jamk.fi

Tietoturvallisuus palvelunhallinnassa

Harjoitustyö

Joni Korpihalkola
Joonas Maninen
Niko Poutanen
Ville Pulkkinen
Mikael Romanov
Niko Tamminen

Kurssityö
Huhtikuu 2018
Tieto-ja viestintätekniikka
Tekniikan ja liikenteen ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisällysluettelo

Kuviot

1 Johdanto

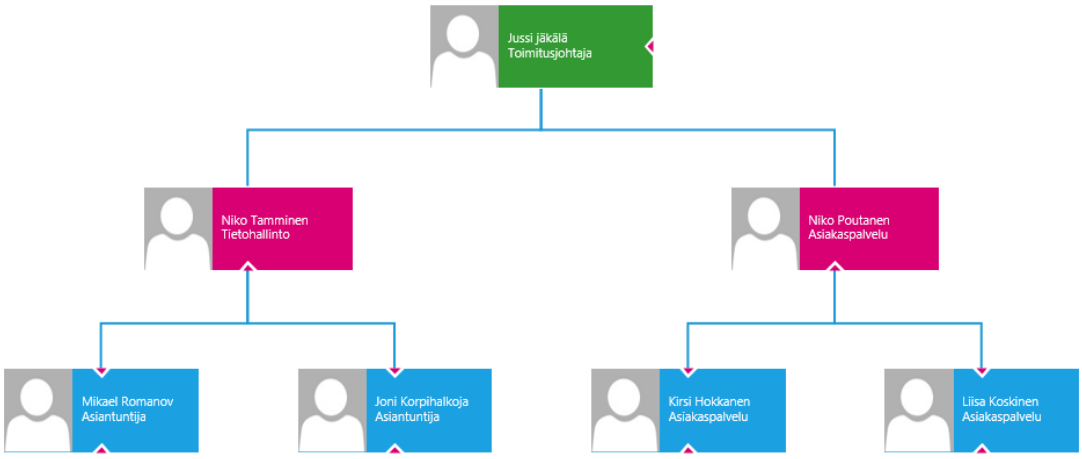
Tietoturvallisuus palvelunhallinnassa kurssityössä piti suunnitella jokin palvelu, sekä kyseisen palvelun prosessit. Työssä suunnitellaan kuvitteellisen yrityksen prosessit jollekin palvelulle sekä palvelut tulee kuvata palveluluettelossa. Työssä keskityttiin tietoturvan hallintaan osana palvelunhallintaa. Tietoturvan toteuttamisessa tutkittiin ISO/27000-sarjan tuoteperhettä joka määrittää turvallisen tiedon käsittelyn yrityksissä.

2 Yritys

Työssä tuli valita kuvitteellinen yritys, jolle suunniteltiin prosessit ja palvelut sekä tietoturvan toteutus soveltaen kahta edellistä. Valitsimme kuvitteelliseksi yritykseksi PupariHosting yrityksen joka toteuttaa räätälöityjä pilvipalveluja sekä webhotelleja yrityksille. Dokumentissa käsitellään vain virtuaalipalvelinten osaa palvelun toteutuksessa.

2.1 Organisaatiorakenne

Organisaatiossa on 2 osastoa, tietohallinto ja asiakaspalvelu. Tietohallinto toimittaa kaikki IT-palvelut ja vastaa teknisistä ratkaisuista. Asiakaspalvelu vastaa asiakkaiden informoinnista, tilausten käsittelystä, ja tapahtumien hallinnasta 1-tasolla. Organisaatio rakenne on kuvattu kuviossa 1. (Kuvio 1)



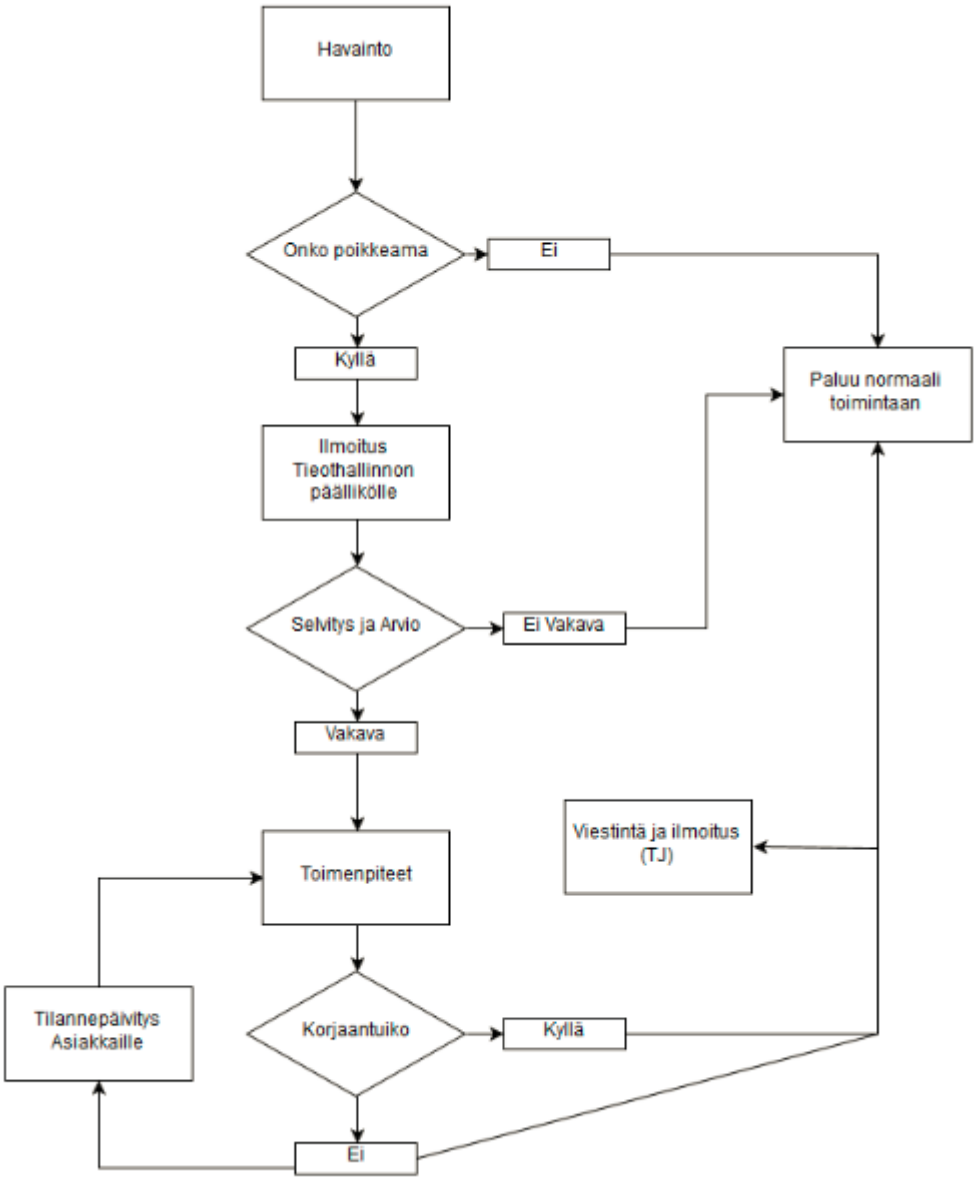
Kuvio 1 Organisaatiorakenne

2.2 Yhteistyökumppanit

Yrityksen yhteistyökumppaneihin kuuluu paikallinen operaattori, sähkön jakokeskus, paikallinen kiinteistövälitys ja Microsoft, joiden kanssa on tehty lisensseistä ja vuosittaisista kuluista sopimus.

2.3 Toimintamalli

Yrityksen toimintamalli poikkeamatilanteessa esimerkiksi sähkökatkos, hyökkäys tai huoltokatkoksen aikana on kuvattu toimintamalli rakenteella. (Kuvio 2)



Kuvio 2 Toimintamalli

3 Palvelu

Yritys toteuttaa useita palveluita, mutta tähän dokumenttiin valittiin yksi lähempää tarkastelua varten. Valitsimme palveluksemme dedikoidut virtuaalipalvelimet. PupariHosting tarjoaa asiakkaalle listan tarjolla olevista virtuaalikoneista, joita asiakas voi lisätä ympäristöönsä resurssiluokan puitteissa (Kuvio 3). Virtuaalikoneiden listaa voidaan kasvattaa asiakkaiden pyyntöjen perusteella. Palvelua on saatavilla kolmessa eri resurssiluokassa (Lite, Medium ja Extreme), jonka rajoitukset ja hinnat on listattu taulukkoon 1. Kiinteän kuukausihinnan lisäksi, asiakas voi ostaa

lisäpalveluna lisää virtuaalikoneita käyttöönsä hintaan 5€/virtuaalikone tai vastaavasti tarpeiden mukaan lisää CPU-ytimiä, RAM-muistia, levytilaa tai kuukausiliikennettä.

Tarjottavat käyttöjärjestelmät	
Distributions	Vesiot
RHEL-based	LTS/normal releases
Fedora-based	LTS/normal releases
openSUSE-based	LTS/normal releases
urpmi-based	LTS/normal releases
Debian-based	LTS/normal releases
Ubuntu-based	LTS/normal releases
Knoppix-based	LTS/normal releases
Pacman-based	LTS/normal releases
Gentoo-based	LTS/normal releases
Windows-based	enterprise

Kuvio 3 Yrityksen tarjoamat käyttöjärjestelmät

3.1 Palvelun saatavuus

Palvelun tulee olla saatavilla poikkeuksetta 24 tuntia vuorokaudessa. Tämä tarkoittaa, että asiakkaan on saatava yhteys virtuaalikoneeseen vuorokauden ajasta riippumatta. Täyttä saatavuutta ei voida taata kuin 95% varmuudella. Riskejä palvelun saatavuuteen voivat olla sähköverkon ongelmat, tietoverkon ongelmat operaattorilla sekä muut fyysiset uhat ja luonnonilmiöt. Palvelusopimuksessa on määritelty tarkemmat vastuut asiakkaan ja toimittajan välillä.

3.2 Palvelupiste

Palvelun asiakaspalvelupiste toimii puhelimitse sekä sähköpostitse. Asiakaspalvelupisteen kautta useimmat asiakasta koskevat prosessit voidaan käynnistää. Asiakas saa haluamaansa palvelua SLA sopimuksen mukaisesti. Asiakaspalvelu hoitaa kaiken tiedottamisen asiakkaan ja toimittajan välillä. Asiakaspalvelu ottaa vastaan herätteitä insidenttien käynnistämiseksi.

4 Palvelun tekniikka

Yrityksellä on pieni konesali betonibunkkerissa, joka on viestintäviraston vaatimusten mukainen. Konesali on kalustettu neljällä 42-yksikön palvelinkehikolla, johon on sijoitettu kaikki aktiivilaitteet. Yksi palvelinkehikko maksaa 700 euroa, joten kehikoiden kokonaishinnaksi tulee 2800€.

Laitteisto on hankittu viiden vuoden päähän sijoitetun tavoitteellisen käyttäjämäärän mukaan, jossa ostettuja palveluita on 1500. Käyttäjät jakautuvat resurssiluokkiin seuraavasti:

- Lite, 1000 ostettua palvelua
- Medium, 300 ostettua palvelua
- Extreme, 200 ostettua palvelua

Laitteistohankinnat on tehty kertomalla resurssiluokkien rajoitukset ostettujen palvelujen määrällä. (Taulukko 1)

Luokka	**Ostetut palvelut (kpl)**	**RAM (GB)**	**Levytila (TB)**
Lite	1000	2000	20
Medium	300	2400	30
Extreme	200	3200	100
Yhteensä	**1500 kpl**	**7600 GB**	**150 TB**

Taulukko 1. Palvelut

Laitteisto vastaavasti alla olevassa taulukossa. (Taulukko 2)

Laite	**Määrä**	**Hinta**
Server HPE ProLiant	20	110 000€
NAS QNAP	1	3000€

UPS MGE	1	10 800€
RAM 64 BG	120 (7680GB)	83 000€
HDD Seagate 10 TB	16 (160TB)	5 760€
Yhteensä		**212 560€**

Taulukko 2. Laitteisto

- Laitteistokulut yhteensä 212 560€
- Arvioidut vuosittaiset kulut viiden vuoden jälkeen: 150 000€
    - Sähkönkulutus
    - Vuokra
    - Internetyhteydet

4.1 Palveluympäristö

Yrityksen serverit käyttävät KVM:tä hypervisorina, joka tarjoaa alustan virtualisoinnille ja huolehtii työn suorittamisesta. Keskitettyä palvelun hallintaa ylläpitää ja hallitsee IT väki Kimchi web käyttöliittymällä. Asiakkaat pääsevät virtuaaliympäristöihinsä kiinni GNOME Boxes managerilla.

4.2 Palvelu hinta

Palvelua on saatavilla kolmessa eri resurssiluokassa. Lite, Medium ja Extreme. Eri palveluissa on erilainen SLA sopimus, joka määrittää palvelun saatavuuteen liittyviä mittareita. (Taulukko 3)

Palvelu	CPU ytimet	RAM-muisti	Levytila	Liikenne/kk	Koneiden määrä	Hinta/kk
Lite	1	2 GB	20GB	1TB	2	30€
Medium	2	8GB	100GB	4TB	4	70€

Extreme	2	16GB	500GB	Rajaton	6	140€

Taulukko 3. Yrityksen tarjoamat palvelut

5 Liiketoimintaperuste

5.1 Palvelun tavoite

Yrityksen liiketoiminta perustuu asiakkaiden ostamien palveluiden ylläpitoon ja myyntiin. Palvelun tavoite on tarjota korkean saatavuuden pilvipalvelua vuorokauden ajasta riippumatta. Palvelun ylläpito ja tukipalvelut ovat myös saatavilla vuorokauden ympäri.

5.2 Kilpailijat

Pilvipalveluilla on kova kilpailu Suomessa ja uuden palvelun tuominen markkinoille on todella riskialtista. Palvelujen hinnat on saatu todella alas, joten kuluttajat valitsevat palvelun yleensä hinnan perusteella. Palvelumme on suunnattu yrityksille, joten panostamme enemmän laatuun ja palveluun kuin tuotteen hintaan.

5.3 Riskit

Palvelulla on useita eri riskejä. Suurimmat riskit koskevat ulkoisia toimijoita kuten operaattorit(verkkoyhteys), sähköyhtiöt(sähköntoimitus) sekä hakkerit(palvelunestohyökkäykset). Riskien vakavuudet määritellään ISO/27005 standardin pohjalta josta kerrotaan myöhemmin.

5.4 ROI-analyysi

ROI-analyysi eli “Return on Investment” kuvaa investoinnin tuottamia kassavirtoja sen sitomaan pääomaan. Palvelun käyttäjämäärä 5 vuoden päästä on arvioitu olevan 1500. Palvelun käyttäjät on jaettu resurssiluokittain seuraavasti:

- Lite 1000 ostettua palvelua
- Medium 300 ostettua palvelua
- Extreme 200 ostettua palvelua

Voimme laskea vuosittaisen tuloksen palvelusta kertomalla kuukausittaisen palvelunhinnan palvelujen määrällä.

- Lite 30 000€
- Medium 21 000€
- Extreme 28 000€

Yhteensä palvelut tuottavat 948 000€ vuodessa.

$$ROI = \frac{Keskimääräinen\ nettotulos\ vuodessa}{palvelun\ tuottamiseen\ käytetty\ pääoma\ keskim.}$$

Palvelun tuottamiseen käytetty pääoma ensimmäisen vuoden aikana on laitekustannukset (212 560€) ja vuosittaiset kiinteät kulut (~150 000€), johon sisältyy vuokra, sähkö, internet sekä lisenssit.

Ensimmäisen vuoden ostettujen palveluiden määrä arvioidaan 100 palveluksi, ja viiden vuoden päästä ostettujen palveluiden määrän ollessa 1500 palvelua, voimme laskea vuotuisen kasvuprosentin.

$x - 1(100) = vuotuinen\ kasvuprosentti$, jossa $x = \sqrt[5]{\frac{1500}{100}}$

Yrityksen vuotuiseksi kasvuprosentiksi ensimmäisen viiden vuoden aikana saadaan näin **71,87 %**.

Ostetut palvelut skaalautuvat seuraavasti:

- Lite 66% ostetuista palveluista
- Medium 20% ostetuista palveluista
- Extreme 14% ostetuista palveluista

Tämän perusteella voimme laskea yrityksen ensimmäisen viiden vuoden kuukausittaiset tulot, käyttäen hyödyksi vuotuista kasvuprosenttia ja ostettujen palveluiden skaalautuvuutta.

Vuosi	**Lite (66%)**	**Medium (20%)**	**Extreme (14%)**	**Yhteensä**
1	66 kpl	20 kpl	14 kpl	100 kpl
	1980 €	**1400 €**	**1960 €**	**5340 €**
2	114 kpl	35 kpl	24 kpl	173 kpl
	3420 €	**2450 €**	**4080 €**	**9950 €**
3	198 kpl	60 kpl	42 kpl	300 kpl
	5940 €	**4200 €**	**7140 €**	**17 280 €**
4	343 kpl	104 kpl	72 kpl	519 kpl
	10 290 €	**7280 €**	**10 080 €**	**27 650 €**
5	593 kpl	180 kpl	125 kpl	898 kpl
	17 790 €	**12 600 €**	**17 500 €**	**47 890 €**
6	1023 kpl	310 kpl	217 kpl	1550 kpl
	30 690 €	**21 700 €**	**30 380 €**	**82 770 €**

Taulukko 4. Ensimmäisen kuuden vuoden vuosittaiset tulot

Ensimmäisen kuuden vuoden vuosittaiset tulot:

1 vuosi	**5340 €/kk**	**64 080 €/vuosi**
2 vuosi	**9950 €/kk**	**119 400 €/vuosi**
3 vuosi	**17 280 €/kk**	**207 360 €/vuosi**

4 vuosi	**27 650 €/kk**	**331 800 €/vuosi**
5 vuosi	**47 890 €/kk**	**574 680 €/vuosi**
6 vuosi	**82 770 €/kk**	**993 240 €/vuosi**

Taulukko 5. Ensimmäisen kuuden vuoden vuosittaiset tulot

6 Palveluluettelo

Palveluluettelossa on kuvattuna kaikki palvelut, niiden omistajat, käytettävät mittarit ja muita tietoja palvelusta. Palveluluettelossa tulisi olla myös yksityiskohtaisia tietoja käytettävyydestä ja huoltokatkoista. (Kuvio 4)

Palvelu	Komponentit	Palvelun saatavuus	Tukipalveluiden saatavuus-aika	Vaste-aika pyyntöihin	Korjaus-aika	Käytettävyys	Saatavuus/kk	palvelun tuottaja/osasto	Luoto(päivämäärä)
Verkkopalveluiden hallintointi	vika-ilmoitukset, muutospyynnöt, käyttäjien hallinta	24/7	8-17 Ma-Pe	30min	1h	2 käyttökatkosta/kk, huoltokatkokset(15min)	99,5%	IT-Osasto	7.2.2018
Käyttäjätunnusten hallinnointi				30min	10min				
Etäkäyttöpalvelut							95 %		
Asiantuntijapalvelut		8-17 Ma-Pe	8-17 Ma-Pe	1pv					7.2.2018
Tilausten hallinta	muutospyynnöt	8-17 Ma-Pe	8-17 Ma-Pe	4h	8h				

Kuvio 4 Palveluluettelo

6.1 Palvelun mittarit

Palvelua voidaan mitata eri mittareilla. Tietoteknisissä palveluissa yleisin mittari on palvelun saatavuus. SLA sopimus on asiakkaan ja palvelun toimittajan välinen sopimus, jossa määritellään esimerkiksi palvelun saatavuus tietyllä aikavälillä, asiakkaan ja toimittajan välinen rajapinta sekä takuu palvelulle. Esimerkiksi jos palvelu ei ole käytettävissä sopimuksen mukaisesti, asiakkaalla on oikeus reklamoida ja saada rahallista korvasta tai muuta taloudellista hyötyä aiheutuneesta ongelmasta.

6.2 Tukipalvelun saatavuus

Tukipalvelut ovat saatavilla arkisin kello 8-16, muina aikoina tukea saa päivystysnumerosta 24 tuntia vuorokaudessa. (Kuvio 5)

Palvelu	SLA	Palvelu arkisin	Palvelu viikonloppuna
Lite	A_8h	08:00-16:00	10:00-16:00
Medium	A_4h	08:00-20:00	10:00-18:00
Extreme	D_15min	24h	24h

Kuvio 5 Tukipalvelun aikataulut

7 Prosessikuvaukset

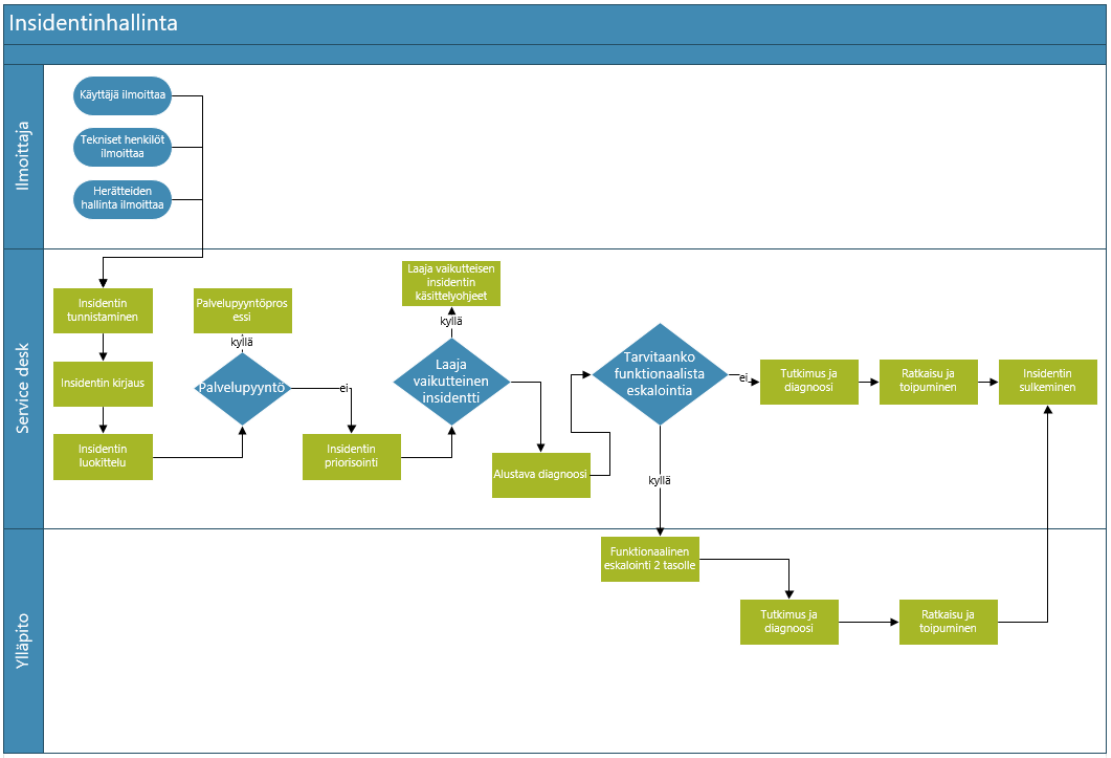
Prosessikuvauksella tarkoitetaan jonkin yrityksen toiminnan kuvausta. Prosessi on siis osa tapahtumanhallintaketjua. Prosesseja voidaan kuvata erilaisilla vuokaavioilla. Palvelun prosesseja voidaan ulkoistaa tai tuottaa sisäisesti. Yleisimpiä prosesseja ovat tapahtuman hallinta, käyttöönoton hallinta, sekä vianhallinta. Tietoturvaa käsitteleviä prosesseja kuvataan myöhemmin nojaten ISO/27000 standardi tuoteperheeseen. Palvelussamme on kuvattuna seuraavat prosessit.

1. Tapahtuman hallinta
2. Ongelman hallinta

Työ käsittelee tietoturvan toteuttamista osana palvelunhallintaa, joten käsittelemme vain prosesseja jotka keskittyvät enemmän tietoturvan toteutukseen.

7.1 Tapahtuman hallinta

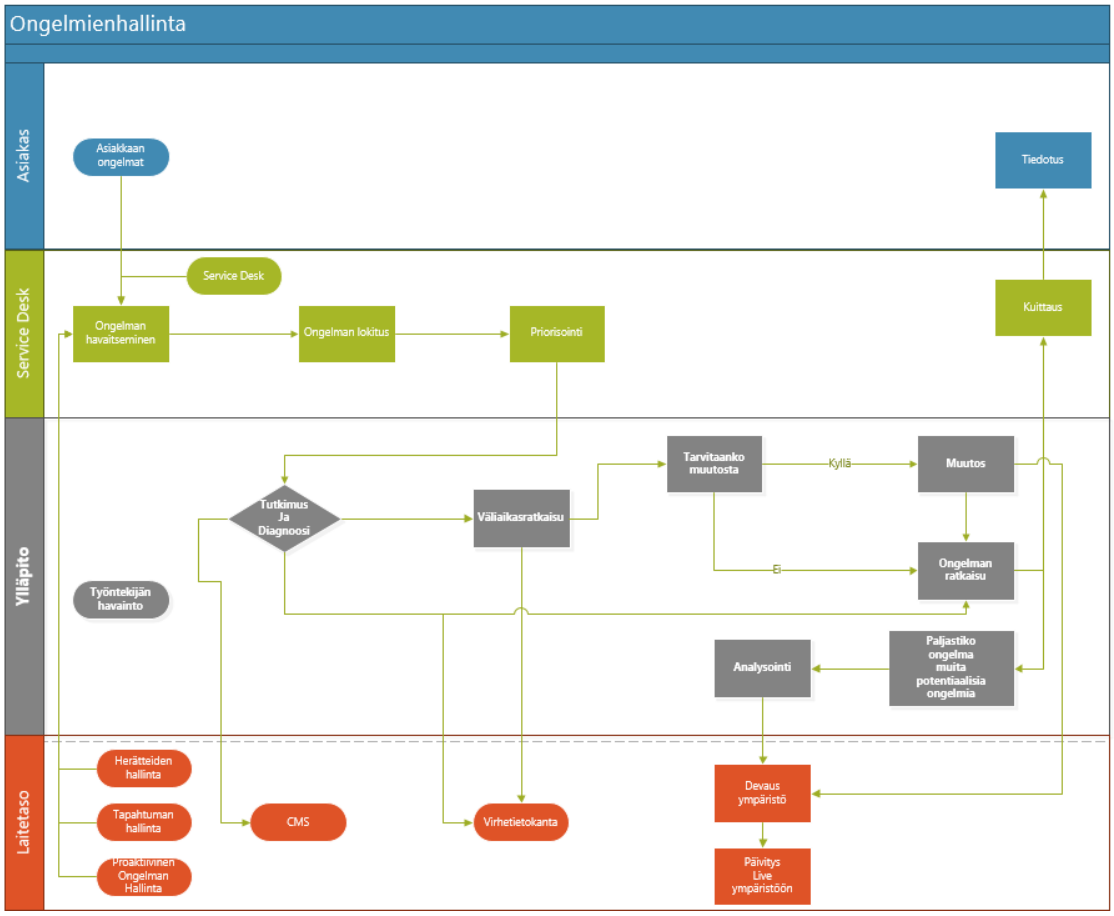
Käyttäjät tai henkilöstö ilmoittaa service deskiin toimintahäiriöistä tai muista tapahtumista. Tapahtumat voi olla myös automaattisten valvontatyökalujen havaitsemia. Service deskissä tapahtumaa aletaan tutkia ja se kirjataan ylös ja luokitellaan. Mikäli tapahtumasta lähetetään palvelupyyntö, se siirtyy palvelupyyntöprosessiin. Tapahtuma priorisoidaan ja mikäli se on laajavaikutteinen, se siirtyy toiseen prosessiin. Mikäli prosessi vaatii funktionaalista eskalointia, se siirtyy IT-ylläpidolle hoidettavaksi. Tämän jälkeen tapahtuma tutkitaan, korjataan ja kuitataan valmiiksi. (Kuvio 6)



Kuvio 6 Insidentinhallinta uimaratakaavio

7.2 Ongelman hallinta

Yrityksen ongelmanhallinta prosessi on kuvattuna alempana. Asiakkaan ongelmatilanteet havaitaan Service Deskissä, josta ongelma lokitetaan ja ongelman ratkaiseminen priorisoidaan. Ongelmatilanteet voidaan havaita myös yrityksen valvontatyökaluista tai nohevien IT-asiantuntijoiden toimesta. Asiakkaat, joilla ongelma vaikuttaa heidän yrityksen toimintaan eniten ja joidenka liiketoiminta on tärkeää PupariHosting yritykselle, saavat isomman prioriteetin ongelman ratkaisemiseen. (Kuvio 7)



Kuvio 7 Ongelmanhallinnan uimaratakaavio

Ongelma lähetetään sitten eteenpäin IT-ylläpidolle, jossa he ensin tutkivat ongelmaa ja tekevät diagnoosin. Ongelman ratkaisemisen apuna IT-ylläpidolla on käytettävissä Content Management System (CMS), jonka avulla useampi työntekijä voi hallita ja muokata ongelmaan liittyviä tietoja. Jos ongelmaan voidaan implementoida väliaikaisratkaisu, joka palauttaa liiketoiminnan toimivuuden asiakkaalle, IT-ylläpito suorittaa sen ennen ongelman ratkaisemista. Ongelman diagnoosi tallennetaan virhetietokantaan, jota yritys voi myöhemmin käyttää ongelmanratkaisussa ja tietolähteenä. Ongelman ratkaiseminen saattaa tarvita muutosta järjestelmiin, joiden tarpeellisuutta IT-asiantuntijat arvioivat.

Kun ongelma saadaan ratkaistua, IT-asiantuntijat kokoontuvat analysoimaan ja pohtimaan, voiko sama ongelma ilmentyä muissa järjestelmissä tai paljastiko ongelma muita heikkoja kohtia yrityksen järjestelmissä. Jos muita ongelmia ei ilmentynyt, ylläpito kuittaa ongelman ratkaistuksi Service Deskille, josta Service Desk tiedottaa eteenpäin asiakkaille, että ongelma on ratkaistu.

IT-asiantuntijoilla on käytettävissä devausympäristö, jossa järjestelmän päivityksiä voi testata, ennen kuin ne implementoidaan live-ympäristöön. Devausympäristö on rakennettu niin, että live-ympäristön voi päivittää devausympäristön pohjalta sulavasti ja pienellä huoltokatkolla, joka kestää yleensä tunnin.

8 Kohteiden suojaus

8.1 Asiakastietorekisterin pitäjä

Yritys laatii tietotilinpäätöksen, joka sisältää raportin tietojen käsittelyä koskevista keskeisistä asioista. Asiakastietorekisterille määritetään rekisterinpitäjä. Rekisterinpitäjälle tulisi antaa selkeät pelisäännöt, miten hän käsittelee asiakastietoja. Rekisterinpitäjä käsittelee asiakastietoja, eikä anna niitä muille yrityksen työntekijöille, jotka eivät tietoja asianmukaisesti tarvitse.

Rekisterinpitäjän tulee luoda ja ylläpitää selostetta hänen vastuulla olevistaan käsittelytoimista, joka on valmiina toimitettavaksi viranomaisille heidän pyynnöstä.

8.2 Tietosuojavastaava

Yrityksen tulisi nimittää tietosuojavastaava, joka valvoo tietosuoja-asetuksen noudattamista henkilötietojen käsittelyssä. Tietosuojavastaava toimii asiakastietorekisterin pitäjän tukena tietosuojaan liittyvissä kysymyksissä sekä seuraa tietosuojasääntöjen noudattamista yrityksessä. Tietosuojavastaavaksi valitaan henkilö, jolla ei ole eturistiriitoja. Eturistiriitoja voisi olla muun muassa se, että henkilö on nimetty jo tietoturvavastaavaksi tai kuuluu yrityksen ylimpään johtoportaaseen. Tietosuojavastaava ei voi myös olla määrittelemässä henkilötietojen käsittelyn tarkoituksia tai keinoja. Kun tietosuojavastaava on nimitetty, hänen yhteystiedot ilmoitetaan valvontaviranomaiselle, jotta yhteydenotto viranomaiselta olisi helppoa ja sujuvaa. (Tietosuojavaltuutetun toimisto. EU:n tietosuojauudistus.)

Tietosuojavastaavan tehtävänä on valvoa, että GDPR tietosuoja-asetuksen tietosuojaperiaatteita toteutusta noudatetaan yrityksessä. Hänen tehtäviin kuuluu tiedottaa yrityksen johdolle tietosuojasääntöjen velvollisuuksista ja neuvoa henkilötietoja käsitteleviä työntekijöitä. Tietosuojavastaava auttaa yritystä tietoturvariskien arvioinnissa, joka on määritelty alempana. (Tietosuojavaltuutetun toimisto. EU:n tietosuojauudistus.)

Jos yritykseen kohdistuu hyökkäys, jossa henkilötietoja vuotaa asiaankuulumattomille henkilöille tai yrityksen työntekijä käyttää henkilötietoja väärään tarkoitukseen, tietosuojavastaavan velvollisuutena on ilmoittaa tapahtumasta valvontaviranomaiselle. (Tietosuojavaltuutetun toimisto. EU:n tietosuojauudistus.)

9 Tietosuojaperiaatteet

Uudessa GDPR tietosuoja-asetuksessa tietosuojaperiaatteet ovat vastaavat:

- Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Tietojen täsmällisyys
- Tietojen säilytyksen rajoittaminen
- Tietojen eheys ja luottamuksellisuus
- Rekisterinpitäjän osoitusvelvollisuus

10 Tietoturvariskien arviointi

Tietoturvariskien hallintaan määritellään omat prosessit, joiden mukaan toimitaan, kun käsitellään tietoturvariskejä. Riskit tulee tunnistaa ja kuvata mahdollisimman tarkasti sekä asettaa tärkeysjärjestykseen.

10.1 Riskien tunnistaminen

Riski on jostakin epätoivotusta tapahtumasta aiheutuvien toiminteiden ja riskin tapahtuman todennäköisyys. Kaikki organisaatioita kohtaan olevat riskit ovat arvioitava ja laitettava tärkeysjärjestykseen. Riskin arviointi kuvaa riskin vakavuuden ja vaikuttavuuden liiketoimintaan siten palveluiden prosesseihin.

10.2 Uhkien tunnistaminen

Kaikki suojattavia kohteita varten tulee tunnistaa erilaiset uhat jotka voivat aiheuttaa vahinkoa kohteelle. Uhat voivat olla tahattomia tai tahallisia. Kaikki uhat ovat tunnistettava, vaikka uhan mahdollisuus ei olisi kovin relevantti tarkastuksen hetkellä. Uhat ja niiden aiheuttajat tulisi listata ja kuvata uhan todennäköisyys ja liiketoimintavaikutus. Alla on kuvattu mahdollisia uhkia jotka kohdistuvat liiketoimintaan tai palveluun. Mahdolliset uhat on määritelty kolmeen eri kategoriaan, tahallinen(D), tahaton(A) sekä ympäristöön liittyvä (E). (Kuvio 8)

Tyyppi	Uhkat	Alkuperä
Fyysinen vaurio	Tuli	A,D,E
	Vesivahinko	A,D,E
	Saastuminen	A,D,E
	Suuronnettomuus	A,D,E
	Laitteiston tuhoutuminen	A,D,E
	Pöly, Korroosio, Jäätyminen	A,D,E
Luonnonilmiöt	Ilmastoon liittyvät ilmiöt	E
	Sääilmiöt	E
	Tulva	E
Välttämättömien palveluiden menettäminen	Ilmastoinnin tai vedenjakelun häiriö	A,D
	Virransyötön katkeaminen	A,D,E
	Tietoliikennelaitteiden häiriö	A,D
Tekniset häiriöt	Laiterikko	
	Laitteen toimintahäiriö	
	Tietojärjestelmän kapasiteetin täyttyminen	
	Ohjelmiston toimintahäiriö	
Luvattomat toimet	Laitteiston luvaton käyttö	
	Tiedon luvaton käsittely	
	Tieton turmeltuminen	
Toimintojen vaarantuminen	Käyttövirhe	A
	Oikeuksien väärinkäyttö	A,D
	Oikeuksien väärentäminen	D
	Toimenpiteiden esto	D
	Henkilöstön käytettävyyden pettäminen	A,D,E

Kuvio 8 Tunnetut uhat

10.3 Suojattavien kohteiden tunnistaminen

Suojattavat kohteet jaetaan kahteen kategoriaan: liiketoimintaprosesseihin, liiketoiminnot ja tietoon. Suojattava kohde on mikä tahansa kohde tai asia jolla on organisaatiolle merkittävää arvoa jota tulisi suojata. Suojattavat kohteet tulee tunnistaan yksityiskohtaisesti riskin arviointia varten. Suojattavalla kohteella on aina oltava omistaja joka vastaa kohteen turvallisuudesta ja sen käsittelystä. (Kuvio 9)

Suojattava kohde	**Tarkenne**
Konesali	Konesali sisältäen palvelimet ja verkkolaitteet
Kannettavat tietokoneet	Työntekijöiden kannettavat tietokoneet, tabletit
Yrityksen fyysinen infrastruktuuri	Toimistotilat, rakennukset
Ohjelmistot	Ohjelmistojen toimttaja
Yrityksen puhelimet	VOIP Puhelimet, yrityksen matkapuhelimet
Muut tietovälineet	sopimuspaperit, asiakastiedot
Prosessit	Yrityksen kaikki prosessit

Kuvio 9 Tunnistetut kohteet

10.3.1 Prosessit

Prosessit, joiden menettäminen johtaisi siihen, ettei organisaation toiminta-ajatusta voida toteuttaa:

Virtuaalikoneiden luonti tai niiden käyttäminen asiakkaiden toimesta. Asiakaspalvelu ongelmatilanteiden ratkaisussa. Konesalin toiminta on myös erittäin oleellinen osa, sekä myös liikenteen reititys konesalista ulos ja sisään. Nämä suojattavat kohteet omistaa Puparihosting yritys, virtuaalikoneet ovat lainassa lisenssillä asiakkaille, konesali on yrityksen omistama.

Prosessit, joiden muuttuminen voi vaikuttaa merkittävästi organisaation toiminta-ajatuksen toteuttamiseen:

Asiakaspalveluprosessi, jos tapahtuu viestintäketjussa väärin tiedottamista. Kulujen maksuprosessi, jos maksuissa tapahtuu virhe, esim. internet-yhteys saatetaan laittaa palveluntarjoajan puolelta poikki.

Prosessit, joita organisaatiossa tarvitaan sopimusten, lakien tai viranomaisvaatimusten täyttämiseen:

GDPR:n mukainen toiminta, liittyy myös tietoon. Noudatetaan tietoturvasuojaa käsitellessä asiakkaiden tietoja tai virtuaalikoneiden sisältämiä tietoja, jotta ei vakoilla meille kuulumattomia tietoja.

10.3.2 Tieto

Organisaation toiminta-ajatuksen tai liiketoiminnan toteuttamisen kannalta välttämättömät tiedot:

Yritykselle tärkeitä tietoja on asiakkaiden yhteystiedot, jolla asiakkaisiin saa yhteyden ongelmatilanteissa. Ongelmatilanteita voi olla laskutuksessa syntyvät ongelmat, esimerkiksi jos käyttäjää on laskutettu liian paljon palvelusta. Toinen ongelmatilanne voi olla tekninen ongelma virtuaalipalveluissa, jossa asiakasta täytyy tiedottaa ongelmatilanteesta. Yritykselle tärkeitä tietoja on myös asiakkaiden laskutustiedot.

Asiakkaiden henkilötiedot tulisi olla hyvin suojattu tietokannassa, niiden vuotaminen aiheuttaisi GDPR:n mukaisesti sakkoja yritykselle. Asiakkaiden käyttäjätunnukset ja salasanat tulisi olla erikseen tallennettu, jotta tietomurron tapauksessa niitä ei voi helposti yhdistää toisiinsa. Salasanojen tallennuksessa tulisi käyttää salasanakohtaisesti suolausta, jotta salattuja salasanoja ei voisi tietokannasta poimia ja verrata toisiinsa selvittääkseen, mikä olisi purettu salasana.

Kalliit tiedot, joiden käsittely, säilyttäminen tai siirtäminen vaativat paljon resursseja, ovat: virtuaalikoneille on asiakkaille varattu paljon levytilaa, jonka siirtäminen vie paljon resursseja palvelimelta.

10.4 Haavoittuvuuksien tunnistaminen

Haavoittuvuuksien tunnistamista varten on oltava luettelo tunnetuista (Kuvio 8) uhkista sekä suojattavista kohteista (Kuvio 9). Haavoittuvuuksia voidaan havaita kaikilla suojattavien kohteiden osa-alueilla. Haavoittuvuuksia voi olla olemassa ilman vahinkoa, vahinko syntyy vasta kun uhka käyttää haavoittuvuutta hyväkseen. Kaikkiin haavoittuvuuksiin ei välttämättä kohistu suoraan mikään uhka. Haavoittuvuudet tulee arvioida kriittisyyden perusteella. Alla on kuvattu mahdollisiin haavoittuvuuksiin kohdistuvat uhkat. (Kuvio 10)

Tyyppi	Haavoittuvuus	Uhka
Laitteisto	Tallennusvälineiden riittämätön ylläpito tai virheellinen asenneus	Tietojärjestelmän ylläpitävyyden pettäminen
	Säännöllisten korvausjärjestelyjen puute	Laitteiston tai tietovälineiden tuhoutuminen
	Altistuminen kosteudelle, pölylle tai likaantumiselle	Pöly, korroosia, jäätyminen
	Altistuminen jännitevaihtelulle	Virransyötön katkeaminen
	Suojaamaton varasto	Tietoväline-ja asiakirjavarkaudet
	Huolimaton käytöstä poistaminen	Tietoväline-ja asiakirjavarkaudet
	Valvomaton kopiointi	Tietoväline-ja asiakirjavarkaudet
Ohjelmistot	Ohjelmistotestaus toteuttamatta tai riittämätön	Oikeuksien väärinkäyttö
	Ohjelmiston tunnetut viat	Oikeuksien väärinkäyttö
	Ei kirjauduta ulos poistuessa työasemalta	Oikeuksien väärinkäyttö
	Tallennusvälineiden hävittäminen tai uusiokäyttö ilman kunnollista tietojen pyyhkimistä	Oikeuksien väärinkäyttö
	Varmuuskopioiden puute	Ohjelmiston peukaloiminen
	Käyttöoikeuksien väärä myöntäminen	Oikeuksien väärinkäyttö
Verkko	Suojaamattomat viestintälinjat	Salakuuntelu
	Yhden pisteen vikaantuminen	Tietoliikennelaitteiden häiriö
	Turvaton verkkoarkkitehtuuri	Etävakoilu
	Salasanojen siirto salaamattomina	Etävakoilu
	Riittämätön verkonhallinta(reitityksen sietokykyisyys)	Tietotjärjestelmän kapasiteetin täyttyminen
	Suojaamaton arkaluontoinen tietoliikenne	Salakuuntelu
Henkilöstö	Henkilöstön poissaolot	Henkilöstön käytettävyyden pettäminen
	Riittämätön turvallisuus koulutus	Käyttövirhe
	Ulkopuolisen henkilöstön tai siivoojien työn valvonnan puute	Tietoväline- tai asiakirjavarkaudet
	Seurantamekanismien puute	Aineiston luvaton käsittely
Toimipaikka	Epävakaa voimaverkko	Virransyötön katkeaminen
	Säännöllisten auditointien puute	Oikeuksien väärinkäyttö
	Palvelutasosopimuksen puute tai riittämättömyys	Tietojärjestelmän ylläpitävyyden pettäminen
	Riittämätön palvelujen ylläpitovaste	Tietojärjestelmän ylläpitävyyden pettäminen

Kuvio 10 Mahdolliset haavoittuvuudet

11 Yrityksen tietoturvaohjelma

Yrityksen tietoturvaohjelmaa varten yritys on tunnistanut suojattavat kohteet ja prosessit, sekä yrityksen liiketoimintatavoitteet. Tämän avulla yritys tekee strategiset toimenpiteet suojatakseen yrityksen liiketoimintatavoitteet ja suojattavat kohteet. Tietoturvaohjelman luonnissa käytetään apuna aiemmin tehtyä riskinhallintaa, jotta voidaan määritellä, minkälainen hyökkäys on yrityksen toiminnan huomioon ottaen todennäköinen. Tietoturvaohjelmasta luodaan toimintasuunnitelma, josta aletaan suorittamaan kovennuksia yrityksen järjestelmiin.

Tietoturvaohjelmaa tulee käydä läpi ajan kuluessa uudestaan, koska hyökkäysmenetelmät ja vektorit muuttuvat koko ajan. Yrityksen liiketoiminnan saatossa saattaa myös ilmetä uusia suojattavia kohteita ja riskejä, jotka tulee arvioida uudestaan.

Tietoturvaohjelman luomisessa käytettiin neuvoja NISTin kirjoittamasta "Framework for Improving Critical Infrastructure Cybersecurity"

11.1Autentikaatio ja kulunvalvonta

Henkilöllisyyden varmistaminen yrityksen palveluissa käyttäjille ja työntekijöille. Asiakkaille tunnistautuminen onnistuu käyttäjätilillä. Yrityksen työntekijät käyttävät myös käyttäjätilejä ja two-factor autentikaatiota. Asiakkaille tämä two-factor-autentikaatio on myös saatavilla lisävahvistuksena käyttäjätilien suojaukseen. Two-factor autentikaatio toimii asiakkaille sähköpostiviestinä, joka lähetetään, kun käyttäjätilille kirjaudutaan uudesta IP-osoitteesta. Työntekijöille two-factor autentikaatio toteutetaan fyysisellä laitteella, josta katsotaan nelinumeroinen koodi aina kirjautumisen yhteydessä.

Yrityksen konesaleilla fyysinen pääsynhallinta lukitulla ovella, jossa elektroninen lukko.

11.2Henkilöstön tietoturvakoulutus

Yrityksessä järjestetään vuosittain tietoturvakoulutus henkilöstölle, ja kaikki uudet työntekijät käyvät läpi tietoturvakoulutuksen osana perehdyttämiskoulutusta. Tietoturvakoulutuksen tavoitteena on saada kaikki yrityksen työntekijät tietoiseksi mahdollisista hyökkäysvektoreista, kuten phishing-sähköposteista ja sosiaalisesta manipuloinnista. Tiedoista tai tietoturvasta vastuussa olevat henkilöt saavat henkilökohtaisen perehdytyksen tehtäväänsä, jotta heidän roolit ja vastuut olisivat selkeitä.

Tietoturvakoulutuksen yhtenä osana yrityksen työntekijöille demonstroidaan, kuinka saastuneen sähköpostiliitteen avaaminen voi antaa hyökkääjälle koko tietokoneen haltuun. Toisessa demonstraatiossa sosiaalista manipulaatiota, jossa uniformuun pukeutunut yrityksen ulkopuolinen henkilö yrittää saada pääsyn yrityksen konesaliin. Henkilöstön koulutustasoa testataan vuosittain red-teamauksella, jossa PupariHosting palkkaa konsultointiyrityksen testaamaan yrityksen tietoturvakontrollien toimivuutta käytännössä.

Tietoturvaperehdytystä järjestetään myös yrityksen yhteistyökumppaneille.

11.3 Ylläpito ja lokitus

Yrityksen palveluita päivitetään aktiivisesti. Uudet päivitykset asennetaan ensin devausympäristön laitteisiin, jossa päivitysten yhteensopivuus ja toimivuus testataan. Jos päivitysten jälkeen palvelut toimivat, tuodaan päivitykset live-ympäristöön.

Puparihosting implementoi keskitetyn lokijärjestelmän, jossa työasemilta kerätään kaikki oleellinen lokitieto liittyen ohjelmien ajoon ja käyttöjärjestelmän muutoksiin. Keskitettyyn lokiin kerätään myös yrityksen palomuurista tietoa tulevista ja menevistä yhteyksistä. Kaikkiin verkkoasemissa oleviin tiedostoihin tehdyt muokkaukset, luomiset ja poistotoimenpiteet lokitetaan myös.

Yrityksen käyttämien laitteiden ohjelmistot määritetään sillä periaatteella, että vain tarvittavat ohjelmat on asennettu eikä muuta ylimääräistä. Tällöin vältytään haavoittuvuuksilta ohjelmistoissa, jota laitteella ei ole tarkoitus käyttää.

11.4 Vastesuunnitelma

Kyberhyökkäyksen sattuessa, yrityksessä muodostetaan IT-ylläpidon asiantuntijoista Incident Response – tiimi. Tiimi suorittaa vastesuunnitelman mukaisesti toimenpiteet, jossa tiedotetaan kyberpoikkeamasta mahdollisesti viranomaisille ja yhteistyökumppaneille. Jos poikkeama vaikuttaa yhteistyökumppaneiden toimintaan, heidän kanssaan sovitaan, miten hyökkäyksen vaikutusta lievennetään ja kuinka hyökkäyksestä toivutaan.

Tiimin tehtävänä on käydä läpi hyökkäyksen aikana kirjattuja lokitietoja ja selvittää, miten hyökkäys pääsi yritykseen läpi. Incident Response - tiimi laatii hyökkäyksestä raportin, joka koostuu hyökkäysvektorista, hyökkääjän toimenpiteistä, hyökkäyksen vaikutuksesta yrityksen toimintaan ja vastatoimenpiteistä, joita yrityksen tulee tehdä vastaavien hyökkäysten torjumiseksi.

Incident Response – tiimi käyttää toiminnassaan TheHive – työkalua, jolla he voivat luoda tapahtumista keissejä. Keisseihin tiimi lisää havaintojaan ja todisteita hyökkäyksen vaikutuksista yrityksen järjestelmiin ja hyökkääjän toimenpiteistä.

Tiimillä on käytettävissään myös laaja valikoima forensiikkatyökalu, kuten Windowsin SysInternals ohjelmat sekä Autopsy – forensiikkatyökalualusta.

Tiimi luo myös parannussuunnitelman, jonka tehtävänä on tehostaa yrityksen toimintaa poikkeustilanteissa, jotta seuraavan hyökkäyksen jälkeen vasteaika olisi pienempi ja hyökkäyksen vektori selvitettäisiin nopeammin.

12 Riskianalyysi

12.1 Riskianalyysimenetelmät

Riskianalyysi voidaan suorittaa kahdella menetelmällä, tai niiden yhdistelmällä. Menetelmät ovat laadullinen ja määrällinen riskianalyysi. Riskianalyysin yksityiskohtaisuuteen vaikuttaa esim. suojattavien kohteiden kriittisyys ja tiedettyjen haavoittuvuuksien laajuus. Usein ensin tehdään laadullinen riskianalyysi, jolla etsitään suurimmat riskit ja saadaan yleiskäsitys riskin tasosta. Määrällistä riskianalyysia voidaan käyttää myöhemmin merkittävimpien riskien tarkempaan analyysiin. Laadullisen analyysin tekeminen on helpompaa ja edullisempaa kuin määrällisen analyysin.

1. Laadullinen riskianalyysi

Seurausten suuruusluokka ja niiden syntymisen todennäköisyys kuvataan laatumääritteiden asteikolla (pieni, keskitasoinen ja iso). Laadullisen analyysin etuna on sen helppo ymmärrettävyys henkilöstölle. Laadullista riskianalyysia voidaan käyttää,

- Jos kyseessä on alustava seulonta, jossa tunnistetaan tarkempaa analyysia edellyttävät riskit
- Jos tällainen analyysi on päätöksenteon kannalta tarkoituksellinen
- Jos käytössä ei ole riittävästi resursseja määrällistä riskianalyysia varten.

2. Määrällinen riskianalyysi

Määrällisessä riskianalyysissa sekä seurauksille että todennäköisyyksille käytetään numeroarvoina esitettyä asteikkoa ja se perustuu useista eri lähteistä saatuun aineistoon. Useimmissa tapauksissa määrällisessä riskianalyysissa hyödynnetään aiempia häiriöitä koskevaa tietoa, jolloin arvioinnin etuna on, että se voidaan liittää suoraan tietoturvatavoitteisiin.

12.2 Seurausten arviointi

Liiketoimintaan kohdistuvat vaikutukset voidaan ilmaista laadullisesti ja määrällisesti. Menetelmä joka esittää vaikutukset rahallisena arvona antaa kuitenkin yleensä enemmän tietoa päätöksentekoon ja edistää päätöksentekoprosessia. Suojattavien kohteiden arvo määritellään luokittelemalla suojattavat kohteet niiden kriittisyyden perusteella, eli arvioidaan miten tärkeitä suojattavat kohteet ovat organisaation liiketoimintatavoitteiden saavuttamisen kannalta.

Seurattavien kohteiden arvon määrittäminen auttaa häiriöskenaarion vaikutusten arvioinnissa, koska tietoturvahäiriö voi vaikuttaa useampaan kuin yhteen suojattavaan kohteeseen. Seuraukset voidaan ilmoittaa jonkun yritykselle merkityksellisen kriteerien perusteella, esim. rahallisten tai teknisten.

12.3 Häiriön todennäköisyyden arviointi

Häiriöskenaarioiden tunnistamisen jälkeen kunkin skenaarion toteutumisen todennäköisyys ja vaikutus arvioidaan laadullisella tai määrällisellä arviointimenetelmällä. Arvioinnissa huomioon otettavia asioita on, kuinka usein uhkia toteutuu ja miten helposti haavoittuvuuksia voidaan käyttää hyväksi. Arvioinnissa otetaan huomioon seuraavat seikat:

- Uhkan todennäköisyyttä koskeva kokemus sekä tilastot
- Tahalliset uhkat
- Tahattomat uhkat
- Yksittäiset ja kasautuvat haavoittuvuudet
- Käytössä olevat hallintakeinot.

12.4 Riskitason määrittäminen

Riskianalyysi perustuu arvioituihin seurauksiin ja todennäköisyyksiin. Riskianalyysissä riskin todennäköisyyden ja seurausten arvot määritellään. Analyysissä voidaan myös ottaa huomioon kustannushyödyt ja sidosryhmien näkemykset. Arvioitu riski on häiriöskenaarion todennäköisyyden ja seurausten yhdistelmä.

13 Tietoturvariskien käsittely

Tietoturva riskien käsittelyä varten on oltava luettelo riskeistä asetettuna tärkeysjärjestykseen riskien merkityksen perusteella. Lähtökohtaisesti riski pyritään poistamaan erilaisia hallintakeinoja käyttäen. Usein riskejä ei pysty poistamaan, mutta riskejä voidaan pienentää tai yrittää välttää muuttamalla toimintatapoja.

Riskin käsittely on prosessi, jossa riskin käsittelyyn on neljä vaihtoehtoa

- Riskin säilyttäminen
- Riskin muokkaaminen
- Riskin välttäminen
- Riskin jakaminen

Riskin käsittely vaihtoehto tulee valita riskianalyysin ja arvioinnin tulosten perusteella. Vaihtoehdot jolla riskiä voidaan pienentää merkittävästi olisi toteutettava, kustannukset huomioon ottaen. Riskien haitalliset seuraukset tulisi saada niin vähäisiksi kuin mahdollista. Riskienkäsittelyn neljä eri vaihtoehtoa eivät ole toisiaan pois sulkevia. Vaihtoehtoja voidaan yhdistellä, jos niiden tuloksista on merkittävää hyötyä jäännösriskin kannalta. Riskisuunnitelman määrittelyn jälkeen täytyy määrittää jäännösriskit. Jäännösriski tulee päivittää ja arvioida uudelleen siten että organisaation hyväksymiskriteerit täyttyvät. Hyväksymiskriteereistä on kerrottu ISO/IEC 27002:2005 kohdassa 0.3.

13.1 Riskin muokkaaminen

Riskin muokkaaminen on toiminto, jossa riskitasoa alennetaan niin että jäännösriski voidaan myöhemmin hyväksyä organisaation hyväksymiskriteerien täyttyessä. Riskin hallintakeinot tulisi valita niin että ne täyttävät riskin käsittelyssä tunnistetut vaatimukset. Riskiä tulee käsitellä kustannukset, aikataulu, tekniset sekä ympäristöön liittyvät näkökohdat huomioon ottaen. Hallintakeinot voivat tarjota suojausta korjaamalla, poistamalla, ehkäisemällä, pienentämällä, estämällä, havaitsemalla, palauttamalla sekä seuraamalla ja tietoa lisäämällä.

Hallintakeinoa valitessa on huomioitava tavallisesti ainakin osa seuraavista:

- Aikarajoitukset
- Tekniset rajoitukset
- Eettiset rajoitukset
- Lakisääteiset rajoitukset
- Ympäristöasioihin liittyvät rajoitukset
- Helppokäyttöisyys
- Toiminnalliset rajoitukset

13.2 Riskin säilyttäminen

Riskin säilyttämisessä riskin annetaan olla muuttumattomana. Yleensä tällainen riski on hyvin epätodennäköinen tai riskiä ei pysty muuttamaan rajoitusten takia. Toisin sanoen riski on hyväksytty ja se toteuttaa organisaation tietoturvapolitiikan ja edellyttävät riskien hyväksymiskriteerit.

13.3 Riskin välttäminen

Riskien välttäminen kuvaa toimintoa jossa riskin käsittelyssä aiheutuvat kustannukset ovat suuremmat kuin riskin muuttamisestä saatu hyöty. Riski voidaan välttää muuttamalla olosuhteita, niin ettei riskiä synny. Konesalin siirtäminen fyysisesti turvallisempaan paikkaan voi olla kustannustehokkaampaan kuin nykyisen konesalin suojaaminen hyväksymiskriteerien mukaiseksi.

13.4 Riskin jakaminen

Riskien jakamisessa riski voidaan jakaa sellaisen osapuolen kanssa, joka pystyy vaikuttavimmin hallitsemaan riskiä arvioinnin perusteella. Esimerkiksi palvelunestohyökkäykset voidaan ohjata operaattorin mustaan aukkoon.

14 Tietoturvariskien hyväksyminen

Tietoturvariskien hyväksymisen toteuttamisessa kuvataan, miten riskejä käsitellään niin, että riskit saadaan täyttämään hyväksymiskriteerit. Organisaatiossa johtajat päättävät hyväksymiskriteereistä ja jäännösriskien hyväksymisestä.

15 Valittu riski

Valitsimme riskianalyysin perusteella suurimman uhan perusteella tietoturvaa koskevan riskin. Suurin riski on tietojärjestelmiin murtautuminen ja samalla asiakkaan luottamuksen menetys. Huonosti suojattu verkko on altis hyökkäyksille.

16 Riskien hallintakeino

Hallintakeino eli kontrolli on riskiä muuttava toimenpide. Kaikki riskiä muuttavat toimenpiteet ovat hallintakeinoja kuten politiikka, laitteet, käytännöt ja prosessit. Tavallisin tietoturvan tekninen hallintakeino on palomuuri, rajoitetaan pääsyä verkkoon. Hallintakeinoksi tulisi valita mahdollisimman kustannustehokas keino joka tuottaa selkeää hyötyä riskinhallintaa.

16.1 Turvaton verkkoarkkitehtuuri

Turvattoman verkkoarkkitehtuurin vaikutus on suuri tarjoamassamme palvelussa. Haavoittuvuuden hallintakeinona käytetään palomuuria. Verkon pääsyn hallinta tulee toteuttaa siten että jokainen käyttäjä autentikoidaan, heidän toimensa

rajoitetaan ja kaikki käyttäjän toimet lokitetaan. Palomuurina käytetään L7-palomuuria joka osaa tutkia tietoa kaikilla OSI-mallin kerroksilla.

16.2 Salausmenetelmät

Palvelun tilaukset tehdään verkkokaupan kautta joten, verkkosivujen liikenne tulee salata TLS salauksella. TLS mahdollistaa useiden kryptograafisten menetelmien ja niiden parametrien käytön tietoliikenteen luottamuksellisuuden, eheyden ja autenttisuuden takaamiseksi. Vahti ohjeen hyvien käytänteiden mukaan turvallisuuden kannalta on oleellista käyttää aina uusinta versiota TLS protokollasta. TLS protokollaa tunnetuimmin käytetään HTTP-liikenteen salaamisessa.

16.3 Tietoturvakoulutukset

Yrityksessä otetaan käyttöön tietoturvakoulutukset jossa jokaiselle henkilölle opetetetaan toimimista tietoturvapoikkeaman sattuessa. Esimerkiksi asiakaspalvelijoille opetetaan turvallista verkkokäyttäytymistä ja epäilyttävien tiedostojen käsittelyä.

17 Insidentin testaaminen

Tietoturvakontrollien käyttöönoton jälkeen kontrollin toimivuus tulee testata määritellyssä palveluympäristössä.

17.1 Insidentti

Palvelua kohtaan yritetään kirjautua satoja kertoja minuutissa, palomuurissa oleva IDS analysaattori huomaa tämän olevan epätavallista liikennettä ja aiheuttaa hälytyksen. Hälytys lähetetään automaattisesti tietohallinnon asiantuntijoille.

17.2 Vertailu

Veerattaan kontrollin hyötyä kustannuksiin. Älykäs palomuuri huomaa 80% kaikista hyökkäyksistä joiden perusteella voidaan tulkita muita teknisiä hyökkäyksiä, joita voidaan tutkia taas riskiarvioinnissa. Asennettu kontrolli siis huomaa aiemmin määritettyjä uhkia sekä mahdollisesti uusia uhkia. Kontrolli on siis kustannustehokas.

18 Tietoturvatoiminnan mittarit

Tietoturvan mittaamiseen käytetään erilaisia mittareita jotka ovat teknisiä ja kustannuspohjaisia. Tietoturvaa mitatessa lasketaan kontrollin asennuksessa käytetyt resurssit ja sen tuomat lisätyötunnit yhteen, josta saadaan jonkinlainen arvo ulos, jonka perusteella voidaan arvioida tietoturvaa.

18.1 Tapahtuneet tietoturvapoikkeamat

Tietoturvapoikkeamine tavoitteena on seurata toiminnalle aiheutuvaa haittaa ja hankkia tietoa tietoturvatoimenpiteiden suunnittelua varten. Kuten aiemmin mainittiin, tuntemattomista uhkista ja riskeistä voidaan ottaa tietoa, joiden perusteella kontrollia voidaan muuttaa tai muokata.

18.2 Tietoturvapoikkeamien hallinta

Poikkeamien hallinnan tarkoituksena on seurata aiemmin toteutettujen kontrollien tehokkuutta. Voidaan seurata esimerkiksi havaittuja virus-ja haittaohjelmia, palvelunestöhyökkäyksiä, epäonnistuneiden tunkeutumisyritysten lukumäärä.

18.3Tietoturvatoimintaa kuvaavia mittareita

Mittareiden tavoitteena on arvioida toiminnan tehokkuutta seuraamalla käytettyjä resursseja ja suoritteita. Tietoturvan mittareita ovat esimerkiksi tietoturvallisuustyön työntunnit ja henkilötyöpäivät, henkilöstölle suunnatut koulutukset, tietoturvaryhmän kokousten lukumäärä.

18.4 Mittareiden luominen

Mittarin luomista varten datasta kerättäviä asioita voisivat olla, lokien –ja skannausten tulokset, liiketoiminnan jatkuvuuteen liittyvien harjoitusten tulokset, häiriötilanteisiin liittyvät tilastot, sisäisten auditointien tulokset ja kyselyt sekä kyselylomakkeet.

19 Arviointi- ja mittausmenetelmät

Tietoturvaa tulee arvioida ja mitata jatkuvasti, sillä uhkia tulee lisää ja niiden myötä riskit kasvavat. Tietoturvan arviointi on oleellinen osa yrityksen toimintamallin ja tietoturvan muodostamista. Arviointeja voidaan tehdä niin sisäisesti kuin ulkopuolisen toimijan kanssa. Näitä arviointeja kutsutaan auditoinneiksi.

Määrällisessä mittaamisessa seurataan käytettyä työaikaa, kustannuksia, tietoturvapoikkeamien lukumäärää sekä tietoturvakoulutuksiin käytettyä aikaa.

19.1 Kustannukset

Alla olevassa taulukossa on listattuna kontrolli, jolla pyritään pienentämään tietoturvariskejä. (Taulukko 6)

Kohde	Kustannus	Hyöty
Palomuuri	5000e	Suurin osa tunnetuista hyökkäyksistä ja haitallisestä liikenteestä voidaan suodattaa
Koulutus	5000e	Tietoturvakoulutus parantaa näkyvyyttä ja lisää ymmärrystä poikkeaman sattuessa.

Salausmenetelmät	1000e	Vahvempien salausmenetelmien käyttö luo turvallisemman verkkoarkkitehtuurin ja vaikeuttaa hyökkäämistä.

Taulukko 6. Tietoturvakontrollit

20 Tulokset

Tietoturvakontrollimme paransivat huomattavasti tietoturvaa ja olivat kustannustehokkaat. Teknisen ja käytännön tietoturvan yhdistäminen luo hyvän pohjan tietoturvan hallinalle.

21 Pohdinta

testataan kun tulee insidentti eli käytännön tapahtuma niin miten se etenee tietoturvakontrolli systeemeiden läpi. Eli joku uhka joka hyödyntää jotain haavottuvuutta jne en ymmärtäny sampoo vittu

Lähdeluettelo

National Institute of Standards and Technology. 2017. Framework for Improving Critical Infrastructure Cybersecurity. Viitattu 9.4.2018. https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

Tietosuojavaltuutetun toimisto. 2018. EU:n tietosuojauudistus. Viitattu 9.4.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

International Organization for Standardization & International Electrotechnical Commission. N.d. ISO 27000 Series.