Opinnäytetyö AMK

Tietojenkäsittely

2019

Petteri Kevo

INHIMILLISEN VIRHEEN OSUUS TIETOTURVASSA JA SEN VÄHENTÄMINEN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2019 | 23 sivua, 3 liitesivua

Petteri Kevo

INHIMILLISEN VIRHEEN OSUUS TIETOTURVASSA JA SEN VÄHENTÄMINEN

Internetin käytön kasvun takia tietoturvasta on tullut osa jokaisen elämää työssä ja sen ulkopuolella. Tämän takia yrityksissä ja normaalissa elämässä tietoturva on tullut tärkeäksi alati kehittyvässä maailmassa. Ihmisten tekemät virheet ovat suuri osa tietoturvan riskeistä. Siksi yhteistyö yritysten eri osastojen välillä on tärkeää.

Opinnäytetyön tarkoituksena on selvittää suurimpia tietoturvauhkia, miten ne vaikuttavat yrityksiin ja työntekijöihin, miten niiltä suojaudutaan ja miten ihmisvirheen osuutta pystytään minimoimaan.

Lähteet ovat verkkosivustojen artikkeleita sekä raportteja tietoturvasta eri järjestöiltä ja yrityksiltä, joita on verrattu toisiin lähteisiin samasta asiasta. Lähteinä toimivat myös omalta koulutusalalta saadut opit ja tiedot.

Työ selvittää ihmisvirheen osuutta tietoturvan eri osa-alueilla ja sitä, miten sitä voidaan vähentää. Lähteitä tutkimalla löytyi tapoja ja keinoja vähentää ihmisvirhettä. Opinnäytetyön mukana tuotettiin tietoturvaohjeistus yrityksille, joka sisältää tapoja ja keinoja tietoturvan parantamiseen ja ihmisvirheen minimoimiseen.

ASIASANAT:

tietoturvariskit, tietoturvaohjeistus, inhimillinen virhe, tietoturva

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2019 | 23 pages, 3 pages in appendices

Petteri Kevo

HUMAN ERROR IN INFORMATION SECURITY AND HOW TO REDUCE IT

The explosive growth of internet has rendered information security important in normal life and in business. For this reason, information security has become an important part of normal life and the business world in the ever-developing world. Human error is a great source of information security risk. Therefore, cooperation between different sections of companies is important.

The goal of this bachelor's thesis was to map some of the larger security risks, how they affect companies and their employees, how companies can be protected against them and how to minimize human error in these cases.

The source material is mostly articles and reports on information security from different companies and organizations that have been cross-referenced with other sources to check their integrity, and applying knowledge that the author acquired during his studies. The methodological approach of this thesis is constructive.

The thesis seeks to figure out the role of human error in the different sections of information security and how to reduce it. Habits and methods of minimizing human error were found during the literature search. The thesis also resulted in the creation of a document with information security instructions for companies that includes methods and good practices for improving information security and minimizing human error.

KEYWORDS:

information security risks, information security instructions, human error, information security

SISÄLTÖ

LIITTEET

KUVAT

Kuva 2 Esimerkki DDoS-hyökkäyksestä

SANASTO

Adware	Haittaohjelma, joka pakottaa mahdollisesti haitallisia mainoksia koneelle
ENISA	European Union Agency for Cybersecurity, EU:n kyberturvavirasto
IoT	Internet of Things, Esineiden internet, tarkoittaa laitteita, jotka ovat yhdistetty internettiin. Laitteet voivat olla leluista suuriin työkoneisiin.
IP-osoite	Numerosarja, jota käytetään laitteen tunnistamiseen
Kryptaaminen	Prossessi, jossa koodataan viestejä tai tietoja lukukelvottomaksi
Kryptovaluutta	Kryptografiaan perustyva virtuaalivaluutta
Slack	Viestintäohjelma, jolla voi viestien lisäksi jakaa tiedostoja.

1 JOHDANTO

Internetin käyttö on yleistynyt valtavasti 2000-luvulla, jopa siihen pisteeseen, että se on välttämätöntä normaalissa elämässä. Kehitys on tapahtunut niin nopeasti, että jotkut ovat jääneet sen jalkoihin. Internet yleistyessään on tuonut mukanansa vaaroja. Tavallisella työntekijällä, jolla ei ole kiinnostusta tapahtuneeseen kehitykseen, on hankala pysyä perässä uusimmista huijauksista ja hyökkäyksistä. Samaa tapahtuu IT-kehittäjien puolella. Kehittäjien on vaikea seurata kaikkea, jolloin on tärkeää, että koordinaatio toimii eri ryhmien välillä, jotta voidaan välttää virheet, jotka voivat maksaa sadasta eurosta moneen miljoonaan.

Ihmisvirhe on asia, joka tulee tapahtumaan. On mahdotonta poistaa sitä kokonaan. Siksi sitä pitää yrittää minimoida. ”SEC_RITY is not complete without U!” on slogan, joka kuvaa tilannetta hyvin monessa yrityksessä (Gupta 2012). Jotta suojaus toimii moitteettomasti, on tarpeellista, että jokainen työntekijä osallistuu tietoturvan parantamiseen. Työntekijät voivat kehittää itseään osallistumalla tietoturvakoulutuksiin, ja IT-puolen tehtävänä on pysyä mukana uusissa käänteissä, joita tapahtuu tietoturvan maailmassa ja pitää käytetyt ohjelmat ja nettisivut ajan tasalla.

Tämän opinnäytteen tarkoituksena on saada selville, mitkä uhat ovat tällä hetkellä suurimmat yrityksille ja sen työntekijöille, miten niitä vältetään ja miten riski saadaan mahdollisimman pieneksi. Opinnäyte sopii niin tavalliselle työntekijälle kuin kehittäjällekin, joka ei ole keskittynyt tietoturvaan. Tavoitteena on saada heille hyvä käsitys riskeistä ja niiden minimoimisesta sekä herättää mahdollinen kiinnostus lukea lisää aiheesta ja siten parantaa koko yrityksen tietoturvaa.

Opinnäytetyö on konstruktiivinen. Tutkimuksesta tuotetaan ohjeistus virheen minimoimiseen. Ohjeistukselle on käyttöä yrityksissä, jotka haluavat parantaa tietoturvaansa. Ohjeistuksessa tulee olemaan keinoja, joilla voidaan ehkäistä virheitä sekä työtapoja, joiden avulla kehittämisessä otetaan tietoturva huomioon.

2 TIETOTURVARISKIT JA ANALYSOINTI

Tietoturvariskejä on monenlaisia, joissa hyökkäykset kohdistuvat eri osa-alueille. Hyökkäykset voivat keskittyä itse ohjelmistoon, laitteistoon tai työntekijöihin. Hyökkäysten vakavuudet ja todennäköisyydet vaihtelevat. Siksi keskitymme tällä hetkellä suurimpiin uhkiin, jotka voivat vaikutta yrityksiin ohjelmisto- tai henkilöstöpuolella. Riskit on valittu vertailemalla useiden lähteiden tekemiä listauksia tietoturvariskeistä sekä omalla harkinnalla. Lähteinä on käytetty seuraavia: ENISA (2019), Kingori (2019), Security First (2019), University of San Diego (2019), Bianculli (2019) ja Center for Internet Security (2019).

Riskianalyysi on tärkeä osa nykyisten yritysten toimintaa. Riskianalyysin tulosten perusteella kirjoitetaan raportteja, joiden perusteella saadaan parempi käsitys riskien vaikutuksesta ja todennäköisyydestä sekä keinoista riskien pienentämiseen.

2.1 Haittaohjelmat

Haittaohjelmat ovat ohjelmia, joiden tarkoitus on vahingoittaa muita järjestelmiä ja laitteita, varastaa dataa tai hidastaa niiden toimintaa. Haittaohjelmat ovat yleisin tapa vahingoittaa toisten järjestelmiä ja laitteita (ENISA 2019). Haittaohjelmia on monenlaisia. Osa niistä aiheuttaa minimaalista vahinkoa, kuten Adware, ja osa voi kryptata koko tietokoneen, kuten ransomware. Haittaohjelmat voivat myös levitä laitteesta toiseen, jos laitteet ovat yhteydessä toisiinsa. Tällä hetkellä käytetyimmät haittaohjelmat ovat Emotet ja WannaCry (Cisecurity 2019).

Emotet on haittaohjelma, joka varastaa tietoja ja käyttää muita pankkitroijalaisia. Emotet leviää todella nopeasti, joten se on vaikea saada pois, jos se on ehtinyt tarttumaan moneen laitteeseen (Cisecurity 2019). WannaCry on kiristysohjelma, joka kryptaa dataa ja vaatii kryptovaluuttaa vastineeksi avaimesta, jolla voi avata kryptatun datan (Cisecurity 2019).

Koska haittaohjelmia on monenlaisia ja ne voivat aiheuttaa suurempaakin tuhoa. Siksi pitää olla tarkkana, että ne eivät pääse laitteistoon. Yleisimpiä tapoja haittaohjelmien pääsyyn laitteisiin ovat sähköpostin liitteet ja linkit. Nämä viestit on naamioitu näyttämään

esimerkiksi tilausvahvistuksina, jotka antavat haitallisen seurantalinkin tai tiedoston, joka on kuitti tilauksesta (Michigan State University 2019).

Jotta haittaohjelmilta voi pysyä suojassa, kannattaa ladata luotettava virustorjuntaohjelma ja tarkastaa sillä laitteisto. Lisäksi on hyvä pitää laitteisto ja sovellukset ajan tasalla sekä käyttää järkeä siinä, miten verkossa käyttäytyy ja mihin verkkoon yhdistää laitteensa (Whatsmyipaddress 2019).

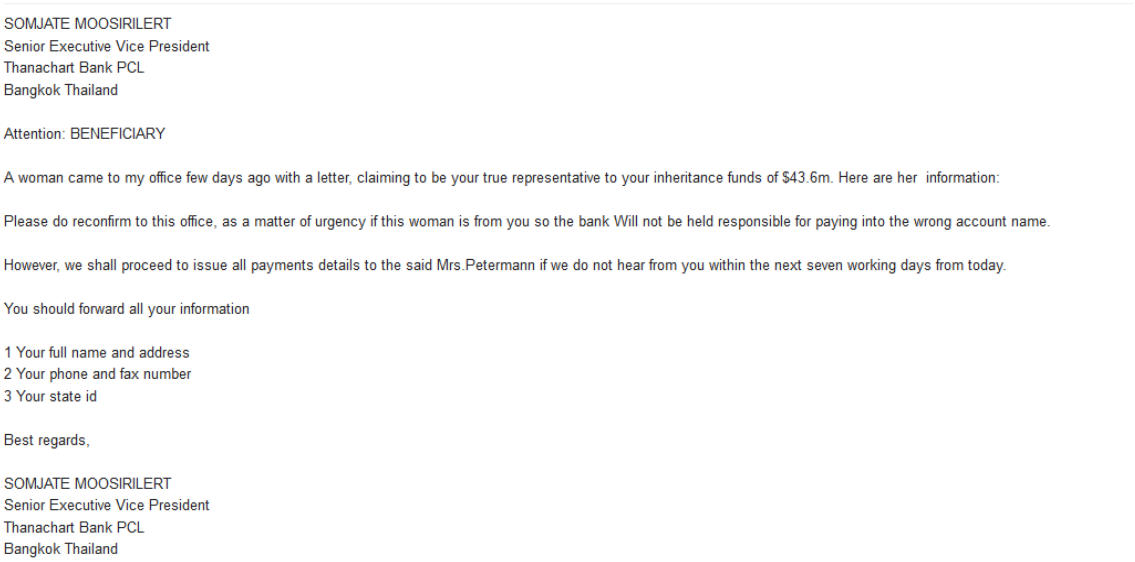
2.2 Verkkourkinta

Phishing eli verkkourkinta on sosiaalista manipulointia, jolla yritetään saada vastaanottajaa avaamaan haitallisia tiedostoja tai linkkejä sekä antamaan tunnuksia oikean näköisillä sivuilla tai lähettämään rahaa. Tämä saavutetaan esiintymällä luotettavana henkilönä tai yhteisönä. Enisan mukaan verkkourkinta on ollut syynä 90 prosenttiin haittaohjelmien sisäänpääsyyn ja 72 prosenttiin tietomurroista (ENISA 2019).

Verkkourkinta voidaan kohdistaa yksityishenkilöön tai yritykseen. Datavuodoissa levinneet henkilökohtaiset tiedot antavat urkkijoille mahdollisuuden rakentaa isompiakin urkintakampanjoita, koska datan avulla voidaan tehdä uskottavampia valheita (ENISA 2019).

Yleisesti verkkourkintaviestit sisältävät liian hyviä tarjouksia, huonoa kielioppia ja kirjoitusasua, uhkauksia tai linkkejä tai tiedostoja (Kuva 1). Verkkourkintaviestejä voidaan vähentää hyvällä sähköpostisuodatuksella ja kaksivaiheisella tunnistuksella (ENISA 2019).

Verkkourkintahyökkäykset matkapuhelimiin ovat lisääntyneet 85 prosenttia vuodesta 2011 (ENISA 2019). Urkinta voi tapahtua tekstiviestin tai muiden viestisovellusten avulla (Whatsapp) tai sosiaalisessa mediassa (Instagram).



SOMJATE MOOSIRILERT
Senior Executive Vice President
Thanachart Bank PCL
Bangkok Thailand

Attention: BENEFICIARY

A woman came to my office few days ago with a letter, claiming to be your true representative to your inheritance funds of $43.6m. Here are her information:

Please do reconfirm to this office, as a matter of urgency if this woman is from you so the bank Will not be held responsible for paying into the wrong account name.

However, we shall proceed to issue all payments details to the said Mrs.Petermann if we do not hear from you within the next seven working days from today.

You should forward all your information

1 Your full name and address
2 Your phone and fax number
3 Your state id

Best regards,

SOMJATE MOOSIRILERT
Senior Executive Vice President
Thanachart Bank PCL
Bangkok Thailand

Kuva 1 Esimerkki huijausviestistä

2.3 Verkkopohjaiset hyökkäykset ja verkkosovellushyökkäykset

Verkkopohjaiset hyökkäykset ja verkkosovellushyökkäykset kohdistuvat yrityksen tai henkilön verkkosivuihin, verkkopalveluihin, selaimeen tai sen lisäosiin sekä sisällönhallintajärjestelmiin. Hyökkääjät voivat esimerkiksi syöttää muuten turvallisiin sivuihin haitallisia osia, jotka voivat varastaa dataa tai levittää haitallisia ohjelmia käyttäjän tietokoneeseen. Haitallisia ohjelmia voi myös tulla mainosten mukana. Mainokset tulevat yleisesti ulkoistettuna, joten sivuston omistajalla ei ole osuutta niihin. Sivustolle voi tulla mainoksia monesta muusta sivustosta, jolloin on helppo olla huomaamatta haitallisten mainosten pääsy sivustolle. (ENISA 2019)

Sivustoille voidaan syöttää haitallista koodia esimerkiksi SQL-injektiolla. SQL-injektiossa käytetään hyväkseen tekstikenttää, jonka kautta syötetään uusia ohjeita tietokantaan. Syöttämällä uusia ohjeita voidaan aiheuttaa tuhoa poistamalla kokonaisia osia tai lisäämällä uudet tunnukset, joilla pääsee sisään ohjelmistoon. (W3schools 2019)

Verkkopohjaisia hyökkäyksiä voidaan välttää pitämällä selaimet ajan tasalla, kryptaamalla verkkoliikenne, välttämällä kolmannen osapuolen liitännäisiä varsinkin tietojärjestelmissä kuten WordPress ja monitoroimalla ohjelmia (ENISA 2019).

Verkkosovellushyökkäyksiä vastaan auttavat palomuurit, liikenteen suodattaminen sekä sovelluskehitykseen luodut tietoturvakäytännöt (ENISA 2019).

2.4 DDoS-hyökkäys

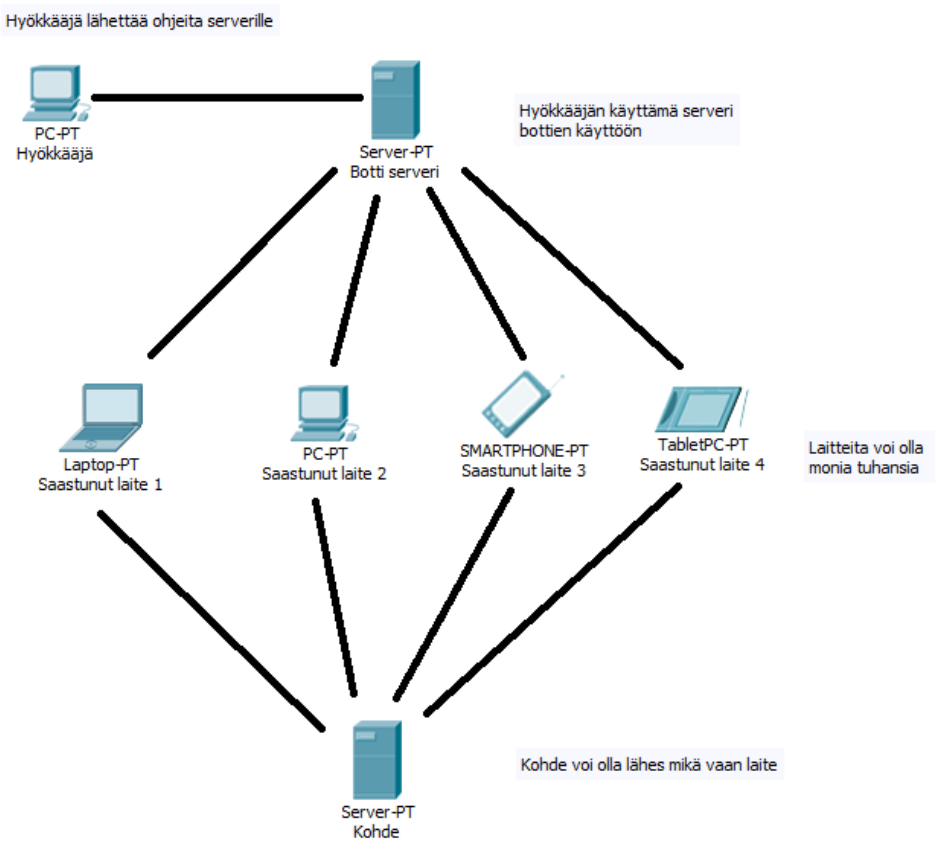
DDoS eli Distributed Denial of Services on hyökkäys, joka kohdistetaan palvelimeen, verkkoon tai palveluun. Hyökkäyksessä lähetetään suuria määriä internetliikennettä kohteeseen, mikä aiheuttaa normaalin toiminnan hidastumisen tai loppumisen. DDoS-hyökkäykset käyttävät hyväkseen suuria määriä laitteita, jotka ovat saastuneet jollain haittaohjelmalla (Cloudflare 2019). Laitteet voivat olla normaaleja tietokoneita tai IoT-laitteita. Hyökkääjä käyttää laitteita samaan aikaan lähettääkseen vastaanottajalle pyyntöjä, jolloin kohteelta loppuu kapasiteetti vastata (Kuva 3).

DDoS-hyökkäykset voivat aiheuttaa suuriakin tuhoja yrityksille ja julkisille palveluille. Monella alalla käytetään paljon IoT-laitteita ja verkkopalveluja, joten niihin hyökkääminen voi lamauttaa kokonaisen sairaalan tai yrityksen toiminnan pidemmäksikin aikaa.

Paras tapa DDoS-hyökkäyksen estämiseksi olisi erotella hyökkääjät oikeista käyttäjistä ja asiakkaista. Tämä on kuitenkin erittäin vaikeaa. Cloudflare:n artikkelin mukaan DDoS-hyökkäystä voidaan lähteä estämään neljällä tasolla: havaitseminen, vastatoimi, reititys, sopeutuminen (Cloudflare 2019).

Havaitseminen tapahtuu seuraamalla tavallisia hyökkäysmalleja, IP-osoitteen mainetta ja aikaisempaa dataa. Vastatoimina voivat toimia bottiliikenteen tunnistaminen ja lopettaminen. Reitittämällä liikenne hyvin moneen eri osioon voidaan jakaa tuleva liikenne

hallittaviin osioihin. Sopeutumalla voidaan koventaa suojausta tulevia DDoS-hyökkäyksiä vastaan.



Kuva 2 Esimerkki DDoS-hyökkäyksestä

2.5 Tietovuoto ja -murto

Tietovuodot ja -murrot ovat ihmisvirheen tai hyökkäyksen lopputuloksia. Tietovuodot ovat jonkun henkilön tai yrityksen vuotamaa tietoa ilman hyökkääjää, tahallaan tai vahingossa. Tietomurrot ovat hyökkääjien aiheuttamia. Tietovuotoja ja -murtoja tapahtuu päivittäin, mikä kuvaa kuinka suuri ilmiö tämä on (ENISA 2019).

Tietovuodoista suurin osa tulee valtioista (ENISA 2019). Tietovuodot voivat johtua vahingossa lähetetyistä sähköposteista, tunnuksien hukkumisista, jolloin data on menetetty, kadonneista laitteistoista tai yrityksen tahallisesta tiedonmyynnistä. Syitä tietovuotoihin on monia. Tietovuodot ovat vahingollisia yrityksille ja valtioille. Strava-sovelluksen kautta vuosi vahingossa Venäjän, Iso-Britannian ja USA:n salaisia tietoja tukikohdista Syyriassa ja Afganistanissa, koska jollain oli kytkettynä laite, joka jakoi sijaintia sovellukseen (ENISA 2019). Myös Twitter oli vuonna 2018 vahingossa tallentanut salasanoja turvattomassa muodossa (Cohen 2018).

Tietomurrot aiheutuvat yleisesti haitallisten ohjelmien tai sosiaalisen manipuloinnin kautta, mutta ne voivat olla myös sisäpiirissä olevan työntekijän tahallaan aiheuttamia. Tietomurtojen estämiseksi pitää olla toimivat tietoturvakäytännöt, joita kaikki noudattavat sekä käytännöt siihen, mitä tehdään murron tapahtuessa ja sen jälkeen. Tietomurrot voivat aiheuttaa suuriakin tuhoja ihmisten elämään, jos dataa ei ole suojattu kunnolla. Esimerkiksi Intiassa vaarantui yli miljardin ihmisen sosiaaliturvatunnukset ja pankkitiedot järjestelmässä olevan heikkouden takia (Whittaker 2019).

2.6 Fyysinen murto, varkaus ja kadottaminen

Fyysisiä uhkia ei tietenkään luetella kyberturvallisuuden uhaksi, mutta ne ovat osa tietoturvaa ja mahdollinen tapahtuma. Jokainen tietää mitä murto, varkaus ja kadottaminen tarkoittavat, mutta niillä voi olla pahoja vaikutuksia, kun kyseessä voi olla joko omaa tai toisten henkilökohtaista tietoa sekä yrityksen immateriaalista omaisuutta. Jos laite on huonosti suojattu, on hyökkääjän mahdollista päästä kiinni suuriinkin määriin dataa. Mitä korkeammalla yrityshierarkiassa kohde on, sitä pahempi vaikutus on. (ENISA 2019)

Koska kadottamisia tai varkauksia tulee tapahtumaan, on niiden vaikutus saatava mahdollisimman alhaiselle tasolle. Kryptaamalla koneen tiedot, pitämällä varmuuskopiota pilvessä ja käyttämällä hyviä tietoturvakäytäntöjä sekä käyttöoikeuksien kontrollia on mahdollista vahingon tai rikoksen tapahtuessa minimoida riski. (ENISA 2019)

Nykyään yrityksillä on työtilojen ulkopuolella IoT-laitteita, kuten sensoreita ja kameroita. Näiden tietoturva ja fyysinen turva pitäisi saada korkealle tasolle, jotta niiden varastaminen olisi hankalaa. Laitteesta lähtevät tiedot pitää kryptata, jotta hyökkääjä ei pääse käsiksi läpi menevään dataan.

2.7 Varjo-IT ja tietoturvakäytäntöjen puutos

Varjo-IT:llä tarkoitetaan sovelluksia, ohjelmistoja tai muita käytäntöjä datan tallentamiseen ja siirtämiseen, joita yrityksen IT-osasto ei ole hyväksynyt. Tämä aiheuttaa ongelmia tietoturvan ja tiedonhallinnan kanssa. Jos käytetyt työkalut ovat joltain henkilöiltä pimitettyjä tai heille ei ole niistä mainittu, on heidän vaikeampi tehdä tehokkaasti työtä, koska heiltä saattaa uupua osa tiedosta minkä he voisivat tarvita. Varjo-IT aiheuttaa päänvaivaa tietoturvapuolelle, koska siellä ei tiedetä, mitä kautta tieto liikkuu ja mitä pitäisi suojata työkalujen käytön levitessä liian suureksi. (Ros 2016)

Varjo-IT johtuu suurimmaksi osaksi IT-puolen, tavallisten työntekijöiden ja ylempien johtajien huonosta kommunikaatiosta ja yhteistyöstä. Työntekijät haluavat tehdä työnsä nopeasti ja vaivattomasti. Kun tarvitaan nopeaa ratkaisua ongelmaan esimerkiksi sovelluksen avulla, IT-puoli voi mahdollisesti kieltää pyynnön, koska se ei noudata heidän asettamiaan tietoturvakäytäntöjä. Silloin on mahdollista, että keksitään itse ratkaisu yrityksen hyväksymien työkalujen ulkopuolelta. Jos näin käy, liiketoiminnan kannalta on vaikea olla hyväksymättä ehdotusta, koska työnteho paranee väliaikaisesti tietoturvan kärsiessä. (Ros 2016).

Tietoturvakäytäntöjen puutos voi johtua yrityksen koosta tai tietämättömyydestä. Pienillä yrityksillä ei aina ole varaa palkata henkilöä tekemään tietoturvakartoitusta ja laatimaan tietoturvakäytäntöjen ohjeistusta tai ostaa niiden tekemistä kolmannelta osapuolelta. Myöskin joillain suuremmilla yrityksillä tietoturva voi jäädä jälkeen tietämättömyyden ja välinpitämättömyyden takia.

2.8 Lokijärjestelmän puutos

Lokijärjestelmällä seurataan tapahtumia järjestelmässä, esimerkiksi salasananvaihtoja, käyttöoikeuksien muutoksia tai kuka on käyttänyt mitäkin ja milloin. Lokit voivat toimia hälytyksinä tietoturvassa ja auttavat seuraamaan kuka on aiheuttanut mitäkin. (Glover 2019)

Jos lokijärjestelmää ei ole, on mahdotonta tietää, kuka on tehnyt mitäkin ja haitalliset tekijät järjestelmässä jäävät helposti huomaamatta. Onneksi lokisysteemeissä on mahdollisuus valita kriteereitä, mistä näytetään loki. Esimerkiksi kriteeriksi voidaan valita uusi kirjautuminen uudesta IP-osoitteesta. (Glover 2019)

Lokijärjestelmää pitää myös ylläpitää ja mukauttaa muuttuvaan yritykseen ja sen muihin järjestelmiinn. Jos lokijärjestelmä ei ole ajan tasalla, on siitä vähän hyötyä. Lisäksi tarvitaan myös henkilö, joka on vastuussa lokien tarkastamisesta ja seuraa niitä, sillä muutoin lokien ottaminen on turhaa.

Gary Glover jakaa lokijärjestelmän käyttöönoton seitsemään osaan (Glover 2019):

1. Miten ja mitä kerätään
2. Säilö kerätyt lokit huolellisesti
3. Valitse lokeille vastuuhenkilö,
4. Valitse ryhmä valmiina tutkimaan hämäriä hälytyksiä
5. Valitse säännöt hälytyksille
6. Säilytä lokit vuoden ajalta
7. Tarkasta yleisesti voiko lokien ottamista parantaa

3 INHIMILLISEN VIRHEEN MINIMOIMINEN

Ihhimillinen virhe käy kalliiksi yrityksille. IBM:n mukaan inhimllinen virhe on syynä 24 prosenttiin datamurroista. Tietomurron aiheuttamat kulut ovat keskimäärin 3,5 miljoonaa Yhdysvaltojen dollaria, yksi kirjaus on arvoltaan keskimäärin 133 dollaria ja murron selvittämiseen kuluu keskimäärin 242 päivää. (IBM 2019.) Ihmisvirheen minimoiminen on moniosainen prosessi, johon kaikkien pitää osallistua hyödyn saamiseksi. Seuraavassa tutkimme parhaita keinoja, joilla voi pienentää inhimillisen virheen riskiä.

3.1 Koulutus

Tietoturva on yhtä vahva kuin sen heikoin lenkki. Siksi kaikkien pitää olla mukana, kun koulutetaan työntekijöitä. Koulutus voi olla suoraan tietoturvasta tai työntekijän omasta roolista yrityksessä. Työntekijöille, jotka käsittelevät kriittistä dataa tai teknologiaa, koulutus on erityisen tärkeätä, koska heidän virheensä voi aiheuttaa pahempaa tuhoa (Diedrich 2019).

Jos koulutusta halutaan luoda sisäisesti, pitää ensin löytää epäkohta, johon tarvitaan korjausta. Esimerkiksi vähän aikaa yrityksessä olleelle henkilölle voidaan tarvita koulutusta datan analysoinnista vanhan työntekijän poistuessa tai rekrytoinnin jälkeen viidelle uudelle työntekijälle pitää saada tietoturvakoulutusta. Koska koulutukset vievät rahaa ja aikaa, on hyvä asettaa tavoitteet koulutukselle ennen kuin se aloitetaan. Työntekijöiden mukaan ottaminen jo suunnitteluvaiheessa parantaa koulutuksen vaikutusta, koska silloin se soveltuu paremmin juuri heille. (Pavlou 2019)

Koulutuksen ulkoistaminen maksaa rahaa, mutta sillä on myös hyvät puolensa. Ulkoistetussa koulutuksessa saadaan ammattilaisia kouluttamaan työntekijöitä. Alansa hyvin tuntevat kouluttajat tietävät mistä puhuvat. Jos koulutettavia ei ole paljon tai koulutuksia ei tulla tarvitsemaan lisää, koulutuksen ulkoistaminen on hyvä vaihtoehto. (Pavlou 2019)

Mielestäni koulutus on tärkeää työntekijöiden moraalin kannalta. Jos osaat tehdä työtäsi hyvin, tekeminen tuntuu huomattavasti mielekkäämmältä ja virheiden määrä vähenee. Koulutus myös lisää ”pitkässä juoksussa” yrityksen tulosta, kun työntekijät tekevät työnsä tehokkaammin ja paremmin. Tietoturvakoulutuksilla annetaan työntekijöille valmius ja tieto huomata mahdolliset hyökkäykset ja huijaukset.

3.2 Käyttöoikeudet ja niiden kontrolli

Käyttöoikeuksien kontrollilla tarkoitetaan suunniteltua järjestelmää, jolla annetaan käyttöoikeuksia työntekijöille, jotka niitä tarvitsevat (Carlson 2017). Esimerkiksi palvelinpuolella työskentelevät tarvitsevat pääsyn palvelimiin tehdäkseen työnsä, mutta asiakaspalvelutyöntekijällä ei ole tarvetta tämän kaltaisiin käyttöoikeuksiin.

Käyttöoikeudet pitää jakaa tarkasti sen mukaan, mitä käyttöoikeuksia tarvitaan eri työntekijöille. Scott Carlson jakaa raportissaan työntekijät neljään osaan: myynti ja asiakaspalvelu, analysointi ja liiketoiminta, järjestelmä ja verkko sekä kehittäjät, sovellustyöntekijät ja datatyöntekijät (Carlson 2017). Mielestäni tämä on hyvä alku, mutta ei kata kaikkia työntekijöitä ja heidän tarpeitaan varsinkaan isoissa yrityksissä. Jos peruskäyttäjällä on liikaa oikeuksia päästä katsomaan esimerkiksi yrityksen keräämää dataa tai palvelimen toimintaa, voivat hyökkääjät päästä varastamaan tai tuhoamaan yrityksen tuotoksia helpommin jo alimman tason tunnuksilla.

Jotta päästäisiin turvalliseen käyttöoikeuksien kontrolliin, pitää tarkasti valita kenellä on mihinkin oikeudet ja muokata niitä tarpeiden mukaan. Ei riitä, että valitaan kerran osiot ja laitetaan niillä käyttöoikeudet jakoon. Käyttöoikeuksien kontrollin täytyy kehittyä yrityksen mukana sen lisätessä työntekijöitä ja työkaluja. Olisi suositeltavaa lisätä kaksivaiheisen tai kolmivaiheisen tunnistautumisen tärkeimpiin tietoihin ja systeemeihin yrityksessä, tietoturvan parantamiseksi. Kaksivaiheinen tunnistautuminen käyttää kahta eri tunnistautumis metodia, kuten salasana ja puhelimessa oleva sovellus, joka antaa erillisen koodin, kun kirjaudut. Kolmivaiheinen tunnistautuminen vaatii kolmea eri tunnistautumis tapaa.

Yhtenä uhkana on myös poistuvat työntekijät. Jos heidän tunnuksia ei poisteta, voi aiheutua tietoturvariski, kun tunnukset varastetaan tai poistuneet työntekijät käyttävät niitä itse tietojen varastamiseen. Tunnukset voivat myös sisältää korkeampiakin oikeuksia kontrollin muuttuessa

3.3 Kommunikointi

Jotta kaikki työntekijät tietäisivät yrityksen käytännöistä ja siihen liittyvistä säännöstöistä ja sovelluksista sekä tietoturvasta, tarvitaan hyvää kommunikaatiota. Hyvällä kommunikaatiolla saadaan yrityksen muutokset kaikille tietoon ja edistetään vapaampaa tiedon

levittämistä. Onnistuneella kommunikaatiolla ongelmista saadaan tieto niille henkilöille, jotka voivat asioita parantaa. Lisäksi kommunikointi parantaa koulutusta, kun saadaan palautetta koulutuksista ja tieto tarvittavista koulutuksista liikkuu eteenpäin.

Ideoiden vähentyessä ongelmia voi olla kommunikaatiossa. Vuonna 2012 tehdyn tutkimuksen mukaan 75 prosenttia ihmisistä eivät tunne saavansa kaikkea irti luovuudestaan (Adobe 2012). Kommunikaation pitää liikkua kolmeen suuntaan: johdolta työntekijöille, työntekijöiltä johdolle ja työntekijöiltä työntekijöille (Axero 2019).

Kommunikoinnin parantamiseen on paljon tapoja. Teknologian kannalta alustat, kuten Slack (slack.com), toimivat hyvinä kommunikaatiovälineinä. Oikein käytettynä voidaan jakaa tarvittava tieto ja tiedostot helposti osastoille, jotka niitä tarvitsevat ja kommunikointi toimii nopeasti.

Kommunikaation IT-osaston ja muiden osastojen välillä on oltava hyvällä tasolla, jotta uusimmat uhat saadaan työntekijöille tietoon ja IT-osasto saa palautetta ja toiveita parannuksista yrityksen järjestelmiin.

3.4 IT-palautussuunnitelma ja sen testaus

Nykyään lähes kaikki yritykset tarvitsevat teknologiaa toimiakseen, mutta mitä tapahtuu kun jokin ei toimi? Kun jotain sattuu, on hyvä olla testattu palautussuunnitelma, jolla saadaan yrityksen toiminta palautettua normaaliin rytmiin. Ilman suunnitelmaa vahingoista ja hyökkäyksistä aiheutuu suurempia ongelmia kuin pitäisi.

IT-palautussuunnitelma pitää tehdä yhdessä toiminnan jatkuvuussuunnitelman kanssa, jolloin ne toimivat rinnakkain. IT-palautussuunnitelma pitää kohdistaa tietojärjestelmiin, dataan, sovelluksiin ja laitteistoon. Suunnitelma sisältää strategioita palauttaa toiminta mahdollisimman nopeasti, listauksen ja kuvauksen laitteista ja resursseista, joita tarvitaan, sekä aikamääreitä, joihin pitää ehtiä ja listan tehtävistä, jotka pitää suorittaa, kun kriisi on ohi (Queensland Goverment 2016).

Palautussuunnitelma pitää olla kunnossa ja testattu, jotta kriiseistä selvitään. Suunnitelma on sitä tärkeämpi, mitä suurempi yritys on. Ihmis- ja laitteistomäärän kasvaessa kriisien vaikutus suurenee, koska ne voivat vaikuttaa monenkin ihmisen elämään ja aiheuttaa suurempia kuluja laitteiston palautuksessa. Kaikki aika, joka on tuhlattu kriisin selvittämiseen, on pois tehokkaasta liiketoiminnasta ja kehittämisestä.

3.5 Automaatio tietoturvan edistäjänä

Automaatio on erittäin hyvä työkalu lähes kaikille yrityksille. Sen avulla voidaan parantaa työntekijöiden tehokkuutta ja vähentää kuluja poistamalla kauan vieviä manuaalisia töitä. Kun työntekijät tekevät toistuvia toimenpiteitä, he saattavat kyllästyä tekemiseen. Kyllästyminen vähentää keskittymistä, joten he tekevät virheitä herkemmin. Automatisoidut prosessit taas tekevät aina saman asian, joten mahdollisuus ihmisvirheelle pienenee huomattavasti. (Ferguson 2019)

Automaatio ei kuitenkaan poista ihmisvirhettä. Automatisoitu prosessi on jonkun tekemä, jolloin on mahdollisuus virheeseen sen luomisessa. Täytyykin olla erittäin tarkkana, kun automoitua prosessia luodaan, jotta vahingolta vältyttäisiin.

Automatisointi mahdollistaa monitoroinnin ja tietoturvapäivitysten paremman hallinnan. Kun yrityksellä on monia tuhansia laitteita, ei ole mahdollista vain ihmistyöllä monitoroida ja ylläpitää laitteistoa. Automatisoimalla päivityksiä ja monitorointia saadaan suurikin määrä laitteistoa turvallisemmaksi ja vapautetaan työntekijöitä tekemään muita tärkeämpiä tehtäviä. (Merritt 2018)

Jotta automatisaatiota voidaan kehittää, täytyy suunnitella tarkasti, mitä halutaan automatisoida ja miten se toteutetaan. Automatisoinilla pitää myös olla jokin haluttu tavoite. Halutaanko nopeuttaa käyttöoikeuksien vaihtoja tai vaikkapa nopeuttaa lähtevän työntekijän tunnuksien poistoa. Tekijöiden täytyy olla alansa ammattilaisia, jotka tietävät automaatiosta ja prosesseista, jota he ovat automoimassa. (Forbes 2018)

Automatisaatio on vieläkin kuuma aihe, johon kaikilla yrityksillä ei ole vielä varaa tai työntekijöitä tekemään automaatiota. Automaatio tulee vieläkin suuremmaksi osaksi yritystoimintaa tulevina vuosina ja yritykset, jotka haluavat pärjätä tässä kehittyvässä kilpailussa joutuvat investoimaan automaatioon.

3.6 Tietoturvapolitiikka

Tietoturvakäytäntöjen ohjeistus eli tietoturvapolitiikka on yrityksen eri osastojen päättäjien yhteistyöllä tehty ohjekirja suojauskeinoista yrityksen tärkeille laitteistoille ja informaatiolle. Tietoturvakäytäntöjä luomassa pitää olla mukana yrityksenjohto, IT-osasto, la-

kiosasto ja henkilöstöosasto. Tietoturvakäytäntöjen ohjeistus ei anna teknologista ratkaisua, vaan selittää tietynlaiset tavat ja olosuhteet, jotka auttavat suojaamaan yrityksen omaisuutta. Tietoturvakäytännöt antavat myös ohjeistusta työntekijöille käytännöistä, resursseista ja mitä ei saa tehdä tai käyttää. (Kumar 2019)

Tietoturvakäytännöt auttavat työntekijöitä ymmärtämään heidän vastuutaan tärkeän datan suojaamisessa. Se opettaa käytäntöjä salasanoista, tiedostojen liikuttamisesta ja tiedostojen tallentamisesta. Tietoturvakäytännöt myös lisäävät työntekijöiden tietoisuutta tietoturvasta kokonaisuutena ja miten sitä voidaan parantaa. (Java T Point 2018)

Tietoturvakäytäntöjen luominen on koko yrityksen yhteinen projekti, joka koskee kaikkia yrityksessä työskenteleviä henkilöitä. Myös yrityksen ulkopuolelta tulevat palveluntarjoajat joutuvat noudattamaan tietoturvakäytäntöjä, jos he käyttävät yrityksen laitteistoa (Kumar 2019).

Tietoturvakäytäntöjen tulisi sisältää fyysisen turvallisuuden, henkilöstöhallinnon sekä laitteisto- ja sovelluspuolen. Fyysinen turvallisuusosio sisältää toimistojen sisäänkäyntien, turvakameroiden ja ovien ohjeet sekä keinoja, joilla työntekijät ja johtajat voivat suojata fyysistä omaisuutta. Henkilöstöhallinnon kannalta pitää löytyä ohjeistusta turvalliseen työn tekemiseen päivittäin, kuten salasanaohjeistus ja salatun tiedon käsittely. Laitteisto- ja sovelluspuoli kertoo esimerkiksi minkälaista teknologiaa saa käyttää sekä verkkokontrollista. (Kumar 2019)

Tietoturvakäytäntöjä pitää myös auditoida. Auditoinnin voi suorittaa sisäisesti tai sen voi ulkoistaa. Auditointi auttaa ymmärtämään uhkia paremmin ja miten tämän hetkinen suojaus vaikuttaa niihin. Auditointi auttaa myös löytämään aukkoja tietoturvakäytännöissä, jotta niitä voidaan parantaa. (McAfee 2019)

4 LOPUKSI

Opinnäytetyön tarkoituksena oli kuvata, miten inhimillinen virhe vaikuttaa tietoturvaan sekä luoda tietoturvaohjeistus, joka antaa ohjeita tietoturvan parantamiseen ja virheen minimoimiseen.

Työni ohjeistaa ihmisiä toimimaan paremmin ja turvallisemmin niin yrityksissä kuin yksityiselämässä tietoturvan kannalta, jotta voidaan välttää ja pienentää riskejä. Lisäksi opinnäyte ohjeistaa toimimaan oikein, jos tietoturvaongelmia esiintyy. Toivon, että työstäni on hyötyä yksityishenkilöille ja yrityksille.

Koska inhimillistä virhettä ei voida poistaa, sitä pitää minimoida. Tämä oli opinnäytetyöni ensimmäinen näkökanta, jonka mukaan lähdin työtäni miettimään eteenpäin. Opinnäytteen tekeminen alkoi hitaasti, mutta kun pääsin kiinni aiheeseen paremmin, työ eteni hyvin. Lähteitä oli mielenkiintoista lukea ja opin niistä itsekin enemmän.

Tulevaisuudessa toivon, että tietoturva tullaan ottamaan mukaan peruskoulutukseen viimeistään lukiossa ja ammattikoulussa sen kasvavan tärkeyden takia. Tietoturva tulee lähes jokaiselle vastaan jossain kohtaa elämää.

LÄHTEET

Adobe. 2012. State of create study. Viitattu 27.11.2019

Axero. 2019. The Cure to What Ails Internal Communications. Viitattu 26.11.2019

Bianculli, L. 2019. 10 Common IT Security Risks in the Workplace. Viitattu 7.11.2019 https://www.ccsinet.com/blog/common-security-risks-workplace/.

Calrson, S. 2017. What is Privilege Management and Where Do You Start? Viitattu 13.11.2019

Center for Internet Security 2019. Top 10 Malware January 2019. Viitattu 7.11.2019 https://www.cisecurity.org/blog/top-10-malware-january-2019/.

Cloudflare 2019. What is a DDoS attack?. Viitattu 12.11.2019 https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

Cohen, D. 2018. Twitter Corrected a Bug That Caused Passwords to Be Stored in Plain Text. Viitattu 14.11.2019. https://www.adweek.com/digital/twitter-corrected-a-bug-that-caused-passwords-to-be-stored-in-plain-text/.

Diedrich, S. 2019. 5 Ways to Prevent Human Error Disasters. Viitattu 25.11.2019 https://blog.newcloudnetworks.com/5-ways-to-prevent-human-error-disasters.

Enisa 2019. ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends. Viitattu 7.11.2019

Ferguson, N. 2019. Human Error: How Automation Can Mitigate Operational Risk. Viitattu 27.11.2019 https://www.automation.com/automation-news/article/human-error-how-automation-can-mitigate-operational-risk.

Glover, G. 2019. The Importance of Log Management. Viitattu 21.11.2019 https://www.security-metrics.com/blog/importance-log-management.

Gupta, V. 2012. SEC_RITY is not complete without U - Secure Your Organization's IT Assets before they join army of Botnets. Viitattu 25.11.2019 https://www.ibm.com/developerworks/community/blogs/48a78681-82cc-434f-9c78-3e9117bfd466/entry/march_2_2012_4_09_am1?lang=en.

IBM Security. 2019. Cost of a Data Breach Report. Viitattu 25.11.2019

Java T Point. 2018. Security Policies. Viitattu 28.11.2019 https://www.javatpoint.com/cyber-security-policies.

Kingori, D. 2019. Top 10 Cybersecurity Risks For 2019. Viitattu 7.11.2019 https://www.uscybersecurity.net/risks-2019/.

Kumar, A. 2019. An Introduction to Cyber Security Policy. Viitattu 28.11.2019 https://resources.infosecinstitute.com/cyber-security-policy-part-1/.

Long, L. 2018. How The Right Automation Road Map Helps Overcome Human Error. Viitattu 27.11.2019 https://www.forbes.com/sites/forbestechcouncil/2018/11/09/how-the-right-automation-road-map-helps-overcome-human-error/#6b1afb60647f.

McAfee. 2019. How Cybersecurity Policies and Procedures Protect Against Cyberattacks. 28.11.2019 https://www.mcafee.com/enterprise/en-hk/security-awareness/cybersecurity/cybersecurity-policies.html.

Merritt, C. 2018. IT Process Automation: How to Reduce Human Error in Your IT Operations Viitattu 27.11.2019 https://www.dataprise.com/resources/blog/reduce-human-error-it-process-automation.

Michigan State University. 2019. How to Recognize a Malware Email. Viitattu 25.11.2019 https://www.egr.msu.edu/decs/security/how-recognize-malware-email.

Pavlou, C. 2019. How to build your first employee training program. Viitattu 25.11.2019 https://resources.workable.com/tutorial/employee-training-program .

Pervilä, M. Varjo-it hyötykäyttöön näillä nikseillä. Viitattu 12.11.2019 https://www.tivi.fi/uutiset/varjo-it-hyotykayttoon-nailla-nikseilla/ea23d25e-8fc1-39ac-b593-1f552e7ca808.

Queensland Goverment. 2016. Developing a recovery plan. Viitattu 28.11.2019 https://www.business.qld.gov.au/running-business/protecting-business/risk-management/recovery-plan.

Ros, P. 2016. Varjo-IT on myrkkyä digitalisaatiolle. Viitattu 12.11.2019. https://www.tivi.fi/kumppaniblogit/salesforce/varjo-it-on-myrkkya-digitalisaatiolle/623e32d9-fa6f-3c0e-ab03-b7f4cca0d041.

Security First 2019. The Top 9 Network Security Threats of 2019 Viitattu 7.11.2019 https://securityfirstcorp.com/the-top-9-network-security-threats-of-2019/.

Sullivan, B & Vincent, L. 2011. Web Application Security, A Beginner's Guide. McGraw-Hill Education.

University of San Diego 2019. Top Cyber Security Threats in 2019. Viitattu 7.11.2019 https://onlinedegrees.sandiego.edu/top-cyber-security-threats/.

W3schools. 2019. SQL Injection. Viitatttu 25.11.2019 https://www.w3schools.com/sql/sql_injection.asp.

Whatsmyipaddress. 2019. Malware Threats: 7 Ways To Protect Your Computer. Viitattu 25.11.2019 https://whatismyipaddress.com/protection-from-malware.

Whittaker, Z. 2019. Indian state government leaks thousands of Aadhar numbers. Viitattu 14.11.2019 https://techcrunch.com/2019/01/31/aadhaar-data-leak/.

Liite

Tietoturvaohjeistus ihmisvirheen vähentämiseksi

1. Koulutus

   Koulutuksella vähennetään ihmisten virheitä heidän tietotaidon kasvaessa ja parannetaan yrityksen tulosta, kun työntekijät voivat tehdä työtään paremmin. Koulutusta voi luoda sisäisesti tai ostaa ulkoisesti.

   Ohje

   - Löydä asia, johon tarvitaan koulutusta
   - Valitse joko ulkoinen tai sisäinen koulutus
   - Jos valitset sisäisen koulutuksen, valmistele se huolellisesti
   - Ota työntekijät mukaan jo koulutuksen kehittämisessä
   - Ota palautetta koulutuksesta

2. Käyttöoikeuksien kontrolli

   Käyttöoikeuksien kontrolli suojaa yrityksen tärkeää omaisuutta niin omien työntekijöiden virheiltä kuin ulkopuolisilta tahoilta. Käyttöoikeuksien kontrolli on jatkuva prosessi, jonka täytyy kehittyä yrityksen mukana.

   Ohje

   - Jaa työntekijät osioihin käyttöoikeuksien suhteen
   - Anna heille vain ne oikeudet, jotka he tarvitsevat työn tekoon
   - Paranna kontrollia tarpeen mukaan yrityksen muuttuessa
   - Sisällytä kaksi- tai kolmivaiheinen tunnistautuminen tärkeimpiin järjestelmiin ja tietoihin
   - Muista poistaa turhat tunnukset, kuten poistuvien työntekijöiden tunnukset

3. Kommunikointi

   Parantamalla kommunikaatiota vähennetään virheitä, jotka johtuvat väärinymmärryksistä. Vapaammalla kommunikaatiolla saadaan yrityksen sisällä olevia ideoita myös esiin.

   Ohje

   - Valitse alusta kommunikaatiolle sähköpostin lisäksi, esimerkiksi Slack
   - Pidä tapaamisia kasvotusten työntekijöiden kanssa
   - Kerro uusille työntekijöille kommunikaatiotavoista

4. IT-palautussuunnitelma

   IT-palautussuunnitelma auttaa yritystä palaamaan normaaliin työntekoon, kun jotain sattuu. Aika on rahaa ja palautussuunnitelma vähentää ajan tuhlaamista.

   Ohje

   - Luo palautussuunnitelma rinnakkain jatkuvuussuunnitelman kanssa
   - Kohdista suunnitelma dataan, tietojärjestelmiin, laitteistoon ja sovelluksiin
   - Tee strategia palautukseen
   - Tee lista ja kuvaa tarvittavista laitteistoista ja resursseista
   - Aikamääreet, joihin pitää ehtiä
   - Auditoi ja testaa palautussuunnitelma

5. Automaatio

   Automaatiolla nopeutetaan tehtäviä ja vähennetään ihmisten tekemiä virheitä toistuvissa töissä. Kun päivityksetkin ovat automatisoitu, vähentyy tunkeutumisen riski. Monitoroinnin automatisoiminen vapauttaa suuren määrän työtunteja.

   Ohje

   - Valitse tarkasti mitä halutaan automatisoida

- Suunnittele toteutus
- Valitse automatisaation tekijöiksi ammattilaisia, jotka tietävät automoitavasta prosessista
- Tarkasta automatisoitu prosessi tarkasti, jotta siinä ei ole virheitä

6. Tietoturvakäytännöt

Tietoturvakäytännöt ovat koko yrityksen laajuinen ohjeistus, jossa kerrotaan tavoista, joilla voidaan suojata yrityksen omaisuutta. Tietoturvakäytännöt auttavat myös työntekijöitä ymmärtämään enemmän tietoturvasta ja antavat heille tapoja parantaa tietoturvaa, kuten salasanakäytäntöjä.

Ohje

- Luo tietoturvakäytännöt yrityksen johdon, IT-puolen, lakiosaston ja HR-osaston kanssa
- Selitä tapoja ja olosuhteita, joilla suojataan omaisuutta
- Sisällytä ohjeita työntekijöille
- Auditoi tietoturvakäytännöt joko sisäisesti tai ulkoisesti