Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan tutkinto-ohjelma

Tietoturvallisuus osana liiketoiminnan jatkuvuussuunnittelua

T-110.5620 Tietoturvallisuuden kehittämisprosessit

16. tammikuuta 2012

Jussi-Pekka Erkkilä

Sisältö

1 Johdanto

Liiketoiminnan jatkuvuus (engl. business continuity, BC) on organisaatioiden ja yritysten harjoittamaa toimintaa jolla pyritään varmistamaan liiketoiminnan jatkuminen riittävällä tasolla erilaisten odottamattomien katastrofien ja onnetomuuksien sattuessa. Motiivina liiketoiminnan jatkuvuussuunnitteluun (business continuity planning, BCP) ja -hallintaan (business continuity management, BCM) ovat tappioiden ja kulujen minimointi, asiakaspalvelun jatkuminen ja lakien ja säädösten noudattaminen. Joillain aloilla jopa ihmishenget voivat olla riippuvaisia liiketoiminnan ja asiakaspalvelun jatkumisesta. [4]

Oleellisia liiketoiminnan jatkuvuuteen liittyviä käsitteitä ovat muun muassa vaikutusanalyysi (engl. business impact analysis), onnettomuudesta toipuminen (engl. disaster recovery), riskienhallinta (engl. risk management). Liiketoiminnan jatkuvuudenhallintaan on olemassa myös useita eri standardeja jotka pyrkivät määrittelemään jatkuvuudenhallintaan liittyviä vaatimuksia ja parhaita käytäntöjä kattavasti [4]. Näihin asioihin palataan vielä myöhemmin tässä paperissa.

Pääpaino tässä dokumentissa on kuitenkin liiketoiminnan jatkuvuussuunnitelussa ja tietoturvallisuuden rooliissa osana jatkuvuussuunnittelua. Viimeisten kahden vuosikymmenen aikana tietotekniikka ja Internet ovat kehittyneet oleelliseksi osaksi lähes kaikkea liiketoimintaa. Tietojärjestelmien ja tiedonkulun toiminnasta ovat riippuvaisia niin pankit, lentoyhtiöt kuin päivittäistavarakaupatkin. Joillain yrityksillä toiminta on jopa keskittynyt yksinomaan Internetiin ja koko toiminnan olemassaolo on riippuvainen tietotekniikasta. Nämä lähtökohdat huomioiden tietotekninen turvallisuus tulisi itsestäänselvästi olla oleellinen osa liiketoiminnan jatkuvuussuunnittelua.

Tämä tutkielma jakautuu viiteen eri lukuun. Johdannon jälkeen perustellaan aiheen olennaisuutta perehtymällä siihen miten tietoturva vaikuttaa liiketoimintaan. Tämän jälkeen tutustutaan erilaisiin liiketoiminnan jatkuvuuteen vaikuttaviin uhkiin ja riskeihin sekä tarkastellaan riskejä tietoturvan näkökulmasta. Neljäs kappale sisältää tämän tutkielman oleellisen asiasisällön, eli liiketoiminnan jatkuvuuden suunnittelun, jatkuvuussuunnitelman tekemisen, aihetta käsittelevät standardit sekä tietoturvanäkökulman. Viidennessä kappaleessa esitetään yhteenvetona johtopäätökset käsitellyistä asioista.

2 Tietoturvan vaikutus liiketoimintaan

Tietoturva sinänsä ei ole mikään aivan uusi asia, mutta sen merkitys on noussut uudelle tasolle tietotekniikan ja viestinnän kehityksen myötä. Tietoturvallisuus on olennainen osa käytännössä kaikkea liiketoimintaa. Siitä huolehtiminen on välttämätöntä paitsi oman kilpailukyvyn säilyttämiseksi, myös työntekijöiden oikeusturvan sekä asiakkaiden ja liiketoimintakumppaneiden kanssa solmittujen sopimusten noudattamiseksi.

Organisaatioiden omistaman immateriaalin turvallinen hallinnointi ja käsittely aiheuttaa omat haasteensa myös yrityksen johto- ja hallintotasolla. Tietoturva ei ole enää pitkään aikaan ollut ainoastaan tekninen haaste vaan myös hallinnollinen haaste. Siitä huolimatta tietoturvasta huolehtiminen on korkeamman johdon tasolla nähty perinteisesti teknisenä ongelmana joka voidaan siirtää IT-osaston vastuulle. [1]

Liiketoiminnan näkökulmasta tietoturvaa voidaan tarkastella samojen käsitteiden kautta kuin teknisestikin. Liiketoiminnan kannalta tärkeän datan, immateriaalin tai tietotaidon luottamuksellisuus on erittäin tärkeää kilpailuedun säilyttämiseksi. Saatavuus puolestaan on välttämätöntä nimenomaan liiketoiminnan jatkuvuuden takaamiseksi. Erityisesti katkokset tietojärjestelmien ja palveluiden saatavuudessa ovat vakava uhka liiketoiminnan jatkuvuudelle. Myös eheys, jota tässä yhteydessä voidaan ajatella esimerkiksi palveluiden toimivuutena ja tietojärjestelmien oikeellisuutena, on oleellinen vaatimus liiketoiminnan kannalta.

Liiketoiminnan jatkuvuuden kannalta tärkeimmät tietoturvavaatimukset on lueteltu alla:

- Palveluiden ja tietojärjestelmien saatavuus
- Luottamuksellisuus asiakkaiden ja yhteistyökumppaneiden välillä sekä sopimusten noudattaminen
- Tärkeän datan, immateriaalin ja muiden kilpailuetujen luottamuksellisuus
- Tietoturvajohtaminen ja hallinnointi, tietoturvapolitiikan määrittely ja noudattaminen

Näiden tavoitteiden saavuttamiseksi liiketoiminnan jatkuvuussuunnittelussa tietoturvaasiat tulisi huomioida tilanteen vaatimalla tavalla. Liiketoiminnan jatkuvuussuunnitteluun ja tietoturvan rooliin siinä tutustutaan luvussa 4.

3 Liiketoimintaan vaikuttavat riskit

Liiketoimintaan vaikuttavilla riskeillä tarkoitetaan tässä yhteydessä kaikkia mahdollisia uhkia, joilla voi olla negatiivista vaikutusta organisaation liiketoiminnan jatkuvuuteen. Riskejä tarkastellaan usein organisaation näkökulmasta ja kutakin organisaatiota koskettavat eri riskit tapauskohtaisesti. Luonnollisesti yritykset myös jakavat tiettyjä riskejä ja monet globaalit riskit kuten suuret luonnonkatastrofit koskettavat yhtä lailla kaikkia organisaatioita. Riskit voidaan kategorioida ulkoisiin ja sisäisiin uhkiin ja nämä vielä erikseen onnettomuuksiin ja tarkoituksella aiheutettuihin ongelmiin.

3.1 Sisäiset riskit

Sisäisillä riskeillä tarkoitetaan organisaation tai yrityksen sisältä itseensä kohdistuvat riskit. Näitä voivat olla esimerkiksi työntekijät, inhimilliset virheet tai virheet tietojärjestelmissä. Myös rekrytointi on omalla tavallaan sisäinen riski, sillä siinä luottamuksellisia asioita paljastuu uusille henkilöille.

Sisäiset riskit ovat toisinaan poistetttavissa tai minimoitavissa huolellisella tietoturvapolitikalla ja auditoinnilla. Tyypillisesti sisäiset riskit ovat vahingossa tapahtuvia, mutta joissain tapauksissa myös talon sisältä voidaan tarkoituksella vuotaa tietoa ulos tai aiheuttaa vahinkoa liiketoiminnalle. Tämän totaalinen estäminen on varsin haastavaa, ellei mahdotonta.

3.2 Ulkoiset riskit

Ulkoisia riskejä ovat organisaatiosta riippumattomat riskit, kuten luonnonkatastrofit, sodat, pandemiat tai teollisuusvakoilu. Esimerkiksi työskentelytilojen tulipalo tai pandemiaaalto joka vie huomattavan osan henkilöstöstä sairauslomalle on omiaan lamaannuttamaan liiketoiminnan lyhyellä varoitusajalla. Ulkoiset riskit voivat olla sekä tahallaan aiheutettuja (terrori-iskut, tietomurrot) tai onnettomuuksia (luonnonkatastrofit).

Ulkoisia riskejä ei tyypillisesti pysty täysin estämään, mutta niihin voi pääsääntöisesti varautua ja niistä aiheutuvat haitat voidaan minimoida asianmukaisella valmistautumisella ja toipumissuunnitelmalla. Toipumissuunnitelmaa ja liiketoiminnan jatkuvuutta käsitellään tarkemmin luvussa 4.

3.3 Riskit tietoturvallisuuden näkökulmasta

Tietoturvan kannalta sekä sisäiset että ulkoiset riskit ovat merkittäviä, joskin hieman eri tavalla. Ulkoiset tietomurrot ovat aina mahdollisia ja historia osoittaa että tietomur-

toja sattuu toisinaan eikä niitä voi täysin estää. Tietomurtojen negatiivisia vaikutuksia ovat luottamuksellisten tietojen vuotaminen, katkokset järjestelmien saatavuudessa (esimerkiksi palvelunestohyökkäykset) sekä varsin merkittävänä tekijänä myös organisaation maineen ja luotettavuuden kärsiminen.

Liiketoiminnan jatkuvuuden kannalta olisikin tärkeää että liiketoiminnalle kriittiset ohjelmistojärjestelmät olisivat jossakin määrin vikasietoisia tietomurroille. Tämä tarkoittaa sitä, että järjestelmään kohdistuva tietomurto ei automaattisesti tarkoittaisi tärkeimpien tietojen vuotamista, sekä järjestelmien tulisi pystyä toiminnassa myös tietomurroille altistuneena. [6]

Tietoturvan kannalta sisäisten riskien luonne on hieman toisenlainen. Usein järjestelmän käyttäjät ovat yksi suurimmista tietoturvariskeista. Tämä voi johtua yksittäisten käyttäjien tai työntekijöiden suurpiirteisestä suhtautumisesta tietoturvaan tai puhtaasta tietämättömyydestä. Erityisesti tämä tekee tietoturvasta myös hallinnollisen haasteen: organisaation tulee kehittää yhteinen tietoturvapolitiikka ja varmistaa että työntekijät ymmärtävät sen merkityksen. Lisäksi tulee huolehtia, että tietoturvapolitiikkaa myös noudatetaan kaikilla tasoilla. Tässä asiassa johtoportaan merkitys korostuu. Toisaalta epäjohdonmukaiset tai liian rajoittavat tietoturvavaatimukset eivät aina palvele tarkoitustaan; kun tietoturva tulee esteeksi tehtävien suorittamiselle, ihmisillä on tapana kiertää tietoturvarajoitukset tavalla tai toisella, jolloin ne menettävät merkityksensä. [5]

Tarkoitukselliset tietovuodot yhtiön sisältä ovat myös oma lukunsa. Niiden ehkäisemiseksi tulee organisaation tietoturvapolitiikka suunnitella siten, että yksittäisillä työntekijöillä on pääsy ja käyttöoikeus vain niihin tietoihin, mitä he tarvitsevat tehtäviensä suorittamisella. Lisäksi työntekijöiden tulee sitoutua salassapitosopimukseen. Organisaation sisäistä tiedonkulkua voi myös pyrkiä kontrolloimaan ja seuraamaan, mutta siinä tapauksessa tulee huomioida työntekijöiden yksityisyydensuoja.

4 Liiketoiminnan jatkuvuussunnittelu

Liiketoiminnan jatkuvuussuunnittelu on prosessi jonka tavoitteena on muodostaa organisaatiolle kattava suunnitelma kaikkien mahdollisten uhkien varalle siten että organisaatio pystyy jatkamaan toimintaansa riittävällä aikavälillä ilman kohtuuttomia vahinkoja. Tosiasia on, että kaikkia katastrofeja ja vahinkoja ei pystytä ehkäisemään, joten asianmukainen tapa on varautua niihin ennalta ja ongelmien sattuessa minimoida niistä aiheutuneet haitat. Jatkuvuussuunnittelun lopputuote on jatkuvuussuunnitelma, joka on käytännössä kokoelma dokumentteja ja ohjeistuksia siitä miten erilaisissa tilanteissa tulisi toimia. Jatkuvuussuunnittelun osana voidaan myös kouluttaa henkilöstöä kriisitilanteita varten ja muokata organisaatiorakennetta vähemmän haavoittuvaksi [3]. Ideaalitilanteesa organisaatio ei olisi riippuvainen yhdestäkään yksittäisestä palasestaan, mutta usein tämän toteuttaminen on haastavaa.

Oleellista on myös jatkuvuussuunnitelman ylläpito ja aktiivinen päivittäminen. Yrityksen tai organisaation tila ja potentiaaliset uhat saattavat muuttua hyvinkin nopeasti ja siksi on tärkeää että jatkuvuussunnitelma on ajan tasainen. Esimerkiksi kymmenen vuotta sitten tehty jatkuvuussuunnitelma saattaa olla nykypäivänä lähes käyttökelvoton johtuen Internetin ja tietotekniikan nopeasta läpimurrosta kaupallisella sektorilla.

Jokainen yritys ja organisaatio on erilainen ja niiden liiketoiminta on riippuvainen eri tekijöistä. Myöskin potentiaaliset riskit ovat usein vaihtelevia riippuen liiketoimintamallista. Tämän vuoksi myöskin liiketoiminnan jatkuvuussuunnitelman täytyy olla organisaatiokohtainen [3]. Jatkuvuussuunnitelman tekemiseen ei myöskään ole tiukkaa *step-by-step*-kaavaa vaan eri asioita täytyy painottaa tapauskohtaisesti. Ohjeistuksia ja standardeja jatkuvuussuunnitelman tekemiseen ja käytöntöihin on kuitenkin olemassa.

Seuraavaksi alaluvussa 4.1 perehdytään jatkuvuussuunnitelman perusasioihin ja määritellään oleellisia käsitteitä sekä esitetään prosesseja ja vaiheita jatkuvuussuunnitelman tekemiseen. Tämän jälkeen luetellaan muutamia jatkuvuussuunnitteluun liittyviä virallisia standardeja sekä sivutaan lyhyesti niiden sisältöä. Alakohdassa 4.3 perehdytään vielä tietoturvan rooliin jatkuvuussuunnitelmassa ja mitä vaikutuksia sillä on jatkuvuussuunnitteluprosessiin.

4.1 Liiketoiminnan jatkuvuussunnitelma tekeminen

Kuten edellä todettiin, liiketoiminnan jatkuvuussuunnitelma on organisaatiokohtainen ja sitä täytyy dynaamisesti kehittää yhdessä organisaation strategian ja liiketoimintasuunnitelman myötä. Cerullo, V. ja Cerullo, M. (2004) [3] esittävät että jatkuvuussuunnitelma tulisi muodostua seuraavasta kolmesta vaiheesta:

1. Liiketoimintaan vaikuttavien uhkakuvien tunnistaminen
2. Suunnitelman kehittäminen riskeistä aiheutuvien vahinkojen vähentämiseksi
3. Henkilöstön kouluttaminen ja suunnitelman testaaminen sekä varmistaminen

Tämän vaatimuksen mukaisen jatkuvuussunnitelman toteuttamiseksi samassa tutkimuksessa esitetään kolme eri komponenttia: vaikutusanalyysi (business impact analysis) jonka osana myös riskienhallinta (risk management), toipumissuunnitelma (disaster recovery plan) sekä kouluttaminen ja testaus. Seuraavissa alaluvuissa käsitellään tarkemmin näitä komponentteja.

4.1.1 Vaikutusanalyysi

Vaikutusanalyysin (business impact analysis, BIA) tehtävä on tunnistaa ne tekijät joista organisaation liiketoiminta on riippuvainen, tunnistaa niihin kohdistuvat riskit ja arvioida uhkien todennäköisyys sekä kuinka kriittisiä nämä tekijät ovat liiketoiminnalle. Dey (2011) [4] ehdottaa vaikutusanalyysin tekemiseksi seuraavanlaista prosessia:

- Tunnista yritykselle tärkeä liiketoiminta sekä siihen vaikuttavat kriittiset tekijät.
- Tunnista yrityksen tarjoamat tuotteet tai palvelut joiden saatavuus lyhyellä varoitusajalla on erityisen tärkeää ja vaikutus liiketoimintaan merkittävä.
- Tunnista näihin tuotteisiin tai palveluihin liittyvät haavoittuvuudet ja riskit.
- Arvioi kuinka pitkään liiketoiminta voi jatkua ilman edellä mainittujen palveluiden tai tuotteiden saatavuutta.
- Määritä palveluiden ja tuotteiden kriittisyys perustuen niiden toimintavarmuuteen, toipumisaikaan sekä merkkittävyyteen liiketoiminnan kannalta. Esitä tulokset osana vaikutusanalyysia.

Vaikutusanalyysin tekemisessä voi olla hyödyllistä etsiä vastaus seuraaviin kysymyksiin: [4]

- Mitkä laitteet, koneet tai resurssit ovat välttämättömiä liiketoiminnan ylläpidon kannalta? Onko näistä jotakin ulkoistettu?
- Mitä liiketoiminnalle tapahtuu mikäli tietokoneet ja verkkoyhteydet eivät ole saatavilla?
- Onko vastuuhenkilöt määritetty eri tehtäviin yllättäviä tilanteita varten ja onko heillä riittävä koulutus?

4.1.2 Riskienhallinta

Kun vaikutusanalyysi on tehty, voidaan edetä riskienhallintaan. Jokaisen havaitun riskin ja haavoittuvuuden kohdalla tulisi arvioida sen todennäköisyys tai toistuvuustiheys, toipumisaika sekä vaikutus liiketoimintaan sekä lyhyellä että pitkällä tähtäimellä.

Näiden tietojen perusteella riskit voidaan lokeroida ryhmiin ja päättää, mitä riskille tehdään. Se esimerkiksi voidaan pyrkiä ehkäisemään eli poistamaan kokonaan, sen vaikutuksia voidaan vähentää tai toipumisaikaa riskistä voidaan parantaa. Yleisesti ottaen riski jonka todennäköisyys on suuri ja vaikutus liiketoimintaan merkittävä, tulisi joko poistaa kokonaan tai vähentää sen vaikutuksia ja todennäköisyyttä. Toisaalta riski jonka todennäköisyys on matala ja vaikutus liiketoimintaan vähäinen, voidaan hyväksyä sellaisenaan. [3]

Esimerkiksi pienyrityksen talous voi olla riippuvainen tietystä asiakkaasta tai projektista. Tällöin vastaavan projektipäällikön sairastuminen tai palveluksesta poistuminen voisi aiheuttaa taloudellista vahinkoa yritykselle. Tässä tapauksessa tulee arvioida kuinka todennäköistä projektipäällikön sairastuminen tai lähteminen organisaatiosta on, kuinka kriittistä tämä olisi yrityksen taloudelle sekä kuinka paljon ylimääräisiä kustannuksia aiheutuisi projektipäällikön sijaisen palkkaamisesta tai kouluttamisesta. Näiden tietojen pohjalta tulisi arvioida, palkataanko projektipäällikölle varahenkilö, koulutetaanko organisaation sisältä sijainen vai otetaanko riski vastaan ja luotetaan että projektipäällikkö jatkaa tehtävässään.

4.1.3 Toipumissuunnitelma

Toipumissuunnitelma (disaster recovery plan, DRP) on suunnitelma tietotekniikan ja verkkoliikenteen palauttamiseksi toimintaan esimerkiksi sähkökatkoksista tai tietomurroista mahdollisimman lyhyellä viipeellä. Käsitteenä toipumissuunnitelmalla tarkoitetaan yleensä nimenomaan IT-tekniikan toimintaan palauttamista, mutta sitä on alettu käyttää myös muissa yhteyksissä käsitteen yleistyttyä.

Toipumissuunnitelma voi kattaa myös laajemman suunnitelman, miten toimitaan erilaisten katastrofien sattuessa. Esimerkiksi avainhenkilöille täytyy olla määritelty sijainen mielellään organisaation sisältä. Toimistotilan tulipalon varalle tulee olla tiedossa vaihtoehtoinen tapaamis- ja työskentelytila. Myös globaaleihin uhkiin, kuten ydinkatastrofeihin ja pandemiatapauksiin liiketoiminnan kannalta tärkeillä alueilla kannattaa varautua.

4.1.4 Koulutus ja testaaminen

Jotta onnettomuuden sattuessa toipumissuunnitelmaa noudatetaan oikeaoppisesti, täytyy organisaatiossa olla tiettyjä henkilöitä jotka ovat perillä toipumissuunnitelmasta ja omaavat riittävän kompetenssin kriisijohtamiseen ja suunnitelman täytäntöönpanoon. Tämän varmistamiseksi katastrofitilannetta voidaan simuloida koetilanteessa [3]. Näin voidaan myös arvioida palautuuko toiminta normaaliksi riittävän nopeasti vai tarvitaanko toipumissuunnitelmaan muutoksia.

4.2 Standardit

Useat standardointiorganisaatiot ovat määritelleet standardeja liiketoiminnan jatkuvuusuunnitelman toteuttamiseen. Standardeissa esitellään muun muassa parhaiksi havaittuja käytäntöjä liiketoiminnan jatkuvuuden hallintaan sekä tarvittavia toimenpiteitä organisaation ja sen sidosryhmien etujen turvaamiseksi katastrofitapauksissa [4]. Muutamia merkittäviä aihetta käsitteleviä standardeja luetellaan ja kuvaillaan seuraavaksi.

- ISO-27031 - Ohjeistukset tietotekniikan ja viestintäteknologian roolista osana liiketoiminnan jatkuvuutta. Tarjoaa menetelmät ja prosessit organisaation ICT-tekniikan kehitykseen siten että palvelut ja järjestelmät ovat toiminnassa myös onnettomuus- ja hälytystilanteen ollessa käynnissä.
- ISO-22399 - Tarjoaa yleisen tason ohjeistukset organisaatioille onnettomuus- ja erikoistilannevalmiuteen sekä toiminnan jatkuvuuden hallintaan.
- BS 25999 - British Standards Institutionin standardit liiketoiminnan jatkuvuuden hallintaan. Kaksiosainen standardi jonka ensimmäinen osa määrittelee yleisellä tasolla prosessit, perusasiat ja käsitteet liiketoiminnan jatkuvuudenhallintaan. Toisessa osassa määritellään formaalisti vaatimukset liiketoiminnan jatkuvuudenhallinan toteuttamiseksi ja parantamiseksi.

4.3 Tietoturvan rooli jatkuvuussuunnitelmassa

Yritysten ja organisaatioiden hallinnoima informaatio ei ole ainoastaan työntekijöitä varten vaan yhä kasvavissa määrin myös asiakkaiden, kumppaneiden ja muiden sidosryhmien käytössä. Informaation lisäksi tämä koskee myös yritysten tuotteita, palveluita ja tietojärjestelmiä. Sidosryhmät ja asiakkaat odottavat palveluiden olevan saatavilla jatkuvasti, joten luotettavat, tehokkaasti toimivat ja aina saatavilla olevat tietojärjestelmät tuovat yritykselle merkittävän kilpailuedun. Tietoturvan peruskäsitteet - luottamukselli-

suus, eheys ja saatavuus - ovat kaikki tärkeitä mutta liiketoiminnan jatkuvuuden kannalta erityisesti informaation ja palveluiden saatavuus nousee esiin. [2]

Toipumissuunnitelma (disaster recovery planning, DRP) liitetään käsitteenä yleensä IT-palveluihin ja niiden toimintaan palauttamiseen. Koko käsite kehitettiin aluperin palvelinkeskusten toiminnan jatkuvuuden takaamiseksi mutta se mielletään nykyään liiketoiminnan jatkuvuussuunnittelun peruskomponentiksi [2]. Kuten aiemmassa luvussa todettiin, toipumissuunnitelman tavoiteena on minimoida katkosten aiheuttamat häiriöt ja palautaa IT-infrastruktuuri käyttökuntoon mahdollisimman pian esimerkiksi sähkökatkoksen jälkeen. Tämän vuoksi toipumissuunnitelma on erittäin oleellinen osa liiketoiminnan jatkuvuussuunnitelmaa vähänkään IT-järjestelmistä riippuvaiselle liiketoiminnalle, joka nykyään tarkoittaa lähes kaikkea liiketoimintaa.

On kuitenkin hyvä huomioida, ettei toipumissuunnitelma yksin riitä liiketoiminnan jatkuvuussuunnitelmaksi. Yksi tietoturvan tärkeimmistä päämääristä on nimenomaan liiketoiminnan jatkuvuuden varmistaminen. Näin ollen, mikäli tietoturva on kunnossa, ei toipumissuunnitelmaan ideaalitilanteessa tarvitsisi koskaan turvautua. Käytännössä tämä ei kuitenkaan toimi näin ja juuri sen takia toipumissuunnitelma tulisikin olla kunnossa.

Tietotekniikan ja informaation saatavuuden kannalta merkittäviä uhkia ovat virukset, sähkökatkokset, ohjelmiston tai laitteiston vikaantuminen sekä käyttäjien huolimattomuus. Tämän lisäksi liiketoiminnan kannalta merkittävää on myös informaation luottamuksellisuus ja salassapito: haitta- tai vakoiluohjelmat, työntekijöiden huolimaton tietojenkäsittely ja tietomurrot. Tietoteknisten uhkien lisäksi on huomioitava myös että tietokone voidaan varastaa.

Kaikki edellä mainitut asiat ovat oleellisia liiketoiminnan jatkuvuuden kannalta, sillä yllättäen löytyvä kriittinen tietoturvahaavoittuvuus voi aiheuttaa palvelukatkoksen järjestelmässä milloin tahansa. Mikäli toipumissuunnitelma on kunnossa, katkos ei välttämättä ole kovin pitkä, mutta huolellisella tietoturvasuunnittelulla katkokset voidaan mahdollisesti välttää kokonaan.

Edellä mainittujen seikkojen vuoksi olisi oleellista, että aktiivinen tietojärjestelmien ja tietoturvatiedotteiden seuranta, kattava tietoturvapolitiikka ja tietoturvahallinnointi kirjattaisiin osaksi liiketoiminnan jatkuvuussuunnitelmaa. Koska kaikkia virhetilanteita ei voida täysin välttäää, myös toipumissuunnitelman tulisi olla oleellinen osa jatkuvuussuunnitelmaa. Lisäksi tietojärjestelmät olisi hyvä pyrkiä kehittämään siten, ettei tietomurto pakota järjestelmien välittömään alasajoon vaan palvelut voisivat jatkaa myös siinä tilanteessa toimintaansa ainakin kriittisimpien funktioiden osalta. [6]

5 Yhteenveto

Liiketoiminnan jatkuvuussuunnittelu on yritysten ja organisaatioiden kannalta elintärkeää yllättävien ja ei-toivottujen tilanteiden varalle. Globaalin talouden, teknologian kehityksen ja luonnonkatastrofien ennustaminen on erittäin vaikeaa. Mahdollisia riskejä voidaan kuitenkin arvioida ja ennakoida ja niitä varten on hyvä varautua parhaalla mahdollisella tavalla. Tämä voi myös tulevaisuudessa olla erittäin hyvä kilpailuvaltti muuttuvassa maailmassa.

On ilmeistä, että tietoturvalla on tärkeä rooli liiketoiminnan jatkuvuussuunnittelussa. Mitä enemmän liiketoiminta on riippuvainen tietojärjestelmistä, sitä kriittisempiä tietoturvahaavoittuvuudet ovat liiketoiminnan jatkuvuuden kannalta. Tämän vuoksi tietoturvaa ei pitäisi käsitellä ainoastaaan teknisenä ongelmana josta IT-osasto huolehtii, vaan yrityksen strategian kannalta merkittävänä tekijänä joka tulisi huomioida myös hallinnollisella tasolla.

Jatkuvuussuunnittelun keskeisistä komponenteista vaikutusanalyysi, riskienhallinta ja toipumissuunnitelma ovat tärkeitä tekijöitä tietoturvan kannalta. Yksi merkittävimmistä syistä tietoturvaongelmiin ovat käyttäjät, jonka vuoksi tietoturvapolitiikan kehittämistä, noudattamista ja henkilöstön koulutusta jatkuvuussuunnittelussa ei tule aliarvioida.

Kuten tietoturvakin, myös liiketoiminnan jatkuvuussuunnittelu on jatkuva prosessi. Jatkuvuussuunnitelmaa täytyy seurata, ylläpitää ja päivittää muuttuvien olosuhteiden ja liiketoimintastrategioiden myötä. Jotta jatkuvuussuunnitelma pysyy ajan tasalla myös tietoturvan osalta, täytyy ylläpidossa huomioida niin uudet tietoturvahaavoittuvuudet kuin muuttuvat tarpeet tietoturvapolitiikan ja hallinnoinnin osalta. Tietoturvasta puhuttaessa on hyvä muistaa, että yksi tietoturvan oleellisimmista päämääristä on nimenomaan liiketoiminnan jatkuvuuden takaaminen.

Lähteet

[1] Basie ja von Solms. Corporate governance and information security. *Computers and Security*, 20(3):215 – 218, 2001. ISSN 0167-4048. doi: 10.1016/S0167-4048(01)00305-4. URL http://www.sciencedirect.com/science/article/pii/S0167404801003054.

[2] Jacques Botha ja Rossouw von Solms. A cyclic approach to business continuity planning. *Information Management and Computer Security*, 12(4):328–337, 2004.

[3] Virginia Cerullo ja Michael J. Cerullo. Business continuity planning: A comprehensive approach. *Information Systems Management*, 21(3):70–78, 2004. doi: 10.1201/1078/44432.21.3.20040601/82480.11. URL http://www.tandfonline.com/doi/abs/10.1201/1078/44432.21.3.20040601/82480.11.

[4] M. Dey. Business continuity planning (bcp) methodology - essential for every business. *GCC Conference and Exhibition (GCC), 2011 IEEE*, sivut 229 –232, feb. 2011. doi: 10.1109/IEEEGCC.2011.5752503.

[5] Donald A. Norman. The way i see it: When security gets in the way. *interactions*, 16: 60–63, November 2009. ISSN 1072-5520. doi: http://doi.acm.org/10.1145/1620693.1620708. URL http://doi.acm.org/10.1145/1620693.1620708.

[6] Gerald Quirchmayr. Survivability and business continuity management. *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32*, ACSW Frontiers '04, sivut 3–6, Darlinghurst, Australia, Australia, 2004. Australian Computer Society, Inc. URL http://dl.acm.org/citation.cfm?id=976440.976441.