietoja tai pyrkii aiheuttamaan muuta erityistä haittaa, joka on omiaan aiheuttamaan jonkinlaista vahinkoa kohteelle. Krakkerit pyrkivät hyödyntämään ohjelmistoissa ja järjestelmissä olevia virheitä, haavoittuvuuksia sekä suojauksien puutteellisuutta hyökkäyksen toteuttamiseen. (Vacca 2009, 323.)

5.2 Palvelunestohyökkäykset

Palvelunestohyökkäykset (eng. denial of service, distriputed denial of service) ovat tehokkaita hyökkäysmenetelmiä, joiden avulla pyritään kaatamaan verkkosivuja, verkkoja, verkkopalveluita tai palvelimia. Hyökkäyksen tarkoituksena on ylikuormittaa verkon liikennettä siten, että kohdejärjestelmän toimivuus estyy osittain tai kokonaan. Perinteinen palvelunestohyökkäys

voidaan toteuttaa yksittäisellä laitteella erilaisia menetelmiä käyttäen tai hajautettuna palvelunestohyökkäyksenä, jossa hyödynnetään useita järjestelmiä koordinoidusti hyökkäyksen toteuttamiseen. (Whitman & Mattord 2011, 27.)

Nykyaikaiset palvelunestohyökkäykset asettavat uudenlaisia haasteita niitä suojautumiseksi. Hajautettujen palvelunestohyökkäyksien toteuttamisessa käytetään usein ns. bottiverkkoja, joilla tehty koordinoitu hyökkäys ei ainoastaan kuormita kohdepalvelinta vaan myös tietoliikenneverkkoja sekä Internetin-palvelutarjoajia (ISP). Monet organisaatiot ovat alttiina tämänkaltaisille hyökkäyksille. (Peltier 2013, 326.)

5.3 Haittaohjelmat

Haittaohjelmat ovat tyypillisiä tieto- ja kyberturvallisuusuhkia, joihin lukeutuvat mm. virukset, madot, vakoiluohjelmat, kiristyshaittaohjelmat sekä troijalaiset. Niiden tarkoituksena on mahdollista luvaton pääsy laitteeseen tai järjestelmään, aiheuttaa vahinkoa tai anastaa arvokasta tietoa. Haittaohjelmat muodostat vakavan uhan yhteiskunnan kaikilla tahoilla, sillä ne ovat tehokkaita työkaluja ja niitä laaditaan yhä vaikeammin havaittaviksi. (Oriyano 2017, 218.)

Haittaohjelmia kehitetään jatkuvasti ja ne luovat uusia uhkia kyberturvallisuudelle (Brooks ym. 2018, 218). Ukrainassa on havaittu erittäin vaarallinen CaddyWiper niminen haittaohjelma, jonka ominaisuuksiin kuuluvat kiintolevylle tallennettujen tiedostojen totaalinen tuhoaminen (Splunk 2022). Tietoturvaa kehittävien tahojen tuleekin pyrkiä pysymään kehitysvauhdin mukana, jotta uusia uhkia vastaan kyetään suojautumaan (Brooks ym. 2018, 218).

5.4 Sosiaalinen manipulointi

Sosiaalinen manipulointi (eng. social engineering) on tekomuoto, johon keskeisesti kuuluu tietojen kalastelu tai tiedon kerääminen erilaisia huijaus- ja manipulointikeinoja käyttäen. Tietojenkalastelu toteutetaan huijaamalla kohde henkilöä luovuttamaan tunnistetietoja, henkilötietoja tai muuta arvokasta tietoa rikoksen toteuttamiseksi. Tietojenkalastelun liittyviä huijauksia voidaan toteuttaa erilaisia kommunikaatiomenetelmiä käyttäen tai fyysisellä toiminnalla. Perinteisiä tietojenkalastelun tekniikoita ovat sähköposti-, viesti- sekä puhelinhuijaukset. (Oriyano 2017, 219.)

Sosiaalinen manipulointi kohdistuu aina ihmiseen ja siinä käytetään hyväksi ihmisten avuntarvetta, auttamishalua, hyvänuskoisuutta tai hyväntahtoisuutta. Manipulointia voidaan harjoittaa myös fyysisiä tekniikoita käyttäen esimerkiksi kurkkimalla toisen henkilön olan yli, kun hän käyttää tietoteknistä laitetta tai seuraamalla tuntematonta työntekijää fyysisesti suojatun rakennuksen sisälle. Sosiaalisen manipuloinnin taustalla ovat useimmiten taloudelliset syyt. (Peltier 2013, 326.)

5.5 Uhkien havaitseminen ja torjunta

Tieto- ja kyberturvallisuuteen liittyvien uhkien havaitseminen vaatii jatkuvaa tilannekuvan ylläpitämistä. Useat eri palveluntarjoajat jakavat ajantasaista tietoa uusista kyberuhista sekä ilmiöistä, jotta uhilta suojautuminen voidaan tehdä riittävän ajoissa. Tietoturva-aukkojen sekä haavoittuvuuksien tunnistamiseen on saatavilla useita ilmaisia haavoittuvuusskannausohjelmia. Riskienhallinnan ja tietoturva-auditoinnin työkalujen avulla yritys voi havaita järjestelmissä ja toiminnoissa sellaisia puutteita, joiden korjaaminen vaatii välittömiä toimenpiteitä. Yksinkertaisimmillaan haittaohjelmilta ja hyökkäyksiltä suojautuminen voidaan toteuttaa torjuntaohjelmia ja palomuuria käyttäen. (Halpert 2011, 27.)

Monesti huolimattomuudesta ja inhimillisistä syistä johtuvia uhkia voidaan pienentää henkilökunnan asianmukaisella ja säännöllisellä koulutuksella. Lisäksi tietoisuuden lisääminen ja oikeanlainen ohjaus toimii yksinkertaisena tehosteena uhkien havaitsemisessa ja niiden torjunnassa. Yritys voi suhteellisen yksinkertaisilla toimenpiteillä vaikuttaa uhkien havaitsemiseen ja torjuntaan. Tämä kuitenkin vaatii ajantasaista tietoturvastrategian ylläpitämistä ja sen noudattamista. (Peltier 2013, 48.)

5.5.1 Palomuurit

Palomuurit ovat tehokkaita komponentteja verkon ja laitteiden välisen yleisen turvallisuustason parantamiseen. Palomuureja on useita erilaisia ja niitä voidaan käyttää erillisinä järjestelminä tai integroituina muihin laitteisiin esimerkiksi palvelimiin sekä reitittimiin. Palomuurin tarkoituksena on eristää verkot toisistaan. Ne suodattavat tehokkaasti verkosta sisään tulevaa tietoliikennettä, estäen haitallisen tietoliikenteen vaihtoa. (Brooks ym. 2018, 515-516.)

Palomuureja on pääsääntöisesti kolmea erilaista tyyppiä eli pakettisuodattimia, yhteissuodattimia ja sovellusyhdyskäytäviä hyödyntäviä palomuureja. Pakettisuodatinta käyttävät palomuurit välittävät tai estävät tietoliikenteen kulun tiettyihin osoitteisiin. Se ei analysoi pakettien tietoja, vaan tekee päätökset paketin osoitetietojen perusteella. Yhteyssuodattimia käyttävät palomuurit toimivat hyvin pitkälti samalla tavalla kuin pakettisuodattimia käyttävät palomuurit, mutta perusominaisuuksien lisäksi ne tarkkailevat yhteyden tilaa merkiten ylös pakettien sisällön. Palomuuri käyttää kyseisiä tietoja suodatuspäätöksien tekemiseen ja välittää eteenpäin ainoastaan hyväksytyt paketit oikean istunnon mukaisesti. Sovellusyhdyskäytävä palomuurit tarkistavat ja ohjaavat liikennettä protokolla perusteisesti. Palomuuri tutkii sisään ja ulos lähteviä paketteja ja välittää ne eteenpäin ainoastaan, jos paketit vastaavat protokollan mukaisia tietoja. Samalla ne pitävät kirjaa tapahtumista. (Brooks ym. 2018, 515-516; Vacca 2009, 349.)

5.5.2 IDS/IPS

IDS (Intrusion Detection System) eli tunkeilijan havaitsemisjärjestelmä on järjestelmä, joka valvoo tietoliikennettä ja raportoi tapahtumista, jotka poikkeavat normaalista toiminnasta. IDS tarkoituksena on havaita erilaisia poikkeavuuksia, hyökkäyksiä ja tunkeutumisyrityksiä sekä antaa niistä hälytyksiä halutulla tavalla. (Peltier 2013, 142.) IDS järjestelmiä on saatavilla verkkopohjaisina NIDS (Network based intusion detection system) ja laitepohjaisina HIDS (Host based intusion detection system). NIDS ovat verkossa toimiviin laitteistoihin sijoitettuja järjestelmiä, jotka tarkkailevat ja valvovat verkkoliikenteessä kulkevia paketteja. HIDS järjestelmät puolestaan valvovat ja seuraavat laitteiston toimintaa sisältä päin. HIDS tarkoituksena on analysoida lokitietoja ja järjestelmän muutoksia. (Brooks ym. 2018, 210-211.)

IPS (Intrusion Prevention System) eli tunkeutumisenestojärjestelmän tarkoituksena on tunnistaa ja estää verkkoon tai laitteeseen kohdistuvia hyökkäyksiä ja tunkeutumisyrityksiä. IPS käytetään valvomaan tietoliikennettä ja hyödyntämään käyttäytymiseen sekä liikenteen sisältöön perustuvia sääntöjä uhkien tunnistamiseksi. IPS tietoliikenne kulkee järjestelmän kautta, jolloin se pystyy havaitsemaan ja estämään poikkeavaa tai haitallista liikennettä. (Vacca 2009, 596.)

IPS ja IDS toiminta perustuu palomuurien tapaan sääntöihin, mutta ne tarkastavat liikennettä syvällisemmällä tasolla valvoen pakettien sisällä olevia tietoja ja yksityiskohtia. Kyseessä ovat toisistaan irrallisia järjestelmiä ja niiden toiminnot eroavat hieman toisistaan. Molemmat ovat tehokkaita järjestelmiä yhdessä käytettyinä. (Oriyano 2017, 171.)

6 Tutkimusmenetelmät

Tämä opinnäytetyö on toteutettu tapaustutkimuksena. Tapaustutkimus on menetelmä, jossa tyypillisesti pyritään tuottamaan hyvin yksityiskohtaista ja syvällistä tietoa tutkittavana olevasta asiasta. Menetelmän avulla saadaan tuotettua tietoa ilmiöistä ja tapahtumista niiden todellisessa toimintaympäristössä. Tämä mahdollistaa tutkimuksenkohteen kokonaisvaltaisen ymmärtämisen. (Ojasalo, Moilanen & Ritalahti 2014, 52-53.)

Tässä työssä tutkimuksen kohteina olivat Selecore Oy:n tietoturvallisuuden eri tasot, niihin liittyvien puutteiden tunnistaminen ja ratkaisuehdotusten löytäminen. Aineiston keruu toteutettiin erilaisia havainnointimenetelmiä, auditointia sekä penetraatiotestausta käyttäen. Tietoturva-auditointiin käytettiin Suomen hallituksen käynnistämän sisäisen turvallisuuden ohjelman myötä kehitettyä Katakri auditointityökalua. Työ tehtiin laadullisia menetelmiä käyttäen ja näiden avulla pyrittiin saamaan kattava käsitys tutkittavana olevasta tapauksesta.

6.1 Havainnointi

Havainnointi eli observointi on yleinen tiedonkeruumenetelmä, jonka avulla saadaan välitöntä ja totuuden mukaista tietoa tutkimuksen kohteesta. Havainnointi voidaan kohdentaa fyysiseen kohteeseen, tapahtumiin tai ihmisten käyttäytymiseen. Tyypillisesti havainnointia tehdään luonnollisessa ympäristössä, mutta sitä voidaan hyödyntää myös teennäisissä tilanteissa. (Ojasalo, Moilanen & Ritalahti 2015, 114-115.)

Havainnointi tapahtuu reaaliajassa todellisia tilanteita seuraten. Se sopii tutkimuksen ensisijaisena tiedonkeruu menetelmäksi tai muita tukevaksi menetelmäksi. Havainnoinnin avulla voidaan arvioida muiden tutkimuksen aikana kerättyjen tietojen paikkansapitävyyttä ja luotettavuutta. (Ojasalo, Moilanen & Ritalahti 2015, 114-115.)

6.2 Penetraatiotestaus tiedonkeruumenetelmänä

Penetraatiotestausta käytettiin yhtenä tiedonkeruumenetelmänä. Penetraatiotestaus on murtotestauksen muoto, jota hyödynnetään tietojärjestelmien turvallisuuden varmistamisessa. testauksessa käytetään keinoja, joiden avulla pyritään tunnistamaan järjestelmien suojausmenetelmissä olevia puutteita. Penetraatiotestaus voidaan toteuttaa yhtä tai useampaa hyökkäysmenetelmää käyttäen ja se voidaan kohdistaa haluttua järjestelmää kohtaan. Penetraatiotestauksen tarkoituksena on mitata järjestelmien suojausmekanismien toimivuutta ja tarjota runsaasti tietoa, jonka avulla voidaan arvioida, että minkälaisia seurauksia tietoturvapuutteilla voi olla järjestelmien toiminnalle. (Oriyano 2017, 2; Vacca 2009, 252.)

Penetraatiotestaus suoritetaan tyypillisesti käyttämällä automatisoituja tai manuaalisia menetelmiä, joiden avulla järjestelmällisesti testataan kohteen suojausominaisuuksia. Testauksessa käytettyjä tyypillisiä kohteita ovat mm. verkot, laitteet, sovellukset, järjestelmät ja palvelimet. (Oriyano 2017, 2.) Penetraatiotestauksessa voidaan hyödyntää usein verkkorakenteiden kartoitukseen ja järjestelmien haavoittuvuuksien tunnistamiseen suunniteltuja ohjelmia kuten Nmap, Zenmap ja OWASP Zap. Tällaisten ohjelmien avulla voidaan etsiä järjestelmissä olevia avoimia portteja sekä tutkia web-sovelluksissa olevia haavoittuvuuksia. (Geer 2015.)

6.3 Reliabiliteetti ja validiteetti

Reliabiliteetti ja validiteetti ovat käsitteitä, joita käytetään tutkimuksen laadun arvioinnissa. Ne kuvaavat tutkimuksen luotettavuutta ja soittavat kuinka johdonmukaisesti tutkimuksessa käytetyt menetelmät vastaavat tutkittavia ilmiöitä. Reliabiliteetilla tarkoitetaan tulosten samankaltaisuutta, mikäli samaa ilmiötä tutkitaan uudestaan useampaan kertaan samoilla menetelmillä. Validiteetilla puolestaan pyritään osoittamaan, että vastasiko tutkimuksen tulos sitä mitä alun perin lähdettiin tutkimaan. (Kothari 2009, 33.)

Tutkimuksen luotettavuutta on pyritty osoittamaan laadukkaan ja ajantasaisen lähdeaineiston käytöllä. Lähdemateriaali on koostunut asiantuntevasta kirjallisuudesta sekä virallisista verkkolähteistä. Työn eri vaiheet ja prosessit on dokumentointi huolellisesti kirjallisten raporttien sekä aihetodisteiden avulla. Tutkimustuloksien uskottavuutta ja toistuvuutta on pyritty varmentamaan useammalla eri testausmenetelmällä ja niistä tehtyjen havaintojen perusteella.

7 Työn toteutus

Opinnäytetyö toteutettiin tapaustutkimuksena havainnoimalla ja tutkimalla kohdeyrityksen tietoturvakäytäntöihin liittyviä toimintamalleja, tietoverkon rakenteita, palvelinlaitteiston suojausjärjestelmien asetuksia sekä lokitietoja. Tutkimuksen avulla haettiin vastauksia tutkimuskysymyksiin: mikä on yrityksen tieto- ja kyberturvallisuuden taso sekä minkälaisia tieto- ja kyberturvallisuus uhkia yritys kohtaa. Tulosten myötä pyrittiin tarjoamaan kehitysehdotuksia turvallisuudentason kohentamiseen.

Nykytilaa lähdettiin selvittämään tietoturva-auditoinnilla, sillä sen avulla haluttiin saada tarpeellista tietoa yrityksen tietoturvallisuuden hallintaan liittyvistä toimista ja mahdollisista puutteista. Työ tehtiin ulkoisena auditointina, sillä tutkijalle ei ollut aikaisempaa tietoutta tutkimuksen kohteena olevasta tietojenkäsittely-ympäristöstä. Tutkimuksessa hyödynnettiin auditointityökalu Katakri 2020 teknisen osion komponentteja kohteen tietoturvallisuuden nykytilan määrittämiseen ja yrityksen kohtaamien uhkien tunnistamiseen. Arvioinnin ulkopuolelle jätettiin Katakin osiot I-14 hajasäteily, I-17 fyysinen turvallisuus sekä eri tietosuojaluokitukset. Kyseisten osioiden poisjättäminen oli osa opinnäytetyön rajausta ja sillä haluttiin kohtuullistaa työmäärää. Lisäksi osion I-14 vaatimuksien ei katsottu koskevan kohdeyritystä. Liite 1 sisältää tarkentavan listan auditoinnissa käytetyistä Katakrin osista. Katakri 2020 käyttöön päädyttiin sen joustavuuden ja ajantasaisuuden takia. Katakrissa esitettyjen vaatimusten mukaiset tasot voidaan saavuutta usealla eri tavalla ja siksi se antaa paljon tulkinnanvaraa.

Auditoinnissa saatuja tietoja haluttiin varmentaa erikseen suoritettavalla penetraatiotestauksella, jonka avulla pyrittiin osoittaa tutkimuksen ja sen tulosten luotettavuutta. Penetraatiotestauksessa käytettiin verkon kartoittamiseen ja haavoittuvuuksien tunnistamiseen soveltuvia työkaluja sekä murtautumiseen soveltuvia tekniikoita. Niiden avulla saadut tiedot analysoitiin ja tuloksia verrattiin toisiinsa. Tutkimuksen vaiheet toteutettiin siten, että tuloksia oli helppo käsitellä ja jalostaa kohdeyrityksen tarkasteltavaksi. Näiden avulla saatiin kattava käsitys yrityksen tieto- ja kyberturvallisuuden tasosta.

8 Tietoturva-auditointiprosessi ja tulokset

Tietoturva-auditoinnin pääpaino kohdistettiin työn toimeksiantajan toiveiden mukaisesti heidän käytössään olevaan verkkopalvelimeen, jonka avulla ylläpidetään useita verkkopalveluita sekä hallinnoidaan tärkeitä tietoja. Yritys katsoi palvelimen toiminnan olevan keskeinen tekijä yrityksen toiminnalle ja siksi olevan alttiina erilaisille tieto- ja kyberturvallisuusuhille. Verkkopalvelimelle pääsy ei ole sidottu aikaan, paikkaan eikä laitteistoon. Auditoinnissa otettiin huomioon myös yrityksen lähiverkko sekä siihen liitetty laitteisto.

Auditointi toteutettiin hyödyntämällä Katakrin teknisessä osiossa käsiteltäviä asioita osana toimitusjohtajan kanssa käytyjä tapaamisia ja lisäksi tutkimalla sekä havainnoimalla järjestelmien asetuksia, lokeja ja yritykseltä saatuja hälytystietoja. Tapaamiset olivat luonteeltaan keskustelunomaisia ja niissä käytiin johdonmukaisesti läpi auditointiin liittyviä aihealueita. Tutkija kirjasi tapaamisten myötä esille tulleet asiat ylös jatkokäsittelyä varten. Avoimeksi jääneiden asioiden osalta palattiin myöhemmin asiaan erikseen käydyissä puhelinkeskusteluissa. Selecore Oy luovutti kaikki tarvittavat tiedot sekä käyttöoikeudet verkkopalvelimeensa tutkimista varten. Yrityksen toimintatavoista ja Katakrin vaatimusten toteutumisesta tehdyt havainnot kirjattiin huolellisesti ylös ja niistä muodostettiin kokonaiskäsityksen antava alustava selvitys, joka toimitettiin toimitusjohtajalle lausuntoa varten. Vastauksena saadut tiedot analysoitiin ja yhdistettiin tapaamisissa saatujen tietojen kanssa.

Kartoituksen myötä ilmeni, ettei yrityksen käytössä ole kirjallisesti laadittuja tietoturvallisuuteen liittyviä dokumentteja, vaan toiminnot ovat perustuneet yrityksen tietoturvakulttuuriin, käytänteisiin ja tietoturvapolitiikkaan. Keskustelut antoivat kuitenkin positiivisen yleisvaikutelman yrityksen tietoturvallisuuden tasosta. Toimitusjohtajalta saatujen tietojen mukaan yritys on panostanut turvallisuuteen olosuhteet sekä lait huomioiden.

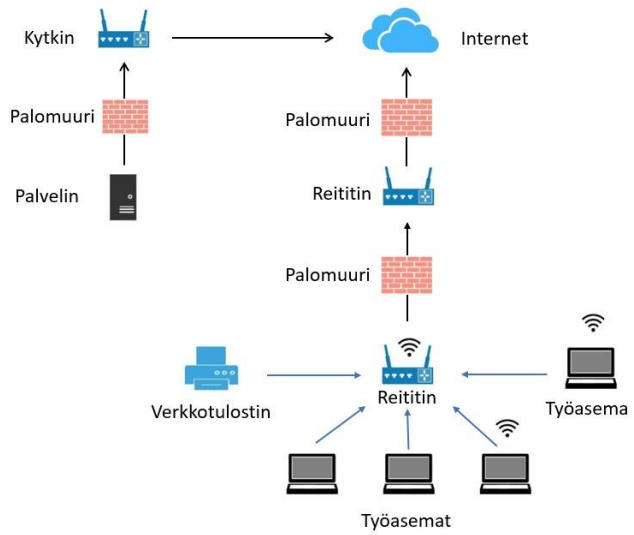
Auditoinnissa ei paneuduttu syvällisesti fyysiseen turvallisuuteen eikä yrityksen käytössä olevien yksittäisten tietoteknisten laitteiden suojaustasoon tai käyttöön. Fyysisestä turvallisuudesta voidaan kuitenkin yleisesti todeta, että toimistorakennus on lukittu tila, eikä sinne ole ulkopuolisilla pääsyä. Kiinteistöä ei kuitenkaan ole varustettu erillisellä teknisellä kulunvalvonnalle eikä valvontajärjestelmällä. Toimitusjohtajan kertoman mukaan liiketoimintatavasta johtuen asiakaskunta ei vieraile kiinteistön alueella ja näin ollen valvonta on voitu luottaa kokonaisuudessaan henkilökunnan käsiin. Yritykselle ei ole laadittu erillistä liiketoiminnan jatkuvuussuunnitelmaa, joten tyypillisimpiä riskejä kuten vesi, tulipalo, laiterikko tai sähkövaurioita ei ole otettu huomioon. Yritys ei säilytä merkittäviä tietoja paperiasiakirjojen muodossa, vaan kaikki on talletettu digitaaliseen formaattiin. (Toimitusjohtaja 2022.)

Tietoturva-auditoinnin tulokset voidaan jakaa toteutuneisiin ja ei toteutuneisiin tilaselvityksiin sekä arviointituloksiin. Auditoinnissa huomiotiin tietoliikenneturvallisuuden, tietojärjes-

telmäturvallisuuden sekä käyttöturvallisuuden osa-alueet. Palvelinratkaisu on selkeästi erotettu yritysverkosta, mutta tuloksia pyrittiin tarkastelemaan yhtenäisesti, jotta saatiin mahdollisimman kattava kokonaiskuva tieto- ja kyberturvallisuuden toteutumisesta sekä kohdatuista uhista. (Liite 1.)

8.1 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuteen liittyvässä osiossa tarkasteltiin verkon rakenteiden, käytettyjen tekniikoiden, protokollien ja suojaustoimien toteutumista tietoliikenneverkkojen kautta tapahtuvan liikenteen luottamuksellisuuden, saatavuuden ja eheyden varmistamiseen. Yrityksen sisäverkko sekä palvelimen verkko ovat täysin erillisiä ratkaisuja ja ne erotettu Internetistä palomuurien avulla. Sisäverkko rakentuu langattomasta WiFi 6 (802.11ax) verkosta ja sitä ylläpitävästä reititinlaitteistosta, joka tukee 2,4Ghz sekä 5Ghz taajuuksia. Langattoman verkon salaustaso on WPA2-PSK (AES). Verkko on johdettu toisen reititinlaitteen avulla vielä erilliseen toimistohuoneverkkoon, jota ylläpitää WiFi 5 (802.11ac) tason verkkolaite, jossa niin ikään WPA2-PSK (AES) salaustaso. Sisäverkon ja Internetin väli on suojattu NAT tekniikalla, kaksisuuntaisella IPS järjestelmällä sekä palomuurilla, jossa erillinen DDoS -suojaus. Palomuuripohjainen DDoS suojaus lisää palomuurisääntöjä, jotka rajoittavat yhteysyritysten suorittamista mm. porttiskannerista ja ICMP PING -kutsujen osalta. Verkon rakenne ja reititinlaitteisto tukee DMZ (Demilitarized zone) aluetta, mutta kyseistä ominaisuutta ei ole toistaiseksi otettu käyttöön. (Toimitusjohtaja 2022; Liite 1.) Kuviossa 2 on hahmoteltu yrityksen sisäverkon rakenne.



Kuvio 2: Karkea kaavio yrityksen verkosta sekä palvelimesta (Toimitusjohtaja 2022).

Yrityksen käytössä oleva palvelin sijaitsee muusta erillään fyysisesti huolella suojatussa ympäristössä. Palvelin on suojattu WAF palomuurilla, johon on lisätty OWASP CRS -hyökkäysten havaitsemissääntöjä, jotka auttavat tunnistamaan ja estämään verkkosovelluksia hyökkäyksiltä.

Suojaustoimenpiteitä tehostetaan Brute Forceja ja Fork Bomb Protection (DDoS) -suojausmenetelmien avulla. (Liite 1.)

Palvelinympäristöön sekä yrityksen verkkoon liitetyt laitteet tunnistetaan, mutta niiden liitettävyyttä ei ole rajattu esimerkiksi ACL tai Host Access Controllin avulla. Verkon sisäinen langaton tietoliikenne on suojattu WPA2-PSK (AES) on salausmenetelmällä. WPA2-PSK (AES) liittyy Brute Force riski, joka on mahdollista toteuttaa toteutettavaa salasanalistaa käyttäen. Etäyhteyksiä sisäverkkoon ei lähtökohtaisesti käytetä, sillä se on katsottu tarpeettomaksi. Palvelimen suuntaan toteutettava etähallinta Internetin ylitse tehdään SSH tietoturvaprotokollaa käyttäen. (Liite 1.)

Ulospäin menevä tietoliikenne suojataan päästä päähän sovellustason salauksella kuten TLS/SSL, SSH FTP:llä sekä verkkotason salauksella HTTPS. Perustason salausta olisi hyvä vahvistaa IPSec-VPN tai TSL-VPN salauksella paremman suojan saavuttamiseksi. Selainpohjaisessa sähköpostiviestinnässä käytetään asiakastilin ja palvelimen välillä salauksena SSL ja TLS protokollia. Heikosti suojattuun liikenteeseen liittyy aina MITM (Man in the Middle) uhka, jossa istunto kaapataan ja kierrätetään hyökkääjän laitteen kautta. (Liite 1.)

Liikenteen suodatus- ja valvontajärjestelmien hallinta on toteutettu asianmukaisesti ja muutoksista vastaa järjestelmävalvoja. Järjestelmien toimintaa ei erikseen testata, vaan seuranta perustuu säännöllisten päivitysten yhteydessä, vikatilanteiden ilmaantuessa tai hälytysten myötä tehtäviin tarkastuksiin. Kaikista suodatuksista ja valvontajärjestelmien tekemistä poikkeushavainnoista tehdään automaattinen ilmoitus järjestelmänvalvojalle. Hallintayhteyksien käyttöoikeuksia on rajattu tietyiltä osin tarpeiden mukaisesti ja niiden valvonta toteutetaan järjestelmävalvojan toimesta. (Liite 1.)

8.2 Tietojärjestelmäturvallisuus

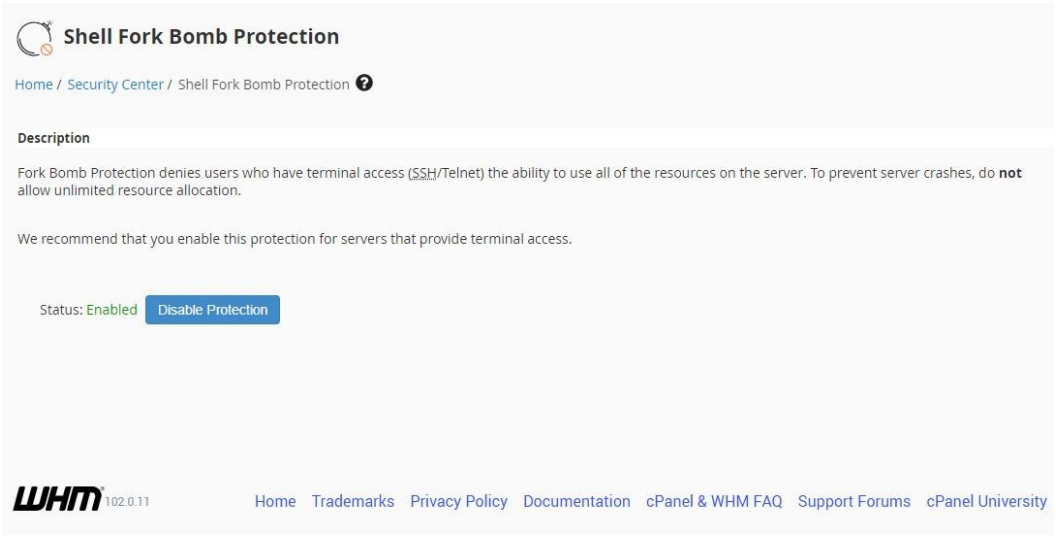
Tietojärjestelmäturvallisuus koostui järjestelmien pääsyoikeuksien hallinnasta, koventamisesta, salauksien ja suojaustoimien käytöstä. Tietojärjestelmien käyttöoikeudet on määritelty ja niitä hallitaan nimetyn henkilön toimesta. Palvelinympäristön rajoitettuja käyttöoikeuksia myönnetään ainoastaan henkilöille, joilla on perusteltu tarve niiden käytölle. Käyttöä seurataan muutosilmoitusten avulla, mutta erillisiä tarkastuksia ei suoriteta. Käyttämättömien tilien käyttöoikeudet perutaan ja tilit poistetaan, jotta väärinkäytöksiä ei tapahtuisi. Kaikkien verkkolaitteiden oletussalasanat on vaihdettu ja niiden käyttö rajattu vain tietyille henkilöille. (Liite 1.)

Palvelinympäristöä käyttävät henkilöt tunnistetaan ja todennetaan kirjautumisten yhteydessä käytettävän vahvan käyttäjätunnuksen ja salasanan avulla. Käyttäjiä ei kuitenkaan velvoiteta käyttämään erikoismerkkejä salasanoissaan eikä vaihtamaan salasanoja määräajan välein. Riittävä määrä virheellisiä kirjautumisyrityksiä, johtaa tunnusten lukitsemiseen. Käyttäjien

heikosti toteutettuun tunnistautumismenetelmään liittyy aina tilin kaappauksen mahdollisuus sekä väsytyshyökkäyksen kohdistaminen kirjautumistilaan. Palvelimessa on käytössä Brute Force Protection järjestelmä, joka tunnistaa ja estää väsytyshyökkäysyritykset. Todennus toteutetaan SSH sertifikaatilla. (Liite 1.)

Toimitusjohtajalta saatujen tietojen mukaan järjestelmäkovennus on tehty kaikkiin yrityksen laitteisiin. Erityisesti palvelinympäristössä on käytössä Kernelcaren kovennetut päivitykset. Tietojenkäsittely-ympäristössä käytössä on ainoastaan luotettavia sovelluksia ja tarpeellisia sovelluksia. Käyttämättömät sovellukset poistetaan käytöstä. Yrityksellä on käytössä menettelytapa, jossa ohjelmat ja niiden lisenssit uusitaan ennen varsinaiset tuen päättymistä. (Liite 1.)

Haittaohjelmilta suojautuminen on toteutettu käyttämällä ajantasaisia virustorjuntaohjelmia palvelinympäristössä sekä yrityskäytössä olevilla laitteistolla. Torjuntaohjelmistojen keräävät lokitietoja ja ilmoittavat hälytyksistä nimetylle henkilölle. Palvelimella tietoturvallisuutta uhkaavia verkkohyökkäyksiä vastaan on suojauduttu WAF tason palomuurilla ja siihen lisätyillä OWASP CRS säännöillä, jotka tunnistavat sekä torjuvat erilaisia uhkia. Tämän lisäksi käytössä Fork Bomb Protection, joka antaa suojaa palvelunestohyökkäyksiä vastaan. (Liite 1.) Kuviossa 3 on ruutukaappaus palvelimen Shell Forrk Bomp Protection järjestelmästä.



Kuvio 3: Ruutukaappaus Shell Fork Bomb Protection (Liite 1).

Tapahtumien jäljitettävyyden varmistamiseksi kaikissa järjestelmissä tapahtuvat muutokset ja poikkeukset lokitetaan ModSecurity työkaluilla, mutta hälytyksien ulkopuolisia tapahtumia ei tarkastella aktiivisesti. Jäljitettävyys on toteutettu asianmukaisesti ja ennalta arvaamattomiin poikkeamiin kyetään reagoimaan hyvissä ajoin. Lokitiedoista otetaan säännölliset varmuuskopiot myöhempiä tarkasteluita varten. (Liite 1.)

Yrityksen sisäverkossa toimivissa työasemissa ei ole käytössä tietojen automatisoituun salaamiseen vaadittavia käytäntöjä eikä salausmenetelmiä. Tiedot ja ulkoiset kiintolevyt salataan ainoastaan tapauskohtaisesti erillistä salausohjelmaa käyttäen. Palvelimella säilytettävät tiedostot, asiakastiedot sekä varmuuskopiot salataan AES-256 salausmenetelmällä. (Liite 1.)

8.3 Käyttöturvallisuus

Käyttöturvallisuuden osalta arvioitiin tiedonsiirron, etähallinnan, ohjelmistojen sekä varmuuskopioinnin liittyvän turvallisuuden varmentamista. Yrityksen laitteet ja kriittiset järjestelmät on suojattu tilikohtaisilla vahvoilla salasanoilla ja vallitsevien tietoturvakäytäntöjen mukaisesti henkilökunta kirjautuu ulos tarpeettomista ohjelmista ja lukitsee tai sammuttaa laitteet aina niiden luota poistuttaessa. Tämä on omiaan vähentämään riskiä luvattomalle käytölle. Työntekijät noudattavat yrityksen kirjoittamatonta tietoturvapolitiikkaa sekä käytäntöjä. Henkilökunnalla on hyvä käsitys tietoturvaan liittyvistä vaaroista ja uhkien torjuntaan käytettävistä toimenpiteistä. Tutkimuksessa oli rajattu ulos sosiaaliseen manipulointiin liittyvät uhkat, joita pääsääntöisesti ilmenee sähköpostitse ja väärennettyjen verkkosivujen kautta tehtyinä tietojenkalasteluna. Näin ollen sähköpostiin liittyvään uhkiin ei syvennyt haittaohjelmientorjuntaa lukuun ottamatta. (Toimitusjohtaja; Liite 1.)

Sisäverkossa toimivat laitteet, järjestelmät sekä ohjelmat saavat säännöllisiä päivityksiä sekä tietoturvapäivityksiä, jotka asennetaan automaattisesti. Automatisointi helpottaa suojaustason ylläpitoa. Varmuuskopiot otetaan säännöllisesti, mutta ne säilytetään fyysisesti samassa tilassa. Tällöin ne ovat haavoittuvaisia rakenteellisille vahingoille esim. tulipalolle ja vesivahingolle. Palvelinympäristössä varmuuskopiot otetaan niin ikään säännöllisesti ja säilytetään fyysisesti eripaikassa. Järjestelmien ja ohjelmien toimivuuteen ei kohdisteta erillisiä tarkistustoimenpiteitä, vaan niiden toimivuus todetaan käytön ja päivitysten asennuksen yhteydessä. (Liite 1.)

Viranomaisten hyväksymiä salausratkaisuja kuten VPN ei ole käytössä. Tiedonsiirto on salattu ja suojattu HTTPS, FTPS ja Pure-FTPd tekniikoita käyttäen, joka on konfiguroitu hyödyntämään TLS Cipher Suitea. Verkon sisäistä tietoliikennettä ei ole suojattu FTP:stä poikkeavin tavoin. Palvelimen suuntaan etähallinnassa toteutetaan SSH:ta käyttäen. Sisäverkossa tapahtuvaan etähallintaan käytetään TLS 1.2 tason salausta. (Liite 1.)

8.4 Havaitut uhat

Tietoturva-auditoinnin aikana tunnistettiin useita palvelimeen kohdistuvia uhkia. Havainnot tehtiin tarkastelemalla palvelimen suojausmekanismien lokitietoja, asetuksia sekä tutkimalla automatisoidun ilmoitusjärjestelmän yritykselle lähettämiä hälytyksiä. Osa uhista toteutuu päivittäistasolla, jolloin erilaisia verkkohyökkäyksiä sekä porttiskannauksia kohdistuu palvelimeen useita kertoja. Yrityksen sisäverkkoon kohdistuvia suoria uhkia ei havaittu. Tämä voi

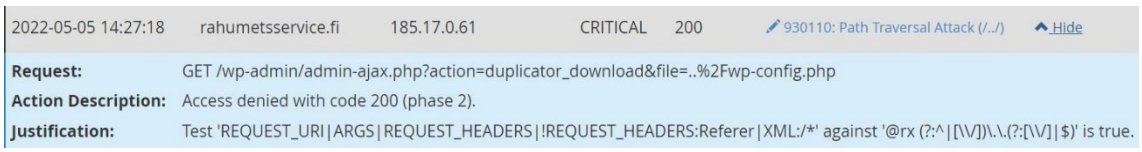
johtua siitä, ettei tavanomaisella piilotetulla toimistoverkolla ole tarpeeksi suurta näkyvyyttä hyökkääjien kannalta. Toimistoverkon IP-osoite ei ollut tutkimusten perusteella helposti löydettävissä julkisesta verkosta. (Liite 1.)

Palvelimeen kohdistuvat hyökkäykset tunnistetaan palomuurin oletussääntöjen sekä OWASP ModSecurity CRS havaitsemissääntöjen avulla. Järjestelmä analysoi hyökkäyksen tyypin, laadun ja pysäyttää sen etenemisen sekä lähettää hälytyksen Contact Managerin kautta nimetylle henkilölle. OWASP CRS on joukko sääntöjä, joita palomuuri voi käyttää järjestelmän suojaamiseen. CRS hyödyntää myös säännöllisesti päivitettävää OWASP Top 10 uhkaluetteloa, joka tarjoaa havaitsemissääntöjä tunnetuimpia ja uusimpia hyökkäyksiä vastaan kuten Cross Site Scripting ja SQL Injection (Liite 1; OWASP 2021).

Palomuuri estää ja raportoi säännöllisesti mm. palvelimeen kohdistuvista Path Traversal Attack, Denial of Service, Remote Code Execution ja Brute Force tyyppisistä hyökkäyksistä sekä erilaisista porttiskannauksista. Hyökkäyksien vakavuudet vaihtelevat hyökkäystyypittäin, mutta niistä ei aiheudu merkittävää vaaraa yrityksen tietoturvallisuudelle, koska järjestelmien eri suojausmekanismit kykenevät torjumaan kaikki hyökkäykset. Mahdollisten väärien positiivisen (false positive) hälytysten poissulkemiseksi, suoritettiin lokien huolellista tutkintaa ja hyökkäyksissä kerättyjen tietojen analysointia. (Liite 1.) Kuvio 4 on kooste palvelimeen kohdistuvista uhista ja niiden vakavuusasteesta.

Ulkoiset uhat	Kriittisyys aste
Path Traversal Attack	Vakava
Remote Code Execution	Vakava
Brute Force	Vakava
Denial of Service	Haitallinen
Restricted File Access Attempt	Vakava
Port scanning	Haitallinen
Ajax request header manipulation	Vähäinen
Anomaly score Exceeded	Haitallinen

Kuvio 4: Esimerkki palvelimen suojausjärjestelmän tekemistä havainnoista (Liite 1).



Kuvio 5: Ruutukaappaus palvelimen havaitsemasta Path Traversal hyökkäyksestä (Liite1).

Kuvio 5 on esimerkki palvelimen havaitsemasta Path Traversal Attack hyökkäyksestä, jossa hyökkääjä pyrki pääsemään käsiksi verkkopalvelimella oleviin tiedostoihin ja hakemistoihin manipuloimalla muuttujia. Hyökkääjä yritti hyödyntää palvelimella olevia tunnistautumismenetelmiä ja mahdollisia järjestelmän haavoittuvuuksia. Palomuurin lokitietojen mukaan kyseessä on hyvin tyypillinen järjestelmää uhkaava hyökkäysmenetelmä. (Liite 1.)

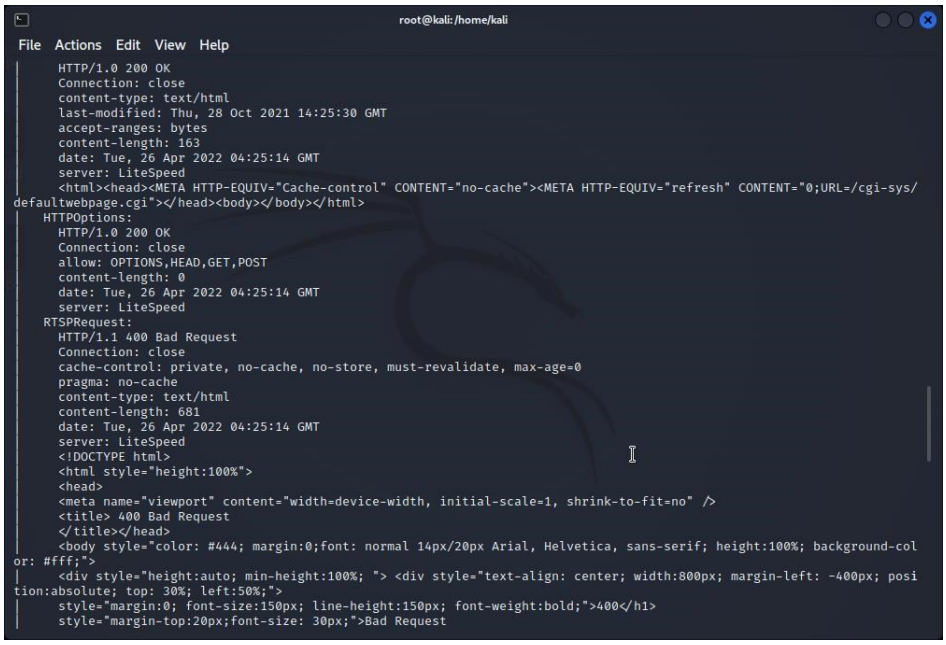
9 Penetraatiotestaus ja tulokset

Auditoinnissa saatujen tulosten luotettavuus perustuu automatisoidun suojausjärjestelmän loki- ja tilastotietoihin sekä tehtyihin havaintoihin järjestelmän asetuksista. Tutkimussuunnitelman mukaisesti yrityksen tieto- ja kyberturvallisuuden tasoa ja siihen kohdistuvien uhkien toteutuvuutta tutkittiin tietoturva-auditoinnin lisäksi myös penetraatiotestauksella. Toimeksiantajan toiveena oli, että murtotestaus kohdistetaan yrityksen palvelimen suojaustason varmentamiseksi. Lähtökohdat testaukselle olivat kuitenkin melko haasteelliset, sillä auditoinnin aikana kävi ilmi, että palvelinympäristö oli hyvin suojattu eikä haavoittuvuuksia havaittu. Alkuperäisen suunnitelman mukaan murtotestaus oli tarkoitus kohdistaa nimenomaan auditoinnissa havaittujen tulosten varmentamiseen, mutta tästä ajatusmallista luovuttiin kokonaan testauksen toteutusvaiheessa. (Liite 2.)

Penetraatiotestaus suunniteltiin aloitettavaksi portti- ja haavoittuvuusskannauksella, joka kohdistettiin palvelimen staattisen IP-osoitteeseen. Tavoitteena oli ensin määritellä sopivat hyökkäysvektorit, sekä tunnistaa mahdolliset uudet haavoittuvuudet ja tämän jälkeen varmistaa saadut tulokset kohdistamalla varsinainen murtotestaus havaittuihin kipupisteisiin. Asiakkaan toiveena oli, että testauksen avulla selvitetään, että löytyykö palvelimelta ja sen turvajärjestelmistä sellaisia haavoittuvuuksia, joita hyväksikäyttämällä yrityksen tiedot voivat vaarantua. Testauksessa käytettävät tekniikat ja työkalut valittiin siten, ettei niiden käytöstä aiheutunut konkreettista vahinkoa palvelimen toiminnalle. (Liite 2.)

Testaus toteutettiin niin sanottuna graybox menetelmänä, jossa testaajalla on käytössä tietyt ennakkotiedot testattavasta tietojärjestelmästä, sovelluksesta, verkosta ja tunnistautumistekniikoista. Testaus aloitettiin avoimien porttien etsinnällä käyttämällä Nmap verkonrakenteiden kartoittamiseen soveltuvaa ohjelmaa. Porttiskannaus suoritettiin skannaamalla portit 22, 23, 53 ja 80. Skannaus päättyi kuitenkin keskeytykseen eikä luotettavia tuloksia saatu. Tämän jälkeen yhteys kohdepalvelimeen estyi kokonaan. Asian tarkastelussa kävi ilmi, että kohteen palomuuri oli blokannut testauksessa käytetyn laitteen IP-osoitteen. Testaus uusittiin VPN yhteydellä ja käyttämällä komentoa Nmap -p0-, jolla pyrittiin skannaamaan kaikki 65535 porttia. Tämäkin skannaus päättyi äkillisesti, eikä luotettavia tuloksia saatu. (Liite 2.)

Toisessa vaiheessa päädyttiin toteuttamaan ns. banner grapping skannaus. Bannerit ovat kohdelaitteesta saatavia palvelutietoja sekä järjestelmätietoja, joita voidaan hyödyntää haavoittuvuuksien paikantamisessa. Skannaus kohdistettiin porttiin 80 komennoilla: Nmap -sS -p 80 -A <IP>. Komento -A mahdollistaa skannauksen toteutumisen ns. aggressiiviissa tilassa, jolloin ohjelma etsii järjestelmien, palveluiden sekä niiden versioiden tunnistetietoja. (Liite 2.) Kuvio 6 on kuvankaappaus Nmap ohjelmalla suoritetusta Banner Grappingista.



Kuvio 6: Ruutukaappaus Nmap ohjelmasta (Liite 1).

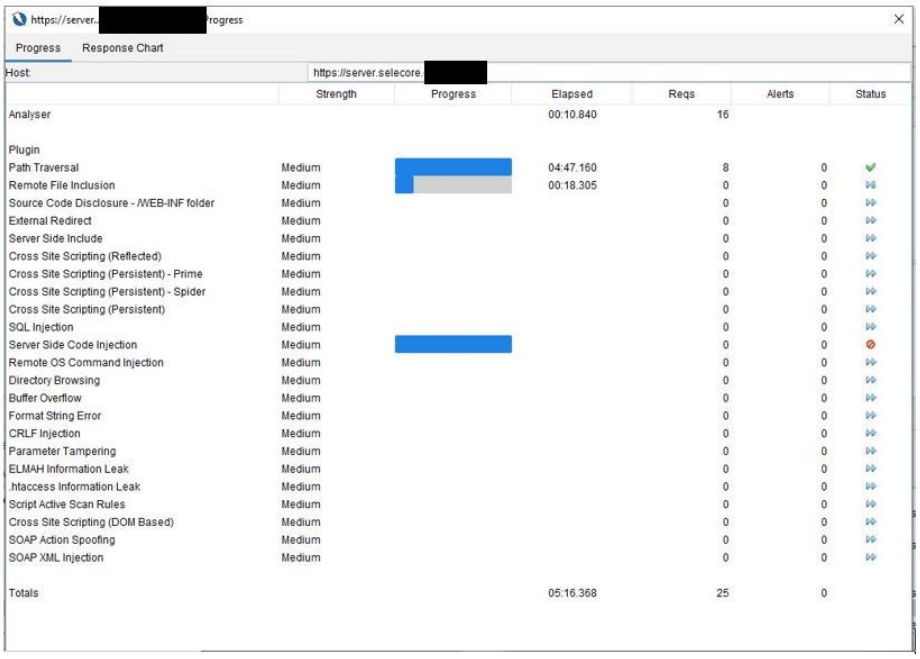
Banner grappingin tuloksena ei niin ikään löytynyt penetraatiotestauksessa hyödynnettävää tietoja. Ensimmäisten skannauksien heikoista tuloksista johtuen porttiskannaus uusittiin käyttämällä Zenmap ohjelmaa, joka on graafinen versio Nmapista. Skannaus tehtiin ns. Stealth tilassa eli SYN-skannauksena, jotta kohteen palomuuri ei reagoisi tapahtuvaan tiedusteluun. SYN-skannaus perustuu siihen, ettei kolmivaiheista kättelyä viedä loppuun asti. Näin ollen suojausjärjestelmät eivät kykene havaitsemaan itse tiedustelua. (Liite 2; Oriyano 2017, 101.) Tuloksena löytyi kymmenen avointa porttia, joiden kautta toimivat palvelimille hyvin perinteiset palvelut kuten HTTPS, FTP, SMTP ja niin edelleen (Liite 2).

Tiedustelun jälkeen suoritettiin haavoittuvuusskannaus hyökkäysvektorien määrittelemiseksi käyttäen Vega nimistä ohjelmaa käyttäen. Vega sisältää laajan kirjon skannaukseen soveltuvia moduuleja, joiden avulla voidaan tarkistaa järjestelmän suojaustaso ja mahdolliset puutteet. Skannaus suoritettiin kahteen kertaan kaikkia moduuleja käyttäen ja sillä pyrittiin tunnistamaan mm. kirjautumiseen, tietokantoihin, JavaScriptiin ja HTML liittyviä haavoittuvuuksia. Testeissä toistui sama ongelma kuin aiemmin suoritetuissa porttiskannauksissa, eli palvelimen

palomuuri esti tutkintalaitteiston IP-osoitteen ja näin ollen skannaus keskeytyi. Vega ehti kuitenkin tunnistamaa muutamia mahdollisia kriittisiä ja lieviä haavoittuvuuksia, joita olivat mm. sokea SQL injektio, Cross-Site Scripting ja kokonaislukujen ylivuotoon liittyviä riskejä. Haavoittuvuuksia ja niiden vaikutuksia on kuvattu tarkemmin liitteessä 2. (Liite 2.)

Varsinainen murtotestaus päätettiin toteuttaa väsytyshyökkäyksenä (Brute Force) ja palvelunestohyökkäyksenä. Väsytyshyökkäys kohdistettiin avoimena olevaan FTP 21-porttiin. Menetelmän avulla pyrittiin murtamaan sivuston FTP tilien tunnukset ja pääsemään käsiksi palvelimella oleviin tiedostoihin sekä saamaan niistä täyden hallinnan. Väsytyshyökkäys perustuu järjestelmällisesti toteutettuihin kirjautumisyrityksiin oikean salasanan löytämiseksi. Hyökkäys toteutettiin Zenmap sovelluksen avulla käyttäen avoimista lähteistä saatavia tunnuslukulistoja sekä käyttäjätunnuslistoja, joita tietoturva-asiantuntijat hyödyntävät penetraatiotestauksessa. Palvelimen Brute Force Protection suojausmekanismi pysäytti hyökkäyksen nopeasti eikä läpimurtoa saatu aikaiseksi. (Liite 2.)

Palvelunestohyökkäys tehtiin niin ikään Zenmap ohjelmalla ja siinä käytettiin ns. Slowloris menetelmää. Slowloris hyökkäyksessä lähetetään hitaasti useita HTTP GET pyyntöjä ylläpitääkseen asiakkaan ja palvelimen välistä yhteyttä, jonka seurauksena kohdepalvelimen voi ruuhkautua ja sen toiminta estyä. Kohteen Fork Bomb Protection suojaus kuitenkin tunnisti hyökkäyksen ja esti välittömästi sen etenemisen, eikä palvelimen toiminta hidastunut lainkaan. Molempien hyökkäysmuotojen tulokset olivat odotettuja. (Liite 2.)



Kuvio 7: Ruutukaappaus OWASP ZAP ohjelmasta (Liite 2.)

Penetraatiotestauksen kolmannessa vaiheessa suoritettiin automatisoitu hyökkäys palvelimen verkkosovelluksia kohtaan käyttäen OWASP Zap ohjelmaa. Sen avulla pyrittiin testaamaan aikaisemmin Vegalla löydettyjä mahdollisia kriittisiä haavoittuvuuksia. Testi toistettiin myös aggressiivisessa tilassa SQL injektion osalta. Molemmat testi päätyivät muiden tavoin keskeytykseen eikä hyökkäys onnistunut toivotulla tavalla. Tämän jälkeen katsottiin, ettei penetraatiotestausta jatketa pidemmälle, sillä suojausjärjestelmien murtamista ulkoa päin pidettiin hyvin epätodennäköisenä. (Liite 2.)

Penetraatiotestauksessa ei saatu ns. läpimurtoa ja tulokset jäivät tältä osin melko laihoiksi. Haavoittuvuusskannauksien myötä ilmeni kuitenkin muutamia injektioluokan ja kokonaislukujen ylivuotoon viittaavia haavoittuvuuksia, jotka liittyvät palvelimella ylläpidettävien verkkosivustojen ja kirjautumissivujen mahdollisiin puutteisiin. Näiden haavoittuvuuksien vaikutuksia ei kuitenkaan kyetty varmentamaan muilla testeillä eikä siksi niiden arvioitu aiheutuvan merkittävää riskiä palvelimen turvallisuudelle. (Liite 2.)

10 Johtopäätös ja kehittämisehdotukset

Tietoturva-auditoinnissa ja penetraatiotestauksessa saatujen tulosten perusteella voidaan todeta, ettei yrityksen tietoverkkoon tai sen palvelinjärjestelmään kohdistu välitöntä vakavaa vaaraa. Palvelinympäristö kohtaa päivittäin useita erilaisia uhkia, joiden kriittisyys vaihtelee tapauskohtaisesti, mutta sen tehokkaiden suojausjärjestelmien ansiosta varsinaista vaaraa ei aiheudu palvelimen toiminalle. Yrityksen tietoturvaa voidaan siis pitää nykyajan vaatimuksen mukaisena ja kyberuhilta suojautumista riittävän tehokkaana. Liiketoiminnan kasvaessa haasteeksi voi muodostua yrityksen sisäinen turvallisuus. Ihmistä pidetään tietoturvan heikoimpana lenkkinä ja siksi turvallisuuskäytäntöjä sekä tietoturvapolitiikkaa tulisi kehittää yhdessä muun turvallisuuden kanssa.

Tietoturva-auditoinnin ja penetraatiotestauksen avulla havaitut puuteteet liittyvät lähinnä, koventamiseen, käyttäjien tunnistamiseen, tilien valvontaan, tietoliikenteen suojaamiseen sekä tiedostojen salaamiseen liittyviin epäkohtiin. Näiden ei kuitenkaan katsottu vaikuttavat merkittävästi yrityksen tämänhetkiseen toimintaan, mutta niihin liittyvät riskit on kuitenkin hyvä tiedostaa. Kehitysehdotusten ja mahdollisten korjaustoimenpiteiden myötä yritys kykenee varautumaan paremmin erilaisiin uhkiin.

Järjestelmien ja verkkojen koventaminen perustuu turvalliseen laitteiden käyttöön, päivitysten asentamiseen, suojaustason korottamiseen sekä ylimääräisten ohjelmien poistamiseen (Vacca 2009, 598). Järjestelmiä voidaan koventaa hyvinkin yksinkertaisilla ratkaisuilla ja täten pienentää merkittävästi hyökkäyspinta-alaa. Yrityksen tulisi ottaa koventaminen osaksi säännöllisiä järjestelmien päivitys- ja tarkastustoimenpiteitä. Koventaminen tulisi kohdistaa myös kaikkiin sisäverkon laitteisiin ja palvelimella ylläpidettäviin verkkosivuihin.

Käyttäjien monivaiheisen tunnistamisen käyttöönotto parantaa laitteiston käyttöturvallisuutta estäen luvattomat kirjautumiset sekä tilinkaappaukset. Palvelinympäristössä havaittiin monivaiheisen tunnistautumisen olevan aktivoituna, mutta todennustekijöitä ei ole määritelty. Tämä ominaisuus on helppo ottaa käyttöön myös muissakin yrityksen käytössä olevissa laitteissa. Tietoliikenteen suojaamisen parantaminen on mahdollista toteuttaa esimerkiksi erillisen VPN ohjelman käyttöönotolla. VPN tarjoaa tehokasta suojaa laitteiden väliseen tietoliikenteeseen. Tämä myös mahdollistaa turvallisen etätyöskentelyn fyysisestä sijainnista riippumatta.

Yrityksellä ei ole käytössä työasemilla säilytettävien tiedostojen ja tietojen salaamiseen soveltuvia automatisoituja menetelmiä. Työasemilla säilytettävät tiedot tulisi salata vaatimusten mukaisella tavalla ja erityisesti henkilötietoja säilyttäessä tulisi noudattaa tietosuoja-asetuksia tietojen turvalliseen säilyttämiseen liittyen. Windows 10 ja 11 käyttöjärjestelmät sisältävät salaukseen sopivan BitLocker nimisen ohjelman, joka sopii erinomaisesti kiintolevyjen sekä ulkoisten tallennusmedioiden salaamiseen. Lisäksi saatavilla on useita ilmaisia ja varsin tehokkaita salausohjelmia.

11 Pohdinta

Opinnäytetyö oli monivaiheinen prosessi, johon kuului useita tapaamisia toimeksiantajan kanssa sekä väliraportointia tutkimuksen etenemisestä. Työn myötä tutkittavaa aineistoa kertyi paljon ja niiden prosessointiin meni runsaasti aikaa. Yhtenä tutkimusmenetelmänä oli alun perin teemahaastattelun toteuttaminen, mutta tästä luovuttiin aikataulullisista syistä. Tapaamiset yrityksen toimitusjohtajan kanssa olivat erittäin antoisia ja sain runsaasti tarpeellista tietoa niiden aikana käytyjen keskusteluiden myötä.

Tietoturva-auditointi sekä penetraatiotestaus osoittautuivat kuitenkin odotettua haasteellisimmiksi kokonaisuuksiksi. Molempien tutkimusmenetelmien hyödyntäminen opinnäytetyön tekemisessä vaati syvällistä perehtymistä testausmenetelmien käyttöön ja niihin liittyvään teoriaan. Työkuorman helpottamiseksi työtä olisi voinut rajata hieman enemmän, jolloin työn laatu olisi voinut olla entistäkin parempi. Toisaalta tietoturva-auditointiin kuuluu tulosten varmentaminen erilaisin teknillisin keinoin, joten tästä syystä kyberuhkiin liittyvien riskien todennäköisyyttä sekä suojausmenetelmien toimivuutta oli syytä tutkia myös konkreettisilla testausmenetelmillä.

Opinnäytetyössä pyrittiin selvittämään mikä on yrityksen tietoturvan nykytila ja minkälaisia uhkia se kohtaa. Lisäksi haluttiin selvittää, että millä keinoilla yritys voi suojautua havaittuja uhkia vastaan. Kaikkiin kysymyksiin saatiin asianmukaiset vastaukset, jotka esiteltiin yrityksen toimitusjohtajalle erillisten raporttien muodossa.

Tietoturva-auditoinnin sekä penetraatiotestauksen myötä saatujen tuloksien perusteella voitiin tarjota kehitysehdotuksia havaittuihin puutteisiin. Tutkimuksen tuloksia voidaan pitää luotettavana useista testauskerroista ja tulosten yhteneväisyydestä johtuen. Toimeksiantajan saamien hyötyjen lisäksi työ oli myös antoisa ja opettavainen tekijälleen. Tietoturva-auditointi ja penetraatiotestaus osoittautuivat hyödyllisiksi sekä tehokkaiksi menetelmiksi tutkittaessa kohde yrityksen turvallisuuden tasoa. Työn toteuttaminen vaati runsaasti perehtymistä käytettäviin menetelmiin sekä työkaluihin. Uskon näistä saamieni oppien olevan hyödyksi minulle myös työelämässä.

Lähteet

Painetut

Bosworth, S., Kabay, M. & Whyne, E. 2014. Computer Security Handbook. New Jersey: Hoboken.

Brewer, D. 2021. ISO/IEC 27001:2013 – Mastering Risk Assessment and the Statement of Applicability. Independently published.

Brooks, C., Grow, C., Craig, P. & Short, D. 2018. Cybersecurity Essentials. Indianapolis: Sybex.

Carter, N. 2004. Auditointi ja ISO 19011. Helsinki: Gummerus Kirjapaino.

Halpert, B. 2011. Auditing Cloud Computing: A Security and Privacy Guide. New Jersey: Hoboken.

Hiles, A. 2013. Business Continuity Management: Global Best Practices. Brookfield: Rothstein.

ISO. 2015. ISO 31000 Risk Management. Practical Quide for SMEs. Switzerland: ISO.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Helsinki: Finanssi ja vakuutuskustannus Finva.

Kothari, C. 2009. Research Methodology: Methods & Techniques. New Delhi: New Age Publication.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro.

Oriyano, S. 2017. Penetration Testing Essentials. New Jersey: Hoboken.

Peltier, T. 2014. Information Security Fundamentals. Second Edition. Florida: CRC Press.

Van Eeckhoutte, P. & Georgia, W. 2014. Penetration Testing: A Hands-On Introduction to Hacking. San Francisco: No Starch Press.

Sähköiset

Communications Security Establishment. 2021. An Introduction to the Cyber Threat Environment. Viitattu 12.5.2022.
https://cyber.gc.ca/sites/default/files/publications/Intro-to-cyber-threat-environment-e.pdf

Coso. 2017. Enterprise Risk Management Integrating with Strategy and Performance. Viitattu 7.4.2022.
https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Eur-Lex. 2016. Euroopan unionin virallinen verkkosivusto. Yleinen tietoturva-asetus. Viitattu 25.4.2022.
https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Fitzgerald, T. 20019. CISO COMPASS:Navigating Cybersecurity Leadership Challenges with Insights from Pioneers. E-kirja. Boca Raton: Auerbach Publications.

Geer, D. 2015. Networkworld. 8 penetration testing tools that will do the job. Viitattu 16.5.2022.
https://www.networkworld.com/article/2944811/8-penetration-testing-tools-that-will-do-the-job.html

Gregory, Peter H. 2018. CISM: Certified Information Security Manager. E-kirja. New York City: McGraw Hill.

Hakala, Juha T. 2004. Opinnäyteopas ammattikorkeakouluille. E-Kirja. Helsinki: Gaudeamus.

KvaliMOTV. 2021. 6.3. Teemahaastattelu. Viitattu 31.3.2022.
https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_2.html

Limnell, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. E-kirja. Jyväskylä: Docendo.

Jyväskylän Yliopisto. 2021. Kyberuhkien viisitasoinen malli. Viitattu 23.4.2022.
https://peda.net/jyu/it/do/kkv/4kjna/4kj/kvm2

OWASP. 2022. OWASP ModSecurity Core Rule Set
https://owasp.org/www-project-modsecurity-core-rule-set/

Puolustusvoimat. 2013. Suomen kyberturvallisuusstrategia. Viitattu 22.4.2022. https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30

Sisäministeriö. 2022. Kyberrikollisuutta torjutaan yhteistyöllä. Viitattu 18.4.2022. https://intermin.fi/poliisiasiat/kyberrikollisuus/kyberrikollisuuden-torjunta

Splunk. 2022. Threat Update: CaddyWiper. Viitattu 14.5.2022. https://www.splunk.com/en_us/blog/security/threat-update-caddywiper.html

Turvallisuuskomitea. 2022. Suomen kyberturvallisuustrategia 2019. Viitattu 18.4.2022. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Ulkoministeriö. 2020. Katakri 2020: Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 21.4.2022. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Vacca, J. 2009. Computer and Information Security Handbook. E-kirja. Burlington: Morgan Kaufmann.

Valtioneuvosto. 2022. Ajankohtaisselonteko turvallisuusympäristön muutoksesta. Viitattu 18.5.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163999/VN_2022_18.pdf?sequence=1&isAllowed=y

Valtionvarainministeriö. 2017. Ohje riskienhallintaan. Viitattu 16.4.2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf

Vilkka, H. 2021. Tutki ja kehitä. E-kirja. Jyväskylä: PS-kustannus.

Whitman, E. & Mattord, H. 2011. Principles of Information Security. E-kirja. Boston: Cengage Learning.

Julkaisemattomat

Toimitusjohtaja. Keskustelu yrityksen verkonrakenteista ja tietoturvaratkaisuista. Viitattu 5.5.2022.

Kuviot

Liitteet

Tietoturva-auditointi

Liite 1: Tietoturva-auditointi

Sivumäärä: 25
Asiakirjan sisältö: Selecore Oy tietoturva-auditointi.

Toimeksiantaja: Selecore Oy
Auditoija: Joonas Muhonen
Päivämäärä: 22.4.2022

Sisällysluettelo:

JOHDANTO

Tietoturva-auditoinnin kohteena oli pilvipalveluita tarjoava Selecore Oy. Tämä raportti on osa opinnäytetyötä ja se sisältää auditoinnin aikana tehdyt havainnot yrityksen sisäverkon sekä palvelimen tietoturvallisuudesta, niihin liittyvistä mahdollisista haavoittuvuuksista ja uhista. Työn pohjana on käytetty viranomaisten käyttöön suunnitellun auditointityökalu Katakrin teknistä osiota. Auditoinnin tulokset perustuvat yritykseltä saatuihin tietoihin sekä auditoijan tekemiin havaintoihin tietojenkäsittely-ympäristöstä.

Tässä raportissa esitetään kohdeyrityksen teknisen tietoturvallisuuden osa-alueiden mukaisten suojaustasojen toimivuutta ja toteutumista virallisten vaatimusten mukaisesti. Työssä esitetään myös lyhyet suositukset hyökkäyspinta-alan pienentämiseen. Työn tuloksia voidaan pitää suuntaa antavina. Katakrin vaatimusluokat on luettavissa osoitteessa https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/

Vaatimuksen mukainen tila on ilmaistu seuraavasti:

Toteutuu = Vastaa vaatimusten mukaisia suojaustapoja ja menettelyjä.
Toteutuu osittain = Vastaa joiltakin osin vaatimusten mukaisia suojaustapoja ja menettelyjä.
Ei toteudu = Ei vastaa riittäviltä osin vaatimusten mukaisia suojaustapoja ja menettelyjä.

Auditoinnissa käsitelty Katakrin seuraavia osa-alueita:

Tietoliikenneturvallisuus

- I-01 Verkon turvallisuus
- I-02 Tietoliikenne-verkon vyöhykkeistäminen ja suodatussäännöstöt
- I-03 Suodatus ja valvontajärjestelmien hallinnointi
- I-04 Hallintayhteydet
- I-05 Langaton tiedonsiirto

Tietojärjestelmäturvallisuus

- I-06 Pääsyoikeuksien hallinnointi
- I-07 Monitasoinen suojaaminen - Toimijoiden tunnistaminen
- I-08 Vähempien oikeuksien periaate - Järjestelmäkovennus
- I-09 Haittaohjelmasuojaus
- I-10 Tapahtumien jäljitettävyys
- I-11 Poikkeamien havainnointikyky ja toipuminen
- I-12 Salausratkaisut
- I-13 Ohjelmistojen suojaaminen verkkohyökkäyksiltä

Käyttöturvallisuus

- I-15 Tiedon sähköinen välitys
- I-16 Muutoshallintamenettelyt
- I-18 Etäkäyttö ja etähallinta
- I-19 Ohjelmistohaavoittuvuuksien hallinta
- I-20 Varmuuskopiointi
- I-21 Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen

KOOSTE AUDITOINNIN TULOKSISTA

Taulukkoon on koostettu yhteenveto auditoitujen osa-alueista ja niiden tilasta.

ALUE	TILA
VERKON TURVALLISUUS	Toteutuu
TIETOLIIKENNE-VERKON VYÖHYKKEISTÄMINEN JA SUODATUS-SÄÄNNÖSTÖT	Toteutuu
SUODATUS JA VALVONTAJÄRJESTELMIEN HALLINNOINTI	Ei toteudu
HALLINTAYHTEYDET	Toteutuu osittain
LANGATON TIEDONSIIRTO	Toteutuu
PÄÄSYOIKEUKSIEN HALLINNOINTI	Toteutuu
TOIMIJOIDEN TUNNISTAMINEN	Toteutuu osittain
JÄRJESTELMÄKOVENNUS	Toteutuu osittain
HAITTAOHJELMASUOJAUS	Toteutuu
TAPAHTUMIEN JÄLJITETTÄVYYS	Toteutuu
POIKKEAMIEN HAVAINNOINTIKYKY JA TOIPUMINEN	Toteutuu
SALAUSRATKAISUT	Toteutuu osittain
OHJELMISTOJEN SUOJAAMINEN VERKKOHYÖKKÄYKSILTÄ	Toteutuu
TIEDON SÄHKÖINEN VÄLITYS	Ei toteudu
MUUTOSHALLINTAMENETTELYT	Ei toteudu
ETÄKÄYTTÖ JA ETÄHALLINTA	Ei toteudu
OHJELMISTOHAAVOITTUVUUKSIEN HALLINTA	Toteutuu
VARMUUSKOPIOINTI	Toteutuu
TURVALLISUUSLUOKITELTUJEN TIETOJEN TUHOAMINEN	Toteutuu

TIETOLIIKENNETURVALLISUUS

Tietoliikenneturvallisuus käsittää yrityksen sisäisessä-, ulkoisessa- ja palvelinverkossa tapahtuvaa tietoliikennettä ja liikenteen suojaamista.

Verkon turvallisuus:

1.1 Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Yrityksen käytössä oleva palvelinlaitteisto on sijoitettu kokonaan erilliseen toimintaympäristöön muusta yrityksen verkosta.

1.2 Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Toimisto- ja verkkolaitteissa on käytössä laitekohtaiset palomuurit. Palvelin on varustettu verkkopohjaisella palomuurilla.

1.3 Hallitun fyysisen turva-alueen ulkopuolelle menevä tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla.

Tila Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Palvelinympäristössä tietoliikenne on suojattu ja salattu SSH, TLS, SSL, HTTPS sekä SFTP protokollilla. Yrityksen sisäverkosta ulos kulkevaa tietoliikennettä suojataan sovellustason salauksella TLS/SSL, HTTPS sekä tarvittaessa salaamalla tiedostot erillisellä ohjelmalla ennen tiedostojen siirtämistä turva-alueen ulkopuolelle. Sähköpostiliikenne salataan GnuPG avoimen lähdekoodin ohjelmistolla.

Suositus: Suositellaan IPSec-VPN tai TLS-VPN käyttöä tietoliikenteen salaamiseen.

1.4 Tietojenkäsittely-ympäristön kytkeminen muiden turvallisuusluokkien ympäristöihin edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymän yhdyskäytäväratkaisun käyttöä.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Käytössä useampi solmu. Turvallisuusluokkia ei ole määritelty soveltuvalla tavalla. Toistaiseksi ei ole tarvetta muutoksille.

Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt:

1.5 Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Tietoverkko on jaettu vyöhykkeisiin ja ulkoa tuleva liikennettä suodatetaan. Ainoastaan välttämätön sisään tuleva liikenne on sallittua. Palvelin sekä työasemat on eroteltu toisistaan. Käytössä protokollat IPv4, HTTPS, SSH, SFTP, SMTP. Verkkoja ei ole jaettu turvallisuusluokittain. Yleisiin verkkohyökkäyksiin on varauduttu käytössä olevien suojausjärjestelmien avulla.

Suodatus ja valvontajärjestelmien hallinnointi:

1.6 Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Järjestelmiä ylläpidetään valmistajien toimesta tarjotuilla säännöllisillä tietoturvapäivityksillä.

1.7 Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen, poistaminen ja valvonta on vastustettu ja organisoitu.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Asetuksiin liittyvät hallinta- ja valvontatoimet ovat tietoturvaa ylläpitävän henkilön vastuulla.

1.8 Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.

Tila: Ei toteudu
Lyhyt kuvaus toteutuksesta: Dokumentointia ei ole toteutettu suositellulla tavalla. Verkko on segmentoitu, mutta suodatus- ja valvontajärjestelmiä ei ole dokumentoitu siten, että niiden toteutustavat voidaan tarkastaa erillisistä dokumenteista.

Suositus: Verkkorakenteen dokumentointia ei katsota kohdeyrityksessä välttämättömäksi.

1.9 Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Tietoturvaa ylläpitävä henkilö seuraa säännöllisesti järjestelmien toimintaa. Toimintaa ei erikseen testata, vaan seuranta perustuu säännöllisten päivitysten yhteydessä tai vikatilanteiden ilmaantuessa tehtäviin tarkastuksiin. Kaikista suodatuksista ja valvontajärjestelmien puuttumisesta liikenteeseen ilmoitetaan turvallisuudesta ylläpitävälle henkilölle 24/7.

Hallintayhteydet:

1.10 Hallintayhteydet on rajattu turvallisuusluokittain, ellei käytössä ole toimivaltaisen viranomaisen ko. turvallisuusluokille hyväksymää yhdyskäytäväratkaisua.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Hallintayhteyksistä vastaa tietoturvallisuudesta vastaava henkilö ja hallintayhteyksiä seurataan riittävällä tasolla. Tietyille toimijoille on annettu rajoitetut käyttöoikeudet palvelinympäristön tiettyihin järjestelmiin. Hallintayhteyksien käyttäjä tunnistetaan ja todennetaan kaikissa laitteissa.

Suositus: Hallintayhteyksien laajempaa määrittelyä ei katsota tarpeelliseksi yrityksen koko huomioon ottaen.

1.11 Hallintaliikenteen sisältäessä turvallisuusluokiteltua tietoa ja kulkiessa matalamman turvallisuusluokan ympäristön kautta, turvallisuusluokitellut tiedot on salattu toimivaltaisen viranomaisen hyväksymällä salaustuotteella.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Käytössä ainoastaan yksi turvallisuusluokka.

Suositus: Useimpien turvallisuusluokkien määrittely on suositeltavaa, mikäli salattavan/suojattavan aineiston liikuteltavuus katsotaan välttämättömäksi.

1.12 Hallintaliikenteen kulkiessa ko. turvallisuusluokan sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Käytössä ainoastaan yksi turvallisuusluokka.

1.13 Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Ainoastaan nimetyillä henkilöillä on käyttöoikeudet.

Langaton tiedonsiirto:

1.14 Langattomassa tiedonsiirrossa tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä salausratkaisulla.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Yritysverkon ylitse siirrettävä tietoliikenne suojataan ja salataan käyttämällä TLS/SLL HTTPS, WPA2+PSK ja AES.

TIETOJÄRJESTELMÄTURVALLISUUS

Tietojärjestelmäturvallisuuteen kuuluvat järjestelmien pääsyoikeuksien hallinta, haittaohjelmientorjunta, käyttäjätilien tunnistaminen ja todentaminen.

Pääsyoikeuksien hallinnointi:

1.1 Tietojärjestelmien käyttöoikeudet on määritelty.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Käyttöoikeudet on määritelty ja niitä hallitaan nimetyn henkilön toimesta. Käyttöoikeuksien myöntämisestä on omat käytännöt.

2.2 Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksista on varmistuttu.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Rajoitettuja käyttöoikeuksia myönnetään ainoastaan henkilöille, joilla on perusteltu tarve niiden käytölle. Käyttö on valvottua. Palvelinympäristössä asiakkaiden käyttöoikeudet rajataan tarpeiden mukaisesti. Tietoja käyttöoikeuksien haltijoista säilytetään asianmukaisesti.

2.3 Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Toteutuu täysmääräisesti käyttäjien osalta.

Suositus: Suositellaan tarkistamaan palvelinympäristössä olevien automaattisten prosessien käyttöoikeudet.

2.4 Käyttöoikeudet on pidettävä ajantasaisina.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Käyttöoikeuksia tarkastellaan tarpeen mukaan. Erillistä katselmointia ei toteuteta.

Suositus: Asiakaskunnan kasvaessa suositellaan käyttöoikeuksien säännöllistä tarkistusta.

Toimijoiden tunnistaminen:

2.5 Tietojenkäsittely-ympäristöä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti.

Tila: Toteutuu osittain

Lyhyt kuvaus toteutuksesta: Palvelinympäristössä tunnistaminen toteutetaan henkilökohtaista käyttäjätunnus ja salasanaparia käyttäen. Tunnistautumista voidaan pitää riittävän yksilöivänä. Salasanaa ei pakoteta vaihtamaan määräajoin. Salasanojen pituusvaatimus on riittävä, mutta erikoismerkkeihin liittyviä vaatimuksia ei ole asetettu. Yhteyskäyttötunnuksia ei ole käytössä. Turvallisuusluokiteltavaa tietoa käytetään ainoastaan yrityksen laitteilla. Tietoja keskenään vaihtavia tietojärjestelmiä eikä laitteita tunnisteta riittävällä tasolla. Vaihtoehtoisia todennustapoja ei ole käytössä.

Palvelinympäristön Brute Force Protection:

- Kirjautumisen Brute Force Protection on käytössä
- Käyttäjänimipohjainen suojaus seuraa käyttäjätilien kirjautumisyrityksiä.
- Brute Force Protection Period (minuuteissa) min 5
- Virheiden enimmäismäärä tilikohtaisesti 15
- Käytä suojausta vain paikallisille osoitteille
- IP-osoitepohjainen suojaus seuraa kirjautumisyrityksiä tietyistä IP-osoitteista
- IP-osoitepohjainen brute Force -suojausjakso 300min.
- Virheiden enimmäismäärä IP-osoitetta kohden 5
- Estää IP-osoitteet palomuuri tasola

Suositus: Tunnistautumisen ja todentamisen puutteellisuuteen liittyy korostunut Brute Force ja MITM riski.

- Suositellaan monivaiheisen/kaksivaiheisin tunnistautumisen käyttöönottoa.

- Pakotetun salasanojen vaihtovälin käyttöönottoa.

- Yksivaiheisen tunnistautumisen ollessa käytössä on suositeltavaa käyttää salasanoja, jotka koostuvat kirjaimista, numeroista ja erikoismerkeistä.

- Salasanan vahvuus tulisi määrittää.

- Erityisehtojen asettamista Host Access Controllille.

Järjestelmäkovennus:

2.6 Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Palvelinympäristössä käytössä on ainoastaan kovennetut järjestelmät ja palvelut. Käytössä olevien ohjelmien, järjestelmien, palveluiden ja yhteyksien määrää on rajoitettu. Yritysverkossa toimivat laitteitta on osittain kovennettu haavoittuvuuspinta-alan pienentämiseksi.

2.7 Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Palvelinympäristössä kovennettavat kohteet on tunnistettu ja kovennettu. Käytössä on mm. Kernelcare ominaisuus, joka ajaa laitteistoon kovennettuja päivityksiä. Kovennuksen toimivuus tarkastetaan järjestelmiin suoritettavien säännöllisten päivityksien yhteydessä. Yrityksen sisäverkossa toimivien päätelaitteiden kovennukseen pyritään tapauskohtaisesti järjestelmien, ohjelmien ja laitteistojen käyttötarkoitus huomioon ottaen. Laitteiston liikuteltavuutta ei ole rajoitettu teknisillä toimenpiteillä. Taustalla voi toimia tarpeettomia prosesseja, joiden sulkeminen olisi suotavaa.

Suositus: Suositellaan sähköpostiin SMTP liittyvää kovennusta. Suositellaan yrityksen sisäverkossa olevien päätelaitteiden kaikkien järjestelmien ja ohjelmien koventamista.

2.8 Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.

Tila: Toteutuu osittain

Lyhyt kuvaus toteutuksesta: Palvelinympäristössä kovennus toteutetaan kaikissa tapauksissa asianmukaisella tavalla. Yrityksen sisäverkossa palveluita ja prosesseja rajataan tapauskohtaisesti järjestelmien koventamiseksi. Oletussalasanat on vaihdettu ja niitä säilytetään suojattuna. Käyttäjät tunnistetaan, laitteet ja rajapinnat lokitetaan. Hallintayhteydet tunnistetaan. Istuntoja ei aikakatkaista.

Palvelinympäristössä Shell Fork Bomb Protection on oletuksena päällä. SFBP estää käyttäjiä, joilla on pääsy päätelaitteeseen (SSH/Telnet) käyttämästä kaikkia palvelimen resursseja.

Suositus: Suositellaan järjestelmällistä koventamista kaikkiin sisäverkossa käyttöönotettaviin ohjelmistoihin, järjestelmiin sekä palveluihin ja niiden käytön rajaamista tarpeen mukaan. Istunnon aikakatkaisu tulisi ottaa käyttöön kaikissa tilanteissa. Suositellaan salasanojen pakotettua vaihtoa määräaikojen välein.

2.9 Kovennusten voimassaolosta ja vaikuttavuudesta huolehditaan koko tietojärjestelmän elinkaaren ajan.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Käytössä on säännölliset seuranta- ja ylläpitotoimet. Koventaminen perustuu yleisiin turvallisuuskäytäntöihin.

Suositus: Järjestelmien, ohjelmien, laitteistojen ja palveluiden koventamisella pienennetään hyökkäyspinta-alaa merkittävästi.

Haittaohjelmasuojaus:

2.10 Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Haittaohjelmilta suojautuminen on toteutettu käyttämällä ajantasaisia haittaohjelmien torjuntaohjelmistoja palvelinympäristössä sekä yrityskäytössä olevilla laitteistolla. Henkilöstöllä on yleistietämys haittaohjelmien torjunnasta ja riskeistä, jotka liittyvät ulkopuolisten tuntemattomien laitteiden (USB) liittämiseen sisäverkkoon. Säännöllisillä tietoturvapäivityksillä ja varmuuskopioilla pyritään turvaamaan mahdollisten haittaohjelmien vaikutukset. Torjuntaohjelmistot keräävät lokitietoja ja ilmoittavat poikkeamista sähköpostitse nimetylle henkilölle.

Tapahtumien jäljitettävyys:

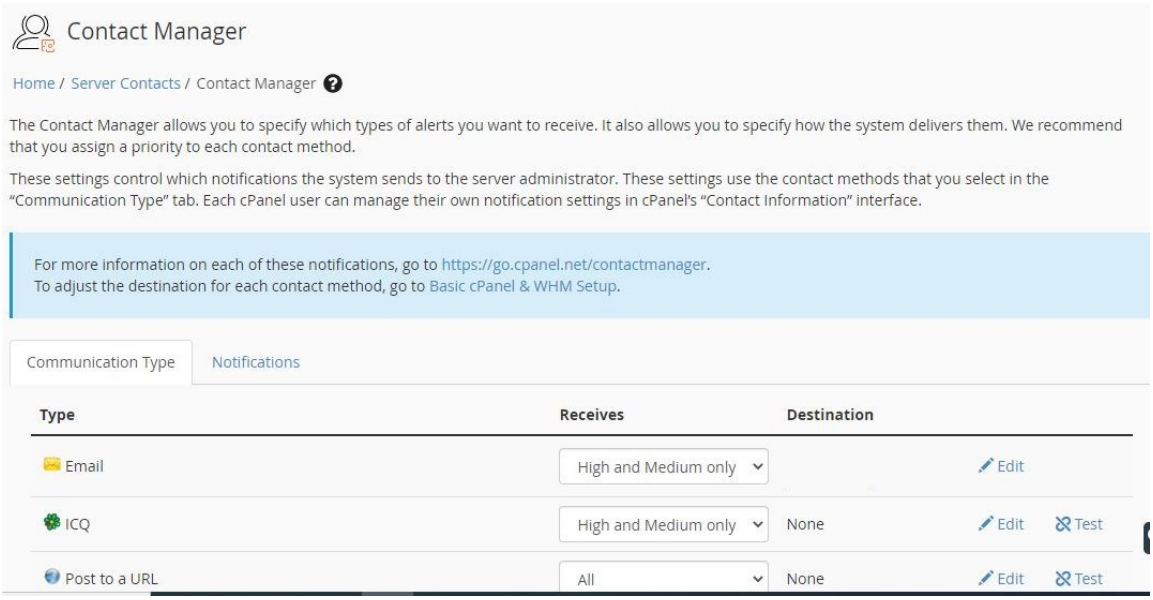
2.11 Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Tapahtumat lokitetaan, mutta hälytyksien ulkopuolisia tapahtumia ei tarkastella aktiivisesti. Jäljitettävyyteen liittyvät käytännöt ovat kuitenkin olemassa ja poikkeamiin kyetään reagoimaan. Lokitiedoista otetaan säännölliset varmuuskopiot myöhempiä tarkasteluita varten. Jäljitettävyys tukee yrityksen toimia poikkeamatilanteissa, jolloin kyetään varmistumaan tapahtumista ja tekemään korjaavia toimia.

Palvelinkerää kaikki tiedot tapahtumista.
Statistiikat kerätään seuraavasti:

- Verkkoliikennetilastot 24 tunnin välein
- Kaistanleveystilastot 2 tunnin välein

Contact Manager hälyttää/ilmoittaa kattavasti eri tapahtumista asetettujen prioriteettien mukaan. Ilmoitukset toimitetaan SMS viestinä sekä sähköpostitse turvallisuudesta vastaavalle henkilölle.



Kuva 1. Ruutukaappaus: Contact Manager.

2.12 Tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Yrityksellä ei ole käytössä SIEM järjestelmää palvelimella eikä yrityksen sisäverkossa. Tapahtumalokitietoja ei seurata aktiivisesti. Tapahtumat lokitetaan ja poikkeamiin puututaan, kun ne havaitaan.

Suositus: Suositellaan keskitettyä SIEM järjestelmän käyttöönottoa poikkeamien havaitsemisen tehostamiseksi.

Poikkeamien havainnointikyky ja toipuminen:

2.13 Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne viipymättä.

Tila: Toteutuu osittain

Lyhyt kuvaus toteutuksesta: Palvelinympäristössä poikkeamien havainnointi on toteutettu automatisoitujen järjestelmien avulla, verkkoliikenteen tapahtumien, lokien ja muutostietojen seuraamisella. CRS sääntöjen avulla poikkeamat kyetään havaitsemaan palomuuri tasolla. Yrityksen sisäverkossa tietoliikennettä valvotaan verkon ensimmäiseen solmuun asennetun IPS järjestelmän avulla.

Salausratkaisut:

2.14 Toimivaltainen viranomainen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. turvallisuusluokalle ko. käyttöympäristössä turvallisuusluokiteltujen tietojen luvattoman paljastumisen ja muuntelun estämiseksi.

Tila: Toteutuu osittain

Lyhyt kuvaus toteutuksesta: Automaattista salausratkaisua ei ole käytössä yrityksen sisäverkossa toimivissa laitteissa. Palvelimella säilytettävät tiedostot sekä asiakastiedot salataan AES-256.

Suositus: Suositellaan turvallisuusluokitellun tiedon salaamista kaikilla laitteilla.

Ohjelmistojen suojaaminen verkkohyökkäyksiltä:

2.15 Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu.

Tila: Ei toteudu
Lyhyt kuvaus toteutuksesta: Turvatoimia ei testata säännöllisesti. Kriittiset ohjelmistot testataan asennukset/käyttöönoton yhteydessä. Ohjelmistojen käyttötarkoitukset tunnistetaan, mutta turvallisuuteen liittyviä riskitekijöitä ei tarkastella erikseen. Käytössä ainoastaan luotettuja sovelluksia, palveluita ja järjestelmiä.

Suositus: Suositellaan tunnistamaan ohjelmistojen riippuvuudet ja rajapinnat, niihin liittyvien haavoittuvuuksien tunnistamiseksi.

2.16 Tietoturvallisuutta vaarantavia verkkohyökkäyksiä vastaan suojaudutaan ja suojauksista sekä niiden toiminnasta huolehditaan tietojenkäsittely-ympäristön elinkaaren ajan.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Palvelinjärjestelmässä on käytössä palomuurilla sekä porttiskannauksia rajoittava OWASP CRS. Tämän lisäksi käytössä on Shell Fork Bomb Protection järjestelmä, joka antaa suojaa hajautettuja palvelunestohyökkäyksiä vastaan. Väsytyshyökkäyksien torjuntaan on käytetty cHulk Brute Force Protectionia. Yrityksen sisäverkon suojaa ylläpidetään IPS järjestelmällä sekä kaksinkertaisella rautatason palomuurilla. Verkko on suojattu DDoS hyökkäyksiltä. Verkkoliikenteen valvonta on automatisoitu ohjelmallisesti. Palvelut, sovellukset ja järjestelmät on sijoitettu suojattuihin ympäristöihin. Lokitetojen perusteella suojausmekanismit kykenevät torjumaan kaikki yleisimmät verkkohyökkäystavat tehokkaasti.

KÄYTTÖTURVALLISUUS

Käyttötavallisuus koostuu yrityksen tietoaineistojen käyttöön sekä hallintaan liittyvistä tietoturvaratkaisuista.

Tiedon sähköinen välitys:

3.1 Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden ulkopuolella, tieto/tietoliikenne salataan toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä turvallisuusluokiteltuja tietoja.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Tiedonsiirto on toteutettu SFTP ja HTTPS tekniikkaa hyödyntämällä. Tietoliikenne salataan TLS/SSL tekniikalla (SSLv2 -SSLv3 -TLSv1 -TLSv1.1). TLS Cipher Suite on käytössä. Sähköpostitse tietoliikenne salataan GnuPG:llä.

3.2 Kun turvallisuusluokiteltua tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella toimivaltaisen viranomaisen erillishyväksyntään perustuen.

Tila: Ei toteudu
Lyhyt kuvaus toteutuksesta: Salausta ei sovelleta sisäiseen tiedonsiirtoon.

Suositus: Yleissuosituksena voidaan pitää salauksen käyttöä turvallisuusluokiteltua materiaalia siirrettäessä.

Muutoshallintamenettelyt:

3.3 Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Havaittuihin muutoksiin pyritään reagoimaan niiden ilmaannuttua. Järjestelmien- ja sovellusten tietoturvallisuutta ja toimintakykyä ylläpidetään säännöllisillä päivityksillä. Tietojenkäsittely-ympäristön kokoonpanosta on ajantasaiset dokumentit.

3.4 Tietoturvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Tietojenkäsittely-ympäristöön kohdistetaan viikoittain arviointi eikä tarkastelutoimenpiteitä. Samalla tarkistetaan manuaalisesti saatavilla olevat päivitykset.

3.5 Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten- ja asetustenhallintaprosessia.

Tila: Ei toteudu
Lyhyt kuvaus toteutuksesta: Turvallisuuteen liittyviä dokumentteja ei ylläpidetä. Dokumentointi on puutteellista.

Suositellaan: Suositellaan tietoturvallisuuteen liittyvien asiakirjojen laatimista ja ylläpitoa.

Etäkäyttö ja etähallinta:

3.6 Käyttäjät ja päätelaitteet tunnistetaan riittävän luotettavasti. Tietojen välitys ja käsittely turvallisuusalueiden välillä on mahdollista vain toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymien korvaavien menettelyjen mukaisesti.

Tila: Ei toteudu
Lyhyt kuvaus toteutuksesta: Erillistä varmennusta ei käytetä. Todennus perustuu käyttäjätunnukseen sekä salasanaan. Palvelinympäristössä ei ole käytössä sellaista päätelaitteita tunnistavia menetelmiä. Yrityksen sisäverkossa laitteistot tunnistetaan, mutta yhteydenluotia ei estetä automaattisesti ACL:llä. Toiminta perustuu manuaalisesti tehtävään estämiseen.

Suositus: Laitteiston tunnistaminen ja pääsynvalvonnan käyttöönotto.

3.7 Turvallisuusluokiteltuja tietoja on turvallisuusalueiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Turvallisuusluokiteltua tietoa ei käsitellä turvallisuusalueiden ulkopuolella. Henkilöstö on saanut perehdytyksen etätyöskentelyyn.

3.8 Elleivät turvallisuusalueiden ulkopuolelle viedyt turvallisuusluokiteltua tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu toimivaltaisen viranomaisen ko. turvallisuusluokalle hyväksymällä menetelmällä, tietovälineitä ei jätetä valvomatta.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Turvallisuusluokiteltua tietoa ei viedä turvallisuusalueen ulkopuolelle.

3.9 Järjestelmien etäkäyttö ja -hallinta edellyttää toimivaltaisen viranomaisen ko. turvallisuusluokan tietojen suojaamiseen hyväksymää liikenteen salausta.

Tila: Toteutuu osittain
Lyhyt kuvaus toteutuksesta: Etähallinta toteutetaan palvelimen suuntaan SSH tekniikkaa hyödyntäen. Yrityksen sisäverkkoon ei lähtökohtaisesti käytetä etähallintaa, muutoin kuin huoltotarkoituksissa. Tällöin liikenne suojataan TLS 1.2 sertifikaatilla.

Suositus: Suositellaan IPSec-VPN tai TLS-VPN käyttöä tietoliikenteen salaamiseen.

3.10 Päätelaitteessa olevat tiedot tulee olla suojattu kyseiselle turvallisuusluokalle riittävän turvallisella, toimivaltaisen viranomaisen hyväksymällä salausratkaisulla, ja päätelaitteen ko. turvallisuusluokalle riittävästä eheydestä tulee huolehtia.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Turvallisuusluokiteltua tietoja ja tiedostoja säilytetään asianmukaisesti. Varmuuskopiot otetaan äännöllisesti.

3.11 Turvallisuusluokiteltuja tietoja ei avata matkalla eikä lueta julkisilla paikoilla.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Noudatetaan yleisiä tietoturvakäytäntöjä.

Ohjelmistohaavoittuvuuksien hallinta:

3.12 Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Ohjelmistojen säännöllinen päivitys. Ohjelmisto/lisenssit uusitaan/vaihdetaan ennen versiotuen päättymistä. Käytetään ainoastaan luotettavien ohjelmistokehittäjien tuotteita. Sertifikaatit uusitaan määräajan välein.

Varmuuskopiointi:

3.13 Turvallisuusluokiteltua tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto on suojattu.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Varmuuskopiot otetaan automaattisesti ennalta määrättyinä ajankohtina. Taajuus on riittävä. Varmuuskopiot siirretään fyysisesti eri tilaan muusta ympäristöstä. Palautusprosessin nopeutta voidaan pitää riittävänä. Varmuuskopioinnin toimivuutta ei testata säännöllisesti. Dokumentointi on riittävää. Erottelumenettelyt on toteutettu järjestelmän sallimalla tavalla.

- Varmuuskopiointi otetaan 3 x viikossa.
- Päivittäinen SnapShot.
- Järjestelmän täysi varmuuskopiointi 1 x viikossa + joka kuun ensimmäinen päivä.
- SQL-tietokantojen kopiointi tilikohtaisesti

Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen:

3.14 Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen on järjestetty luotettavasti. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.

Tila: Toteutuu
Lyhyt kuvaus toteutuksesta: Toteutettu asianmukaisesti ja hallitusti.

AUDITOINNIN YHTEYDESSÄ HAVAITUT UHAT

Tietoturva-auditoinnin aikana havaittiin useita yrityksen verkkopalvelimeen kohdistuvia uhkia, joista osa ilmenee päivittäistasolla. Havainnot on tehty tarkastelemalla palvelimen lokitietoja sekä tutkimalla yrityksen turvallisuudesta vastaavalta toimitusjohtajalta saatuja hälytysilmoituksia. Yrityksen tietojenkäsittely-ympäristöön kohdistuvia suoria uhkia ei havaittu. Tästä johtuen erittelemme ainoastaan palvelinympäristöön kohdistuvat todetut uhat.

- Palvelimen cHulk Brute Force Protection oli havainnut auditointia edeltäneiden viimeisten 3600 minuutin aikana 199 epäonnistunutta kirjautumisyritystä. Yritykset viittaavat väsytyshyökkäyksellä (Brute Force) tehtyihin kirjautumisyrityksiin. Väsytyshyökkäyksessä hyökkääjä yrittää päästä murtautumaan järjestelmään sisälle kokeilemalla useita tunnus- ja salasanapareja oikean yhdistelmän löytämiseksi. Alla lyhyt otanta kirjautumisiin liittyvistä epäonnistumisista ja niiden IP-osoitteista.

34.140.248.32	BE
103.15.74.235	IN
178.32.197.86	FR
130.211.54.158	BE
23.224.186.219	US
182.77.56.193	IN
201.91.226.38	BR
217.72.125.206	GB
125.21.161.102	IN
195.133.156.187	IL

Kuva 1. Otanta havaituista IP-osoitteista.

- Palomuuri estää ja raportoi säännöllisesti useista peräkkäin tehtyjä SYN-skannauksia, joista jäljet (IP-osoitteet) vievät ulkomailla toimivien operaattorien tai palvelimien osoiteavaruuteen. Porttiskannauksien avulla hyökkääjät yrittävät selvittää tietojärjestelmien tietoliikenneporteissa toimivia järjestelmiä, ohjelmia, palveluita ja niihin liittyviä haavoittuvuuksia tai vaihtoehtoisesti kuormittaa palvelinta. Hälytyksen tiedot viittaavat SYN Flood hyökkäykseen (DoS), jonka tarkoituksena on ollut kuormittaa palvelinta ja estää sen toiminta. Alla lyhyt osa palomuurin antamasta hälytyksestä tapaukseen liittyen:

  Time: Thu May 5 22:35:55 2022 +0300
  IP: 175.163.72.101 (CN/China/-)
  Hits: 11
  Blocked: Temporary Block for 3600 seconds [PS_LIMIT]

  Sample of block hits:
  May 5 22:32:29 server kernel: Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=00:50:56:3e:33:1f:28:99:3a:4d:30:af:08:00 SRC=175.163.72.101 DST=167.86.86.242 LEN=52 TOS=0x00 PREC=0x00 TTL=115 ID=20463 DF PROTO=TCP SPT=45845 DPT=1420 WINDOW=8192 RES=0x00 SYN URGP=0 May 5 22:32:32 server kernel: Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=00:50:56:3e:33:1f:28:99:3a:4d:30:af:08:00 SRC=175.163.72.101 DST=167.86.86.242 LEN=52 TOS=0x00 PREC=0x00 TTL=115 ID=24814 DF PROTO=TCP SPT=45845 DPT=1420 WINDOW=8192 RES=0x00 SYN URGP=0 May 5 22:32:38 server kernel: Firewall: *TCP_IN Blocked* IN=eth0 OUT= MAC=00:50:56:3e:33:1f:28:99:3a:4d:30:af:08:00 SRC=175.163.72.101……..

- OWASP ModSecurity Core Rule Set (CRS) WAF-palomuurin säännöt tunnistavat ja estävät satunnaisia Path Traversal Attack hyökkäys yrityksiä. Path Traversal Attack hyökkäyksessä hyökkääjä pyrkii pääsemään käsiksi verkkopalvelimella oleviin tiedostoihin ja hakemistoihin manipuloimalla muuttujia. Alla esimerkki suojausmekanismien tekemästä tuoreesta havainnosta:

  Time: Wed May 4 21:53:23 2022 +0300
  IP: 37.115.205.176 (UA/Ukraine/37-115-205-176.broadband.kyivstar.net)
  Failures: 5 (mod_security)
  Interval: 3600 seconds
  Blocked: Permanent Block [LF_MODSEC]

  Log entries:
  [Wed May 04 21:53:19.979829 2022] [error] [client 37.115.205.176] ModSecurity: Access denied with code 200, [Rule: 'REQUEST_URI_RAW|ARGS|REQUEST_HEADERS|!REQUEST_HEADERS:Referer|XML:/*' '@rx (?i)(?:\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0% 25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8%8)?0%8|e)0%80%a|bg%q)f|%3(?:2(?:% 25af|(?:%

- WAF palomuurin CRS säännöt mahdollistavat myös Restricted File Access Attempt ja Web Application Attacks kategoriaan kuuluvat tunkeutumisyritykset. Alla kaksi toteutunutta hyökkäys yritystä:

  Time: Wed May 4 19:37:24 2022 +0300
  IP: 193.56.252.245 (RO/Romania/-)
  Failures: 5 (mod_security)
  Interval: 3600 seconds
  Blocked: Permanent Block [LF_MODSEC]

  Log entries:
  [Wed May 04 19:37:16.470276 2022] [error] [client 193.56.252.245]
  ModSecurity: Access denied with code 200, [Rule: 'REQUEST_HEADERS:Host' '@rx
  ^[\d.:]+$'] [id "920350"] [msg "Host header is a numeric IP address"] [logdata
  "167.86.86.242"] [severity "WARNING"] [tag "application-multi"] [tag "language-multi"] [tag
  "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
  "capec/1000/210/272"] [tag "PCI/6.5.10"] [hostname "167.86.86.242"] [uri "/.env"] [Wed
  May 04 19:37:16.470849 2022] [error] [client 193.56.252.245]

  ModSecurity: Access denied with code 200, [Rule: 'REQUEST_FILENAME'
  '@pmFromFile restricted-files.data'] [id "930130"] [msg "Restricted File Access Attempt"]
  [logdata "Matched Data: /.env found within /.env: /.env"] [severity "CRITICAL"] [tag "ap-
  plication-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-lfi"] [tag "para-
  noia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/255/153/126"] [tag "PCI/6.5.4"] [host-
  name "167.86.86.242"] [uri "/.env"] [Wed May 04 19:37:16.470980 2022] [error] [client
  193.56.252.245]
  ModSecurity: Access denied with code 403, [Rule: 'TX:ANOMALY_SCORE' '@ge %{tx.in-
  bound_anomaly_score_threshold}'] [id "949110"] [msg "Inbound Anomaly Score Exceeded
  (Total Score: 8)"] [severity "CRITICAL"] [tag "application-multi"] [tag "language-multi"] [tag
  "platform-multi"] [tag "attack-generic"] [hostname "167.86.86.242"] [uri "/.env"] [Wed May
  04 19:37:17.888630 2022] [error] [client 193.56.252.245]

- Alla esimerkkejä kohdepalvelimen palomuurin tallentamista lokitiedoista ja havaituista hyökkäyksistä:

PHP INJECTION:
server.selecore.com 185.253.97.244 CRITICAL 933120:
PHP Injection Attack: Configuration Directive Found
Request: POST /?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Action Description: Access denitaed with code 200 (phase 2).
Justification: Test 'MATCHED_VARS' against '@pm =' is true.

911100: Method is not allowed by policy More
913100: Found User-Agent associated with security scanner More
949110: Inbound Anomaly Score Exceeded (Total Score: 10) More
913100: Found User-Agent associated with security scanner More
920340: Request Containing Content, but Missing Content-Type header More
933120: PHP Injection Attack: Configuration Directive Found More
933140: PHP Injection Attack: I/O Stream Found More
949110: Inbound Anomaly Score Exceeded (Total Score: 17) More
913100: Found User-Agent associated with security scanner More

Liite 2: Penetraatiotestaus

Asiakirjan sisältö: Tutkimuksen kohteena oli Selecore Oy:n vuonna 2019 käyttöönottama palvelinjärjestelmä, jonka avulla yritys tuottaa palveluita asiakkailleen. Tämä raportti sisältää keskeiset tiedot yritykseen suoritetusta penetraatiotestauksesta ja on osa opinnäytetyötä.

Toimeksiantaja: Selecore Oy

Testaaja: Joonas Muhonen

Päivämäärä: 24.2.202

Verkkopalvelimen tekniset tiedot

CPU: Intel Xeon Silver 4114
- Ydin: Skylake Lake, 10 ydintä
- Säikeiden lukumäärä: 20
- Kellotaajuus (base): 2,2 GHz
- Kellotaajuus (turbo): 3,0 GHz
- Cache: 16 MB L3 Cache

GPU: Integroitu

Emolevy: FCLGA3647
- Piirisarja: Intel C621
- IGPU

Keskusmuisti: 60Gt
- DDR4
- ECC RAM (Pariteetti)
- 2400 MHz

Muisti: SSD 1,6Tb

Verkko: Valokuitu (Erillisverkko)

Käyttöjärjestelmä: CentOS (Community Enterprise Operating System)
- versio: v7.9.2009

Hallinta: cPanel & WHM
- versio: 102.0.11

Palvelinmalli

Palvelin toimii yhteisöpilvipalvelu (community cloud) periaatteella, joka on jaettu useammalle käyttäjäryhmälle. Palvelinympäristö on toteutettu multitenant arkkitehtuurilla eli yhdellä palvelinlaitteistolla voidaan hallita ja suorittaa useiden käyttäjien palveluita samanaikaisesti. Palvelimelle pääsy edellyttää käyttäjältä internetyhteyttä sekä päätelaitetta. Käyttäjän ja palvelimen välinen liikenne on salattu SSH:lla.

Yleistietoa testauksesta

Penetraatiotestauksen toteuttamisesta sovittiin toimeksiantajan kanssa erikseen käydyissä palavereissa, jolloin laadittiin testaussuunnitelma. Suunnitelman tarkoituksena oli antaa selkeät raamit testauksen eri vaiheille ja ohjata testauksen suorittamista. Testauksen avulla haluttiin teknisesti todentaa tietoturva-auditoinnissa havaittujen uhkien mahdollisuus läpäistä järjestelmän suojaustasot sekä tunnistaa sellaisia haavoittuvuuksia, joita ei auditoinnin aikana tunnistettu.

Testauksen kohde rajattiin asiakkaan toiveiden mukaisesti kohdistumaan verkkopalvelimen IP-osoitteeseen sekä yhteen palvelimella toimivaan sivustoon. Asiakkaan toiveena oli selvittää, että löytyykö kyseisestä kohteesta haavoittuvuuksia, joiden kautta yrityksen toiminta voi vaarantua. Lisäksi sovittiin, ettei testausta toteuta sellaisia menetelmiä käyttäen, joista voi aiheutua vaaraa tai vahinkoa palvelimen, ohjelmien tai sivustojen toimivuudelle.

Testaus toteutettiin niin sanottua ”graybox” menetelmää käyttäen, jossa testaajalla oli käytössään rajoitettu määrä ennakkotietoa testattavasta tietojärjestelmästä, sovelluksesta, verkosta ja tunnistautumistekniikoista. Tämän avulla voidaan ohittaa testaukseen alkupään vaiheita, jotka liittyvät kohteen tunnistamiseen. Tietoturvasyistä osa palvelimen tunnistetiedoista on peitetty.

Testauksessa käytetyt työkalut

VirtualBox:
VirtualBox on käyttöjärjestelmien virtualisointiin tarkoitettu ohjelma.

Windows 10 Sandbox:
Windows Sandbox on virtuaalikone, jota voidaan käyttää erilaisten ohjelmien sekä järjestelmien testaamiseen.

Kali Linux:
Kali Linux on Linux distribuutio, joka on suunniteltu käytettäviksi erilaisissa tietoturvatehtävissä, ja se soveltuu käytettäväksi tietoteknisessä rikostutkinnassa, penetraatiotestauksessa ja tietoturva-auditoinnissa.

VPN:
Virtual private network, joka luo suojatun ja salatun yhteyden asiakkaiden välille.

Nmap:

Nmap (Network Mapper) on verkon rakenteiden sekä laitteiden tutkimiseen käytetty ohjelma. Ohjelmaa voidaan käyttää suorittamaan porttiskannauksia, käytössä olevien palvelujen, käyttöjärjestelmien ja niiden versioiden tunnistamiseen.

Zenmap:

Zenmap on graafinen versio portti- ja haavoittuvuusskannauksien soveltuvasta Nmapista.

Vega:

Vega on haavoittuvuusskanneri ja penetraatiotestaukseen käytetty ohjelma. Se avulla voidaan havaita verkkosovelluksissa ja järjestelmissä olevia haavoittuvuuksia sekä suorittaa murtotestausta.

OWASP ZAP:

OWASP ZAP on verkkosovellusten haavoittuvuusien ja suojauksien tarkistamiseen käytetty ohjelma. Ohjelma soveltuu myös penetraatiotestaukseen.

Tiedustelu 1

Testauksessa hyödynnettiin aktiivisen tiedonkeruun menetelmiä, johon kuului automaattiset sekä manuaaliset skannausmenetelmät. Työn toimeksiantaja sai reaaliaikaisesti tietoa testauksen etenemisestä sekä työn eri vaiheista. Tiedusteluvaiheessa kerättyä tietoa käytettiin mahdollisten hyökkäysvektorien tunnistamisessa.

Tiedustelu toteutettiin skannaamalla ja etsimällä kohdepalvelimen avoimia portteja Nmap ohjelmalla komennoilla:

Nmap -p 22,23,53,80 167.86.86.242 (skannaa portit 22, 23, 53 ja 80).

Nmap -p0-, (skannaa kaikki 65535 porttia).

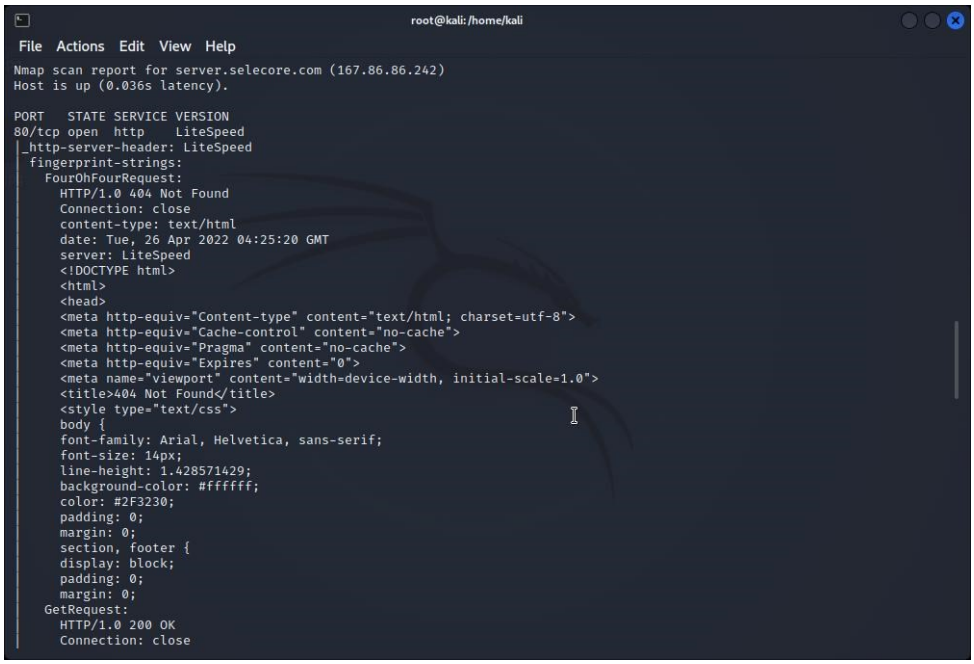
Skannaukset keskeytyivät odottamattomista syistä, eikä luotettavia tuloksia saatu avoimista porteista. Palvelimen palomuurin lokitiedoista ilmeni, että skannausta suorittavan laitteen IP-osoite oli estetty. Tiedustelua jatkettiin Banner grabbing eli ”bannerin kaappaus” -yrityksellä, jonka avulla pyrittiin keräämään tietoa palvelimen osoitteista, tunnistetiedoista, avoimista porteista, käytössä olevista sovelluksista sekä niiden versiotiedoista. Banner grabbing toteutettiin testilaitteella olevan Kali Linux -distribuution Nmap sovellusta käyttäen.

Tiedonkeruussa käytetyt Nmap komennot:

Nmap -sS -p 80 -A 167.86.86.242

Yllä olevien komentojen tarkoitukset:
-sS = SYN-skannaus
-p = portin numero
-A = aggressiivinen skannaus

Ensimmäisen tiedonkeruuvaiheen tuloksena ei löytynyt avoimia suojaamattomia portteja, eikä merkittäviä tietoja, jotka voisivat johtaa haavoittuvuuksien havaitsemiseen. Alla testaajan ottamat kuvankaappaukset tuloksista:



Kuva 1: Nmap Banner Grapping skannauksen tuloksista.

Tiedustelu 2

Porttiskannaus uusittiin käyttämällä Zenmap ohjelman Stealth (SYN-skannaus) ominaisuutta, joka etsii avoimia portteja siten, ettei palomuuri havaitse skannausta. SYN-skannaus on huomaamaton sillä se ei suorita TCP-yhteyksien viimeistelyä. Sen avulla tunnistettiin useita tavanomaisia, auki olevia portteja sekä niissä toimivia palveluita.

Komento: nmap -p 65535 -T4 -A -v 167.86.86.242

Skannauksen tulokset:
Initiating SYN Stealth Scan at 09:15
Scanning server.selecore.com (167.86.86.242) [65535 ports]
Discovered open port 143/tcp on 167.86.86.242
Discovered open port 110/tcp on 167.86.86.242
Discovered open port 53/tcp on 167.86.86.242
Discovered open port 80/tcp on 167.86.86.242
Discovered open port 995/tcp on 167.86.86.242
Discovered open port 587/tcp on 167.86.86.242
Discovered open port 21/tcp on 167.86.86.242
Discovered open port 25/tcp on 167.86.86.242
Discovered open port 993/tcp on 167.86.86.242
Discovered open port 443/tcp on 167.86.86.242
SYN Stealth Scan Timing: About 8.82% done; ETC: 09:21 (0:05:20 remaining)

Porttien kautta toimivat palvelut voitiin varmistaa Zenmapilla suoritettavan TOP ports -skannauksen avulla.

Komennolla: nmap –top-ports

Tulokset:

PORT	**STATE**	**SERVICE**
21/tcp	open	ftp
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
143/tcp	open	imap
443/tcp	open	https
993/tcp	open	imaps
995/tcp	open	pop3s

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds

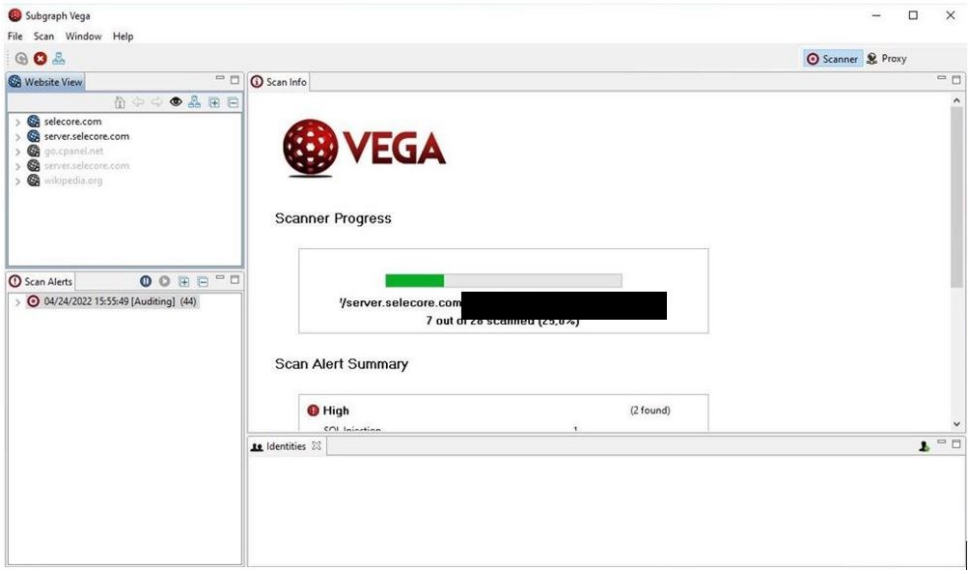
Haavoittuvuuksien tunnistaminen

Haavoittuvuuksia voidaan tunnistaa skannaamalla ennalta määritetty kohde siihen soveltuvalla ohjelmalla. Tällöin on mahdollista paikantaa laitteissa, järjestelmissä sekä sovelluksissa olevia avoimia portteja sekä haavoittuvuuksia. Haavoittuvuusskannerit suorittavat erilaisia ennalta määriteltyjä testejä, joiden avulla ohjelma voi antaa tarkkoja tai epätarkkoja tuloksia. Ne voivat myös olla aiheellisia tai aiheettomia hälytyksiä. Tällaiset ovat väärät positiiviset (false positive) ja/tai väärät negatiiviset (false negative) tuloksia. Siksi tulokset pitää aina tarkistaa tapauskohtaisesti ja arvioida niiden vaikutukset.

Haavoittuvuuksien skannaus suoritettiin Vega ohjelmalla kahdessa eri vaiheessa kohdepalvelimen IP-osoitteeseen.

Skannauksessa käytettiin seuraavia komponentteja:

Injektio moduulit:	**Käsittely moduulit**
Bash Enviroment variable blind OS injection	HTTP authentication over uncryption
XSS injection checks	HTTP header check
Remote file checks	RSS/Atom/OPL feed detector
Local file checks	Ajax detector
Cross Domain policy auditor	Insecure cross-domain policy
Shell injection checks	Internal IP addresses
Eval code injection	Insecure script
HTTP trace probes	Meta tag detection
Blind SQL text injection checks	Source code disclosure
URL injection checks	Error page detection
XML injection checks	Cookie scope detection



Kuva 2: Vega haavoittuvuus skannaus.

Testi toteutettiin kahteen kertaan tulosten luotettavuuden todentamiseksi. Molemmat skannaukset kuitenkin keskeytyivät kohdepalvelimen palomuurin tunnistettua tapahtuvat hyökkäykset ja estäen lähde IP-osoitteen. Keskeytyksistä huolimatta Vegalla saatiin osittaisia tuloksia molemmista skannauksista. Tulokset toistuivat yhteneväisesti.

Vegan havaitsemat uhat, jotka luokiteltu alla tapauskohtaisesti:

Haavoittuvuus	**Vakavuus**	**Määrä**
SQL Injection	Merkittävä	1
Shell Injection	Merkittävä	1
Integer Overflow	Merkittävä	3
Possible HTTP PUT File upload	Kohtalainen	2
Form password field with autocomplete enabled	Vähäinen	1
Possible XSS injection	Vähäinen	1
Possible AJAX code detected	Huomion arvoista	12
Meta tags detected	Huomion arvoista	14
Cookie secure flag not set	Huomion arvoista	2
Coocie HTTPOnly Flag not set	Huomion arvoista	1
X-Frame-Option Header not set	Huomion arvoista	19

Selvitys merkittävistä ja kohtalaisista uhista:

Mahdollinen sokea SQL injektio haavoittuvuus havaittu seuraavasti:

Classification Input Validation Error
Resource https://server.selecore.com/javascript:void(0)
Parameter locale
Method GET
Detection Type Blind Text Injection Differential
Risk High

REQUEST

GET /javascript:void(0)?locale="%20AND%201=2%20--%20

RESOURCE CONTENT

```
<!DOCTYPE html>
<html lang="ar" dir="rtl">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">
    <meta name="google" content="notranslate" />
    <meta name="apple-itunes-app" content="app-id=1188352635" />
    <title>إلى الدخول تسجيل WHM</title>
    <link ...
```

Kuva 3: SQL-Injection havainto.

SQL tietokantoihin liittyvää haavoittuvuutta voidaan hyödyntää, kun haitallista syötettä käytetään SQL kyselyn tekemiseen. Tämä voi mahdollistaa tietokannassa olevien tietojen luvattoman lukemisen sekä muokkaamisen.

Mahdollinen Shell injektio haavoittuvuus havaittu seuraavasti:

Classification Information Resource /javascript:void(0) Parameter locale Method GET Risk High

REQUEST

GET /javascript:void(0)?locale=ar"`true`"

Kuva 4: Shell Injection havainto.

Shell injektioon liittyviä haavoittuvuuksia voidaan hyödyntää syöttämällä haitallisia tietoja järjestelmän kuoreen (system shell) haavoittuvien web-applikaatioiden kautta. Shell injektio voivat toteutuessaan mahdollistaa järjestelmän etähallinnan.

Mahdollinen Integer Overflow haavoittuvuus havaittu seuraavasti:

Classification Boundary Condition Error Resource /javascript:void(0)?locale=2147483647 Parameter locale Method GET Risk High

Integer overflow eli kokonaislukujen ylivuoto tapahtuu, kun kokonaislukutietotyypit ylittävät enimmäisarvon. Tämä tapahtuu ohjelmissa, jotka on kirjoitettu oliopohjaisella kielellä esim. C:llä. Haavoittuvuus voi aiheuttaa puskurin ylivuodon, jonka seurauksena arvokasta tietoa voi päätyä ulkopuolisten haltuun.

Mahdollinen HTTP PUT haavoittuvuus havaittu seuraavasti:

Classification Configuration Resource https://server.selecore.com/PUT-putfile Method PUT Risk Medium

HTTP PUT tarkoituksena on mahdollistaa http client (asiakkaan) resurssien tallentamisen http palvelimelle. Menetelmää voidaan hyödyntää hyökkäyksen toteuttamiseen tallentamalla sopimattomia tiedostoja verkkosivujen juuri tiedostoihin. Tämä voi mahdollistaa avoimen yhteyden luomisen palvelimeen ja sen sovellusten hallinnan.

Brute Force

BruteForce eli väsytyshyökkäys on tyypillinen hyökkäystekniikka, joka perustuu heikkojen tunnistautumistietojen hyväksikäyttöön. Kyseistä hyökkäystä päätettiin kokeilla avoimena olevaan FTP-porttiin: 21. Hyökkäyksen suorittamisessa hyödynnettiin käyttäjänimen ja salasanan osalta julkisesti saatavilla olevia listoja:

- username.txt koostuu 86771 eri käyttäjätunnus variaatiosta.
- rockyou.txt koostuu 14341564 erilaiseen salasanaan.

Hyökkäys suoritettiin komennolla: nmap --script ftp-brute -p 21 167.86.86.242 --script-args userdb=username.txt,passdb=rockyou.txt

Tulos:
Starting Nmap 7.92 (https://nmap.org) at 2022-04-24 12:21 Finnish summer time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.08 seconds

Hyökkäys estyi odotetulla tavalla, sillä tietoturva-auditoinnin yhteydessä ilmeni, että palvelimessa on käytössä Brute Force Protection -ominaisuus, joka havaitsee tämäntyyppiset hyökkäysyritykset ja estää lähde IP-osoitteesta tulevat syötöt.

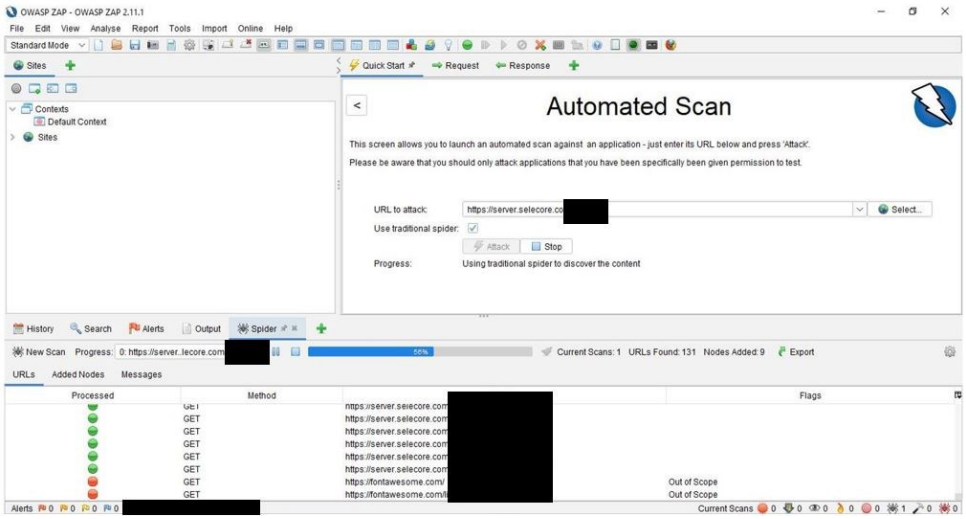
Denial of service

Palvelunestohyökkäyksellä pyrittiin testaamaan palvelimen kykyä kestää rasitusta. Testaus toteutettiin Slowloris hyökkäyksellä käyttäen Zenmappia. Slowloris hyökkäyksessä lähetetään hitaasti HTTP GET pyyntöjä verkkopalvelimeen tarkoituksenaan ruuhkauttaa ja hidastaa sen toimintaa. Kohde palvelimen DDoS-Guard tunnisti hyökkäyksen välittömästi ja esti sen etenemisen.

Komento: nmap 167.86.86.242 -max-parallelism 800 -Pn --script http-slowloris --script-args http-slowloris.runforever=true

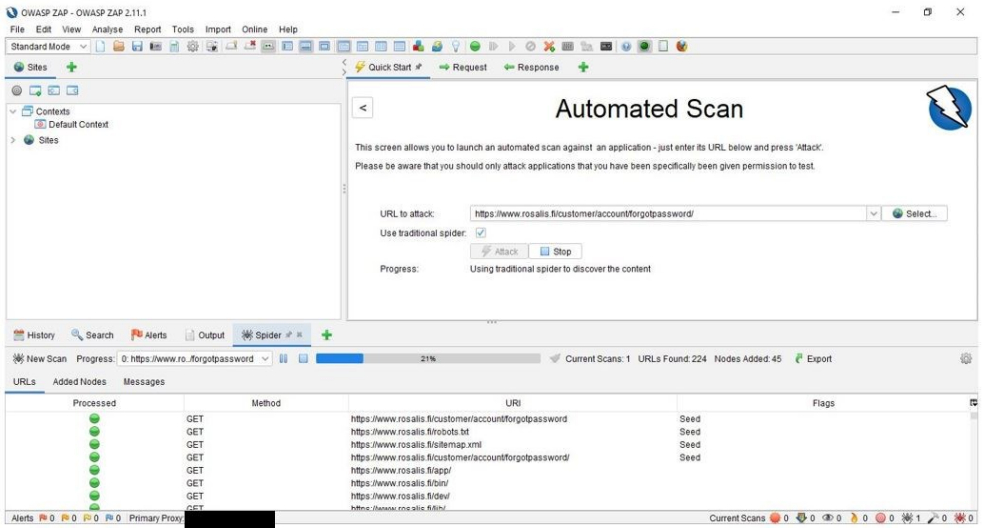
OWASP ZAP

Viimeisessä testausvaiheessa suoritettiin automatisoitu hyökkäys palvelimen verkkosovelluksia kohtaan OWASP ZAP ohjelmalla. Testauksella pyrittiin varmentamaan Vegalla tehtyjä löydöksiä mm. SQL Injection ja Cross-Site Scripting osalta. Hyökkäys toteutettiin ns. aggressiivisessa tilassa käyttäen Spider -ominaisuutta, joka etsii kohdesivustoon liittyviä URL-osoitteita ja tutkii niiden rakenteita.



Kuva 5: OWASP ZAP.

Prosessi keskeytyi samalla tavalla kuin aikaisemmissakin testeissä ja testauslaitteen IP-osoite estettiin kohdepalvelimella. Testaus uusittiin kohdistaen hyökkäys kohdepalvelimella toimivan verkkokaupan osoitteeseen: https://www.rosalis.fi. Hyökkäyksessä hyödynnettiin useita SQL syötteitä, joiden osalta testaus estyi lähes välittömästi palvelimen tekemään estoon.



Kuva 6: OWASP ZAP.

Testin jälkeen tarkasteltiin palvelimen palomuurin lokitietoja, joista ilmeni järjestelmän tekemät havainnot suoritetusta hyökkäyksestä. Alla lyhyt kooste lokitetuista tapahtumista:

2022-04-24 10:15:14 www.rosalis.fi 176.125.229.133
CRITICAL 930130: Restricted File Access Attempt More

2022-04-24 10:15:14 www.rosalis.fi 176.125.229.133
CRITICAL 949110: Inbound Anomaly Score Exceeded (Total Score: 5) More

2022-04-24 10:15:13 www.rosalis.fi 176.125.229.133
CRITICAL 930130: Restricted File Access Attempt More

2022-04-24 10:15:13 www.rosalis.fi 176.125.229.133
CRITICAL 949110: Inbound Anomaly Score Exceeded (Total Score: 5) More

2022-04-24 10:15:12 www.rosalis.fi 176.125.229.133
CRITICAL 930130: Restricted File Access Attempt More

2022-04-24 10:15:12 www.rosalis.fi 176.125.229.133
CRITICAL 949110: Inbound Anomaly Score Exceeded (Total Score: 5) More

2022-04-24 10:15:12 www.rosalis.fi 176.125.229.133
CRITICAL 930130: Restricted File Access Attempt More

2022-04-24 10:15:12 www.rosalis.fi 176.125.229.133
CRITICAL 949110: Inbound Anomaly Score Exceeded (Total Score: 5) More

OWASP ZAP tehtyjen testien perusteella ei saatu varmennettua aikaisemmin Vegalla tehtyjä havaintoja injektioluokan ja kokonaislukujen ylivuotoon liittyvistä mahdollisista haavoittuvuuksista. Näin olen Vegan tuloksia voidaan pitää ainoastaan suuntaa antavina. Erityisesti SQL-injektioniin ja Cross-Site Scriptingiin liittyvät haavoittuvuudet tulisi tarkistaa ja varmentaa erillisillä testeillä.