PHYSIO-CYBERSECURITY

Kyberturvallisuuden suunnittelu, toteuttaminen ja ylläpitäminen

Johanna Hakonen

27.3.2025

Sisällysluettelo

1 Yleistä

Projektin aihe on kyberturvan suunnittelu ja toteuttaminen fiktiiviselle asiakasyritykselle fysioterapiakeskus Physiolle. Yrityksen hoitohenkilökunnan määrä on viisi ja tietohallinnosta vastaa yksi henkilö. IT-ympäristö sisältää Windows-palvelimen ja -työasemia, Active Directoryn ja lähiverkon. Yrityksellä on Physio-verkkosivut ajanvarausta varten ja niiden haavoittuvuudet tutkitaan. Yrityksessä käsitellään asiakastietoja, mikä vaatii kyberturvaan liittyvien lakien selvittämistä ja opastamista.

2 Määrittely

2.1 Asiakasvaatimukset

Kyberuhkien hallinta- ja suojautumiskeinoja käytetään suojaamalla laitteita päivityksillä ja ohjelmistoilla, hallitsemalla työasemia hallintatyökaluilla sekä vertailemalla eri salausmenetelmiä ja valitsemalla tarkoituksenmukaiset salausmenetelmät.

Kyberturvariskejä hallitaan valvomalla tietoverkkoa hyödyntämällä erilaisia analysointityökaluja, skannaamalla haavoittuvuuksia tarkastelun kohteena olevasta verkosta ja varmentamalla järjestelmien haavoittuvuuksia. Lisäksi tehdään kehittämisehdotuksia kyberturvan parantamiseksi.

Kyberturvallisuusratkaisuja edistetään selvittämällä tietoturvaan ja tietosuojaan liittyvät lait, asetukset ja muut viranomaismääräykset sekä havainnollistamalla kyberuhkia ja niitä vastaavia riskejä. Työtehtävissä noudatetaan tietoturvaohjeita. Lisäksi opastetaan työntekijöitä kyberturva- tai tietosuoja-asioissa.

2.2 Ratkaisuvaihtoehdot, ympäristöt ja työvälineet

Työssä voidaan simuloida IT-ympäristöä virtuaalikoneilla VMwaressa Windows-palvelimella ja -työasemilla sekä skannata haavoittuvuuksia Kali Linux-koneella. Lisäksi voidaan käyttää Microsoft Developer E5 testiympäristöä sekä Hack the Box-sivuston ja Testout Security Pro -kurssin tehtäviä.

3 Suunnittelu

3.1 Projektisuunnittelu

3.1.1 Aikataulu

Projektityö toteutetaan 20.1.–28.3.2025 Kuva 1 mukaisella aikataululla.

Tehtävä	Vko 2	Vko 3	Vko 4	Vko 5	Vko 6	Vko 7	Vko 8	Vko 9	Vko 10	Vko 11	Vko 12	Vko 13	Vko 14
Projektin hallinta													
Määrittely ja suunnittelu													
Katselmoinnit													
Näyttö													
Kyberuhkien hallinta- ja suojautumiskeinojen käyttäminen													
Laitteen suojaus päivityksillä ja ohjelmistoilla													
Laitteen hallinta hallintatyökaluilla													
Eri salausmenetelmien vertailu ja tarkoituksenmukaisen salausmenetelmän valinta													
Kyberturvariskien hallinta													
Tietoverkon valvonta hyödyntämällä erilaisia analysointityökaluja													
Haavoittuvuuksien skannaus tarkastelun kohteena olevasta sovitusta verkosta													
Järjestelmien haavoittuvuuksien varmennus													
Kehittämisehdotukset kyberturvan parantamiseksi													
Kyberturvallisuusratkaisujen edistäminen													
Tietoturvaan ja tietosuojaan liittyvien lakien, asetusten sekä muiden viranomaismääräysten tunteminen													
Kyberuhkien ja niitä vastaavien riskien havainnollistaminen													
Tietoturvaohjeiden noudattaminen työtehtävissä													
Kyberturva- tai tietosuoja-asioissa opastaminen													

Kuva 1 Aikataulu.

3.1.2 Dokumenttien hallinta

Dokumentit varmuuskopioidaan OneDriveen ja virtuaalikoneet ulkoiselle kovalevylle.

3.2 Työsuunnitelma

IT-ympäristöä simuloidaan VMwaressa virtuaalikoneilla Windows-palvelimella ja -työasemalla sekä haavoittuvuuksia skannataan Linux-koneella (Kali, Parrot).

Työkaluina käytetään Microsoft Defender-ohjelmaa ja Windows-palvelimen hallintakonsoleita (mm. Active Directory, Group Policyt). Skannauksissa käytetään Wireshark-, Nmap- ja Nessus-ohjelmia. Kokeillaan, huomataanko Nmap-skannaukset Wiresharkilla.

Lisäksi käytetään Hack the Box-sivuston ja Testout Security Pro -kurssin tehtäviä.

3.2.1 Kyberuhkien hallinta- ja suojautumiskeinot

3.2.1.1 Laitteen suojaus päivityksillä ja ohjelmistoilla

Ympäristönä käytetään Windows-työasemaa VMwaressa. Työasema päivitetään Windows-updaten kautta ja konfiguroidaan tarvittaessa. Emolevyn ja oheislaitteiden ajurit sekä UEFI ja laiteohjaimet päivitetään tarvittaessa tuoreemmiksi. Työasemat ja palvelimet suojataan haittaohjelmien torjuntasovelluksilla kuten WithSecure ja Microsoft Defender sekä palomuureilla, jotka konfiguroidaan yrityksen tietoturvakäytänteiden mukaan. Reititin päivitetään.

3.2.1.2 Laitteen hallinta hallintatyökaluilla

Ympäristönä käytetään Windows-palvelinta ja -työasemaa VMwaressa tai Microsoft Developer E5 testiympäristöä. Windows-työasemien, palvelimien ja tarvittaessa mobiililaitteiden tietoturva toteutetaan Microsoft Defenderin, palomuurin ja muiden tietoturva-asetusten avulla. Hallinta voidaan hoitaa pilvipalveluna M365 Admin Centerin, Intunen tai WithSecure Policy Managerin/Elements-palveluiden kautta. Toimialueympäristössä hallintatyökaluina käytetään Windows-palvelimen hallintakonsoleita (Active Directory, Group Policyt), ja Powershellia voidaan käyttää automatisoimaan tehtäviä.

3.2.1.3 Eri salausmenetelmien vertailu ja tarkoituksenmukaisen salausmenetelmän valinta

Asiakasympäristöön kartoitetaan ja suunnitellaan tarvittavat salausmenetelmät. Vaihtoehtoina ovat esimerkiksi työasemien suojaus Bitlockerilla, datan ja muistitikkujen suojaus, tietoliikenteen suojaus (HTTPS, SSL, VPN) ja sähköpostin salaus.

3.2.2 Kyberturvariskien hallinta

3.2.2.1 Tietoverkon valvonta hyödyntämällä erilaisia analysointityökaluja

Ympäristönä käytetään Windows-palvelinta ja -työasemaa, joka on päivitetty viimeksi vuonna 2023, sekä Kali Linux-konetta VMwaressa tai Hack the Box-sivuston tehtäviä. Wiresharkkia hyödynnetään verkon tietoliikenteen analysoinnissa Physio-ajanvaraussovelluksen ollessa käynnissä. Tutkitaan jo tässä kohdassa, havaitaanko Kali Linux-koneella tehtyjä Nmap-skannauksia. Lisäksi voidaan käyttää Microsoftin, Windowsin ja aktiivilaitteiden monitorointi- ja raportointityökaluja.

3.2.2.2 Haavoittuvuuksien skannaus tarkastelun kohteena olevasta sovitusta verkosta

Ympäristönä käytetään Windows-palvelinta ja -työasemaa sekä Kali Linux-konetta VMwaressa tai Parrot Linux-konetta Hack the Box-sivuston tehtävissä. Skannataan Nmapilla mahdollisia avoimia verkkoyhteyksiä. Haavoittuvuuksia etsitään Nessus Essentials ja SQLmapilla.

3.2.2.3 Järjestelmien haavoittuvuuksien varmennus

Analysoidaan haavoittuvuusskannausten tiedot ja raportit ja tehdään tietoturvakartoitus ja -katselmointi.

3.2.2.4 Kehittämisehdotukset kyberturvan parantamiseksi

Suoritetaan kartoitusten ja analyysien pohjalta riskienhallintaa ja listataan tarvittavat toimenpiteet tietoturvan parantamiseksi.

3.2.3 Kyberturvallisuusratkaisujen edistäminen

3.2.3.1 Tietoturvaan ja tietosuojaan liittyvien lakien, asetusten sekä muiden viranomaismääräysten tunteminen

Kartoitetaan muutamilla esimerkeillä asiakasyrityksen toimintaan liittyvät tärkeimmät tietoturvaan ja -suojaan liittyvät lait ja määräykset.

3.2.3.2 Kyberuhkien ja niitä vastaavien riskien havainnollistaminen

Selvitetään ja kuvataan lyhyin esimerkein tämän hetken yleisimmät ja kriittisimmät tietoturvauhat sekä mitä riskejä ne asiakasyrityksessä merkitsevät.

3.2.3.3 Tietoturvaohjeiden noudattaminen työtehtävissä

Toteutetaan lyhyt ja tiivis alustava tietoturvaohjeen asiakasyritykselle.

3.2.3.4 Kyberturva- tai tietosuoja-asioissa opastaminen

Tehdään muutama koulutuscase-esimerkki käytännön työssä huomioitavista kyberturva-asioista yrityksen työntekijöille ja it-asiantuntijoille.

4 Toteutus

4.1 Kyberuhkien hallinta- ja suojautumiskeinot

4.1.1 Laitteen suojaus päivityksillä ja ohjelmistoilla

Ympäristönä käytetään Windows-työasemaa VMwaressa, jonka suojausta käsitellään liitteessä 1 Windows-työaseman suojaus päivityksillä ja ohjelmistoilla. Siellä myös esitellään tarkemmin käytännössä tehdyt päivitysten asennukset sekä verkko- ja tietoturva-asetukset.

Windows-työasema päivitettiin Windows-updaten kautta. Laitehallinnasta tarkistettiin, tarvitseeko jokin laite ajureiden päivitystä ja päivitettiin Tietoliikenneportin (COM1) ajurit etsimällä ohjaimia automaattisesti. Etsittiin uusia versiota laiteohjelmistoista valmistajien sivuilta. Päivitettiin reititin. Varmistettiin, että Windowsin suojaus on ajan tasalla. Otettiin käyttöön Sovellusten ja selainten hallinta. Suoritettiin Virusten ja uhkien torjunta -työkalulla perusteellinen tarkistus. Perehdyttiin Windowsin palomuuriin (Microsoft Learn), tutustuttiin sen asetuksiin ja konfiguroitiin sitä muutaman säännön verran.

4.1.2 Laitteen hallinta hallintatyökaluilla

Windows-työaseman hallintaa toimialueympäristössä toteutettiin Windows-palvelimen hallintakonsoleilla, group policyillä (GPO) ja Powershellillä. Hallintakonsoleista käytettiin seuraavia: Server Manager, ADUC, ADDS, FSRM, DHCP, DNS Manager, Event Viewer, GPMC, Windows Server Backup ja Print Management. GPO:lla toteutettiin esimerkiksi salasanan pituuden määrääminen, työasemien päivittäiset päivitykset ja osastokohtaiset yhteiskansiot. Powershellillä harjoiteltiin tehtävien automatisointia (käyttäjien haku nimen mukaan, tietyn OU:n käyttäjien haku, käyttäjän lisääminen). Laitteen hallintaa käsitellään tarkemmin liitteessä 2 Windows-työaseman hallinta hallintatyökaluilla, jossa esitellään tehdyt toimenpiteet toimialueympäristössä.

4.1.3 Eri salausmenetelmien vertailu ja tarkoituksenmukaisen salausmenetelmän valinta

Vertailtiin eri salausmenetelmiä sekä kartoitettiin ja suunniteltiin asiakasympäristöön tarvittavat salausmenetelmät (liite 3): työasemien suojaus Bitlocker, ajanvaraussivujen tietoliikenteen suojaus HTTPS/TLS, asiakastietojen etäkäsittely VPN, sähköpostin salaus S/MIME, salasanojen suojaus Bitwarden ja hajautus Node.js:n bcrypt-kirjastolla, MFA Windows Hello.

Case-esimerkkinä suunniteltiin ja aloitettiin Bitlockerin käyttöönottoa GPO:na, mutta se jäi kesken ajanpuutteen vuoksi.

Erillisenä käytännön esimerkkinä tehtiin Testout Security Pro -kurssin OpenStego-salaus.

4.2 Kyberturvariskien hallinta

Kyberturvariskejä hallitaan esimerkiksi valvomalla tietoverkkoa ja skannaamalla haavoittuvuuksia erilaisilla ohjelmilla. Projektissa yhdistettiin nämä havainnoimalla Nmap-skannauksia Wiresharkilla (Wireshark Foundation, 2025). Tehtiin kevyt verkonvalvontasuunnitelma (liite 4a), josta tehdyt osat on esitelty alla. Ympäristönä käytettiin Windows-palvelinta ja viimeksi vuonna 2023 päivitettyä työasemaa (wks2) sekä Kali ja Parrot Linux-koneet VMwaressa. Käynnistettiin Physio-ajanvaraussovellus (Github, 2025) työasemassa ja tutkittiin sen liikennettä ja haavoittuvuuksia.

4.2.1 Tietoverkon valvonta hyödyntämällä erilaisia analysointityökaluja

Verkonvalvontasuunnitelmasta toteutettiin työaseman (liite 4b) ja siinä pyörivän oman Physio-websovelluksen (Github, 2025) (liite 4c) verkkoliikenteen analysointi Wiresharkilla. Tehtiin samalla skannauksia Kali Linux-koneen Nmapilla (Hack the Box, 2025) työasemaan. Versioskannauksen tulos on esitetty kokonaisuudessaan liitteessä 4d. Nmap-skannaukset ja esimerkiksi Physio-websovelluksen tietokantayhteydet MongoDB Atlas-palveluun havaittiin Wiresharkilla.

Lisäksi kirjautumisyrityksiä tarkasteltiin jo Laitteen hallinta hallintatyökaluilla -kohdan liitteessä 2 muokkaamalla Default Domain Conrollers Policy GPO:ta toteuttamaan sekä onnistuneiden että epäonnistuneiden toimialueelle kirjautumisten tarkistus sekä tarkastelemalla kirjautumisia Server Managerin Event Viewer -konsolissa (Windows Logs > Security). Epäonnistuneet kirjautumiset näkyivät Audit failurena: Event ID:llä 4771 Kerberos Authentication Service: Kerberos pre-authentication failed.

4.2.2 Haavoittuvuuksien skannaus tarkastelun kohteena olevasta sovitusta verkosta

Kali Linux-koneen Nmapilla skannattiin mahdollisia avoimia verkkoyhteyksiä työasemassa Wiresharkilla analysoitaessa ja löydettiin käytössä olevat IP-osoitteet, avoimet portit ja Windows-käyttöjärjestelmä (liite 4b) sekä Physio-web-sovelluksessa käytetty Node.js Express framework (liite 4c, 4d). Verkonvalvontasuunnitelmasta toteutettiin haavoittuvuuksien skannaus palvelimessa Nessus Essentialsilla (liite 5b). Nessus-skannausten raportit on esitetty liitteissä 5c-f (5e liian iso tiedosto, ei mukana materiaalissa). Physio-web-sovelluksen tietokannan injektiohaavoittuvuuksien tutkimista aloitettiin Burp Suitella (Liite 5h).

Lisäksi tehtiin case-esimerkkinä Hack the Box -sivuston Network Enumeration with Nmap -moduuli (Hack the Box, 2025) Parrot Linux-koneella Firewall and IDS/IPS Evasion - Easy Lab -tehtävään asti (liite 5a, ei mukana materiaalissa).

Tehtiin myös Helsingin Yliopiston ja MOOCH.fi:n Cyber Security Base -kurssisarjan Securing Software -kurssin Port Scanner -tehtävä (Helsingin Yliopisto & MOOC.fi, 2025), jossa skannataan portit annetulla välillä (liite 5g, ei mukana materiaalissa).

4.2.3 Järjestelmien haavoittuvuuksien varmennus

Tässä tehtiin yhteenveto (liite 6) edellisten kohtien Nmap- ja Nessus Essentials -haavoittuvuusskannausten tulosten ja raporttien analyyseistä (liitteet 4b-d, 5b). Nmapilla skannattiin vain työasemaa Physio-web-sovelluksen kanssa ja ilman, ja sitäkin suppeammin kuin Nessuksella. Nessuksella skannattiin myös palvelinta. Tutkitut asiat vastasivat toisiaan.

4.2.4 Kehittämisehdotukset kyberturvan parantamiseksi

Kehittämisehdotukset haavoittuvuusskannausten (Nmap, Nessus Essentials) pohjalta tietoturvan parantamiseksi esitellään liitteessä 6. Palvelimen portista 443 löytynyt keskivahvan SSL-salauksen tukeminen

täytyy poistaa. Vanhentunut SSL-sertifikaatti tulee uusia ja vanhojen TSL-versioiden tuki poistaa. Työaseman portissa 445 löytynyt vanha SMB-versio tulee hoitaa ja pakottaa SMB-kirjautuminen.

Physio-web-sovelluksesta täytyy ottaa käyttöön Express-frameworkin Helmet.js-väliohjelmisto, joka suojaa Express-pohjaisia sovelluksia asettamalla http-otsikoita oikein. Koodiin tulee myös lisätä ei-toivottujen http-metodien estäminen, HTTPS:n pakottaminen ja sisällön suojauskäytäntöön liittyvän vastausotsikon asettaminen kieltäväksi. NoSQL-tietokannan injektiohaavoittuvuuksia tulee vielä tutkia.

4.3 Kyberturvallisuusratkaisujen edistäminen

4.3.1 Tietoturvaan ja tietosuojaan liittyvien lakien, asetusten sekä muiden viranomaismääräysten tunteminen

Yrityksessä käsitellään terveydenhuollon asiakas- ja potilastietoja, joita koskevat lait ja asetukset esitellään liitteessä 7. Näitä ovat laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023), EU:n yleinen tietosuoja-asetus (2016/679, GDPR) ja tietosuojalaki (1050/2018) sekä terveydenhuollon ammattihenkilöistä annetty laki (559/1994). Lisäksi rikoslain (39/1889) 38. luku ”Tietotekniikkaan liittyvät rikokset” määrittelee tietomurrot, tietojen oikeudettoman käytön ja tietojärjestelmiin kohdistuvat rikokset ja laki sähköisestä tunnistamisesta ja luottamuspalveluista (533/2016) säätelee vahvaa sähköistä tunnistautumista.

Asiakastietolain mukaan terveydenhuollon palvelunantajan on liityttävä Kanta-palvelujen käyttäjäksi, jos asiakkaiden tietoja käsitellään sähköisessä asiakas- tai potilastietojärjestelmässä. Physionvelvollisuutena on muun muassa käyttää olennaiset vaatimukset täyttävää tietojärjestelmää ja laatia tietoturvasuunnitelma. GDPR:n mukaisesti Physion tulee tehdä myös julkinen tietosuojaseloste, jossa kerrotaan mitä tietoa kerätään ja miksi, kauan tietoja säilytetään sekä kuvaus rekisteröidyn oikeuksista.

4.3.2 Kyberuhkien ja niitä vastaavien riskien havainnollistaminen

Selvitettiin ja kuvattiin lyhyin esimerkein tämän hetken yleisimmät ja kriittisimmät tietoturvauhat sekä mitä riskejä ne asiakasyrityksessä merkitsevät (Liite 8). Kyberturvallisuuskeskuksen Pienyritysten kyberturvallisuusoppaan mukaan yleisimmät kyberuhat ovat tietojenkalastelu, haittaohjelmat ja kiristyshaittaohjelmat. ChatGPT listaa myös haittaohjelmat (esim. kiristyshaittaohjelmat), tietojenkalastelu, käyttäjätunnusten ja salasanojen murrot, sisäpiiriuhat, päivitysten ja haavoittuvuuksien hallinnan laiminlyönti sekä IoT-laitteiden tietoturvariskit. OWASP Foundationin vuoden 2021 Top 10 -listalla web-sovellusten tietoturvariskeistä yleisimpiä olivat rikkinäinen käyttöoikeuksien valvonta, kryptografiset viat, injektiot, ei-turvallinen suunnittelu ja virheelliset tietoturva-asetukset.

Physion kohdalla riski eri uhkien kanssa on asiakas- ja potilastietojen päätyminen vääriin käsiin, mistä aiheutuu sanktioita, mainehaittaa ja toimintahäiriöitä.

4.3.3 Tietoturvaohjeiden noudattaminen työtehtävissä

Toteutettiin lyhyt ja tiivis alustava tietoturvaohje asiakasyritykselle (Liite 9).

4.3.4 Kyberturva- tai tietosuoja-asioissa opastaminen

Tehtiin Tietoturvaopastus-Powerpoint-esitys kolmesta pienestä käytännön työssä huomioitavasta kyberturva-asiasta yrityksen työntekijöille: huijaussähköposti, sähköpostin salaus Outlookissa, Bitwardenin käyttöönotto (Liite 10).

Lähdeluettelo

Github, I. (1. Maaliskuu 2025). *Github - hannahakonen/physio-web-pages*. Noudettu osoitteesta https://github.com/hannahakonen/physio-web-pages

Hack the Box. (25. Helmikuu 2025). *Network Enumeration with Nmap*. Noudettu osoitteesta https://academy.hackthebox.com/module/details/19

OpenAI. (17. Maaliskuu 2025). *ChatGPT*. Noudettu osoitteesta chatgpt.com

Wireshark Foundation. (18. Helmikuu 2025). *Wireshark*. Noudettu osoitteesta https://www.wireshark.org/

Liitteet

Liite 1	Windows-työaseman suojaus päivityksillä ja ohjelmistoilla
Liite 2	Windows-työaseman hallinta hallintatyökaluilla
Liite 3	Salausmenetelmät
Liite 4a	Verkon valvonta: ympäristö ja suunnitelma
Liite 4b	Verkon valvonta ja haavoittuvuuksien skannaus: Case-esimerkki Wireshark ja Nmap
Liite 4c	Verkon valvonta ja haavoittuvuuksien skannaus: Case-esimerkki Physio, Wireshark ja Nmap
Liite 4d	Verkon valvonta ja haavoittuvuuksien skannaus: Case-esimerkki Physio, Wireshark ja Nmap: Versioskannaus
(Liite 5a	Haavoittuvuuksien skannaus: Case-esimerkit Hack the Box: Network Enumeration with Nmap)
Liite 5b	Haavoittuvuuksien skannaus: Case-esimerkki Nessus
Liite 5c	Nessus Host Discovery Scan -raportti
Liite 5d	Nessus Ping-Only Discovery Scan -raportti
(Liite 5e	Nessus Basic Network Scan -raportti)
Liite 5f	Nessus Web Application Tests -raportti