Opinnäytetyö (AMK)

Tietojenkäsittely

2023

Eetu Kaasalainen

Sovellusten käyttöönotto yrityksessä

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tietojenkäsittely

Syksy 2023 | 28 sivua

Eetu Kaasalainen

Sovellusten käyttöönotto yrityksessä

Opinnäytetyössä selvitettiin, mitä ovat tietoturva ja tietosuoja, miksi ne ovat tärkeitä, sekä niihin liittyvät tärkeimmät ja oleellisimmat standardit. Työssä selvitettiin ja esiteltiin myös, mitä huomioitavia asioita sovelluksen käyttöönotossa on tietoturvan ja tietosuojan kannalta.

Työssä kehitettiin sovelluksen käyttöönotto prosessia kohdeyritykselle, joka oli havainnut prosessissa epäselvyyttä ja mahdollisia tietoturva- ja tietosuoja-aukkoja.

Prosessia kehitettiin selkeyttämällä prosessin kulkua ja täten tekemällä siitä virtaviivaisemman, nopeamman ja tietoturvallisemman. Prosessiin kehitettiin myös avuksi uusi työkalu, jonka avulla tietoturvatiimi voi arvioida uuden halutun sovelluksen riskiä ja työkalun avulla päättää voiko sovelluksen käyttöönottaa vai ei.

Asiasanat:

tietoturva, tietosuoja, standardi, sovellus

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Information Technology

Fall 2023 | 28 pages

Eetu Kaasalainen

Application deployment in an organization

The objective of the thesis was to provide a comprehensive understanding of information security and data protection, elucidating their significance and the paramount standards associated with them. An additional objective was to highlight the primary concerns and issues that arise during the implementation of a new application with respect to security and data protection.

For this thesis, An improved application deployment process was developed for the target company after identifying ambiguities and potential security and data protection gaps in their existing system.

The process was improved by clarifying the process flow, therefore making it more streamlined, faster, and more secure. A new tool was also developed to help the process, allowing the cybersecurity team to evaluate the risk of the new desired application and to decide whether it could be deployed security wise.

Keywords:

data security, data privacy, standard, application

SISÄLLYS

Kuvat

Lyhenteet

CIA	Confidentiality, Integrity, Availability, Luotettavuus, Eheys ja Saatavuus
GDPR	General Data Protection Regulation, Yleinen tietosuoja-asetus
ISO27001	Tietoturvastandardi
IDS	Intrusion Detection System, Tunkeilijan havaitsemisjärjestelmä
MFA	Multi-Factor Authentication, Monivaiheinen tunnistautuminen
ITIL	Information Technology Infrastructure Library, Prosessikehys
ITSM	IT Service Management, IT-palvelun hallinta

1 Johdanto

Nykyaikaisella digitaalisella aikakaudella tieto on korvaamaton voimavara, ja sen turvallisuuden varmistaminen on jokaisen organisaation velvollisuus. Tehokas tietoturvastrategia ei ainoastaan suojaa uhkia vastaan, vaan myös parantaa organisaation mainetta, varmistaa sääntöjen noudattamisen ja edistää sen luottamusta. Pohjimmiltaan tietoturva ja tietosuoja ei ole vain tekninen vaatimus vaan olennainen osa organisaation kokonaisstrategiaa ja visiota. Organisaatiot, jotka asettavat kyberturvallisuuden etusijalle, pystyvät menestymään nykyisellä aikakaudella ja turvaamaan omaisuutensa, maineensa ja menestyksensä.

Opinnäytetyön tarkoitus on kehittää kohdeyrityksen sovelluksen käyttöönotto prosessia siten, että prosessista tehdään selkeämpi, suoraviivaisempi ja turvallisempi niin tietoturvan kuin tietosuojankin kannalta.

Opinnäytetyö on toteutettu toimeksiantona suomalaiselle ICT-yritykselle. Yritys havaitsi puutteita organisaation sovelluksen käyttöönottoprosessissa ja halusi parantaa sitä tekemällä siitä turvallisemman tietoturvan ja tietosuojan kannalta tekemällä prosessista myös samalla virtaviivaisemman ja täten tehokkaamman.

Opinnäytetyön teoriaosuudessa käydään läpi tietoturvan ja tietosuojan tarkoitus ja merkitys sekä käydään läpi myös tärkeimmät niihin liittyvät standardit ja käytännöt. Osuudessa käydään läpi myös sovelluksen käyttöönotossa tärkeimmät huomioonotettavat asiat tietoturvan ja tietosuojan näkökulmasta.

Käytännönosuudessa keskitytään prosessin kehittämiseen siten, että siitä tehdään parempi tietoturvan ja tietosuojan kannalta, sekä samalla tehden siitä yksinkertaisempi, kontrolloidumpi ja täten myös tehokkaampi jo käytössä olevilla työkaluilla ja toimenpiteillä. Prosessia varten suunnitellaan ja kehitetään uusi arviointityökalu, jolla käyttöönotettavan sovelluksen tietoturvallisuus ja tietosuojallisuus varmistetaan, mikäli se ei jo olemassa olevalla tavalla onnistu.

2 Tietoturva

Tietoturva on tietojen suojaamista erilaisilta riskeiltä toteuttamalla strategioita, joilla estetään tietojen luvaton käyttö, luovuttaminen, häirintä, muuttaminen tai tuhoaminen. Sillä varmistetaan järjestelmien käsittelemien, tallentamien tai siirtämien tietojen turvallisuus, jotka voivat olla digitaalisessa tai fyysisessä muodossa. Henkilökohtaiset, taloudelliset ja arkaluonteiset tai salassa pidettävät tiedot kuuluvat kaikki suojauksen piiriin. Tietoturva edellyttää monialaista lähestymistapaa, jossa käytetään ihmisiä, prosesseja ja teknologiaa mahdollisimman tehokkaaseen toimintaan. (rashi_garg, 2023)

Tehokas tietoturvastrategia kattaa kaikki tietoturvan osa-alueet teknologian, politiikat ja menettelyt, sekä ihmiset. Se edellyttää myös jatkuvaa seurantaa, arviointia ja mukauttamista uusien uhkien ja haavoittuvuuksien torjumiseksi. (rashi_garg, 2023)

Tietoturvaa tarkoitus on arvokkaiden ja salassa pidettävien tietojen suojaamiseen erilaisilta uhkilta, kuten varkauksilta, vakoilulta ja tietoverkkorikollisuudelta. Se on elintärkeää tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi riippumatta siitä, ovatko tiedot tallennettu digitaalisesti vai jossain muussa muodossa, kuten paperiasiakirjoina. (rashi_garg, 2023)

Tässä ovat tärkeimmät syyt, miksi tietoturva on ratkaisevan tärkeää:

- Arkaluonteisten tietojen suojaaminen tapahtuu tiettyjen tietoturvatoimien avulla, joilla pyritään estämään sitä, etteivät luvattomat tahot pääse käsiksi arkaluonteisiin tietoihin, kuten henkilö- ja taloudellisiin tietoihin, liikesalaisuuksiin sekä hallituksen ja armeijan turvaluokiteltuihin tietoihin, eivätkä ne pääse paljastumaan tai muuttumaan.
- Riskien vähentämistä yritetään tehostaa tietoturvaprotokollien käyttöönotolla. Organisaatiot voivat vähentää verkkouhkiin ja muihin tietoturvaloukkauksiin liittyviä riskejä, mikä sisältää tietomurtojen, palvelunestohyökkäysten ja muiden haitallisten toimintojen todennäköisyyden vähentämisen.
- Lainsäädännön noudattaminen monilla toimialoilla on erityisen tärkeää, sillä on olemassa erilaisia määräyksiä, jotka koskevat arkaluonteisten tietojen suojaamista. Tietoturva auttaa noudattamaan näitä sääntöjä, mikä vähentää oikeudellisten seuraamusten ja vastuun mahdollisuutta. (rashi_garg, 2023)

Maineen suojaaminen on erittäin tärkeää, sillä tietoturvaloukkaukset voivat vahingoittaa organisaation mainetta ja johtaa liiketoiminnan menetyksiin. Vankka tietoturva voi auttaa säilyttämään yrityksen maineen vähentämällä tietoturvaloukkausten todennäköisyyttä. (rashi_garg, 2023)

Liiketoiminnan jatkuvuuden varmistaminen on tärkeää. Tietoturva auttaa ylläpitämään kriittisiä liiketoimintoja myös tietoturvaloukkauksen aikana. Tähän sisältyy keskeisten järjestelmien ja tietojen käyttömahdollisuuksien säilyttäminen ja häiriöiden vaikutusten minimointi. (rashi_garg, 2023)

Tietoturvaohjelmat rakentuvat yleensä kolmen keskeisen tavoitteen ympärille, jotka tunnetaan yleisesti nimellä CIA (Luottamuksellisuus, Eheys, Saatavuus) (rashi_garg, 2023)

2.1 Luottamuksellisuus

Luottamuksellisuus tarkoittaa organisaation pyrkimyksiä varmistaa, että tiedot pysyvät salassa ja yksityisinä. Tätä varten tietoihin pääsyä on valvottava, jotta estetään tietojen luvaton jakaminen. Luottamuksellisuuden säilyttämisen keskeinen osa on varmistaa, että henkilöitä, joilla ei ole asianmukaista valtuutusta, estetään pääsemästä käsiksi niille kuulumattomiin tietoihin. Vastaavasti on varmistettava myös se, että niillä, joilla on oltava pääsy tietoihin, on tarvittavat oikeudet. Esimerkiksi niiden, jotka työskentelevät organisaation käyttäjähallinnan parissa, pitäisi päästä käsiksi organisaatiossa työskentelevien henkilöiden käyttäjätileihin ja tietoihin. Suurimmalle osalle muista työntekijöistä ei kuitenkaan myönnetä käyttöoikeuksia. Jotta voidaan varmistaa, että näitä käytäntöjä noudatetaan, on otettava käyttöön tiukat rajoitukset, joilla rajoitetaan sitä, kuka voi nähdä tiettyjä tietoja. Luottamuksellisuus voi vaarantua monella tavalla. Kyse voi olla suorista hyökkäyksistä, joilla pyritään saamaan pääsy järjestelmiin, joihin hyökkääjällä ei ole oikeuksia. Hyökkääjä voi myös yrittää suoraan tunkeutua sovellukseen tai tietokantaan, jotta hän voi viedä tietoja tai muuttaa niitä. Luottamuksellisuutta voi suojata luokittelemalla ja merkitsemällä tiedot, ottamalla käyttöön pääsynvalvontakäytännöt ja salaamalla tiedot sekä käyttämällä monivaiheista tunnistautumista (MFA). On myös suositeltavaa varmistaa, että kaikilla organisaation työntekijöillä on tarvittava koulutus ja tiedot vaarojen tunnistamiseksi ja välttämiseksi. (Fortinet, 2023)

2.2 Eheys

Eheys tarkoittaa sen varmistamista, että tietoja ei ole peukaloitu ja että niihin voidaan näin ollen luottaa eli tieto on oikeaa, aitoa ja luotettavaa. Verkkokaupan asiakkaat esimerkiksi odottavat, että tuote- ja hintatiedot ovat oikeita ja että tuotteiden määrää, hintaa, saatavuutta ja muita tietoja ei ole muutettu tilauksen tekemisen jälkeen. Pankkiasiakkaiden on voitava luottaa siihen, että heidän pankkitietojaan ja tilisaldojaan ei ole peukaloitu. Eheyden varmistaminen edellyttää tietojen suojaamista käytön aikana, siirron aikana (esimerkiksi sähköpostia lähetettäessä tai tiedostoa ladattaessa) ja silloin, kun ne on tallennettu kannettavaan tietokoneeseen, kannettavaan tallennuslaitteeseen, tietokeskukseen tai pilvipalveluun. Kuten luottamuksellisuus myös eheys voi vaarantua hyökkääjän päästessä peukaloimaan IDS-järjestelmiä, muokkaamaan konfigurointitiedostoja tai muuttamaan järjestelmän lokitietoja välttääkseen hyökkäyksen havaitsemisen. Eheys voi vaarantua myös tahattomasti inhimillisen erehdyksen, huolimattomuuden tai riittämättömien käytäntöjen, menettelyjen ja suojausmekanismien puuttumisen kautta. (Walkowski, 2019)

2.3 Saatavuus

Vaikka tiedot pidettäisiin luottamuksellisina ja niiden eheys säilytettäisiin, ne ovat usein hyödyttömiä, elleivät ne ole organisaation työntekijöiden ja heidän asiakkaidensa

saatavilla. Tämä tarkoittaa, että järjestelmien, verkkojen ja sovellusten on toimittava asianmukaisesti silloin ja siten, kuten niiden pitäisi. Henkilöiden, joilla on pääsy tiettyihin tietoihin, on myös voitava käyttää niitä tarvittaessa, eikä tietojen saaminen saisi viedä kohtuuttomasti aikaa. Jos esimerkiksi sähköt katkeavat, eikä käytössä ole oikeanlaista palautusjärjestelmää, jonka avulla käyttäjät pääsevät takaisin kriittisiin järjestelmiin, saatavuus vaarantuu. Myös luonnonkatastrofi, kuten tulva tai jopa kova lumimyrsky voi estää käyttäjiä pääsemästä toimistoon, joka voi keskeyttää heidän työasemiensa ja muiden laitteidensa, käytettävyyden sillä työasemat ja laitteet tarjoavat liiketoimintakriittisiä tietoja tai sovelluksia. Saatavuus voi vaarantua myös tahallisten sabotaasitekojen, kuten palvelunestohyökkäysten (DoS) tai lunnasohjelmien käytön vuoksi. Saatavuuden varmistamiseksi organisaatiot voivat käyttää redundantteja verkkoja, palvelimia ja sovelluksia. Nämä voidaan ohjelmoida niin, että ne ovat käytettävissä, kun ensisijainen järjestelmä on häiriintynyt tai rikkoutunut. Käytettävyyttä voi parantaa myös pysymällä ajan tasalla ohjelmistopakettien ja tietoturvajärjestelmien päivityksistä. Tällä tavoin teet sovelluksen toimintahäiriön tai suhteellisen uuden uhan tunkeutumisen järjestelmään epätodennäköisemmäksi. Varmuuskopioinnit ja täydelliset palautussuunnitelmat auttavat yritystä myös palauttamaan käytettävyyden nopeasti kielteisen tapahtuman jälkeen. (Fortinet, 2023)

2.4 Kiistämättömyys

Tietoturvan CIA-kolmikon (luottamuksellisuus, eheys, saatavuus) lisäksi toinen keskeinen periaate on kiistämättömyys. Sen avulla varmistetaan, että kumpikaan tapahtuman tai viestinnän osapuolista ei voi kieltää osallistumistaan. Tyypillinen esimerkki tästä on salaus, jossa viesti vastaa lähettäjän yksityisellä avaimella allekirjoitettua digitaalista allekirjoitusta, joka todistaa, että vain lähettäjä on voinut lähettää viestin muuttamatta sitä lähetyksen aikana. (rashi_garg, 2023)

Kaksi keskeistä kiistämättömyyden vaatimusta ovat tietojen eheys ja autenttisuus. Autenttisuus varmistaa käyttäjien henkilöllisyyden ja takaa, että kaikki vastaanotetut syötteet ovat peräisin luotettavasta lähteestä, mikä takaa pätevän ja autenttisen lähetyksen esimerkiksi, kun lähettäjä lähettää viestin, jossa on digitaalinen allekirjoitus, joka on luotu viestin hash-arvon ja yksityisen avaimen avulla, vastaanottaja purkaa allekirjoituksen julkisella avaimella ja tuottaa hash-arvon. Jos tämä arvo vastaa viestin hash-arvoa, lähetystä pidetään pätevänä ja aitona. (rashi_garg, 2023)

Vastuullisuus on toinen tärkeä periaate, joka edellyttää, että yksikön toimet voidaan jäljittää yksiselitteisesti kyseiseen yksikköön. Näin varmistetaan, että vain valtuutetut henkilöt voivat muuttaa tietoja. Esimerkiksi organisaatiossa tietyt osastot käsittelevät tietomuutoksia saatuaan ylemmän viranomaisen vahvistamat pyynnöt. Tämä prosessi tallentaa aikaleimat sekä käyttäjän tiedot, mikä mahdollistaa toimien yksilöllisen jäljitettävyyden. (rashi_garg, 2023)

3 Tietosuoja

Tietosuoja tarkoittaa yksilön oikeutta hallita sitä, miten, milloin ja missä määrin hänen henkilökohtaisia tietojaan jaetaan tai luovutetaan muille. Tällaisia henkilötietoja voivat olla esimerkiksi nimi, maantieteellinen sijainti, yhteystiedot sekä verkko- tai fyysinen toiminta. Samoin kuin yksityisyyden suoja henkilökohtaisissa keskusteluissa, monet verkkokäyttäjät haluavat rajoittaa tai estää tietynlaisten henkilötietojen keräämisen. (Cloudflare, Data Privacy, 2023)

Ajansaatossa lisääntyneessä internetin käytössä yksityisyyden merkitys on kasvanut samassa suhteessa. Digitaaliset alustat, kuten verkkosivustot, sovellukset ja sosiaalisen median verkostot, edellyttävät usein käyttäjien henkilötietojen keräämistä ja säilyttämistä palvelujensa tarjoamiseksi. Tietyt sovellukset ja alustat saattavat kuitenkin ylittää käyttäjien odotukset tietojen keräämisestä ja käytöstä, mikä heikentää käyttäjien yksityisyyttä enemmän kuin he odottivat. Jotkin muut alustat ja sovellukset eivät ehkä kykene varmistamaan keräämiensä tietojen riittävää suojaamista, mikä voi johtaa mahdollisiin tietomurtoihin, jotka vaarantavat käyttäjien yksityisyyden. (Cloudflare, Data Privacy, 2023)

3.1 Tietosuojan tärkeys

Monilla oikeusalueilla yksityisyyttä pidetään olennaisena ihmisoikeutena, ja tietosuojasäädökset puolustavat tätä etuoikeutta. Tietosuojan merkitys on myös siinä, että se edistää sitoutumista verkkoon; yksilöiden on uskottava, että heidän yksityisiä tietojaan käsitellään vastuullisesti. Yritykset käyttävät tietoturvastrategioita vakuuttaakseen asiakkailleen ja käyttäjilleen, että heidän henkilötietojensa käsittelyyn voi luottaa. Henkilökohtaisia tietoja voidaan käyttää hyväksi monin tavoin, jos niitä ei ole suojattu asianmukaisesti tai jos yksilöillä ei ole mahdollisuutta valvoa niiden käyttöä. (Cloudflare, Data Privacy, 2023)

Petostentekijät voivat käyttää henkilötietoja huijauksiin tai uhreiksi joutumiseen. Organisaatiot saattavat myydä henkilötietoja markkinoijille tai muille ulkopuolisille tahoille ilman käyttäjän lupaa, jolloin käyttäjä voi saada ei toivottuja tarjouksia tai mainoksia. Henkilön toimintojen seuranta ja valvonta voi estää hänen sananvapauttaan, erityisesti autoritaaristen hallintojen yhteydessä. (Cloudflare, Data Privacy, 2023)

Yksilöiden kannalta tällaiset olosuhteet voivat johtaa haitallisiin seurauksiin. Yrityksille tällaiset tapaukset voivat vahingoittaa niiden mainetta peruuttamattomasti ja ne voivat johtaa taloudellisiin seuraamuksiin, viranomaispakotteisiin ja muihin oikeudellisiin seuraamuksiin. Yksityisyyden suojan loukkausten konkreettisten seurausten lisäksi monet yksilöt ja kansakunnat ovat sitä mieltä, että yksityisyyden suojan arvo on luontainen. Yksityisyyden suoja on vapaan yhteiskunnan kannalta välttämätön perusihmisoikeus, joka on samankaltainen sananvapauden kanssa. (Cloudflare, Data Privacy, 2023)

Teknologian kehittymisen myötä tiedonkeruu- ja seurantajärjestelmät ovat parantuneet. Hallitukset ovat maailmanlaajuisesti alkaneet säätää lainsäädäntöä, jossa määrätään, minkä tyyppisiä tietoja käyttäjistä voidaan kerätä, miten näitä tietoja voidaan käyttää ja miten tietojen tallentamista ja suojaamista koskevia ohjeita annetaan. Mainitsemisen arvoisia yksityisyyden suojaa sääteleviä keskeisiä regulaatioita on muun muassa GDPR (Yleinen tietosuoja-asetus). (Cloudflare, Data Privacy, 2023)

4 Tietoturva- ja Tietosuojastandardit

Tietoturvastandardit ovat joukko ohjeita ja käytäntöjä, joita organisaatiot voivat tai joita organisaatioiden on käytettävä parantaakseen kyberturvallisuuttaan.

Organisaatiot voivat käyttää kyberturvallisuuden standardeja, joiden avulla ne voivat tunnistaa ja toteuttaa asianmukaisia toimenpiteitä järjestelmiensä ja tietojensa suojaamiseksi kyberuhkilta. Standardit voivat myös antaa ohjeita siitä, miten kyberturvallisuuspoikkeamiin vastataan ja miten niistä toivutaan

Kyberturvallisuuden viitekehyksiä voidaan yleisesti soveltaa kaikkiin organisaatioihin niiden koosta, toimialasta tai sektorista riippumatta. Tässä luvussa kerrotaan yleisistä kyberturvallisuuden standardeista, jotka muodostavat vahvan perustan mille tahansa kyberturvallisuusstrategialle.

Tietoturva, kyberturvallisuus ja yksityisyyden suoja ovat nykyisessä tilanteessa yrityksille ja organisaatioille kriittisiä. ISO/IEC 27000 -standardisarjalla on ratkaiseva rooli niiden turvallisuuden ylläpitämisessä määrittelemällä yrityksen ISMS:n vaatimuksia tarjoamalla suosituksia tietoturvallisuuden riskeihin, hallintaan ja kontrollointiin.

4.1 Yleinen tietosuoja-asetus

GDPR (General Data Protection Regulation) on Yleinen tietosuoja-asetus, joka tuli voimaan 25. toukokuuta 2018 ja se on perusteellinen tietosuojaan liittyvä lainsäädäntö, joka tarjoaa rakenteen henkilötietojen keräämiselle, käsittelylle, tallentamiselle ja siirtämiselle. Laki edellyttää, että kaikkia henkilötietoja on hallinnoitava turvallisesti ja se sisältää rangaistustoimenpiteitä yrityksille, jotka rikkovat näitä määräyksiä. Se antaa myös yksilöille lukuisia henkilötietoihin liittyviä oikeuksia. (Cloudflare, GDPR, 2023)

Tietosuojan merkitys on noussut etualalle teknologian kehittymisen ja tiedonkeruun yleistymisen myötä. Yleistä tietosuoja-asetusta pidettiin sen voimaan tullessa kattavimpana tietosuojalakina. Siihen sisällytettiin erilaisia tietosuojasäännöksiä kaikkialta Euroopan unionista (EU) ja laajennettiin näiden säännösten lainkäyttövaltaa kattamaan EU:n ulkopuoliset organisaatiot, jos ne hallinnoivat EU:n alueella kerättyjä henkilötietoja. (Cloudflare, GDPR, 2023)

Yleistä tietosuoja-asetusta sovelletaan yleisesti kaikkiin yrityksiin tai organisaatioihin niiden maantieteellisestä sijainnista riippumatta, kunhan ne tarjoavat tavaroita ja palveluja EU:ssa oleville henkilöille tai seuraavat heidän käyttäytymistään EU:ssa. (Cloudflare, GDPR, 2023)

Yleisessä tietosuoja-asetuksessa laajennettiin henkilötietojen määritelmää siten, että se kattaa kaikki erotettavissa olevaan luonnolliseen henkilöön liittyvät yksityiskohdat. Tähän sisältyvät selvästi henkilökohtaiset tiedot, kuten henkilön nimi ja osoite, mutta siinä otetaan huomioon myös muut tiedot, joita voidaan käyttää henkilön

tunnistamiseen, kuten IP-osoite ja internetin selailuistuntoon sidotut evästetunnisteet. (Cloudflare, GDPR, 2023)

GDPR on maailman tiukin yksityisyyttä ja turvallisuutta koskeva laki, ja se rankaisee sen rikkojia ankarasti määräämällä ankaria sakkoja ja rangaistukset voivat olla jopa kymmeniä miljoonia euroja. (Cloudflare, GDPR, 2023)

4.2 ISO/IEC-standardit

Tietoturva, kyberturvallisuus ja yksityisyyden suoja ovat nykyisessä tilanteessa yrityksille ja organisaatioille kriittisiä. ISO/IEC 27000 -standardisarjalla on ratkaiseva rooli niiden turvallisuuden ylläpitämisessä. (ISO, ISO/IEC 27000 family, 2023)

ISO/IEC 27001 on maailmanlaajuisesti tunnustettu tietoturvallisuuden hallintajärjestelmien (ISMS) ja niihin liittyvien vaatimusten vertailustandardi, joka määrittelee vaatimukset, joita ISMS:n on täytettävä. Yli kymmenessä muussa ISO/IEC 27000 -sarjan standardissa käsitellään parhaita käytäntöjä tietosuojassa ja kyberkestävyydessä. Yhdessä nämä standardit mahdollistavat sen, että kaikkien toimialojen ja erikokoiset organisaatiot voivat turvallisesti hallita omaisuutta, kuten taloudellisia tietoja, fyysistä omaisuutta, työntekijöiden tietoja ja kolmansien osapuolten jakamaa tietoa. (ISO, ISO/IEC 27001, 2023)

Kyberturvallisuuden uhkien lisääntyessä ja uusien vaarojen noustessa jatkuvasti pintaan kyberriskien hallinta voi tuntua pelottavalta tai jopa ylitsepääsemättömältä tehtävältä. ISO/IEC 27001 -standardi auttaa organisaatioita tiedostamaan nämä riskit ja tunnistamaan ja torjumaan haavoittuvuudet aktiivisesti. (ISO, ISO/IEC 27001, 2023)

ISO/IEC 27001 -standardi kannustaa ottamaan tietoturvan kokonaisvaltaisesti huomioon ja tarkastelemaan yksilöitä, menettelyjä ja teknologiaa. Kun tietoturvallisuuden hallintajärjestelmä on rakennettu tämän standardin mukaisesti, se toimii välineenä riskien käsittelyssä, kyberkestävyyden vahvistamisessa ja toiminnallisen ylivoimaisuuden saavuttamisessa. (ISO, ISO/IEC 27001, 2023)

ISO 27701 -standardin tavoitteena on tarjota maailmanlaajuinen näkökulma yksityisyyden suojaan, joka on tietoturvan keskeinen osa-alue. Standardi otettiin käyttöön elokuussa 2019. (isms.online, 2023)

ISO 27701 on tietosuojaa koskeva kehys, joka laajentaa ISO 27001 -standardia. Se tarjoaa viimeisimmät tietosuojaa koskevat parhaat käytännöt ja ohjaa organisaatioita GDPR:n ja muiden tietosuojaa/yksityisyyden suojaa koskevien sääntöjen ja lakien noudattamiseen tarvittaviin käytäntöihin ja menettelyihin. (isms.online, 2023)

Tietosuojan hallintajärjestelmästandardina ISO 27701 tarjoaa laajan joukon toiminnallisia tarkistuslistoja, jotka voidaan mukauttaa lukuisiin säännöksiin, myös GDPR:ään. Yritykset sovittavat toimintalinjojaan, prosessejaan, pöytäkirjojaan ja toimintojaan näihin tarkistuslistoihin, jotka sisäiset ja ulkoiset tarkastajat sitten

tarkastavat. Auditointitulokset toimivat kattavana todisteena standardin noudattamisesta. ISO 27701 auttaa yrityksiä ylläpitämään tehokasta yksityisyyden suojaa ja tietoturvaa koskevaa järjestelmää ja vähentämään samalla yksityisyyden suojaan liittyviä riskejä. (isms.online, 2023)

ISO 27701 toimii kuluttajille, ulkoisille organisaatioille ja sisäisille sidosryhmille vahvana osoituksena siitä, että käytössä on vankat mekanismit tietojen suojaamiseksi ja GDPR:n ja muiden tietosuojalakien noudattamisen varmistamiseksi. (isms.online, 2023)

Koska ISO 27701 on ISO 27001 -standardin laajennus, ISO 27701 -sertifikaatin saavuttamiseen pyrkivillä organisaatioilla on oltava ISO 27001 -standardi tai niiden on otettava käyttöön molemmat standardit samanaikaisesti. (isms.online, 2023)

4.3 NIST SP 800-53

NIST SP 800-53 auttavat organisaatioiden tietojärjestelmien tietoturva- ja yksityisyydensuojatoimenpiteiden kanssa. Niiden tarkoituksena on suojella toimintatapoja, yksilöitä, muita yhteisöjä ja jopa koko maata monilta erilaisilta uhkilta ja riskeiltä. (NIST, 2023)

Nämä riskit voivat vaihdella vihamielisistä hyökkäyksistä ja inhimillisistä virheistä luonnonkatastrofeihin, rakenteellisiin häiriöihin, ulkomaan tiedustelun uhkiin ja yksityisyyden suojan loukkauksiin. Tarjotut toimenpiteet ovat mukautuvia ja niitä voidaan räätälöidä organisaation erityistarpeisiin sopiviksi ja niitä käytetään osana organisaation kattavaa riskinhallintaprosessia. (NIST, 2023)

Toimenpiteet vastaavat erilaisia vaatimuksia, jotka johtuvat liiketoiminta- ja tehtävätavoitteista sekä oikeudellisista velvoitteista, toimeenpanokäskyistä, direktiiveistä, määräyksistä, politiikasta, standardeista ja ohjeista. (NIST, 2023)

Valvontatoimien kattavassa luettelossa otetaan huomioon sekä toiminnallisuus (valvontamekanismien ja valvonta toimintojen tehokkuus), sekä varmuus (luottamuksen taso valvontatoimien tarjoaman suojan suhteen) turvallisuuden ja yksityisyyden suojan näkökulmista. Keskittymällä näihin molempiin näkökohtiin varmistetaan, että tietotekniikkatuotteiden ja niistä riippuvaisten järjestelmien luotettavuuteen voidaan luottaa. (NIST, 2023)

5 Sovelluksen käyttöönotto

Nykypäivän digitaalisella aikakaudella sovellusten käyttöönotosta on tullut liiketoiminnan kasvun ja innovoinnin perustekijä. Kun yritykset ottavat käyttöön uusia teknologioita on kuitenkin ensiarvoisen tärkeää varmistaa tietoturva, tietosuoja, yksityisyys ja säännösten ja lakien noudattaminen. Kun sovellusta otetaan käyttöön liiketoimintaympäristössä, on otettava huomioon useita kriittisiä seikkoja, jotta arkaluonteiset tiedot voidaan suojata ja täten säilyttää asiakkaiden ja sidosryhmien luottamus. Tässä opinnäytetyössä perehdytään keskeisiin seikkoihin, jotka yritysten on otettava huomioon sovellusta käyttöönotettaessa, ja keskitytään tietojenkäsittelyyn, tietoturvaan, integrointiin, hallinnollisiin oikeuksiin, tiedonhallintaan kansainvälisissä yhteyksissä ja tietokantojen valintaan.

5.1 Tietojen käsittely ja tietotyyppi

Ennen sovelluksen käyttöönottoa on tärkeää analysoida perusteellisesti sovelluksen käsittelemät henkilötiedot. Selvittämällä perustuuko sovellus pelkästään käyttäjän antamiin tietoihin, kuten käyttäjätunnukseen, joka toimii tunnisteena vai käsitelläänkö siinä arkaluonteisempia tietoja kuten potilas- tai terveystietoja. Käsiteltävien tietojen tyypin ymmärtäminen on ratkaisevan tärkeää asianmukaisten turvatoimien suunnittelussa ja vaatimustenmukaisuusvaatimusten määrittämisessä.

5.2 Tietojen säilyttämiskäytäntö

Selkeän tietojen säilyttämiskäytännön laatiminen on olennaisen tärkeää sen määrittämiseksi, kuinka kauan järjestelmä säilyttää käyttäjätietoja. Hyvin määritellyllä käytännöllä varmistetaan, että tietoja ei säilytetä pidempään kuin on tarpeen ja minimoidaan tarpeettoman tiedon säilyttämiseen liittyvät mahdolliset riskit. Lisäksi läpinäkyvä tietojen säilyttämiskäytäntö voi auttaa rakentamaan luottamusta käyttäjien keskuudessa ja osoittaa organisaation sitoutumisen tietosuojaan.

5.3 Tietojen salaus

Tietoturva on ensiarvoisen tärkeää kaikissa arkaluonteisia tietoja käsittelevissä sovelluksissa. Vankkojen salausprotokollien käyttö auttaa suojaamaan tietoja sekä tallennuksen että siirron aikana. Salaus mahdollistaa ylimääräisen suojakerroksen, joka estää arkaluonteisten tietojen luvattoman käytön, vaikka tietoturvaloukkaus tapahtuisi.

5.4 Tietojen siirto

Jos sovellukseen liittyy tietojen siirtämistä organisaation sisällä tai sen ulkopuolella, on varmistettava, että tiedot siirretään salatussa muodossa. Siirrettiinpä tietoja sitten saman infrastruktuurin sisällä tai lähetettiinpä niitä ulkoisille osapuolille. Salaus varmistaa niiden luottamuksellisuuden, sekä eheyden siirron aikana ja vähentää tietojen sieppaamisen tai manipuloinnin riskiä

5.5 Kirjaaminen ja tarkastusloki

Kattavan lokitusmekanismin käyttöönotto on olennaisen tärkeää sovelluksen sisällä tapahtuvien toimintojen seuraamiseksi. Tarkastusloki auttaa seuraamaan käyttäjän toimia, havaitsemaan mahdolliset tietoturvaloukkaukset ja yksinkertaistamaan tietosuojasäännösten noudattamista. Tapahtuman sattuessa tarkastusloki voi tarjota arvokkaita tietoja, joiden avulla voidaan tunnistaa rikkomuksen lähde ja laajuus.

5.6 Integrointi muiden sovellusten tai järjestelmien kanssa

Varmista sovelluksen integroitumista muihin liiketoimintaympäristön järjestelmiin. Saumaton integraatio helpottaa tiedonvaihtoa, tehostaa työnkulkuja ja parantaa yleistä tehokkuutta. On kuitenkin ratkaisevan tärkeää varmistaa, että kaikki integroidut järjestelmät noudattavat samoja korkeita tietoturvastandardeja haavoittuvuuksien välttämiseksi.

5.7 Hallinnolliset oikeudet

Varmistaa, edellyttääkö sovellus tietyiltä käyttäjiltä järjestelmänvalvojan oikeuksia tiettyjä toimintoja varten. Järjestelmänvalvojan oikeuksien rajoittaminen pienentää luvattoman käytön ja tahattoman tietojenkäsittelyn riskiä ja vähentää näin tietoturvaloukkausten mahdollisuutta.

5.8 Palvelun kuvaus ja koulutus

Sovelluksen toimintojen yksityiskohtainen kuvaus ja selkeät käyttöohjeet työntekijöille ovat ratkaisevan tärkeitä. Asianmukaisella koulutuksella varmistetaan, että käyttäjät

käsittelevät sovellusta asianmukaisesti, mikä vähentää virheiden ja tietojen vääränlaisen käsittelyn todennäköisyyttä. Säännölliset koulutustilaisuudet voivat myös auttaa työntekijöitä pysymään ajan tasalla uusista tietoturvaprotokollista ja vaatimustenmukaisuustoimenpiteistä.

5.9 Kansainvälinen tiedonhallinta

Kansainvälisesti toimivissa yrityksissä tiedonhallinnasta tulee monimutkaisempaa. Vaikka tietosuoja-asetus ei sovellettaisikaan, on tärkeää, että käytössä on käytännöt ja valvonta, joilla suojellaan tietoja ja noudatetaan paikallisia tietosuojalakeja. Yritysten olisi tehtävä perusteellista tutkimusta ymmärtääkseen niiden maiden erityissäädökset, joissa ne toimivat, ja räätälöitävä tiedonhallintastrategiansa sen mukaisesti.

5.10 Tietokannan valinta

Tietokannan valinta on kriittinen näkökohta sovellusten käyttöönotossa. Määritä, onko sovelluksella oma tietokanta vai hyödynnetäänkö olemassa olevia tietokantoja, kuten Active Directorya tai Azure Active Directorya. Tietokannan valinta vaikuttaa tietojen tallennukseen, saatavuuteen, skaalautuvuuteen ja tietoturvaan, ja sen tulisi olla linjassa organisaation tarpeiden ja vaatimustenmukaisuusvaatimusten kanssa.

6 Sovelluksen käyttöönottoprosessin kehitys kohdeyrityksessä

Nykyinen sovellusten käyttöönottoprosessi organisaatiossa on hajanainen, eikä siinä ole yhtenäistä kaavaa tai kanavaa pyyntöjen käsittelyyn. Työntekijät voivat tällä hetkellä lähettää sovelluspyyntönsä kolmelle eri osastolle: kyberturvatiimille, sovellusten käyttöönottoryhmälle ja muutoksenhallintaryhmälle. Pyynnöissä ei tällä hetkellä ole mitään vaadittuja tietoja ja siksi pyynnöstä voi puuttua kaikki sovellusta koskevat olennaiset tiedot mikä aiheuttaa sen, että tietoturvatiimiltä kuluu paljon ylimääräistä aikaa etsiessä sovelluksen tietoja. Tämä hajautettu lähestymistapa voi myös johtaa valvonnan puutteeseen, epäjohdonmukaisuuksiin prosessin toteutuksessa ja mahdollisiin tietoturva-aukkoihin.

Tavoitteena on virtaviivaistaa sovellusten käyttöönottoprosessia ja varmistaa, että kaikki sovellukset täyttävät yrityksen tietoturva- ja vaatimusten mukaisuusstandardit tekemällä prosessista hallitumpi.

Sovelluspyyntölomake on toimitettava ensin kyberturvatiimille, joka varmistaa, että sovellus on riittävän turvallinen tietoturvan ja tietosuojan kannalta käyttöönotettavaksi. Jos kyberturvatiimi toteaa, että sovellus on tarpeeksi turvallinen ja kyberturvatiimi hyväksyy sen, voidaan lomake lähettää takaisin pyynnön esittäneelle osapuolelle, joka voi tämän jälkeen edetä prosessissa ja lähettää lomakkeen muutoksenhallintaryhmälle, jonka jälkeen prosessi jatkuu normaalisti sovellusten käyttöönottoryhmälle.

Prosessissa hyödynnetään myös kohdeyrityksessä käytössä olevaa IT-Standardia ITIL:iä (Information Technology Infrastructure Library), sekä Microsoft Defender for Cloud Apps:ia.

6.1 Information Technology Infrastructure Library (ITIL)

ITIL (Information Technology Infrastructure Library) on jäsennelty kehys, jonka tarkoituksena on standardisoida tietotekniikkapalvelujen hallinta koko elinkaaren ajaksi yrityksessä. Ensisijaisena tavoitteena on lisätä tehokkuutta ja saavuttaa johdonmukainen palveluntarjonta. ITIL-kehystä noudattamalla IT-hallinnoijat muuttuvat strategisiksi liiketoimintakumppaneiksi pelkän backend-tuen sijaan. ITIL:in laatimilla ohjeilla ja parhailla käytännöillä varmistetaan, että IT-osaston toimet ja menot ovat tiiviisti linjassa liiketoiminnan kehittyvien tarpeiden kanssa. (techtarget, 2022)

ITIL sai alkunsa 1980-luvulla vastauksena hajauttamiseen ja maantieteellisesti erilaisten arkkitehtuurien käyttöönottoon datakeskuksissa. Tämä muutos käytännöissä johti epäjohdonmukaisuuksiin prosesseissa ja käyttöönotoissa, mikä johti organisaatioiden IT-palvelujen suorituskyvyn heikkenemiseen. (techtarget, 2022)

Yhdistyneen kuningaskunnan Central Computer and Telecommunications Agency (CCTA) ilmoitti, että tietotekniikka on nähtävä palveluna ja että standardisoituja käytäntöjä on otettava käyttöön ja kehitti siksi Government Information Technology Infrastructure Management -menetelmän. Tämän työn tuloksena julkaistiin ITIL v1 vuonna 1989. Myöhemmin vuonna 2000 CCTA yhdistyi Office of Government Commerce -virastoon ja otti käyttöön ITIL v2:n seuraavana vuonna. (techtarget, 2022)

ITIL v3 otettiin käyttöön vuonna 2007, ja sitä päivitettiin vuonna 2011 käyttäjien ja koulutusyhteisön panoksen huomioon ottamiseksi sekä virheiden ja epäjohdonmukaisuuksien korjaamiseksi. Vuonna 2013 Ison-Britannian Cabinet Office ja Capita PLC perustivat Axelosin, jonka tehtävänä on parantaa yksilöiden ja organisaatioiden tehokkuutta käytännön ohjeiden, sisällön ja pätevyyksien avulla, jotka perustuvat käytännön kokemuksiin ja kehittyviin käytäntöihin. Tällä hetkellä Axelos vastaa ITIL:in jatkuvasta kehittämisestä. Organisaatio esitteli uusimmat ITIL-ohjeet vuonna 2017 ja ottaa käyttöön ITIL v4:n ja siihen liittyvät moduulit vuosina 2019-2020. Axelos vastaa edelleen parhaiden käytäntöjen ja menetelmien, kuten ITIL:in ja PRINCE2:n, edistämisen ja sertifioinnin valvonnasta. (techtarget, 2022)

Vuonna 1989 ITIL v1:n ensisijaisena tavoitteena oli standardoida IT-palvelujen hallinta (ITSM). Tämä ensimmäinen julkaisu tarjosi organisaatioille kattavan näkemyksen siitä, miten niiden palveluja voidaan optimoida, ja auttoi ylläpitäjiä parhaiden käytäntöjen käyttöönotossa. (techtarget, 2022)

ITIL v2 esitteli ylläpitäjille käytännöllisemmän ja johdonmukaisemman viitekehyksen palvelujen tukemiseen ja toimittamiseen. Siinä esiteltiin konkreettisia prosesseja, joita organisaatiot voivat toteuttaa ja noudattaa. (techtarget, 2022)

ITIL v3 laajensi IT-palveluiden soveltamisalaa ja sisälsi ohjeet palvelustrategiaa, suunnittelua, siirtymistä ja toimintaa varten. Lisäksi siinä esiteltiin menetelmiä, joiden avulla yritykset voivat jatkuvasti parantaa palvelujaan. Kehyksen keskeisiin julkaisuihin koottiin parhaita käytäntöjä, jotka vastaavat kutakin IT-palvelunhallinnan päävaihetta. (techtarget, 2022)

6.1.1 ITIL:in Hyödyt ja haitat

ITIL käsittää muutakin kuin vain IT-alan perus- ja rutiinitaitoja. Sertifikaatissa tarkastellaan myös sitä, miten järjestelmänvalvojat voivat integroida tietonsa organisaationsa laajempaan kontekstiin ja sovittaa ne yhteen liiketoimintakäytäntöjen kanssa, mikä merkitsee merkittävää muutosta ja edistystä IT-roolissa. Järjestelmänvalvojilla on nyt entistä yhtenäisemmät parhaat käytännöt, jotka koskevat

kaikkia IT-hallinnan osa-alueita. Tämän vuoksi ITIL-sertifiointiin liittyy kuusi merkittävää etua:

- IT-osastojen ja liiketoiminnan tavoitteiden parempi yhteensovittaminen.
- Paremmat palveluaikataulut ja suurempi asiakastyytyväisyys.
- Toimintamenojen vähentäminen resurssien tehokkaamman käytön ansiosta.
- IT-budjetin ja -kustannusten avoimuuden lisääminen.
- Virtaviivaistettu reagointi ja palveluhäiriöiden hallinta.
- Sopeutumiskykyisempi palveluympäristö, joka pystyy mukautumaan saumattomasti muutoksiin.

ITIL toimii myös vankkana perustana organisaatioille, joilla ei ole vakiintuneita palvelukehyksiä tai parhaita käytäntöjä, ja tarjoaa ylläpitäjille mahdollisuuksia erikoistuneisiin tehtäviin. (techtarget, 2022)

Ansioistaan huolimatta ITIL:illä on kuitenkin myös mahdollisia haittapuolia yrityksille:

- Kattavat ja aikaa vievät koulutusvaatimukset sekä asiantuntijahenkilöstön tarve onnistuneen täytäntöönpanon varmistamiseksi.
- Toteutukset voivat kestää vuosia ennen kuin ne saadaan täysin integroitua ja hiottua.
- Aloitteiden välitön tuotto voi olla rajallinen.
- Aloitteista johtuvat muutokset voivat häiritä nykyisiä prosesseja ja infrastruktuuria.
- Lyhytaikaiset hankkeet ja aloitteet voivat häiritä pitkän aikavälin pyrkimyksiä.

Järjestelmänvalvojien on oltava varovaisia sen suhteen, miten johto tulkitsee ja toteuttaa ITIL:iä. Vaikka se on alan standardi se ei automaattisesti ratkaise sisäisen henkilöstön tai vaatimustenmukaisuuden haasteita. Sen käytäntöönpano-ohjeet voivat helpottaa prosessien kehittämistä, mutta ne eivät ehkä täysin vastaa innovatiivisia prosesseja tai teknologioita. ITIL:in käyttöönotto vaatii henkilöstön aikaa, koulutusta ja asiantuntemusta, minkä vuoksi organisaatioiden on varmistettava, että niillä on tarvittavat resurssit ja sertifioitu henkilöstö ennen ITIL:in käyttöönoton aloittamista. (techtarget, 2022)

6.2 Microsoft Defender For Cloud Apps

Microsoft Defender for Cloud Apps, joka tunnettiin aiemmin nimellä Cloud App Security, antaa organisaatioille yksityiskohtaista tietoa niiden ympäristössä toimivista pilvisovelluksista. Yksi sen keskeisistä vahvuuksista on kyky arvioida ja luokitella yksittäisiä sovelluksia erilaisten turvallisuus- ja vaatimustenmukaisuusmittareiden

perusteella. Tämä antaa yrityksille mahdollisuuden tehdä tietoon perustuvia päätöksiä käyttämistään sovelluksista ja varmistaa sekä toimivuuden että turvallisuuden. (Microsoft, 2023)

Sovelluksen tarkistukset sisältävät mm:

- Vaatimustenmukaisuuden tarkistus: Maailmanlaajuisten tietosuojasäännösten lisääntyneen tietoisuuden ja täytäntöönpanon myötä Defender for Cloud Apps tarjoaa tietoa sovelluksen vaatimustenmukaisuudesta tärkeimpien standardien suhteen. Tämä sisältää muun muassa seuraavat seikat:

- GDPR (yleinen tietosuoja-asetus): Tietoa siitä noudattaako sovellus Euroopan unionin määrittelemää tietosuoja-asetusta (Microsoft, 2023).

- ISO 27001: Saat tietoa sovelluksen tietoturvan hallintajärjestelmistä ja siitä, täyttävätkö ne kansainvälisen standardin (Microsoft, 2023).

- Tunnistusprotokollat: Arvioi, tukeeko sovellus vankkoja todennusmenetelmiä, kuten MFA (Multi-Factor Authentication): Tarkistaa tarjoaako sovellus tehostettua turvallisuutta vaatimalla kahta tai useampaa varmennusmenetelmää sisään kirjautuessa. (Microsoft, 2023)

- Riskinarviointi: Alusta antaa jokaiselle sovellukselle riskipisteytyksen, joka perustuu eri parametreihin, kuten sovelluksen tietoturvatilanteeseen, sen tietojen mahdolliseen vaikutukseen ja vakiintuneiden standardien noudattamiseen. (Microsoft, 2023)

- Tietosuojan oivallukset: Ymmärrä, miten kukin sovellus käsittelee tietoja. Tämä sisältää tietoja salauksesta (sekä siirron aikana että levossa), tietojen säilytyspaikasta ja siitä, onko sovelluksessa tapahtunut viimeaikaisia tietomurtoja. (Microsoft, 2023)

- Yksityiskohtaiset metatiedot: Saat kustakin havaitusta sovelluksesta yksityiskohtaisia tietoja, kuten sovelluksen kategorian, sen suosioarvosanan ja pilvipalveluntarjoajan. Nämä metatiedot auttavat kontekstualisoimaan sovelluksen paikan laajemmassa IT-maisemassa. (Microsoft, 2023)

- Integrointikyky: Selvitä, tarjoaako sovellus integrointimahdollisuuksia muiden kriittisten yritysratkaisujen kanssa. Tämä on erityisen tärkeää suuremmille organisaatioille, jotka vaativat toisiinsa liitettyjä järjestelmiä saumatonta toimintaa varten.

Pohjimmiltaan Microsoft Defender for Cloud Apps tarjoaa kokonaisvaltaisen näkymän jokaisen sovelluksen tietoturvasta, tietosuojasta ja vaatimustenmukaisuudesta. Se antaa IT- ja tietoturvatiimille mahdollisuuden tehdä tietoon perustuvia päätöksiä ja varmistaa, että jokainen käytössä oleva sovellus organisaatiossa on linjassa sen turvallisuus- ja vaatimustenmukaisuuden vertailuarvojen kanssa (Microsoft, 2023)

6.3 Uuden sovelluksen käyttöönoton prosessin kulku

Pyynnön aloitus:

Työntekijöiden, jotka haluavat ottaa sovelluksen käyttöön työvälineissään, on täytettävä kattava pyyntölomake. Lomakkeella kerätään olennaiset tiedot, kuten sovelluksen nimi, toimittaja (esim. Microsoft, Google), versionumero, sovelluksen mahdollisesti sisältämät henkilötiedot (kuten sosiaaliturvatunnukset, nimet, osoitteet), tietojen tallennuspaikka (GDPR:n noudattamisen varmistamiseksi) ja mikäli sovelluksessa on mahdollisuus monivaiheiseen tunnistautumiseen.

Kyberturvallisuuden arviointi:

Kun pyyntölomake on täytetty, se ohjataan kyberturvatiimille. Tiimi käyttää Microsoft Defender for Cloud Apps -työkalua ensisijaisena työkaluna tarkistaakseen, onko pyydetty sovellus luettelossa, ja arvioi sen tietoturvatason annettujen pisteiden perusteella.

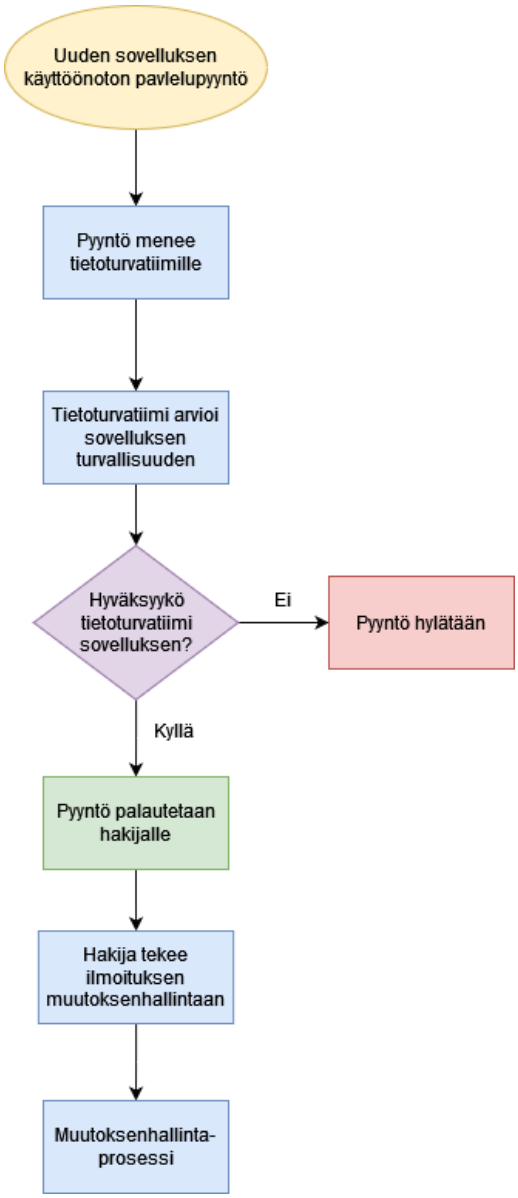
Jos sovellusta ei ole listattu Microsoft Defender for Cloud Apps -ohjelmassa, tiimi turvautuu räätälöityyn Excel-työkaluun. Tämä työkalu sisältää kysymyksiä lomakkeesta ja muutamia lisätietoja, kuten iso 27001 vaatimuksenmukaisuuden. Lomakkeesta johdetut kysymykset, joita on täydennetty muilla turvallisuusnäkökohdilla, auttavat määrittämään sovelluksen riskipisteet. Kyberturvatiimi päättää joko Defender for Cloud Apps:in arvion tai Excel-työkalun riskipisteytyksen perusteella, täyttääkö sovellus organisaation turvallisuuskynnyksen käyttöönoton kannalta.

Prosessin eteneminen:

Arvioinnin jälkeen kyberturvatiimi ilmoittaa päätöksestä (hyväksyminen tai hylkääminen) alkuperäiselle pyynnön esittäjälle.

Muutoksenhallintaprosessi:

Jos lomake hyväksytään, se kanavoidaan muutoksenhallintatiimille. Muutoksenhallintatiimi valvoo ja vastaa kaikista organisaatiossa tapahtuvista muutoksista ja varmistaa, että prosessit toimivat ITIL:in (Information Technology Infrastructure Library) mukaisesti. Muutoksenhallintaprosessin jälkeen lomake siirtyy prosessin mukaisesti integrointia ja käyttöönottoa varten sovellusten käyttöönotto tiimille. Prosessi on esitetty kuvassa 1.



Kuva 1. Paranneltu prosessi

7 Avustava työkalu sovelluksen arviointiin

Tietoturvan ylläpitäminen vaatii työkaluja, joilla voidaan varmistaa sovellusten turvallisuus ja vaatimustenmukaisuus. Vaikka Microsoft Defender for Cloud Apps on vakaa ensimmäinen arviointilinja, se ei valitettavasti kata kaikkia sovelluksia. Avustava Riskiarviointi -työkalu kehitettiin täyttämään tämä aukko ja varmistamaan, että kaikki sovelluspyynnöt tutkitaan yhtä tarkasti.

Keskeisimmät kysymykset: Työkalu on varustettu keskeisillä kysymyksillä, jotka vastaavat hakemuspyyntölomakkeen ensisijaisia huolenaiheita kuten:

- Käytetäänkö sovelluksessa monitekijätodennusta (MFA)?
- Tallennetaanko sovelluksen tiedot Euroopan unionin alueella GDPR-vaatimusten mukaisesti?
- Onko toimittaja tunnettu, kuten Microsoft?
- Hakeeko sovellus tietoja ulkoisista lähteistä?
- Hakeeko jokin ulkopuolinen tietoja sovelluksesta?
- Siirtääkö sovellus tietojaan muihin paikkoihin?
- Käsitteleekö sovellus henkilötietoja, kuten henkilötunnuksia, nimiä tai osoitteita?

Työkalun erityispiirre on sen kyky laskea riskipistemäärä väliltä 0-100.

- 0–55: Matala riski - Osoittaa, että sovellus vastaa hyvin organisaation turvallisuusstandardeja.
- 55–75: Keskisuuri riski - Ilmaisee mahdollisia ongelmia, jotka saattavat edellyttää lisätarkastelua tai ehdollista käyttöönottoa.
- 75–100: Korkea riski - viittaa huomattaviin tietoturva, tietosuoja tai vaatimustenmukaisuushaasteisiin mikä viittaa siihen, että sovellus ei ehkä sovellu käyttöönotettavaksi.

Tämä riskilaskenta on räätälöity tätä työkalua varten. Siinä painotetaan merkittävästi ensisijaisia turvallisuustekijöitä, kuten MFA:ta, tietojen sijaintia GDPR:n osalta, sekä tiedon siirtämistä.

Tietojen syöttö ja analysointi:

Työkalu ei tarkista itsenäisesti sovellusversioita tai muita tietoja. Sen sijaan kyberturvaryhmä syöttää manuaalisesti sovelluspyyntölomakkeesta saadut tiedot. Näiden tietojen perusteella työkalu johtaa riskinarviointinsa.

Mukautuva kehys:

Työkalu on rakennettu joustavasti, joten sitä voidaan tarkentaa tai laajentaa kehittyvien tietoturvatarpeiden tai uusien haasteiden perusteella.

Käyttötarkoitus:

Vaikka Microsoft Defender for Cloud Apps on pääasiallinen arviointimekanismi, avustava työkalu toimii täydentävänä järjestelmänä sovelluksille, joita ei ole lueteltu defenderissä. Tämä täydentävä lähestymistapa takaa perusteellisen turvallisuusarvioinnin jokaiselle sovellukselle.

Työkalu on tarkoitettu pääosin vain tukevaksi ratkaisuksi mikäli kyseessä olevaa sovellusta ei löydy Defender for Cloud Apps:ista, joten tietoturva-asiantuntijoiden tarvitsee silti tehdä joitakin itsenäisiä mietintöjä liittyen Sovelluksen turvallisuuteen. Sovellus kuitenkin nopeuttaa prosessia, sillä se antaa suuntaa antavan riskipisteytyksen.

8 Yhteenveto

Tämän opinnäytetyön tavoitteena oli sovelluksen käyttöönotto prosessin kehitys siten, että siitä tehtiin turvallisempi tietoturvan ja tietosuojan kannalta, sekä tekemällä prosessista suoraviivaisempi ja hallitumpi, sekä pakottamalla käyttäjän kertomaan sovelluksesta olennaisia tietoja. Kehitystyö avustavassa sovelluksessa jatkuu.

Kyberturvallisuuden dynaamisessa ympäristössä on ensiarvoisen tärkeää, että organisaatiot kehittävät ja mukauttavat jatkuvasti tietoturvakäytäntöjään ja varmistavat, että tietojen ja infrastruktuurin pyhyys säilyy vaarattomana. Tässä opinnäytetyössä on tutkittu kattavasti tieto- ja tietoturvan merkitystä erityisesti nykyaikaisessa liiketoimintaympäristöissä ja tarkasteltu perusteellisesti vakiintuneita standardeja, kuten GDPR:ää, ISO 27001:ää ja NIST SP-800-53:a.

Yksi merkittävä esiin noussut haaste oli sovellusten käyttöönoton hajanainen prosessi organisaatiossa. Prosessin epäselvyys aiheutti mahdollisia tietoturva- ja tietosuojariskejä, sillä työntekijöillä oli useita väyliä, joiden kautta he saattoivat esittää sovelluspyynnön uudelle sovellukselle, eikä tarvittavaa turvallisuusarviointia varten ollut jäsenneltyä menetelmää. Tämä ei ainoastaan aiheuttanut toiminnallista tehottomuutta vaan myös kriittisen turvallisuusriskin.

Paranneltu prosessi varmisti, että prosessi oli virtaviivainen ja turvallinen. Luomalla selkeän ja yksiselitteisen väylän sovelluspyyntöjä varten minimoidaan virhemahdollisuudet. Prosessin keskittäminen siten, että kyberturvatiimi on ensisijainen kanava, varmistaa, että jokainen hakemus käy läpi tiukan turvallisuusarvioinnin. Microsoft Defender for Cloud Apps -palvelun avulla tiimi voi arvioida tehokkaasti useimpien sovellusten turvallisuutta. Excel-pohjaisen arviointityökalun käyttöönotto varmistaa turvallisuuden kuitenkin niiden sovellusten osalta, joita ei defenderistä löydy. Yksinkertaisen mutta riittävän ja joustavan arviointityökalun avulla, joka on sekä helppo että kattava varmistaa sen, että jokainen sovellus riippumatta Sovelluksen suosiosta tai alkuperästä käy läpi tietoturvatiimin tarkastelun ja vertaa sovellusta organisaation turvallisuusmääritelmiä vasten.

Lisäksi integroimalla ITIL-käytännöt ja pitämällä muutoksenhallinta mukana vasta tietoturva-arvioinnin jälkeen prosessista tulee tehokas, jolloin sovellusten nopea käyttöönotto ja tietoturvastandardien säilyttäminen pysyvät tasapainossa.

Yhteenvetona voidaan todeta, että tunnistamalla nykyisen prosessin heikkoudet ja ottamalla käyttöön uusi, virtaviivaistettu ja turvallinen työnkulku tämä työ on vastannut perustavanlaatuiseen haasteeseen, jonka monet nykyaikaiset yritykset kohtaavat. Toteutetuilla toimenpiteillä varmistetaan, että organisaation työntekijät saavat käyttöönsä tarvitsemansa välineet säilyttämällä silti tietojen eheys, luottamuksellisuus ja saatavuus loukkaamattomina.

Työkalu on rakennettu joustavasti, joten sitä voidaan parantaa, muuttaa tai laajentaa tarvittaessa, mikäli epäkohtia huomataan, sekä turvallisuuvaatimusten tai uusien haasteiden perusteella.

Lähteet

Cloudflare. (2023). *Data Privacy*. Haettu 18. 6 2023 osoitteesta https://www.cloudflare.com/learning/privacy/what-is-data-privacy/

Cloudflare. (2023). *GDPR*. Haettu 20. 6 2023 osoitteesta https://www.cloudflare.com/learning/privacy/what-is-the-gdpr/

Fortinet. (2023). *CIA Triad*. Haettu 12. 6 2023 osoitteesta https://www.fortinet.com/resources/cyberglossary/cia-triad

isms.online. (2023). *isms.online*. Haettu 9. 7 2023 osoitteesta https://www.isms.online/iso-27701/

ISO. (2023). *ISO/IEC 27000 family*. Haettu 20. 6 2023 osoitteesta https://www.iso.org/standard/iso-iec-27000-family

ISO. (2023). *ISO/IEC 27001*. Haettu 20. 6 2023 osoitteesta https://www.iso.org/standard/27001

Microsoft. (2023). *Microsoft Defender for Cloud Apps overview*. Haettu 2. 9 2023 osoitteesta https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Microsoft. (2023). *Working with the risk score*. Haettu 3. 9 2023 osoitteesta https://learn.microsoft.com/en-us/defender-cloud-apps/risk-score

NIST. (2023). *SP 800-53 Rev. 5*. Haettu 9. 7 2023 osoitteesta https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

rashi_garg. (2023). *What is Information Security?* Haettu 12. 6 2023 osoitteesta https://www.geeksforgeeks.org/what-is-information-security/

techtarget. (2022). *ITIL (Information Technology Infrastructure Library)*. Haettu 2. 9 2023 osoitteesta https://www.techtarget.com/searchdatacenter/definition/ITIL

Walkowski, D. (2019). *What Is the CIA Triad?* Haettu 19. 7 2023 osoitteesta https://www.f5.com/labs/learning-center/what-is-the-cia-triad