Veeti Help

Fyysinen tietoturva yrityksessä ISO/IEC 27001 -standardin mukaisesti

Metropolia Ammattikorkeakoulu

(AMK)

Ohjelmistotekniikka

Insinöörityö

6.4.2022

Tiivistelmä

Tekijä:	Veeti Help
Otsikko:	Fyysinen tietoturva yrityksessä ISO/IEC 27001 -standardin mukaisesti
Sivumäärä:	24 sivua
Aika:	6.4.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Ohjelmistotuotanto
Ohjaajat:	Laatupäällikkö Kai Kuusela Lehtori Ilpo Kuivanen

Insinöörityö tehtiin osana laajempaa tietoturvan kehitysprojektia, jossa kohdeyrityksen tavoitteena on saada itselleen ISO/IEC 27001 -standardin mukainen tietoturvasertifikaatti. Insinöörityössä keskityttiin ISO/IEC 27001 -standardin määrittelemän viitekehyksen fyysistä tietoturvaa käsittelevään osaan.

Työn tarkoituksena oli kartoittaa kohdeyrityksen fyysisen tietoturvan nykytila, selvittää puutteellisuudet standardin viitekehykseen nähden ja luoda suunnitelma, millä tavoin kohdeyritys saavuttaa standardin täyttävän tason fyysisen tietoturvan osalta. Kartoitusvaiheessa käytettiin apuna konsulttiyritystä, joka teki fyysisen tietoturvan auditoinnin kohdeyritykselle. Konsulttiyrityksen raportin pohjalta saatiin selkeä kuva puutteista ja kehityskohdista.

Puutteiden ja kehityskohtien korjaamiseksi laadittiin suunnitelma, jota noudattamalla kohdeyritys pystyy läpäisemään virallisen auditoinnin sekä saavuttamaan ISO/IEC 27001 -standardin täyttävän tason fyysisessä tietoturvassaan.

Avainsanat: fyysinen tietoturva, ISO/IEC 27001 -standardi

Abstract

Author:	Veeti Help
Title:	Physical information security according to ISO/IEC 27001 standard
Number of Pages:	24 pages
Date:	6 April 2022
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Software engineering
Supervisors:	Kai Kuusela, Quality Manager Ilpo Kuivanen, Senior Lecturer

---

The thesis was carried out as part of a wider information security development project, in which the subject of this case study aims to obtain an information security certificate in accordance with the ISO/IEC 27001 standard. The thesis focused on the physical security part of the framework defined by the ISO/IEC 27001 standard.

The purpose of the work was to map out the current state of the physical security of the target company, to find out the shortcomings in relation to the reference framework of the standard and to create a plan for how the target company will achieve a standard-compliant level of physical security. The mapping phase was assisted by a consulting firm that performed a physical security audit for the target company. Target company, based on the report of the consulting company, formed a clear picture of the shortcomings and points of development was obtained.

To amend the shortcomings and the points of development, a plan was developed to enable the target company to pass the official audit and to achieve a level of physical security that meets the framework defined by the ISO/IEC 27001 standard.

Keywords: physical information security, ISO/IEC 27001 standard

Sisällys

1 Johdanto

Opinnäytetyö on tehty osana kohdeyrityksen laajempaa tietoturvan kehitysprojektia, jonka päämääränä on, että kohdeyritys saavuttaa ISO/IEC 27001 -standardin mukaisen tietoturvasertifikaatin. Sertifikaatti antaa kohdeyritykselle mahdollisuuden todistaa, että tietoturva on huolellisesti suunniteltua, toteutettua ja se vastaa yleisesti hyväksyttyä standardia. Sertifikaatin saamiseksi yrityksen dokumentaatio, prosessit ja toimintatavat saatetaan standardissa määritellylle tasolle.

Kohdeyritys on suomalainen PK-yritys, joka toimii Suomen markkinoilla ja toimittaa asiakkailleen kokonaisvaltaisia laite-, instrumentointi- ja järjestelmäratkaisuja. Kohdeyritys on asiantuntijaorganisaatio ja kuuluu monikansalliseen teknologia- ja teollisuusliiketoimintakonserniin. Tietoturvasta on tullut entistä tärkeämpi osa kohdeyrityksen strategiaa liiketoiminnan keskittyessä enenevissä määrin järjestelmäratkaisuihin.

Opinnäytetyön tarkoituksena on edesauttaa kohdeyritystä saavuttamaan ISO/IEC 27001 -standardin mukainen tietoturvasertifikaatti. Työn vaiheisiin kuuluu kohdeyrityksen fyysisen tietoturvan nykytilan kartoitus ja tarvittavien korjaustoimenpiteiden suunnittelu ja toteutus. Tavoitteena on löytää kehityskohdat ja puutteet ja laatia suunnitelma, jota noudattamalla kohdeyrityksen fyysinen tietoturva saadaan vastaamaan standardissa määriteltyjä vaatimuksia.

2 Fyysisen tietoturvan parantaminen ISO/IEC 27001 -viitekehyksen mukaisesti

2.1 Fyysinen tietoturva

Fyysinen tietoturva on yrityksen omaisuuden suojelemista aina kiinteistöistä, laitteista ja työkaluista henkilöstöön ja yritykselle tärkeään dataan. Voidaan ajatella, että fyysisen tietoturvan tekijät koostuvat kolmesta osa-alueesta, jotka ovat ennaltaehkäisy, havainnointi ja elpyminen. (1.)

Yrityksen täytyy toimia ennaltaehkäisevästi voidakseen estää suurimmat uhat ja minimoidakseen riskejä. Ennaltaehkäisyyn kuuluvat mm. kiinteistön suojaaminen toimivalla lukkojärjestelmällä sekä kameravalvonta ja hälytysjärjestelmä. Henkilöstön kouluttaminen ja tiedottaminen fyysisestä tietoturvasta ovat avainasemassa ennaltaehkäisyvaiheessa. Yrityksen on löydettävä ”kultainen keskitie” ennaltaehkäisevissä toimenpiteissään, sillä monessa tapauksessa riskin tiedostaminen, dokumentointi ja hyväksyminen ovat huomattavasti tehokkaampia tapoja säästää rahaa ja resursseja kuin eliminoida riskin mahdollisuus kokonaan. Yrityksen on pystyttävä optimoimaan kaikki turvallisuustoimenpiteensä ja vältettävä ylimitoittamasta varautumistaan toimilla, jotka maksavat enemmän kuin realistisesti määritetyt potentiaaliset vahingot.

Havainnointivaiheessa yrityksen tulee pystyä tunnistamaan mahdollinen uhka, haitta tai jo tapahtunut vahinko ja sen mittasuhteet mahdollisimman nopeasti. Yrityksen on toimittava ennalta määritetyn protokollan mukaan ja pyrittävä neutralisoimaan tilanne, oli se sitten edelleen aktiivinen tai jo tapahtunut vahinko. Havainnointivaihetta seuraa elpyminen, jolloin yritys käyttää suunnittelemiaan tietoturvatoimenpiteitä vahinkojen minimoimiseksi ja uhkan eliminoimiseksi. Elpymisvaiheessa yritys alkaa myös korjata vahinkoja ja pyrkii pääsemään jälleen toimintakykyiseksi niin pian kuin mahdollista. Tässä vaiheessa on myös tärkeää ottaa opiksi ja kehittää tietoturvatoimintoja siten, että tulevaisuudessa vastaavilta uhkilta ja vahingoilta voidaan välttyä tehokkaammin.

Case-esimerkki tietoturvan pettämisestä

Vuonna 2018 Ylen toimittaja teki tutkivaa journalismia ja testasi 11:n yhteiskunnalle merkittävän yrityksen tai instituution tietoturvaa. Testissä toimittaja pukeutui huomioliiveihin, laittoi kaulaansa nimettömän ja kuvattoman henkilökortin ja otti tikkaat kainaloonsa. Hän pyrki pääsemään sisään kohteisiin kertomatta, kuka on tai millä asialla liikkuu. Toimittaja onnistui pääsemään sisään kaikkiin kohteisiin, yhtä lukuun ottamatta. Kohteina olivat mm. Suomen Pankki, Helsinki-Vantaan lentoasema, Viestintävirasto, Fortum ja Säteilyturvakeskus. Testin tulos on karu, muttei välttämättä yllättävä, kun pohditaan, miksi kohteiden ennalta ehkäisy ja havainnointi pettivät. (2.)

Kaikissa yrityksissä ja instituutioissa oli selvästi varauduttu tämänkaltaiseen tunkeutumisyritykseen, ja kohteissa oli ennalta määritetty protokolla, miten henkilöstön tulee tällaisessa tilanteessa toimia. Testissä kuvatut videot näytettiin kohteiden edustajille ja heitä pyydettiin kommentoimaan tapahtunutta ja miten näin pääsi käymään. Virhe tapahtui havainnointivaiheessa. Haastateltaessa kohteiden edustajia useimmat haastateltavat kertoivat syyksi, että on tapahtunut ”inhimillinen virhe”. Tämä testi osoittaa selvästi ja käytännön tasolla, kuinka ihminen on aina heikoin lenkki, kun tehokasta tietoturvaa pyritään toteuttamaan.

Ei ole suurtakaan merkitystä, jos jokin organisaatio on investoinut suuria summia tietoturvaansa ja hankkinut markkinoiden parhaat ja moderneimmat järjestelmät käyttöönsä, jos yksi ihminen voi päätöksellään päästää tunkeutujan näiden järjestelmien ohi. Näin kuitenkin usein on ja henkilöstön koulutuksen ja tarkkojen toimintaohjeiden merkitys korostuu.

Suomessa vallitsee ns. luottamuksen kulttuuri ja lähtökohtaisesti ihmiset ajattelevat, että sisään pyrkivä henkilö liikkuu varmasti oikealla asialla. Testi osoittaa, että organisaatioiden on huomattavan vaikea jalkauttaa turvallisuuden kulttuuria ja tahtotilaa koskemaan kaikkea henkilöstöä. Pohjoismainen ajattelutapa pyrkii välttämään konflikteja, eikä kellekään haluta aiheuttaa ylimääräistä vaivaa. Tästä syystä ei yksinkertaisesti kehdata kysyä ”millä asialla liikut.”

Sillä, että tunkeutuja onnistuu pääsemään sisälle organisaation tiloihin, ei välttämättä ole vielä suurtakaan merkitystä. Se riippuu pitkälti siitä, mikä on tunkeutujan motiivi. Haluaako tunkeutuja varastaa organisaatiolta laitteita ja myydä ne eteenpäin, onko hänen tarkoituksensa vain aiheuttaa vahinkoa organisaatiolle vai pyrkiikö hän pääsemään käsiksi toiminnan kannalta kriittisiin tietoihin. Ellei valvomatta organisaation tiloissa liikkuva tunkeutuja pääse suoraan käsiksi tietoihin tai pysty anastamaan esimerkiksi läppäreitä tai muuta organisaation omaisuutta, hänelle voi avautua mahdollisuus liittää jokin fyysinen laite organisaation verkkoon ja alkaa urkkia tietoja etäyhteyden avulla. (3.)

Testin jälkeen useimmissa organisaatioissa päädyttiin tarkentamaan toimintaohjeita, ja jotkin organisaatiot päätyivät tässä elpymisvaiheessa suunnittelemaan

ennalta ehkäisevät toimenpiteensä kokonaan uusiksi. Esimerkiksi kohteen pääoven lukitsemisella saadaan tehokkaammin valvottua organisaatiossa vierailevia henkilöitä. Tällöin voidaan saman tien varmistaa, millä asialla henkilö liikkuu. Organisaation henkilöstöstä voi asianomainen isäntä saapua aulaan vastaanottamaan vierailijan. Näin ei ulkopuolisia henkilöitä pääse liikkumaan organisaation tiloissa ilman saattajaa.

2.2 Tietoturvan seitsemän kerrosta

Fyysisen tietoturvan suunnittelussa on hyödyllistä ajatella tietoturvaa kerrosmallin avulla. Kaikkia tietoturvariskejä ei koskaan voida täysin sulkea pois, joten täydellistä ja täysin aukotonta systeemiä on mahdoton saavuttaa. Yleinen harhakuvitelma on, että jollain yhdellä tietyllä tietoturvamenetelmällä tai -ohjelmistolla saavutettaisiin organisaation täydellinen turvallisuus. Koska sataprosenttinen turvallisuus on joka tapauksessa mahdotonta saavuttaa, on järkevintä muodostaa turvattavan datan ympärille useampi vaikeasti läpäistävä kerros. Yrityksen toiminnalle kriittistä tietoa suojaavat kerrokset ovat tiedonsiirto ja -säilytys, ohjelmistot, päätelaitteet, verkko, toimialue ja henkilöstö eli ihminen. (4.)

2.2.1 Yrityksen toiminnalle elintärkeä tieto

Kaiken keskiössä on yritykselle elintärkeä omaisuus, data, joka halutaan pitää turvassa. Yrityksen on pystyttävä tunnistamaan ja luokittelemaan sen tuottama ja hallussa oleva data. Kaikki tieto ei suinkaan ole yrityksen toiminnan kannalta kriittistä tai tarkoin varjeltavaa, luottamuksellista dataa. Strategiset yrityssalaisuudet, kahdenväliset sopimukset ja asiakkaiden taloustiedot on pystyttävä pitämään salassa ja estettävä niiden vuotaminen organisaation ulkopuolelle.

Yrityksen on myös hyvä pohtia tiedon saatavuutta ja sitä, onko kaiken tiedon pakko olla saatavilla jatkuvasti. Joissakin organisaatioissa tietoturvaa toteutetaan siten, että viikonlopuksi kaikista järjestelmistä ns. ”vedetään töpseli seinästä”, eli kaikki yrityksen järjestelmät irrotetaan verkosta siksi aikaa, kun työntekijät ovat vapaalla. Tätä voidaan ajatella eräänlaisena salassapitoon tai piilotteluun perustuvana turvallisuutena (security by obscurity). Perusideana on, että

turvallisuuden rakenne ja toteutustapa pysyvät salassa. (5.) Työntekijöiden palatessa töihin myös verkkoa valvotaan intensiivisemmin. Tällainen ei tietenkään ole monessakaan organisaatiossa tänä päivänä mahdollista, mutta on hyvä muistaa, että päätelaite on tavalla tai toisella haavoittuvainen ja altis hyökkäyksille aina, kun se on kiinni missä tahansa verkossa.

2.2.2 Turvallinen tiedonsiirto ja -säilytys

Ensimmäinen tietoja suojaava kerros muodostuu datan turvallisesta säilyttämisestä, varmuuskopioinnista ja siirtämisestä. Luonnollisesti dataa käytetään ja käsitellään jatkuvasti ja tiedonsiirto ja -säilytys on oltava turvallista. Kriittisen tiedon vuotamisella organisaation ulkopuolelle tai sen katoamisella voi olla organisaatiolle tuhoisat seuraukset. Tietojen säilyttämiseen on oltava selkeä ja turvallinen protokolla ja varmuuskopioinnista on huolehdittava kahdentamalla tiedot toisistaan riippumattomiin paikkoihin. Säilytettävän, arkistoidun tiedon salaus on myös ensiarvoisen tärkeää siinä tapauksessa, että tietoja pääsee vuotamaan organisaation ulkopuolelle.

2.2.3 Ohjelmistojen turvallisuus

Toinen kerros on yrityksessä käytössä olevien ohjelmien ja ohjelmistojen turvaamista. Käytettävien ohjelmien tulee olla luotettavia, eikä niissä saa esiintyä pääsynhallintaan tai tietovuotoihin liittyviä heikkouksia. Yrityksellä täytyy olla tiedossa organisaatiossa käytettävät ohjelmistot ja hallittava niiden pääsyä kriittisiin tietoihin. Ohjelmistojen sisäiset tietoturvaratkaisut on selvitettävä ja todettava, että tietoturvasta huolehditaan riittävällä tasolla.

On yrityksen edun ja tietoturvan maksimoimisen kannalta järkevää, että käytössä olevista ohjelmista päättää keskitetysti yrityksen tietoturvasta huolehtiva taho. Ohjelmistoista on lähes poikkeuksetta turvallisinta käyttää uusinta ohjelmistoversiota, sillä uusia tietoturvaheikkouksia löytyy lisää kaiken aikaa, ja ohjelmistojen kehittäjät pyrkivät parhaansa mukaan korjaamaan näitä puutteita ja pitämään ohjelmistonsa turvallisina. Kun organisaation ohjelmistoista vastaa keskitetysti yksi taho, on myös ohjelmistojen ajan tasalla pitäminen helpompaa

ja kontrolloidumpaa, kun esimerkiksi IT-osasto voi päivittää ohjelmistot ja pakottaa käyttäjän käynnistämään päätelaitteensa uudelleen. Mikäli henkilöstössä herää tarve uudelle ohjelmistolle, tietoturvasta vastaavalla taholla tulee olla käytössään prosessi ohjelmiston tietoturvan tason toteamiseksi ja testaamiseksi.

2.2.4 Päätelaitteiden turvallisuus

Yrityksen dataa käytetään ja tuotetaan eri ohjelmistoilla, jotka toimivat erilaisilla päätelaitteilla. Yrityksen tietokoneet, läppärit ja mobiililaitteet on suojattava ohjelmallisesti ja henkilöstölle on koulutettava laitteiden tietoturvallisen käytön perusperiaatteet. Käytettävät laitteet tulee olla yrityksen tiedossa ja ainoastaan henkilö, jolle laite on osoitettu, on oikeus käyttää laitetta. Pääsynhallinta tulee olla kontrolloitua ja laitteiden ohjelmistoversiot on pidettävä ajan tasalla.

Myös laitteiden oikeaoppinen ja tietoturvallinen säilyttäminen ja etenkin organisaation turva-alueiden ulkopuolinen käyttö tulee ohjeistaa henkilöstölle riittävällä vakavuudella. Turvallisin ratkaisu on, että yrityksen pilvipalveluita ja muita ohjelmistoja käytetään ainoastaan organisaation osoittamilla laitteilla, eikä esimerkiksi henkilökohtaisella tietokoneella tai varsinkaan julkisessa käytössä olevalla päätelaitteella. Organisaatio pystyy kontrolloimaan osoittamiaan laitteita huomattavasti tarkemmin ja esimerkiksi tietokoneiden kovalevyt voidaan salata. On myös tärkeää, että organisaation osoittamilla laitteilla on ainoastaan työhön liittyvät ohjelmat, eikä henkilökohtaiseen käyttöön tarkoitettuja sovelluksia käytetä yrityksen päätelaitteilla.

Päätelaitteet vanhenevat, ja tyypillinen laitteiden käyttöikä on 2–3 vuotta. Monet yritykset käyttävät leasing-sopimuksia, jolloin organisaation ei tarvitse ostaa laitetta itselleen, vaan ainoastaan vuokrata pitkäaikaiseen käyttöön. (6.) Tällöin organisaation tietoturvasta vastaavalla taholla täytyy olla prosessi myös laitteen oikeaoppiseen poistoon, kun leasing-sopimus loppuu ja laite poistuu käytöstä. Yleensä tässä kohtaa kaikki laitteeseen tallennettu data poistetaan ja laite palautetaan tehdasasetuksille. Tämä tehdään siitä huolimatta, vaikka laitteen käyttäjä lunastaisikin laitteen itselleen.

2.2.5 Yrityksen verkon turvallisuus

Vain ennalta määritetyillä ja yrityksen tiedossa olevilla päätelaitteilla tulee olla pääsy yrityksen verkkoon, ja kaikkien tunnistamattomien laitteiden pääsy pitää pystyä estämään. Yrityksen verkon tulee olla eriytetty julkisesta internetistä, ja julkisen verkon yli tapahtuvat yhteydet toteutetaan virtuaalisen erillisverkon eli VPN:n avulla.

Turvallisuuden lisäämiseksi on myös järkevää segmentoida eli jakaa yrityksen verkko erilaisiin ryhmiin siten, että työntekijöillä on pääsy ainoastaan sellaisiin verkon osiin, joita he todella tarvitsevat työssään. Mitä vähemmän pääsy- ja käyttöoikeuksia jaetaan, sitä helpompaa verkon kontrolloiminen on. Mikäli yrityksen verkkoon liitetään päätelaitteita verkkokaapelein, fyysiset portit, jotka eivät ole käytössä, tulisi pitää kokonaan irti verkosta. Näin ollen kukaan ulkopuolinen ei pysty liittämään fyysistä laitetta suoraan yrityksen verkkoon.

Verkkoon liitetyistä laitteista tulee olla tarkka kirjanpito. Yrityksen verkosta vastaava taho voi jakaa vapaana olevia kiinteitä IP-osoitteita laitteille sitä mukaa, kun niitä tarvitaan. Samalla yritys voi kontrolloida käytettäviä DNS-palvelimia. Toinen vaihtoehto on, että yrityksen verkkoon liitytään MAC-osoitteen perusteella, jolloin uusi laite lisätään yrityksen verkkoon ja käyttötarkoitus sekä käyttäjä kirjataan muistiin.

Organisaation osoittamien päätelaitteiden kaiken liikenteen tulisi kulkea yrityksen palomuurin läpi, jotta yrityksen tietoturvasta vastaava taho pystyy kaiken aikaa pysymään ajan tasalla siitä, miten paljon ja minne liikennöintiä tapahtuu. Poikkeavista tiedonsiirtomääristä tai epäilyttävistä palveluntarjoajista voidaan määritellä hälytyksiä ja näin valvontaa saadaan automatisoitua.

Organisaation osoittamien tietokoneiden ja läppäreiden kaikki liikenne voidaan ohjata kulkemaan yrityksen palomuurin kautta, jolloin tietoturvariskejä pystytään minimoimaan, riskialtis käyttö saadaan nopeasti kiinni ja henkilöstöä voidaan ohjeistaa toimimaan tietoturvallisesti. Mobiililaitteiden osalta organisaation tietoturvasta vastaava taho voi jakaa laitteen henkilökohtaista ja työkäyttöä varten.

Näin yritys pystyy valvomaan itselleen kriittisen datan käyttöä, mutta käyttäjän yksityisyyttä ei myöskään loukata.

2.2.6 Toimialueen turvallisuus

Kuudes kerros on puhtaasti fyysisen tietoturvan optimointia digitaalisen tietoturvan tueksi. Toimialueen turvaamisessa on otettava huomioon kaikki fyysiseen tietoturvaan liittyvät tekijät. Tämä kerros muodostaa yrityksen verkon uloimman osan ja kattaa verkon fyysiset tukiasemat ja liittymispisteet.

Nykyään päätelaitteina ei ole pelkästään tietokoneita, jotka ovat verkkokaapelilla kiinni yrityksen verkossa. Yrityksellä voi olla useita langattomia verkkoja eri tarkoituksiin. Pöytätietokoneet, läppärit ja tabletit, tulostimet ja kopiokoneet, neuvotteluhuoneiden langattomat äänen- ja kuvansiirtojärjestelmät sekä älypuhelimet tarvitsevat langatonta verkkoa toimiakseen. Yrityksen verkosta vastaavalla taholla täytyy olla selkeä kuva kaikesta tästä ja sen on pystyttävä tunnistamaan turvalliset laitteet tuntemattomista ja mahdollisesti haitallisista laitteista. Verkkoon liittymispisteet eivät ole enää yhden toimistokompleksin seinien sisällä, vaan käyttäjät toimivat enemmän ja enemmän etäyhteyksin, milloin mistäkin.

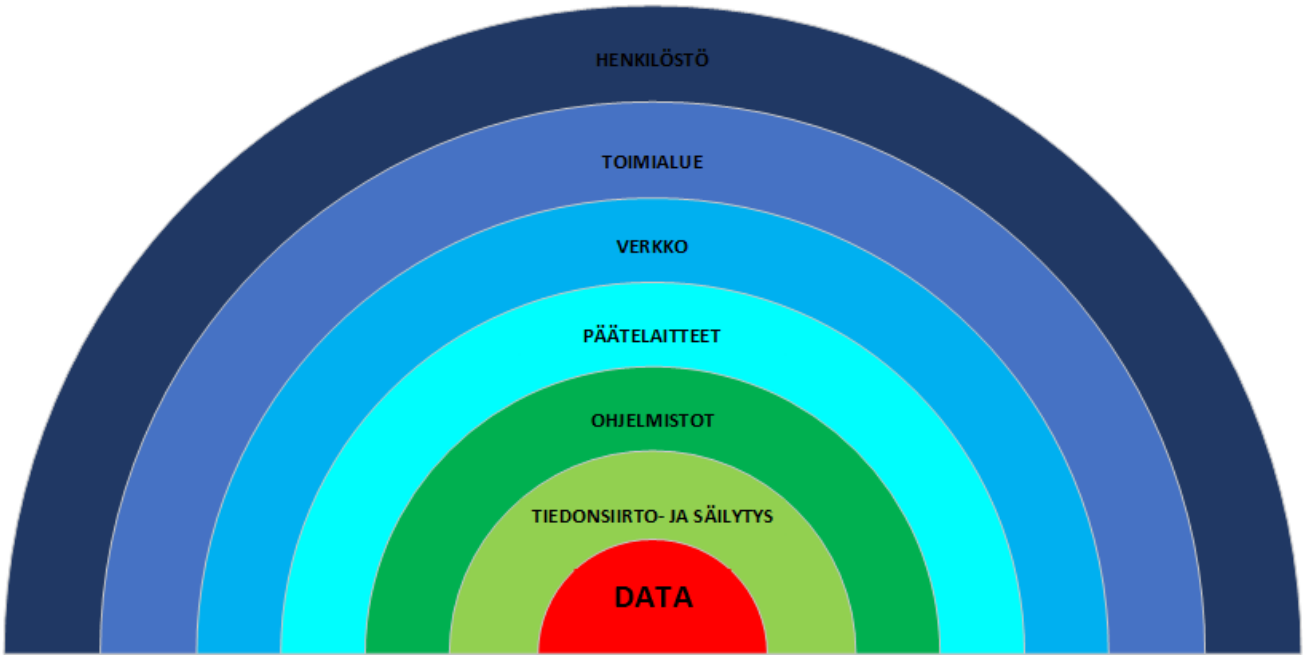
Toimialueen fyysisestä turvallisuudesta voisi laatia oman kerrosmallinsa. Kaiken keskiössä on turvattava data ja sen ympärille rakennetaan vaikeasti läpäistäviä kerroksia. Tämä onnistuu lukitusjärjestelmien, kameravalvonnan ja henkilöstön koulutuksen avulla.

2.2.7 Ihminen osana tietoturvaa

Seitsemäs, viimeinen ja varmasti heikoin kerros on henkilöstö eli ihminen. Ihminen tekee tietokonetta herkemmin virheitä ja on yleensä aina riskialttein tekijä missä tahansa systeemissä. Yrityksen työntekijät ovat alttiita jakamaan epähuomiossa tärkeätä dataa tai voivat joutua tietojenkalasteluhyökkäysten uh-

reiksi. Yrityksen tulee olla tietoinen siitä, että kaikki tietoturvaratkaisut, jotka jäävät puhtaasti ihmisen vastuulle, ovat huomattavasti riskialttiimpia kuin muilla keinoin toteutettuna.

Kun jokin tietoturvatoimenpide on kokonaan ihmisen vastuulla, koulutuksen ja tiedotuksen määrä ja laatu korostuvat. Yrityksen on panostettava henkilöstön kouluttamiseen ja pyrittävä jalkauttamaan sama tietoturvan tahtotila koskemaan jokaista henkilöstön jäsentä. Yleisesti ihmiset eivät tieten tahtoen halua aiheuttaa vahinkoa organisaatiolleen tai päästää hyökkääjää sisään avoimista ovista. Monessa tapauksessa kyse on siitä, ettei täysin ymmärretä, että juuri tämä asia voi olla tietoturvariski tai miksi tällainen toimintatapa voi saattaa organisaation liiketoiminnalle kriittisen datan vaaraan.



Kuva 1: Tietoturvan kerrosmalli. (7.)

2.3 ISO/IEC 27001 -viitekehys

ISO/IEC 27001 on kansainvälinen standardi, jossa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Tietoturvallisuuden hallintajärjestelmän tarkoitus on suojata tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla. Avainasia on, että organisaatio on suunnitellut, toteuttanut ja dokumentoinut hallintakeinot ja määritellyt toimintatavat poikkeustilanteissa.

ISO/IEC 27001 -standardissa fyysisen tietoturvan velvoitteet on määritelty hallintatavoitteiden ja -keinojen luettelossa. Fyysisen turvallisuuden ja ympäristön turvallisuuden hallintatavoitteet on jaettu turva-alueiden ja laitteiden turvallisuuteen.

Turva-alueiden ja niihin liittyvien hallintakeinojen määrityksen tavoite on suojata organisaation tietoaineistot ja tietojenkäsittelypalvelut niin, että luvaton taho ei pääse häiritsemään tai vahingoittamaan organisaation toimintaa. Fyysiset turva-alueet tulee määritellä sekä suojata asianmukaisella kulunvalvonnalla. Turva-alueiden määritys kattaa toimistojen, tilojen ja laitteistojen suojauksen lisäksi varautumisen ulkoisia ja ympäristön aiheuttamia uhkia vastaan. Näihin lukeutuvat mm. luonnonkatastrofit, onnettomuudet ja vihamieliset hyökkäykset.

Laitteiden osalta hallintakeinojen ja -tapojen tavoitteena on turvata organisaation toimintojen jatkuminen ja estää omaisuuden katoaminen, vahingoittuminen, varastaminen tai vaarantuminen. Organisaation on määriteltävä hallintakeinot laitteiden käyttöönotosta aina poistoon asti huollot mukaan lukien. Lisäksi on tärkeää ottaa huomioon aivan perustavan laatuiset asiat laitteiston turvallisesta sijoittelusta sähkökatkoilta varautumiseen ja sähkökaapeloinnin turvaamiseen. Organisaation on myös määritettävä hallintakeinot ja politiikat turva-alueiden ulkopuolella käytettävien laitteiden ja ilman valvontaa jäävien laitteiden varalta.

Puhtaan pöydän ja puhtaan näytön periaate on ehkä työntekijöille näkyvin ja konkreettisin laitteisiin liittyvä hallintatavoite. Itsestään selvältä vaikuttava termi

kattaa papereiden, siirrettävien tallennusvälineiden ja tietojenkäsittelypalveluiden oikeaoppisen ja huolellisen käsittelemisen ja säilyttämisen.

2.4 Fyysisen tietoturvan parantamisen työkalut

2.4.1 Riskienhallinta

Riskienhallinnan perusperiaatteena on analysoida, millaisia riskejä organisaatio voi kohdata ja millaiset mahdolliset seuraukset ovat riskien toteutuessa. Kun nämä asiat on kartoitettu, voi organisaatio päättää tapauskohtaisesti, miten riski pienennetään hyväksyttävälle tasolle. (8.)

Luonnollisesti paras vaihtoehto on poistaa riski kokonaan. Näin tapahtuu, kun löydetty haavoittuvuus voidaan korjata tai toimintatapoja voidaan muuttaa niin, että haavoittuvuus häviää. Usein tämä ei ole kuitenkaan mahdollista, eikä kannattavaa. Tällöin riskin todennäköisyyttä pyritään pienentämään esimerkiksi tiukentamalla turva-alueen kulunvalvontaa, jolloin riski huomattavasti pienenee, mutta on silti olemassa. Vaihtoehtoisesti voidaan pyrkiä pienentämään havaitun riskin vaikutuksia varautumalla ja nostamalla reagointikykyä. Esimerkiksi erilaisten vakuutusten avulla riskin vaikutuksia saadaan jälkikäteen osin kompensoitua.

Yleensä pyritään siihen, että riskin todennäköisyys ja seuraukset saadaan minimoitua sellaiselle tasolle, että jäljelle jäävä jäännösriski voidaan hyväksyä ja dokumentoida.

2.4.2 Gap-analyysi

Gap-analyysi eli kuilu- tai puuteanalyysi on menetelmä, jolla organisaatio kartoittaa nykyisen ja halutun tilanteensa eron. Gap-analyysi ei ole pelkästään tietoturvan suunnittelun työkalu, vaan sitä voidaan käyttää monessa muussakin tarkoituksessa, kun organisaatio haluaa kehittää toimintatapojaan. Ideana on saada selville, mitkä asiat toteutetaan jo tällä hetkellä halutulla tavalla ja mitkä asiat vaativat parannuksia. Gap-analyysia voidaan käyttää apuna monenlaiseen

organisaation resurssien optimointiin. Analyysin avulla organisaatiolle piirtyy selkeä kuva, millä osa-alueilla täytyy tehdä muutoksia ja minne resursseja kannattaa kohdistaa. (9.)

Gap-analyysilla organisaatio selvittää, kuinka suuri kuilu nykyisen ja halutun tilanteen välillä on, ja tämän pohjalta on helpompi alkaa tehdä suunnitelmaa kuilun umpeen kuromiseksi.

Organisaation on ensin määriteltävä tavoitetaso, johon tähdätään. Seuraavaksi mitataan organisaation nykytilan suorituskyky, ja analysoidaan saadut tulokset. Tämän jälkeen raportoidaan havainnot ja raportin pohjalta voidaan alkaa suunnitella, kuinka tavoitetaso saavutetaan mahdollisimman tehokkaasti.

3 Kohdeyrityksen fyysisen turvallisuuden nykytilan kartoitus

Kohdeyritys on suomalainen PK-yritys, joka toimii Suomen markkinoilla ja toimittaa asiakkailleen kokonaisvaltaisia laite-, instrumentointi- ja järjestelmäratkaisuja. Kohdeyritys on asiantuntijaorganisaatio ja kuuluu monikansalliseen teknologia- ja teollisuusliiketoimintakonserniin. Tämä asettaa omat rajoitteensa ja vaatimuksensa tietoturvalle ja kaikelle toiminnalle. Kohdeyrityksen liikevaihto koostuu pääsääntöisesti laitetoimituksista. Tästä syystä varaston merkitys on oleellinen myös tietoturvan kannalta. Viime vuosina kohdeyritys on panostanut enemmän ja enemmän myös järjestelmäpuolelle uusin innovaatioin.

3.1 Fyysinen auditointi

Tietoturva-auditoinnin tarkoituksena on kartoittaa mahdolliset haavoittuvuudet ja tietoturvariskit, joita mahdolliset hyökkääjät voisivat tavalla tai toisella käyttää hyväksi. Ensisijainen tavoite on tunnistaa ja korjata haavoittuvuudet sekä ennaltaehkäistä hyökkääjien yritykselle aiheuttama vahinko. Kattava auditointi on siis monella tapaa kilpailuetu organisaatiolle. Parantunut tietoturva minimoi riskejä ja mahdollistaa kestävän liiketoiminnan kehittämisen. (10.)

Ulkopuolinen konsulttiyritys suoritti fyysisen tietoturvan auditoinnin kohdeyritykselle lokakuussa 2021. Tarkastus suoritettiin toimitetun dokumentaation, haastattelun ja kohdekäynnin perusteella. Tietoturvan nykytasoa verrattiin ISO/IEC 27001:2017 standardin määrittämiin vaatimuksiin sekä muuhun sovellettavaan ohjeistukseen ja lainsäädäntöön. Auditoinnin tavoitteena oli määrittää kohdeyrityksen fyysisen tietoturvan nykytilanne ja vaatimustenmukaisuus.

3.2 Havainnot

Tietoturva-auditoinnissa tehtiin yhteensä 16 havaintoa, jotka luokiteltiin *merkittäviin* ja *vähäisiin*. Merkittävät havainnot on korjattava tietoturvan hallintajärjestelmän vaatimusten täyttämiseksi. Vähäisten havaintojen korjaamista hallintajärjestelmä ei vaadi, mutta korjausta suositellaan tietoturvan parantamiseksi.

Kohdeyrityksellä on tällä hetkellä jonkin verran fyysisen tietoturvan hallintaan liittyviä prosesseja ja politiikkoja. Kaikkia näitä käytäntöjä ei kuitenkaan noudateta politiikassa määritellyllä tavalla ja jotkin osa-alueista ovat puutteellisia.

3.2.1 Turva-alueet

Standardi velvoittaa organisaation määrittelemään fyysiset turva-alueet, jotka on suojattu asianmukaisella kulunvalvonnalla arkaluonteisen tai kriittisen tiedon ja tietojenkäsittelypalveluiden suojaamiseksi. Organisaation tulee myös suunnitella ja toteuttaa toimistojen, tilojen ja laitteiston suojaus ulkoisia ja sisäisiä uhkia, kuten luonnonkatastrofeja, vihamielisiä hyökkäyksiä tai onnettomuuksia vastaan.

Kohdeyrityksen fyysisiä turva-alueita ei ole tarkasti määritelty, ja ne sekoittuvat konsernin muiden yritysten kanssa. Kohdeyritys toimii toimistokompleksissa yhdessä viiden muun samaan konserniin kuuluvan yrityksen kanssa ja eri yritysten työntekijät pääsevät vapaasti liikkumaan toimitilojen välillä. Tämän vuoksi turva-alueiden yksiselitteinen määritys on haasteellista ja myös osin mahdotonta.

Kohdeyrityksen varasto on yhteisvarasto, jossa toimii myös saman konsernin kolme muuta tytäryhtiötä. Varastossa on siis henkilökuntaa muistakin organisaatioista kuin kohdeyrityksestä. Varastopaikat on jaoteltu yrityksittäin, mutta eri alueille ei ole toteutettu erikseen kulunvalvontaa. Myös yritysten muulla henkilöstöllä, kuin varastotyöntekijöillä, on vapaa pääsy varastolle. Tavaraa liikkuu molempiin suuntiin, eli tavarantoimittajat sekä tuovat uutta tavaraa varastoon, että noutavat asiakkaille lähtevää tavaraa varastosta. Näin ollen varaston osalta on todettava, ettei sitä voida lukea ehdoitta turva-alueeksi, johon olisi pääsy ainoastaan kohdeyrityksen työntekijöillä.

Tuotekehitys ja toimistotilat sijaitsevat omassa kerroksessaan, johon on pääsy ainoastaan kohdeyrityksen ja toisen samassa kerroksessa työskentelevän yrityksen työntekijöillä. Tuotekehitys on omassa erillisessä tilassaan, mutta kulunvalvontaa ei ole toteutettu.

Palvelinhuone on erillinen lukittu tila, jossa on sammutusjärjestelmä ja lattiakaivo. Palvelimet on nostettu räkkeihin eivätkä ne näin ollen ole maan tasalla. Palvelinhuoneessa on myös lämpötila-anturi ja ohjelmoitava mittausyksikkö, joka monitoroi huoneen lämpötilaa ja lähettää hälytystekstiviestin, mikäli lämpötila laskee tai nousee liikaa. Palvelimet on myös kahdennettu, eli data on peilattu toiseen palvelinhuoneeseen, joka sijaitsee fyysisesti täysin eri paikassa.

3.2.2 Kulunvalvonta

Turva-alueet on standardin mukaan suojattava asianmukaisella kulunvalvonnalla, jotta voidaan varmistua siitä, että vain luvan saaneilla henkilöillä on pääsy alueelle. Kulunvalvonnalla tarkoitetaan teknisillä laitteilla tai vartioinnilla toteutettua tietyn alueen tai rakennuksen valvontaa. Erilaisissa kohteissa kulunvalvonta voidaan hoitaa kameravalvonnalla, lukkojärjestelmillä tai esimerkiksi aulapalvelulla. Tärkeintä on olla perillä siitä, ketkä alueella tai rakennuksessa liikkuvat ja miksi.

Fyysisessä auditoinnissa myös kohdeyrityksen kulunvalvonnasta löytyi puutteita. Kiinteistössä on kuorisuoja ja ulkona kameravalvonta. Ulko-ovet ja lastauslaiturit ovat kameravalvonnassa, mutta auditoinnissa kävi ilmi, että yksi ovista on katveessa. Ulko-ovet on lukittu lukuun ottamatta lastauslaiturin vastaanottotoimistoa, josta tavarantoimittajat pääsevät asioimaan varastolle. Merkittävä havainto oli, että vastaanottotoimisto oli auditointikierroksen aikana tyhjillään ja hyökkääjällä olisi ollut vapaa pääsy vartioimattomille tietokoneille.

Kiinteistön sisätiloissa kulunvalvonta on toteutettu sähkölukoilla, joissa on RFID-lukijat ja näin ainoastaan yritysten työntekijöillä, joilla on tunnisteet, on mahdollisuus liikkua vapaasti eri tilojen välillä. Myös hississä on RFID-lukija ja ilman sopivaa tunnistetta on vapaa pääsy ainoastaan aulakerrokseen. Kiinteistöstä löytyi lukitsemattomia ovia, jotka johtavat turva-alueille, ja ovia, joissa oli avain paikallaan. Nämä ovat merkittäviä havaintoja. Koska jos kyseessä on rauta-avain, sen voi olettaa käyvän myös muihin kiinteistön oviin.

Myös asiattomien henkilöiden kulunvalvonta oli puutteellista, sillä kohdeyrityksen henkilökunnalle ei ole määritetty pakkoa käyttää näkyvissä olevia henkilökortteja yrityksen tiloissa. Tämä asettaa kohdeyrityksen ja muut samassa kiinteistössä toimivat yritykset alttiiksi Social Engineering -tyyppisille hyökkäyksille.

3.2.3 Ulkoistetut palvelut

Ulkoistetut palvelut on aina harkittu lisäriski organisaatiolle. Kohdeyrityksen kiinteistössä toimii ulkoistettu aulapalvelu, jonka työntekijät vaihtuvat ajoittain. Auditoinnissa kävi ilmi, että aulapalvelun henkilöillä on yhteiskäyttötunnus, jolla on huomattavan laajat oikeudet konserniyritysten sisäisiin dokumentteihin. Tämä on merkittävä tietoturvariski, sillä kohdeyrityksen ja muiden konserniyritysten tiedot ovat ulkopuolisen henkilön käytettävissä ja oikeudet ovat toimenkuvaan nähden ylimitoitetun laajat. Suurin riski on liiketoiminnalle kriittisen tiedon menettäminen tai vuotaminen taholle, joka voisi tavalla tai toisella hyötyä tiedoista tai tehdä vahinkoa yrityksille.

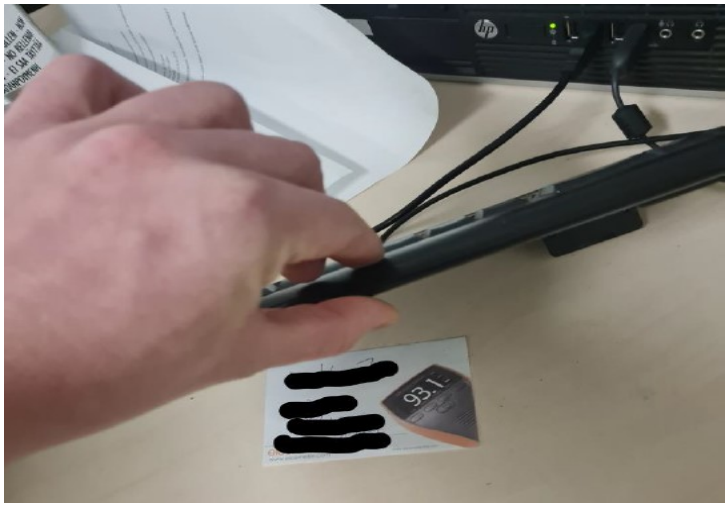
Kohdeyritys käyttää myös ulkoista siivouspalvelua, joka toimii iltaisin täysin valvomatta ja tuntemattomien henkilöiden toimesta. Ulkopuolisen henkilön olisi helppo varastaa kohdeyrityksen omaisuuttaa myytäväksi eteenpäin tai liittää valvomattomaan päätelaitteeseen jokin fyysinen laite tietojen keräystä varten. Tämä on vähäinen havainto, mutta luottamukseen perustuva sopimussuhde voi olla hyvin vahingollinen ja mikäli väärinkäytöksiä ilmenee, syyllisen selvittäminen voi olla jossain tapauksessa jopa mahdotonta.

3.2.4 Puhtaan pöydän ja puhtaan näytön periaate

Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän periaate sekä tietojenkäsittelypalveluja koskeva puhtaan näytön periaate on standardissa oleva suositus. Tämä tarkoittaa sitä, että työntekijöiden on huolehdittava, ettei pöydille tai neuvotteluhuoneisiin jää mitään luottamuksellista materiaalia. Paperit ja muistitikut, jotka sisältävät luottamuksellista tietoa on säilytettävä suojatussa varmassa paikassa.

Kohdeyrityksessä pöytien puhtaanapitokäytäntö on olemassa, mutta sitä ei noudateta tarvittavalla vakavuudella. Auditoinnin yhteydessä kävi ilmi, että toimiston pöydillä oli siellä täällä tietosuojan alaisia dokumentteja. Myöskään turvatulostusta ei ole määritetty, ja tämä mahdollistaa luottamuksellisten asiakirjojen joutumisen vääriin käsiin. Turvatulostuksen perusidea on, että tulostettavat asiakirjat saa tulostimesta ainoastaan tulostuksen tehnyt henkilö sen jälkeen, kun on tunnistautunut laitteelle. Auditointikäynnin yhteydessä löytyi myös tietokone, jonka salasana oli piilotettu näppäimistön alle. Tämä on perustavaa laatua oleva tietoturvariski, sillä salasanoja ei tulisi lähtökohtaisesti koskaan kirjoittaa ylös tai säilöä suojaamattomissa paikoissa.

Kuva 2. Salasana piilotettuna näppäimistön alle.



4 Toimenpiteet puutteiden korjaamiseksi

4.1 Turva-alueet

Turva-alueita koskevia tietoturvapuutteita lähdetään korjaamaan riskinhallinnan keinoin. Osa puutteista pyritään eliminoimaan kokonaan ja osa dokumentoidaan, otetaan vakavana riskinä huomioon ja jätetään hyväksyttävälle tasolle. Kohdeyrityksen on pystyttävä optimoimaan kustannustehokkaat ratkaisut hankaloittamatta työntekijöiden perusarkea liikaa.

Varaston osalta riskit minimoidaan ottamalla muuttamalla käytäntöjä siten, että vastaanotossa on oltava aina henkilökuntaa ottamassa vastaan tavarantoimittajia ja muita ulkopuolisia. Tämä toteutetaan kouluttamalla varaston henkilöstö ja porrastamalla esim. lounasaikaan ruokailuvuorot niin, ettei varasto jää missään kohtaa päivää tyhjäksi.

Toimiston saattaminen hyväksyttäväksi turva-alueeksi tapahtuu tarkentamalla kohdeyrityksen ja toisen samassa kerroksessa toimivan sisaryrityksen väliset rajat ja dokumentoimalla, millä henkilöillä on pääsy kerrokseen. Tämä onnistuu muokkaamalla sähkölukkojen ja hissin RFID-lukijan oikeudet niin, että ainoastaan kohdeyrityksen henkilökunnalla, sisaryrityksen henkilökunnalla ja ennalta määritellyllä kiinteistön henkilökunnalla on pääsy kerrokseen. Tässä on siis esimerkki riskistä, joka dokumentoinnin ja minimoinnin keinoin saatetaan hyväksyttävälle tasolle, sekoittamatta liikaa osapuolten perustoimintoja. On selvää, että koko kerroksen eristäminen kohdeyrityksen käyttöön olisi liian kallis ja aikaa vievä ratkaisu, sisaryrityksen kun pitäisi etsiä uudet toimitilat.

Palvelinhuone on toteutettu tietoturvallisesti ja sisäisiin ja ulkoisiin riskeihin on varauduttu standardin vaatimalla tavalla. Varmuuskopioinnin turvaamiseksi palvelinhuone on kahdennettu ja tiedot peilataan fyysisesti täysin toisaalla sijaitsevaan palvelinhuoneeseen. Tässä mahdollinen kehityskohta, jonka voisi tulevaisuudessa ottaa paremmin huomioon, on palvelinhuoneen sijainti. Palvelinhuone sijaitsee kiinteistön pohjakerroksessa, ja vaikka palvelimet on sijoitettu räkkeihin

maanpinnan yläpuolelle, huoneen fyysinen sijainti altistaa palvelimet vesivahingolle suuremmalla todennäköisyydellä, kuin mikäli palvelinhuone sijaitsisi ylemmissä kerroksissa.

4.2 Kulunvalvonta

Kohdeyritys ja samassa kiinteistössä toimivat viisi muuta sisaryritystä toteuttavat kulunvalvontaa, ja se onkin jo verrattain hyvällä tasolla, mutta muutamia puutteita on korjattava, jotta kohdeyritys saavuttaa standardin määrittelemän tason.

Sähkölukkojen ja eri kerrosten välistä liikennettä hissillä tulee rajata niin, ettei ulkopuolisilla henkilöillä ole pääsyä kohdeyrityksen tiloihin. Tässä tapauksessa ulkopuolisiksi lasketaan myös muut samassa kiinteistössä toimivat viisi sisaryhtiötä, lukuun ottamatta yhtä, jonka toimitilat sijaitsevat samassa kerroksessa. Tämä voi hieman vaikeuttaa työntekijöiden perusarkea, mutta kulkua on yksiselitteisesti rajattava, jotta riski saadaan minimoitua riskienhallinnan mukaisesti ja dokumentoitua riittävän kattavasti.

Tuotekehityksen ja toimiston välinen kulunvalvonta toteutetaan sähkölukolla, johon annetaan oikeudet ainoastaan tiloissa työskenteleville henkilöille. Tilat pidetään jatkossa aina lukittuna, ellei paikalla ole henkilökuntaa. Tällä tavoin tuotekehitys saadaan rajattua omaksi turva-alueekseen. Ratkaisulla saadaan edelleen minimoitua riskiä, että joku ulkopuolinen pääsisi käsiksi tuotekehityksen lähdekoodeihin ja muihin tietosuojan alaisiin tietoihin.

Kohdeyritys on tehnyt päätöksen kuvallisteen henkilökorttien käytöstä kiinteistön sisätiloissa liikkuessa. Vierailijoille annetaan myös omat henkilökortit, kun he saapuvat aulan vastaanottoon. Jatkossa siis yrityksen toimitiloissa liikkuvat ihmiset ovat yrityksen työntekijöitä tai heillä on mukanaan saattaja, joka on osa organisaatiota. Tällä toimenpiteellä pystytään välttämään Social Engineering -tyyppiset hyökkäykset, jossa hyökkääjä pyrkii pääsemään kohteen tietoihin käsiksi tekeytymällä asialliseksi vierailijaksi ja vaikuttamalla kohteen työntekijöihin päästäkseen anastamaan tai vahingoittamaan kohteen tietoja. Henkilökorttien

käyttöönoton myötä kiinteistössä ei oletusarvoisesti tulisi liikkua yhtäkään henkilöä ilman, että joku olisi ottanut heidät vastaan jo aulassa.

Lukitsemattomat ovet lukitaan ja paikallaan olevat rauta-avaimet poistetaan. Riski on näin eliminoitu kokonaan. Työntekijöiden kulkureittiä eri tilojen välillä muutetaan kokonaan ja nykyinen kulkureitti suljetaan pois käytöstä. Toinen vaihtoehto olisi voinut olla muuttaa ovien lukot sähkölukoiksi ja antaa oikeudet vain niille henkilöille, jotka työskentelevät ko. tiloissa.

4.3 Ulkoistetut palvelut

Kohdeyritys yhdessä muiden kiinteistössä toimivien sisaryhtiöiden kanssa teki päätöksen ulkoistetun aulapalvelun alas ajamisesta ja tuottamalla aulapalvelun sisäisesti. Tällä muutoksella eliminoidaan aulapalvelun yhteiskäyttötunnuksista johtuva luottamuksellisten tietojen vaarantuminen, sillä konserniyritysten työntekijöillä on pääsy ainoastaan oman yrityksensä tietoihin ja tiedostoihin. Myös koulutuksen tarve sekä aulatyöntekijöiden vaihtuvuus pienenevät radikaalisti, mikä myös pienentää riskiä huomattavasti.

Ulkoistetun siivouspalvelun aiheuttamaa riskiä voitaisiin pienentää kahdella tavalla. Työajan ulkopuolinen, ilta-aikaan tapahtuva siivous voitaisiin siirtää tapahtuvaksi päiväsaikaan niin, että kohdeyrityksen henkilökuntaa on koko ajan paikalla. Tässä haasteena on se, että sekä kohdeyrityksen työntekijöiden, että siivouspalvelun tuottavan yrityksen työntekijöiden työrauha voi kärsiä. Kohdeyritys päätti, ettei siirrä siivouksen ajankohtaa, mutta pitää jatkossa ajantasaista kirjanpitoa siivouspalvelun henkilöstöstä, jotta mikäli jotain tapahtuu organisaatio voi helpommin selvittää, millä henkilöillä oli luvallinen pääsy kiinteistöön kyseisenä aikana.

Toinen vaihtoehto on lisätä kameravalvontaa yrityksen sisätiloihin, mutta lainsäädäntö asettaa tähän ratkaisuun huomattavia haasteita. Kuvaaminen on lähtökohtaisesti kiellettyä julkisrauhan suojaamissa, yleisöltä suljetuissa paikoissa, kuten liikehuoneistoissa, virastotiloissa ja kokoushuoneissa. Jo yksityisyyttä

loukkaavan kuvaamisen yritys tai suunnittelu on rangaistavaa. Kuvattavan vapaaehtoisella suostumuksella lähtökohtaisesti kielletty kameravalvonta voi muuttua sallituksi. Tästä on kuitenkin sovittava etukäteen yhteistoiminta- ja kuulemismenettelyssä ja työnantajan on määriteltävä työntekijöihin kohdistuvan teknisen valvonnan käyttötarkoitus ja käytettävät menetelmät sekä luonnollisesti tiedotettava henkilöstöä näistä menetelmistä. (11.)

Ilta-aikaan tapahtuva toimistotilojen kameravalvonta on mahdollista toteuttaa ja perustella omaisuuden suojaamisella ja rikosten ennaltaehkäisyllä ja jo tapahtuneen rikoksen selvittämisellä. Kohdeyritys teki päätöksen kameravalvonnan lisäämisestä sisätiloihin. Kameravalvonnan kohdistuessa sisäänkäynteihin ei ketään yksittäistä henkilöä aseteta teknisen valvonnan kohteeksi. Kameravalvonta perustellaan toimitilojen suojaamisella, ja koska henkilöstön henkilökohtaisia työpisteitä ei kuvata, menee valvonnan toteutus läpi ilmoitusluontoisena asiana ja kameravalvonnasta ilmoittavat kyltit riittävät, eikä yksittäisen työntekijän suostumusta tarvita.

4.4 Puhtaan pöydän ja puhtaan näytön periaate

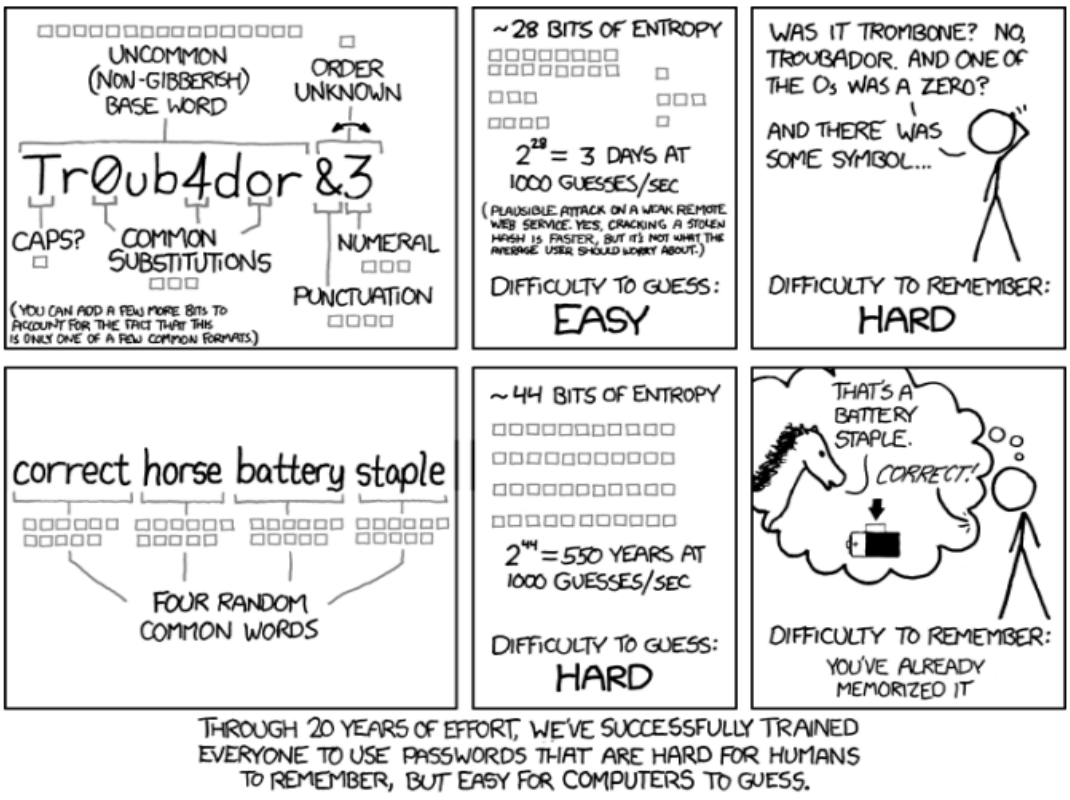
Puhtaan pöydän ja puhtaan näytön periaatetta ei noudateta kohdeyrityksessä tarvittavalla vakavuudella ja huolellisuudella, vaikkakin asiaa koskeva politiikka on käytössä. Syy siihen, ettei periaatteita noudateta, on selvästi ohjeistuksen puutteellisuus ja vajavainen tiedotus.

Nimikin jo sanoo, mistä periaatteissa on kysymys, ja ne voivat vaikuttaa hyvinkin itsestään selviltä. Tästä syystä niiden ydinidea ja vaadittava vakavuus unohtuu helposti. Työntekijän työpisteellä voi vierailla ulkopuolisia henkilöitä työkavereista siivoojaan tai asiakkaaseen. Luottamuksellista tietoa voi pahimmillaan vuotaa jo yhdellä silmäyksellä, mikäli dokumentteja lojuu ympäriinsä työpisteellä. Myös dokumenttien kuvaaminen onnistuu nopeasti ja huomaamattomasti, jos niitä ei säilytetä varmassa ja turvallisessa paikassa. Jokaisella kohdeyrityksen työntekijällä on työpisteellään lukittava kaappi tai laatikosto tätä tarkoitusta varten. Ainoa tarvittava toimenpide näiden periaatteiden saattamiseksi standardin vaatimalle tasolle on asiasta tiedottaminen ja ohjeistuksen teroitus.

Myös hyvää salasanakäytäntöä on syytä tarkentaa kohdeyrityksessä. Salasanaa ei tulisi lähtökohtaisesti koskaan kirjoittaa ylös, kertoa kenellekään tai lähettää sitä sähköpostilla. Salasana tulisi siis joko opetella ulkoa ja painaa mieleen tai vaihtoehtoisesti käyttää salasanan hallintaohjelmaa, jolla voi generoida satunnaiset ja riittävän vahvat salasanat eri palveluihin. Käyttäjän muistettavaksi jää ainoastaan pääsalasana itse hallintaohjelmaan.

Salasanasuositukset ovat muuttuneet vuosien varrella. Vielä muutama vuosi sitten pidettiin hyvänä käytäntönä valita sanakirjasta sana ja muuttaa esim. vokaalit numeroiksi siten, että salasana on edelleen muistettavissa, muttei ole suoraan löydettävissä sanakirjasta. Esimerkiksi: t13t0turv4. Tutkimukset kuitenkin osoittavat, että tällainen salasana on ihmiselle vaikeampi muistaa ja tietokoneelle taas huomattavan helppoa arvata.

Nykyään Valtion tieto- ja viestintätekniikkakeskus suosittelee salasanalauseiden käyttöä. Tässä käytännössä valitaan useampi tavallinen sanakirjasana ja erotetaan ne välilyönneillä. Ihmiselle tällaisen salasanan muistaminen on huomattavan helppoa verrattuna numero-kirjanyhdistelmiin ja tietokoneen näkökulmasta oikean yhdistelmän löytäminen vaikeutuu monikymmenkertaisesti. Ensimmäisen esimerkin kaltaisen salasanan murtamiseen menee tietokoneohjelmalta keskimäärin noin 3 päivää, kun arvaustiheys on 1000 arvausta sekunnissa. Jälkimmäisen esimerkin mukaisen salasanalauseen, joka koostuu neljästä tavallisesta sanakirjasanasta murtamiseen, kuluu arviolta 550 vuotta samalla arvaustiheydellä. Salasanalause on siis ylivertainen vaihtoehto tutumpaan käytäntöön verrattuna. (12.)



Kuva 3. Salasanalauseen ylivertaisuus

5 Yhteenveto

Tämän opinnäytetyön tavoitteena oli tuottaa suunnitelma, jonka avulla kohdeyrityksen fyysinen tietoturva saadaan vastaamaan ISO/IEC 27001-standardissa määriteltyä tasoa. Tavoitteeseen päästiin suurelta osin. Joidenkin kehityskohtien korjaus ja toimintatapojen muuttaminen vievät aikaa, mutta tässä opinnäytetyössä esitellyin toimenpitein ne on mahdollista saattaa standardissa esitetylle tasolle.

Opinnäytetyössä kartoitettiin kohdeyrityksen fyysisen tietoturvan nykytilanne ja selvitettiin puutteet ja kehityskohdat standardiin nähden. Insinöörityöprosessin aikana opittiin, ettei kaikkia riskejä pystytä eliminoimaan, vaan kaikkein tärkeintä on olla tietoinen riskeistä ja dokumentoida toimenpiteet ja toimintatavat riskien välttämiseksi sekä jo tapahtuneiden vahinkojen elpymistoimet.

Tätä työtä hyödynnetään kohdeyrityksen valmistautuessa viralliseen auditointiin, joka johtaa sertifikaatin saamiseen. Sertifikaatin saaminen ei kuitenkaan ole kaikki kaikessa, vaan kokonaisvaltainen työ- ja toimintatapojen kehittyminen, sekä näiden uusien käytäntöjen saattaminen osaksi yrityksen toimintaa. Tässä työssä käsiteltyjä aihealueita tullaan jalkauttamaan organisaation jokapäiväiseen toimintaan ja näin kohdeyritys kehittyy niin markkinatoimijana kuin työnantajanakin.

Lähteet

1 Verkkokurssi. 2021. TestOut Ethical Hacker Pro - Physical Security

2 Peiponen, Pasi. 2018. Ylen toimittaja testasi tärkeiden yritysten ja laitosten turvallisuutta. Verkkoaineisto. <https://yle.fi/uutiset/3-10320853> 25.7.2018. Luettu 12.3.2022.

3 YLE. 2018. Paneelikeskustelu. <https://areena.yle.fi/1-50005710?>

4 The seven layers of IT security. 2021. Verkkoaineisto. ManhattanTech-Support.com <https://www.manhattantechsupport.com/blog/the-seven-layers-of-it-security> 21.1.2021 Luettu 17.1.2022.

5 Turvallinen tuotekehitys: Kohti hyväksyntää. 2018. Verkkoaineisto. Liikenne- ja viestintä virasto. Kyberturvallisuuskeskus. <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Turvallinen_tuotekehitys_Suomi_J003_2018.pdf> Luettu 14.10.2021.

6 Mikä on leasingsopimus? 2022. Verkkoaineisto. Minilex. <https://www.minilex.fi/a/mik%C3%A4-on-leasingsopimus> Luettu 15.3.2022.

7 Climer, Shioban; Khan, Mishaal. 2020. What Are The 7 Layers Of Security? A Cybersecurity Report. Verkkoaineisto. <https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security> 14.7.2020 Luettu 5.11.2021.

8 Huttunen, Elina. 2019. Riskienhallinta tietoturvassa. Verkkoaineisto. <https://sfs.fi/riskienhallinta-tietoturvassa> 14.2.2019 Luettu. 18.2.2022.

9 Kenton, Will. 2020. Gap Analysis. Verkkoaineisto. <https://www.investopedia.com/terms/g/gap-analysis.asp> 27.2020. Luettu 7.11.2022.

10 Mitä hyötyjä tietoturva-auditointi tuo yritykselle? 2022. Verkkoaineisto. 2NS Second Nature Security. <https://www.2ns.fi/palvelut/testaus-ja-auditointi> Luettu 22.11.2021.

11 Rikoslaki ja kameravalvonta. 2022. Verkkoaineisto. Minilex. <https://www.minilex.fi/a/rikoslaki-ja-kameravalvonta> Luettu 16.3.2022.

12 Simula, Tommi; Janhunen, Kimmo. 2022. Verkkoaineisto. Valtion tieto- ja viestintäkeskus. <https://vm.fi/documents/10623/5390546/JHDTTV5/79764e6d-84e1-497b-b3d6-5ad57fe49e8b> Luettu 13.1.2022.