EIOPA-BoS-20/600

Ohjeet tieto- ja viestintätekniikan turvallisuudesta ja hallinnosta

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Saksa – puh. + 49 69-951119-20;
Faksi + 49 69-951119-19; sähköpostiosoite: info@eiopa.europa.eu verkkosivusto: www.eiopa.europa.eu

Sisällys

Tausta

1. Asetuksen (EU) N:o 1094/2010 16 artiklan mukaan EIOPA voi antaa toimivaltaisille viranomaisille ja finanssilaitoksille osoitettuja ohjeita ja suosituksia yhdenmukaisten, tehokkaiden ja toimivien valvontakäytäntöjen aikaansaamiseksi sekä unionin oikeuden yhteisen, yhtenäisen ja johdonmukaisen soveltamisen varmistamiseksi.

2. Kyseisen asetuksen 16 artiklan 3 kohdan mukaisesti toimivaltaisten viranomaisten ja finanssilaitosten on kaikin tavoin pyrittävä noudattamaan ohjeita ja suosituksia.

3. EIOPA katsoi direktiivin 2009/138/EY 41 ja 44 artiklan nojalla, että tieto- ja viestintätekniikan turvallisuudesta ja hallinnosta on laadittava erityiset ohjeet Euroopan komission FinTech-toimintasuunnitelmaan (COM(2018) 109 final) vastauksena laaditun analyysin ja EIOPAn valvonnan lähentämistä koskevan suunnitelman 2018–2019[1] yhteydessä sekä useiden sidosryhmien kanssa käytyjen keskustelujen[2] perusteella.

4. Kuten Euroopan valvontaviranomaisten yhteisessä lausunnossa Euroopan komissiolle todettiin, EIOPAn ohjeissa hallintojärjestelmästä ei käsitellä asianmukaisesti tieto- ja viestintätekniikan riskien (myös kyberriskien) hallinnasta huolehtimisen merkitystä. Niissä ei anneta ohjeita keskeisistä tekijöistä, joiden katsotaan yleisesti olevan osa asianmukaista tieto- ja viestintätekniikan turvallisuutta ja hallintoa.

5. Edellä mainitun yhteisen lausunnon analyysi nykyisestä (lainsäädännöllisestä) tilanteesta EU:ssa osoitti, että valtaosa EU:n jäsenvaltioista on määrittänyt kansalliset säännökset tieto- ja viestintätekniikan turvallisuudelle ja hallinnolle. Vaikka vaatimukset ovat samanlaisia, sääntelykehys on edelleen hajanainen. Lisäksi tutkimus nykyisistä valvontakäytännöistä paljasti käytäntöjen moninaisuuden. Käytäntöjä on alkaen siitä, että ”erityistä valvontaa ei ole” aina ”vahvaan valvontaan” asti (mukaan lukien paikan ulkopuolella ja paikalla tehtävät tarkastukset).

6. Tieto- ja viestintätekniikka myös monimutkaistuu jatkuvasti ja tieto- ja viestintätekniikkaan liittyvät poikkeamat (myös kyberpoikkeamat) yleistyvät. Niin yleistyy myös kyseisten poikkeamien haitallinen vaikutus yritysten operatiiviseen toimintaan. Tämän vuoksi tieto- ja viestintätekniikka- sekä turvallisuusriskien hallinta on olennaisen tärkeää, jotta yritys pystyy saavuttamaan strategiset, organisaation laajuiset, toimintaan liittyvät sekä mainetta koskevat tavoitteensa.

7. Koko vakuutusalalla käytetään sekä perinteisissä että innovatiivisissa liiketoimintamalleissa myös jatkuvasti yhä enemmän tieto- ja viestintätekniikkaa vakuutuspalvelujen tarjoamisessa ja yritysten tavanomaisessa operatiivisessa toiminnassa. Tämä koskee muun muassa vakuutusalan digitalisaatiota (vakuutusteknologia, esineiden internet jne.) sekä yhteenliitettävyyttä televiestintäkanavien (verkko, mobiilit ja langattomat yhteydet sekä suuralueverkot) kautta. Tämän vuoksi yritysten toiminta altistuu turvapoikkeamille, myös kyberhyökkäyksille. Siksi on tärkeää varmistaa, että yritykset ovat valmistautuneet asianmukaisesti tieto- ja viestintätekniikka- sekä turvallisuusriskiensä hallintaan.

---

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] EIOPAn Euroopan komission FinTech-toimintasuunnitelmaan vastauksena julkaiseman raportin voi ladata täältä.

8. Sen lisäksi, että yritysten on oltava valmistautuneita kyberriskeihin[3] ja niillä on oltava vakaat kyberturvallisuuden puitteet, kyberturvallisuutta käsitellään ohjeissa myös osana yrityksen tietoturvatoimenpiteitä. Ohjeissa todetaan, että kyberturvallisuutta on käsiteltävä yrityksen yleisen tieto- ja viestintätekniikka- sekä turvallisuusriskien hallinnan osana. On kuitenkin tärkeää tuoda esiin, että kyberhyökkäyksillä on joitakin erityisominaisuuksia, jotka on otettava huomioon, jotta varmistettaisiin, että tietoturvatoimenpiteet vähentävät kyberriskiä asianmukaisesti:

   a) Kyberhyökkäyksiä on usein vaikeampi hallita (eli tunnistaa ja havaita niitä, suojella niiltä, reagoida niihin ja palautua niistä täysin) kuin useimpia muita tieto- ja viestintätekniikka- sekä turvallisuusriskien lähteitä. Myös vaurion laajuutta on vaikea määrittää.

   b) Jotkin kyberhyökkäykset voivat tehdä yleisistä riskinhallintaa ja liiketoiminnan jatkuvuutta koskevista järjestelyistä sekä palautumismenettelyistä tehottomia, koska ne voivat levittää haittaohjelmistoja varajärjestelmiin siten, että niitä ei voida käyttää, tai pilata varmuustiedot.

   c) Palveluntarjoajista, välittäjistä, (hallinnoinnista vastaavista) asiamiehistä ja edustajista voi tulla kyberhyökkäysten levittämiskanavia. Tarttuvat hiljaiset uhat voivat hyödyntää yhteenliitettävyyttä kolmannen osapuolen televiestinnän kanssa ja siirtyä yrityksen tieto- ja viestintätekniseen järjestelmään. Siksi verkottuneesta yrityksestä, jonka yksittäinen merkitys on pieni, voi tulla haavoittuva ja riskin leviämisen lähde. Sillä voi olla vaikutusta koko järjestelmään. Heikoimman lenkin periaatteen vuoksi kyberturvallisuuden ei pidä koskea vain suurimpia markkinatoimijoita tai kriittisten palvelujen tarjoajia.

9. Näiden ohjeiden tavoitteena on

   a) tarjota markkinaosapuolille selkeyttä ja avoimuutta tieto- ja kyberturvallisuudelta vähintään odotetuista valmiuksista eli turvallisuuden perustasosta

   b) estää mahdollinen sääntelyn katvealueiden hyväksikäyttö

   c) edistää valvonnan lähentämistä tieto- ja viestintätekniikan turvallisuuden ja hallinnon osalta sovellettavissa odotuksissa ja menettelyissä tieto- ja viestintätekniikka- sekä turvallisuusriskien hallinnan ratkaisevana tekijänä.

[3] Kyberriskin määritelmään voi tutustua finanssimarkkinoiden vakauden valvontaryhmän 12. marraskuuta 2018 laatimassa kyberalan sanastossa osoitteessa https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Ohjeet tieto- ja viestintätekniikan turvallisuudesta ja hallinnosta

Johdanto

1. Euroopan vakuutus- ja lisäeläkeviranomainen (EIOPA) antaa asetuksen (EU) N:o 1094/2010[4] 16 artiklan mukaisesti nämä valvontaviranomaisille osoitetut ohjeet siitä, miten vakuutus- ja jälleenvakuutusyritysten (yhteisesti jäljempänä 'yritykset') olisi sovellettava direktiivissä 2009/138/EY[5] ("Solvenssi II -direktiivi") ja komission delegoidussa asetuksessa (EU) 2015/35[6] ("delegoitu asetus") tarkoitettuja hallintovaatimuksia tieto- ja viestintätekniikan turvallisuuden ja hallinnon yhteydessä. Sitä varten nämä ohjeet perustuvat Solvenssi II -direktiivin 41, 44, 46, 47, 132 ja 246 artiklaan ja delegoidun asetuksen 258–260, 266, 268–271 ja 274 artiklaan. Ohjeissa hyödynnetään myös EIOPAn hallintojärjestelmää koskevia ohjeita (EIOPA-BoS-14/253)[7] sekä EIOPAn ohjeita ulkoistamisesta pilvipalvelujen tarjoajille (EIOPA-BoS-19/270)[8].
2. Nämä ohjeet koskevat sekä yksittäisiä yrityksiä että soveltuvin osin ryhmiä[9].
3. Toimivaltaisten viranomaisten on näitä ohjeita noudattaessaan tai niitä soveltaessaan otettava huomioon suhteellisuusperiaate[10], jolla on varmistettava, että hallintojärjestelyt, myös tieto- ja viestintätekniikan turvallisuuteen ja hallintoon liittyvät, ovat oikeassa suhteessa niiden riskien luonteeseen, laajuuteen ja monimutkaisuuteen, joita yrityksillä on tai voi olla.
4. Näitä ohjeita on luettava yhdessä Solvenssi II -direktiivin, delegoidun asetuksen, EIOPAn hallintojärjestelmää koskevien ohjeiden ja EIOPAn pilvipalvelujen tarjoajille ulkoistamisesta antamien ohjeiden kanssa ja rajoittumatta niihin. Näiden ohjeiden on tarkoitus olla teknologiasta ja menetelmästä riippumattomia.

Määritelmät

5. Jos termiä ei ole määritelty näissä ohjeissa, sillä on sama merkitys kuin Solvenssi II -direktiivissä.
6. Näissä ohjeissa käytetään seuraavia määritelmiä:

---

[4] Euroopan parlamentin ja neuvoston asetus (EU) N:o 1094/2010, annettu 24 päivänä marraskuuta 2010, Euroopan valvontaviranomaisen (Euroopan vakuutus- ja lisäeläkeviranomainen) perustamisesta sekä päätöksen N:o 716/2009/EY muuttamisesta ja komission päätöksen 2009/79/EY kumoamisesta (EUVL L 331, 15.12.2010, s. 48).

[5] Euroopan parlamentin ja neuvoston direktiivi 2009/138/EY, annettu 25 päivänä marraskuuta 2009, vakuutus- ja jälleenvakuutustoiminnan aloittamisesta ja harjoittamisesta (Solvenssi II) (EUVL L 335, 17.12.2009, s. 1).

[6] Komission delegoitu asetus (EU) 2015/35, annettu 10 päivänä lokakuuta 2014, vakuutus- ja jälleenvakuutustoiminnan aloittamisesta ja harjoittamisesta annetun Euroopan parlamentin ja neuvoston direktiivin 2009/138/EU täydentämisestä (Solvenssi II) (EUVL L 12, 17.1.2015, s. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_fi?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_fi?source=search

[9] Direktiivin 2009/138/EY 212 artiklan 1 kohta.

[10] Direktiivin 2009/138/EY 29 artiklan 3 kohta.

Resurssien omistaja	Henkilö tai yksikkö, jolla on vastuu tiedoista sekä tieto- ja viestintäteknisistä resursseista sekä valta niihin.
Käytettävyys	Resurssien saatavuus ja käytettävyys valtuutetun yksikön pyynnöstä (oikea-aikaisuus).
Luottamuksellisuus	Tietoja ei anneta valtuuttamattomien henkilöiden, yksiköiden, prosessien tai järjestelmien saataville eikä paljasteta niille.
Kyberhyökkäys	Mikä tahansa tieto- ja viestintätekniseen järjestelmiin kohdistuva tietomurto, joka johtaa vahingolliseen/haitalliseen yritykseen tuhota, paljastaa, muuttaa, tehdä toimintakyvyttömäksi tai varastaa tietoresursseja taikka hankkia niihin luvaton pääsy tai käyttää niitä luvattomasti.
Kyberturvallisuus	Tietojen ja/tai tietojärjestelmien luottamuksellisuuden, luotettavuuden ja käytettävyyden säilyttäminen verkkovälineellä.
Tieto- ja viestintätekniset resurssit	Joko ohjelmisto- tai laitteistoresurssit, joita käytetään liiketoimintaympäristössä
Tieto- ja viestintätekniikan hankkeet	Kaikki hankkeet tai niiden osat, joissa tieto- ja viestintäteknisiä järjestelmiä muutetaan, vaihdetaan tai toteutetaan.
Tieto- ja viestintätekniikka- sekä turvallisuusriski	Operatiivisen riskin osatekijänä tappion riski, joka johtuu salassapitovelvollisuuden rikkomisesta, järjestelmien ja datan luotettavuuden rikkoutumisesta, järjestelmien ja datan sopivuudessa tai saatavuudessa olevista ongelmista tai siitä, että tieto- ja viestintätekniikkaa ei pystytä vaihtamaan kohtuullisen ajan kuluessa ja kohtuullisin kustannuksin, kun ympäristö- ja liiketoimintavaatimukset muuttuvat (ts. joustavuus). Tähän kuuluvat kyberriskit sekä tietoturvariskit, jotka johtuvat riittämättömistä tai epäonnistuneista sisäisistä prosesseista tai ulkoisista tapahtumista, muun muassa kyberhyökkäyksistä tai riittämättömästä fyysisestä turvallisuudesta.

Tietoturva	Tietojen ja/tai tietojärjestelmien luottamuksellisuuden, luotettavuuden ja käytettävyyden säilyttäminen. Siihen voi liittyä myös muita tekijöitä, kuten aitous, vastuuvelvollisuus, kiistattomuus ja varmuus.
Tieto- ja viestintätekniset palvelut	Palvelut, joita tieto- ja viestintätekniset järjestelmät ja palveluntarjoajat tarjoavat yhdelle tai useammalle laitoksen sisäiselle tai ulkopuoliselle käyttäjälle.
Tieto- ja viestintätekniset järjestelmät	Sovellusten, palvelujen, tietoteknisten resurssien, tieto- ja viestintäteknisten resurssien tai muiden tietojen keräämisen osatekijöiden kokonaisuus, joka sisältää toimintaympäristön.
Tietoresurssit	Kokoelma aineellisia tai aineettomia tietoja, jotka ovat suojaamisen arvoisia.
Luotettavuus	Tarkkuutta ja täydellisyyttä koskeva ominaisuus.
Operatiivinen poikkeama tai turvapoikkeama	Yksittäinen tapahtuma tai toisiinsa liittyvien suunnittelemattomien tapahtumien sarja, joka vaikuttaa tai todennäköisesti vaikuttaa haitallisesti tieto- ja viestintäteknisten järjestelmien ja palvelujen luotettavuuteen, käytettävyyteen ja luottamuksellisuuteen.
Palveluntarjoaja	Kolmas osapuoli, joka toteuttaa prosessin, palvelun tai toimen tai osan siitä ulkoistamisjärjestelyn nojalla.
Uhkaan perustuva tietoturvallisuuden tason testaus	Hallittu yritys vaarantaa yksikön kyberuhkien sietokyky jäljittelemällä todellisen elämän uhkatekijöiden taktiikoita, tekniikoita ja menettelyjä. Se perustuu kohdennettuun tiedonhankintaan uhista, ja siinä keskitytään yksikön ihmisiin, menettelyihin ja teknologiaan siten, että ennakkotietoja on vähän ja vaikutus operaatioihin pieni.
Haavoittuvuus	Resurssin tai valvonnan heikko kohta, alttius tai vika, jota yksi tai useampi uhka voi hyödyntää.

7. Näitä ohjeita sovelletaan 1. heinäkuuta 2021 alkaen.

Ohje 1 – Oikeasuhteisuus

8. Yritysten on sovellettava näitä ohjeita oikeassa suhteessa niiden liiketoimintaan liittyvien riskien luonteeseen, laajuuteen ja monimutkaisuuteen.

Ohje 2 – Tieto- ja viestintätekniikka hallintojärjestelmässä

9. Hallinto-, johto- tai valvontaelimen on varmistettava, että yrityksen hallintojärjestelmä, erityisesti riskinhallinnasta ja sisäisestä valvonnasta vastaava järjestelmä, hallinnoi yrityksen tieto- ja viestintätekniikka- sekä turvallisuusriskejä asianmukaisesti.

10. Hallinto-, johto- tai valvontaelimen on varmistettava, että yrityksen henkilöstön määrä ja osaaminen ovat asianmukaisia niiden tieto- ja viestintätekniikan operatiivisten tarpeiden ja niiden tieto- ja viestintätekniikka- sekä turvallisuusriskien hallintaprosessien tukemiseksi jatkuvasti sekä niiden tieto- ja viestintätekniikan strategian toteuttamiseksi. Henkilöstön on myös saatava säännöllisesti asianmukaista koulutusta tieto- ja viestintätekniikka- sekä turvallisuusriskeistä, myös tietoturvasta, ohjeen 13 mukaisesti.

11. Hallinto-, johto- tai valvontaelimen on varmistettava, että edellä mainittujen vaatimusten täyttämiseen on osoitettu riittävästi resursseja.

Ohje 3 – Tieto- ja viestintätekniikan strategia

12. Hallinto-, johto- tai valvontaelimellä on yleinen vastuu yrityksen kirjallisen tieto- ja viestintätekniikan strategian laatimisesta ja hyväksymisestä osana yleistä liiketoimintastrategiaa ja sen mukaisena sekä siitä tiedottamisen ja sen täytäntöönpanon valvonnasta.

13. Tieto- ja viestintätekniikan strategiassa on määritettävä vähintään

    a) se, miten yritysten tieto- ja viestintätekniikkaa pitäisi kehittää, jotta sillä voitaisiin tukea tehokkaasti niiden liiketoimintastrategiaa ja toteuttaa se, muun muassa kehittämällä organisaatiorakennetta, liiketoimintamalleja, tieto- ja viestintäteknisiä järjestelmiä ja keskeisiä riippuvuuksia palveluntarjoajien kanssa

    b) tieto- ja viestintäteknisen rakenteen kehitys, myös palveluntarjoajien riippuvuudet ja

    c) selkeät tietoturvatavoitteet, joissa keskitytään tieto- ja viestintäteknisiin järjestelmiin ja palveluihin, henkilöstöön ja prosesseihin.

14. Yritysten on varmistettava, että tieto- ja viestintätekniikan strategia pannaan täytäntöön ja hyväksytään ja että siitä tiedotetaan kaikille asianomaisille työntekijöille ja soveltuvin osin palveluntarjoajille asianmukaisesti ja ajoissa.

15. Yritysten on myös laadittava menettely tieto- ja viestintätekniikan strategiansa toteuttamisen tehokkuuden seuraamiseksi ja mittaamiseksi. Menettelyä on tarkistettava ja päivitettävä säännöllisesti.

Ohje 4 – Tieto- ja viestintätekniikka- sekä turvallisuusriskit riskinhallintajärjestelmässä

16. Hallinto-, johto- tai valvontaelimellä on yleinen vastuu siitä, että yrityksen yleisen riskinhallintajärjestelmän osana perustetaan tehokas järjestelmä tieto- ja viestintätekniikka- sekä turvallisuusriskien hallitsemista varten. Tähän kuuluvat kyseisiä riskejä koskevan riskinsietokyvyn määrittäminen yrityksen riskistrategian mukaisesti ja hallinto-, johto- tai valvontaelimelle säännöllisesti osoitettu kirjallinen raportti riskinhallintaprosessin tuloksesta.

17. Yritysten on osana yleistä riskinhallintajärjestelmäänsä otettava (jäljempänä kuvattuja tieto- ja viestintätekniikan suojeluvaatimuksia määrittäessään) tieto- ja viestintätekniikka- sekä turvallisuusriskien osalta huomioon ainakin seuraavat:

    a) Yritysten on tehtävä kartoitus säännöllisine päivityksineen liiketoimintaprosesseistaan ja liiketoimistaan sekä yrityksen toiminnoista tehtävistä ja resursseista (esim. tietoresurssien ja tieto- ja viestintäteknisten resurssien) , jotta voitaisiin määritellä niiden merkitys ja riippuvuudet tieto- ja viestintätekniikka- sekä turvallisuusriskien kannalta.

    b) Yritysten on määritettävä ja mitattava kaikki asianomaiset tieto- ja viestintätekniikka- sekä turvallisuusriskit, joille ne ovat alttiita, ja luokiteltava määritetyt liiketoimintaprosessit ja liiketoimet sekä yrityksen toiminnot, tehtävät ja resurssit (esim. tietoresurssit ja tieto- ja viestintätekniset resurssit) kriittisyyden kannalta. Yritysten on myös arvioitava suojeluvaatimukset, jotka koskevat vähintään kyseisten liiketoimintaprosessien ja liiketoimien sekä yrityksen toimintojen, tehtävien ja resurssien (esim. tietoresurssien ja tieto- ja viestintäteknisten resurssien) luottamuksellisuutta, luotettavuutta ja käytettävyyttä. Resurssien luokittelusta vastaavat resurssien omistajat on määritettävä.

    c) Kriittisyyden sekä vaaditun suojan tason määrittämiseen erityisesti luotettavuutta, käytettävyyttä ja luottamuksellisuutta koskevien suojelutavoitteiden osalta käytettävillä menetelmillä on varmistettava, että tuloksena saatavat suojeluvaatimukset ovat johdonmukaisia ja kattavia.

    d) Tieto- ja viestintätekniikka- sekä turvallisuusriskit on mitattava sellaisten määritettyjen tieto- ja viestintätekniikka- sekä turvallisuusriskejä koskevien kriteerien perusteella, joissa otetaan huomioon liiketoimintaprosessien ja liiketoimien sekä yrityksen toimintojen, tehtävien ja resurssien (esim. tietoresurssien ja tieto- ja viestintäteknisten resurssien) kriittisyys, tunnettujen haavoittuvuustekijöiden laajuus ja yritykseen aiemmin vaikuttaneet poikkeamat.

    e) Tieto- ja viestintätekniikka- sekä turvallisuusriskien arviointi on tehtävä ja dokumentoitava säännöllisesti. Tämä arviointi on myös tehtävä ennen kuin infrastruktuuriin, prosesseihin tai menettelyihin tehdään suuria muutoksia, jotka vaikuttavat liiketoimintaprosesseihin ja liiketoimiin sekä yrityksen toimintoihin, tehtäviin ja resursseihin (esim. tietoresursseihin ja tieto- ja viestintäteknisiin resursseihin).

    f) Riskinarvioinnin perusteella yritysten on vähintään määritettävä ja toteutettava toimenpiteitä, joilla hallitaan yksilöityjä tieto- ja viestintätekniikka- sekä turvallisuusriskejä ja suojellaan tietoresursseja niiden luokituksen mukaisesti. Myös jäljellä olevien jäännösriskien hallintatoimenpiteet on määritettävä.

18. Hallinto-, johto- tai valvontaelimen on hyväksyttävä tieto- ja viestintätekniikka- sekä turvallisuusriskien hallintaprosessien tulokset ja sisällytettävä ne operatiivisten riskien hallintaprosessiin osana yrityksen yleistä riskinhallintaa.

Ohje 5 – Tarkastus

19. Tarkastajien, joilla on riittävästi tietämystä, osaamista ja kokemusta tieto- ja viestintätekniikka- sekä turvallisuusriskeistä, on tarkastettava yrityksen tieto- ja viestintätekniikka- sekä turvallisuusriskejä koskevat hallintotavat, järjestelmät ja

prosessit säännöllisesti yrityksen tarkastussuunnitelman[11] mukaisesti, jotta niiden tehokkuudesta voitaisiin antaa riippumaton varmistus hallinto-, johto- tai valvontaelimelle. Kyseisten tarkastusten tiheyden ja kohteen on oltava oikeassa suhteessa asianomaisiin tieto- ja viestintätekniikka- sekä turvallisuusriskeihin.

Ohje 6 – Sisäiset turvallisuuskäytännöt ja -toimenpiteet

20. Yritysten on laadittava hallinto-, johto- tai valvontaelimen hyväksymät kirjalliset tietoturvakäytännöt, joissa on määritettävä korkean tason periaatteet ja säännöt yrityksen tietojen luottamuksellisuuden, luotettavuuden ja käytettävyyden suojelemiseksi, jotta tieto- ja viestintätekniikan strategian toteuttamista voidaan tukea.

21. Käytäntöjen täytyy sisältää kuvaus tietoturvahallinnan keskeisistä tehtävistä ja vastuista, ja siinä on esitettävä työntekijöitä, prosesseja ja teknologiaa koskevat vaatimukset tietoturvan osalta ja todettava, että jokaisen tason työntekijällä on vastuualueita yritysten tietoturvan varmistamisessa.

22. Käytännöistä on tiedotettava yrityksessä, ja niitä on sovellettava koko henkilöstöön. Soveltuvin osin ja tarpeen mukaan tietoturvakäytännöistä tai niiden osista on myös tiedotettava palveluntarjoajille ja niitä on sovellettava näihin.

23. Yritysten on käytäntöjen perusteella laadittava ja toteutettava entistä täsmällisempiä tietoturvamenettelyjä ja tietoturvatoimenpiteitä, jotta voitaisiin muun muassa vähentää tieto- ja viestintätekniikka- sekä turvallisuusriskejä, joille yritykset altistuvat. Näiden menettelyjen ja tietoturvatoimenpiteiden on sisällettävä kaikki näissä ohjeissa kuvatut prosessit soveltuvin osin.

Ohje 7 – Tietoturvatoiminto

24. Yritysten on laadittava hallintojärjestelmäänsä suhteellisuusperiaatteen mukaisesti tietoturvatoiminto, jossa vastuut on osoitettu nimetylle henkilölle. Yrityksen on varmistettava tämän tietoturvatoiminnon riippumattomuus ja puolueettomuus erottamalla tieto- ja viestintäteknisten operaatioiden kehitys ja prosessit siitä asianmukaisesti. Toiminto on hallinto-, johto- tai valvontaelimen alainen.

25. Tietoturvatoiminnon yleisenä tehtävänä on

    a) tukea hallinto-, johto- tai valvontaelintä yrityksen tietoturvakäytäntöjen määrittämisessä ja ylläpitämisessä ja niiden käyttöönoton valvonnassa

    b) raportoida ja antaa neuvontaa hallinto-, johto- tai valvontaelimelle säännöllisesti ja tapauskohtaisesti tietoturvan ja sen kehityksen tilasta

    c) seurata ja arvioida tietoturvatoimenpiteiden toteuttamista

    d) varmistaa, että palveluntarjoajia käytettäessä noudatetaan tietoturvavaatimuksia

    e) varmistaa, että kaikille työntekijöille ja palveluntarjoajille, joilla on pääsy tietoihin ja järjestelmiin, tiedotetaan asianmukaisesti tietoturvakäytännöistä, esimerkiksi tietoturvakoulutuksessa ja tietämystä lisäävissä tapahtumissa

    f) koordinoida operatiivisten poikkeamien tai turvapoikkeamien tutkintaa ja ilmoittaa merkityksellisistä poikkeamista hallinto-, johto- tai valvontaelimelle.

[11] Delegoidun asetuksen 271 artikla.

Ohje 8 – Looginen turvallisuus

26. Yritysten on määritettävä, dokumentoitava ja toteutettava loogista pääsynvalvontaa tai loogista turvallisuutta koskevia menettelyjä (henkilöllisyyden ja pääsyn valvonta) ohjeessa 4 määritettyjen suojeluvaatimusten mukaisesti. Nämä menettelyt on toteutettava, niitä on valvottava, seurattava ja tarkistettava säännöllisesti, ja niihin on sisällyttävä myös tarkastukset poikkeamien seuraamiseksi. Menettelyissä on toteutettava vähintään seuraavaa (käyttäjä tarkoittaa myös teknisiä käyttäjiä):

    a) Tiedonsaantitarve, pienimmän valtuuden periaate ja tehtävien erillään pitäminen: yritysten on hallinnoitava tietoresursseja, myös etäkäyttöä, ja niiden tukijärjestelmiä koskevia oikeuksia tiedonsaantitarpeen perusteella. Käyttäjille on annettava vain välttämättömät tehtävien suorittamisen edellyttämät käyttöoikeudet, (pienimmän valtuuden periaate), jotta estettäisiin perusteeton tietoihin pääsy tai estettäisiin sellaisten käyttöoikeusyhdistelmien myöntäminen, joita voidaan käyttää valvonnan kiertämiseen (tehtävien erillään pitämisen periaate).

    b) Käyttäjän vastuuvelvollisuus: yritysten on rajoitettava mahdollisimman laajasti yleisten ja yhteisten käyttäjätilien käyttöä ja varmistettava, että käyttäjät voidaan tunnistaa ja jäljittää aina tieto- ja viestintäteknisissä järjestelmissä toteutettavista toimista vastuulliseen luonnolliseen henkilöön tai toimien osalta valtuutettuun tehtävään asti.

    c) Erityiskäyttöoikeudet: yritysten on vahvistettava erityiskäyttöoikeuksien valvontaa rajoittamalla tiukasti tilejä, joilla käyttöoikeudet ovat muita laajemmat (esim. ylläpitäjän tilit), ja valvomalla niitä tiiviisti.

    d) Etäkäyttö: turvallisen viestinnän varmistamiseksi ja riskin pienentämiseksi hallintaoikeudellinen etäpääsy kriittisiin tieto- ja viestintäteknisiin järjestelmiin on myönnettävä vain tarvepohjaisesti ja vahvojen todennusratkaisujen ollessa käytössä.

    e) Käyttäjätoimien kirjaaminen: käyttäjien toimet on kirjattava ja niitä on seurattava riskien kannalta oikeasuhteisesti siten, että ne sisältävät vähintään erityiskäyttäjien toimet. Käyttölokit on suojattava luvattomalta muuttamiselta ja poistamiselta, ja niitä on säilytettävä asiaankuuluva aika yksilöityjen liiketoimintojen, tukiprosessien ja tietoresurssien kriittisyyden perusteella, rajoittamatta kuitenkaan EU:n ja kansallisessa lainsäädännössä asetettuja säilytysvaatimuksia. Yritysten on käytettävä näitä tietoja helpottaakseen sellaisten poikkeavien toimien tunnistamista ja tutkintaa, jotka on havaittu palveluja tarjottaessa.

    f) Käyttöoikeuksien hallinta: käyttöoikeuksia on myönnettävä, poistettava ja muutettava oikea-aikaisesti sellaisten hyväksyntää koskevien ennalta määritettyjen rutiinien mukaisesti, joihin soveltuva tietoresurssien omistaja osallistuu. Jos käyttöön ei ole enää tarvetta, käyttöoikeudet on kumottava ripeästi.

    g) Käyttöoikeuksien arviointi: käyttöoikeudet on tarkistettava määräajoin, jotta voitaisiin varmistaa, että käyttäjillä ei ole liiallisia erioikeuksia ja että käyttöoikeudet peruutetaan/poistetaan, kun niitä ei enää tarvita.

    h) Käyttöoikeuksien myöntäminen, muuttaminen ja kumoaminen on dokumentoitava ymmärtämistä ja analysointia edistävällä tavalla

i) Todennusmenetelmät: yritysten on valvottava, että todennusmenetelmät ovat riittävän vahvat, jotta voidaan varmistaa asianmukaisesti ja tehokkaasti käyttöoikeuksien valvontakäytäntöjen ja -menettelyjen noudattaminen. Todennusmenetelmien on oltava oikeassa suhteessa käytettävien tieto- ja viestintäteknisten järjestelmien, tietojen tai prosessin kriittisyyteen. Tämän on sisällettävä vähintään vahvoja salasanoja tai tavallista vahvempia todennusmenetelmiä (kuten kahden tekijän todennus) asianomaisen riskin perusteella.

27. Sähköinen pääsy tietoihin ja järjestelmiin sovellusten avulla on rajoitettava vähimmäisvaatimuksiin, joita asiaankuuluvan palvelun tarjoaminen edellyttää.

Ohje 9 – Fyysinen turvallisuus

28. Yritysten fyysistä turvallisuutta koskevat toimenpiteet (esim. suoja sähkökatkolta, tulipalolta, vesivahingolta ja luvattomalta fyysiseltä käytöltä) on määritettävä, dokumentoitava ja toteutettava yritysten tilojen, tietokeskusten ja arkaluonteisten alueiden suojelemiseksi luvattomalta pääsyltä ja ympäristövaaroilta.

29. Fyysinen pääsy tieto- ja viestintäteknisiin järjestelmiin on sallittava vain valtuutetuille henkilöille. Valtuudet on annettava vain henkilöiden tehtävien ja vastuiden mukaisesti ja vain asianmukaisesti koulutetuille ja valvotuille henkilöille. Fyysinen pääsy on tarkistettava määräajoin sen varmistamiseksi, että tarpeettomat käyttöoikeudet kumotaan/poistetaan viipymättä, kun niitä ei enää tarvita.

30. Ympäristövaaroilta suojaavien asianmukaisten toimenpiteiden on oltava oikeassa suhteessa rakennusten merkitykseen ja kyseisissä rakennuksissa sijaitsevien operaatioiden tai tieto- ja viestintäteknisten järjestelmien kriittisyyteen nähden.

Ohje 10 – Tieto- ja viestintäteknisten operaatioiden turvallisuus

31. Yritysten on otettava käyttöön menettelyjä, joilla varmistetaan tieto- ja viestintäteknisten järjestelmien ja palvelujen luottamuksellisuus, luotettavuus ja käytettävyys, jotta voitaisiin vähentää turvallisuustekijöiden vaikutusta tieto- ja viestintäteknisten palvelujen toimittamiseen. Näihin menettelyihin täytyy kuulua asianmukaisesti seuraavat toimenpiteet:

    a) sellaisten mahdollisten haavoittuvuuksien tunnistaminen, jotka on arvioitava ja korjattava, varmistamalla, että tieto- ja viestintätekniset järjestelmät ovat ajan tasalla, myös yritysten sisäisille ja ulkoisille käyttäjilleen tarjoamat ohjelmistot, ottamalla käyttöön kriittisiä turvallisuuskorjauksia tai toteuttamalla korvaavia tarkastuksia

    b) turvallisten perustason konfigurointien käyttöönotto kaikkia kriittisiä komponentteja, kuten käyttöjärjestelmiä, tietokantoja, reitittimiä tai kytkimiä, varten

    c) verkon segmentoinnin, tietojen vuotamisen ehkäisyjärjestelmien ja verkkoliikenteen salauksen toteuttaminen (tietoresurssien luokituksen mukaisesti)

    d) päätepisteiden, myös palvelinten, työasemien ja mobiililaitteiden, suojelun käyttöönotto; yritysten on arvioitava, täyttääkö päätepiste niiden määrittämät turvallisuusvaatimukset ennen kuin sille myönnetään pääsy organisaation laajuiseen verkkoon

e) sen varmistaminen, että tieto- ja viestintäteknisten järjestelmien luotettavuuden todentamiseksi on käytössä luotettavuuden tarkastusjärjestelmät

f) levossa ja siirrossa olevien tietojen salaus (tietoresurssien luokituksen mukaisesti).

Ohje 11 – Turvallisuuden seuranta

32. Yritysten on laadittava ja toteutettava menettelyjä ja prosesseja, joilla seurataan jatkuvasti yrityksen tietoturvaan vaikuttavia toimia. Seurannassa on käsiteltäviä ainakin seuraavia:

    a) sisäiset ja ulkoiset tekijät, mukaan lukien liiketoiminta ja hallinnolliset tieto- ja viestintätekniset toiminnot

    b) palveluntarjoajien, muiden yksikköjen ja sisäisten käyttäjien tapahtumat

    c) mahdolliset sisäiset ja ulkoiset uhat.

33. Seurannan perusteella yritysten on otettava käyttöön asianmukaisia ja tehokkaita valmiuksia poikkeavien toimintojen ja uhkien havaitsemista, niistä ilmoittamista ja niihin reagointia varten. Tämä koskee muun muassa fyysistä tai loogista tunkeutumista, tietoresurssien luottamuksellisuuden, luotettavuuden ja käytettävyyden rikkomista, haitallista koodia sekä ohjelmistojen ja laitteistojen yleisesti tunnettuja haavoittuvuuksia.

34. Turvallisuusseurannasta ilmoittamisen on määrä auttaa yrityksiä ymmärtämään sekä operatiivisten poikkeamien että turvapoikkeamien luonnetta, määrittämään suuntauksia ja tukemaan yritysten sisäisiä tutkimuksia sekä edistämään asianmukaisten päätösten tekemistä.

Ohje 12– Tietoturvatarkastukset, -arviointi ja -testaus

35. Yritysten on tehtävä useita erilaisia tietoturvatarkastuksia, -arviointeja ja -testauksia voidakseen varmistaa tieto- ja viestintäteknisten järjestelmiensä ja palvelujensa haavoittuvuuksien tehokkaan havaitsemisen. Yritykset voivat esimerkiksi tehdä puuteanalyysin tietoturvastandardien, vaatimustenmukaisuustarkastusten, tietojärjestelmien sisäisten ja ulkoisten tarkastusten tai fyysisen turvallisuuden tarkastusten perusteella.

36. Yritysten on laadittava ja toteutettava tietoturvan testauskehys, jossa validoidaan niiden tietoturvatoimenpiteiden vahvuus ja tehokkuus ja varmistetaan, että kehyksessä otetaan huomioon uhat ja haavoittuvuudet, jotka on havaittu uhkien seurannassa ja tieto- ja viestintätekniikka- sekä turvallisuusriskien arviointiprosessissa.

37. Testaus on tehtävä turvallisesti ja varmasti, ja sen tekevät riippumattomat testaajat, joilla on riittävästi tietämystä, osaamista ja kokemusta tietoturvatoimenpiteiden testaamisesta.

38. Yritysten on tehtävä testejä säännöllisesti. Testauksen laajuuden, tiheyden ja menetelmän (kuten tietoturvallisuuden tason testauksen, myös uhkaan perustuvan tietoturvallisuuden tason testauksen) on oltava oikeassa suhteessa määritetyn riskin tasoon. Kriittisten tieto- ja viestintäteknisten järjestelmien testaus ja haavoittuvuusarvioinnit on tehtävä vuosittain.

39. Yritysten on varmistettava, että turvallisuustoimenpiteet testataan, kun infrastruktuuriin, prosesseihin tai menettelyihin tulee muutoksia tai jos muutoksia

tehdään merkittävien operatiivisten poikkeamien tai turvapoikkeamien vuoksi tai siksi, että julkaistaan uusia tai huomattavasti muuttuneita kriittisiä sovelluksia. Yritysten on valvottava ja arvioitava turvallisuustestien tuloksia ja päivitettävä turvatoimenpiteensä vastaavasti ja ilman tarpeetonta viivytystä kriittisten tieto- ja viestintäteknisten järjestelmien osalta.

Ohje 13 – Tietoturvakoulutus ja -valistus

40. Yritysten on laadittava kaikille työntekijöille, myös hallinto-, johto- tai valvontaelimelle, tietoturvakoulutusohjelma varmistamaan, että heidät on koulutettu täyttämään tehtävänsä ja vastuunsa inhimillisten virheiden, varkauksien, petosten, väärinkäytösten tai katoamisten vähentämiseksi. Yritysten on varmistettava, että koulutusohjelmassa annetaan koko henkilöstölle säännöllistä koulutusta.
41. Yritysten on laadittava ja toteutettava määräaikaisia turvallisuusvalistusohjelmia, joilla työntekijöille, myös hallinto-, johto- tai valvontaelimelle, annetaan koulutusta tietoturvaan liittyvien riskien käsittelystä.

Ohje 14 – Tieto- ja viestintäteknisten operaatioiden johtaminen

42. Yritysten on johdettava tieto- ja viestintäteknisiä operaatioitaan tieto- ja viestintätekniikan strategian perusteella. Asiakirjoissa on määritettävä, miten yritykset käyttävät, seuraavat ja valvovat tieto- ja viestintäteknisiä järjestelmiä ja palveluita, muun muassa dokumentoivat kriittisiä tieto- ja viestintäteknisiä prosesseja, menettelyjä ja operaatioita.
43. Yritysten on toteutettava kriittisten tieto- ja viestintäteknisten operaatioiden kirjautumis- ja seurantamenettelyt virheiden havaitsemiseksi, analysoimiseksi ja korjaamiseksi.
44. Yritysten on pidettävä yllä ajantasaista luetteloa tieto- ja viestintäteknisistä resursseistaan. Tieto- ja viestintäteknisten resurssien luettelon on oltava riittävän yksityiskohtainen, jotta tieto- ja viestintätekniset resurssit, turvaluokitus ja omistus voitaisiin yksilöidä ripeästi.
45. Yritysten on seurattava ja hallittava tieto- ja viestintäteknisten resurssien elinkaarta, jotta varmistettaisiin, että ne täyttävät jatkuvasti liiketoiminnan ja riskinhallinnan vaatimukset ja tukevat niitä. Yritysten on valvottava, että niiden toimeksisaajat tai sisäiset kehittäjät tukevat niiden tieto- ja viestintäteknisiä resursseja ja että kaikki asiaankuuluvat korjaukset ja parannukset tehdään dokumentoidun prosessin perusteella. Vanhentuneista tai tukea vailla olevista tieto- ja viestintäteknisistä resursseista johtuvat riskit on arvioitava ja niitä on vähennettävä. Käytöstä poistetut tieto- ja viestintätekniset resurssit on käsiteltävä ja poistettava käytöstä turvallisesti.
46. Yritysten on toteutettava suorituskyvyn ja valmiuksien suunnittelua ja seurantaa koskevat prosessit, jotta voidaan estää ja havaita tieto- ja viestintäteknisten järjestelmien merkittävät suorituskykyongelmat ja tieto- ja viestintätekniikan kapasiteettipuutteet ja reagoida niihin ajoissa.
47. Yritysten on määritettävä ja toteutettava tietojen ja tieto- ja viestintäteknisten järjestelmien varmistus- ja palauttamismenettelyt, jotta voidaan varmistaa niiden tarvittavan toimintakunnon palauttaminen. Varmistusten laajuus ja tiheys on määritettävä liiketoiminnan palauttamista koskevien vaatimusten ja tietojen ja tieto- ja viestintäteknisten järjestelmien kriittisyyden mukaisesti ja arvioitava

tehdyn riskinarvioinnin mukaisesti. Varmistus- ja palautusmenettelyt on testattava määräajoin.

48. Yritysten on varmistettava, että tietojen ja tieto- ja viestintäteknisten järjestelmien varmuuskopiot tallennetaan päätoimipaikan ulkopuolelle yhteen tai useampaan paikkaan, joka on turvallinen ja riittävän kaukana päätoimipaikasta, jotta voidaan estää altistuminen samoille riskeille.

Ohje 15 – Tieto- ja viestintäteknisten poikkeamien ja ongelmien hallinta

49. Yritysten on laadittava ja toteutettava poikkeamien ja ongelmien hallintaprosessi, jolla seurataan operatiivisia poikkeamia tai turvapoikkeamia ja kirjataan ne ja jonka avulla yritykset voivat häiriötapauksessa jatkaa kriittisiä liiketoimintoja ja -prosesseja tai palauttaa ne.

50. Yritysten on määritettävä asianmukaiset kriteerit ja kynnysarvot sille, että tapahtuma luokitellaan operatiiviseksi poikkeamaksi tai turvapoikkeamaksi, sekä varhaiset varoitusmerkit, jotka antavat hälytyksen, jotta operatiivisten poikkeamien tai turvapoikkeamien varhainen havainnointi otetaan käyttöön.

51. Jotta haitallisten tapahtumien vaikutusta voitaisiin vähentää ja palauttaa toimintakunto ajoissa, yritysten on laadittava asianmukaiset prosessit ja organisaatiorakenteet, joilla varmistetaan operatiivisten poikkeamien ja turvapoikkeamien johdonmukainen ja yhdennetty valvonta, käsittely ja seuranta, jotta voidaan varmistaa, että perimmäiset syyt määritellään ja käsitellään, ja että toteutetaan korjaavia toimia/toimenpiteitä, joilla estetään poikkeamien toistuminen. Poikkeamien ja ongelmien hallintaprosessissa on vähintään vahvistettava

    a) menettelyt poikkeamien havaitsemiseksi, jäljittämiseksi, kirjaamiseksi, ryhmittelemiseksi ja luokittelemiseksi yrityksen määrittämän ensisijaisuuden mukaan liiketoimintaa koskevan kriittisyyden ja palvelusopimusten perusteella

    b) tehtävät ja vastuut eri poikkeamaskenaarioissa (esim. virheet, toimintahäiriöt, kyberhyökkäykset)

    c) ongelmien hallintamenettely yhden tai useamman poikkeaman takana olevan perimmäisen syyn havaitsemiseksi, analysoimiseksi ja ratkaisemiseksi; yrityksen on analysoitava operatiiviset poikkeamat tai turvapoikkeamat, jotka on tunnistettu tai jotka ovat ilmenneet organisaatiossa ja/tai sen ulkopuolella, ja otettava huomioon, mitä näistä analyyseista on opittu, ja päivitettävä turvatoimenpiteitä sen mukaisesti

    d) tehokkaat sisäiset viestintäsuunnitelmat, myös poikkeamailmoitukset ja laajentumismenettelyt, jotka kattavat myös turvallisuuteen liittyvän kielteisen asiakaspalautteen ja joilla varmistetaan, että

        i. poikkeamista, joilla on mahdollisesti suuri haitallinen vaikutus kriittisiin tieto- ja viestintäteknisiin järjestelmiin ja palveluihin, raportoidaan asianomaiselle toimivalle johdolle

        ii. hallinto-, johto- tai valvontaelimelle ilmoitetaan tapauskohtaisesti merkittävistä poikkeamista ja ilmoitetaan vähintään vaikutuksesta, reagoinnista ja lisätarkastuksista, jotka on määriteltävä poikkeamien vuoksi

e) poikkeamiin reagointia koskevat menettelyt, jotta voidaan lieventää poikkeamiin liittyviä vaikutuksia ja varmistaa, että palvelu voidaan ottaa käyttöön ja varmistaa ajoissa

f) erityiset ulkoiset viestintäsuunnitelmat kriittisille liiketoiminnoille ja prosesseille, jotta voidaan

   i. tehdä yhteistyötä asiaankuuluvien sidosryhmien kanssa, jotta poikkeamaan voidaan reagoida ja palautua siitä tehokkaasti

   ii. antaa ajankohtaista tietoa, myös poikkeamaraportteja, ulkoisille osapuolille (esim. asiakkaille, muille markkinaosapuolille, asianomaisille (valvonta)viranomaisille) tarpeen mukaan ja sovellettavan lainsäädännön mukaisesti.

Ohje 16 – Tieto- ja viestintätekniikan hankkeiden johtaminen

52. Yritysten on otettava käyttöön tieto- ja viestintätekniikan hankkeiden menetelmä (joka sisältää riippumattomia turvallisuusvaatimuksia koskevia näkökohtia) sekä asianmukainen hallintoprosessi ja hankkeiden toteuttamisen johtamiskäytäntö, jotta voidaan tehokkaasti tukea tieto- ja viestintätekniikan strategian toteuttamista tieto- ja viestintätekniikan hankkeilla.

53. Yritysten on asianmukaisesti valvottava ja lievennettävä riskejä, jotka johtuvat niiden tieto- ja viestintätekniikan hankevalikoimasta, ja otettava myös huomioon riskit, jotka voivat johtua keskinäisistä riippuvuuksista eri hankkeiden välillä sekä useiden hankkeiden riippuvuudesta samoista resursseista ja/tai asiantuntemuksesta.

Ohje 17 – Tieto- ja viestintäteknisten järjestelmien hankinta ja kehittäminen

54. Yritysten on kehitettävä ja otettava käyttöön prosessi, jolla säännellään tieto- ja viestintäteknisten järjestelmien hankintaa, kehittämistä ja ylläpitoa, jotta voitaisiin taata, että käsiteltävien tietojen luottamuksellisuus, luotettavuus ja käytettävyys on varmistettu kokonaisvaltaisesti ja että määritetyt suojeluvaatimukset täytetään. Tämä prosessi on suunniteltava riskipohjaista lähestymistapaa käyttäen.

55. Yritysten on varmistettava, että ennen järjestelmien hankkimista tai kehittämistä koskevien toimien toteuttamista määritetään selkeästi toimintaan ja muuhun kuin toimintaan liittyvät vaatimukset (myös tietoturvavaatimukset) ja tekniset tavoitteet.

56. Yritysten on varmistettava, että käytössä on toimenpiteitä, joilla estetään tietoteknisten järjestelmien tahaton muuttaminen tai tahallinen peukalointi kehittämisen aikana.

57. Yrityksillä on oltava käytössä menetelmä tieto- ja viestintäteknisten järjestelmien ja palvelujen sekä tietoturvatoimenpiteiden testaamiseen ja hyväksymiseen.

58. Yritysten on testattava asianmukaisesti tieto- ja viestintäteknisiä järjestelmiä ja palveluja sekä tietoturvatoimenpiteitä, jotta voitaisiin yksilöidä mahdolliset heikkoudet, loukkaukset ja poikkeamat turvassa.

59. Yritysten on varmistettava tuotantoympäristöjen pitäminen erillään kehittämisestä, testaamisesta ja muista kuin tuotantoympäristöistä.

60. Yritysten on otettava käyttöön toimenpiteitä tieto- ja viestintäteknisten järjestelmien lähdekoodien (kun ne ovat saatavilla) eheyden suojelemiseksi. Niiden

on myös dokumentoitava tieto- ja viestintäteknisten järjestelmien kehitys, toteuttaminen, toiminta ja/tai konfiguraatio kattavasti, jotta voidaan vähentää mahdollista tarpeetonta riippuvuutta alan asiantuntijoista.

61. Tieto- ja viestintäteknisten järjestelmien hankintaa ja kehittämistä koskevia yritysten prosesseja on myös sovellettava tieto- ja viestintäteknisiin järjestelmiin, joita liiketoiminnon loppukäyttäjät kehittävät ja hallinnoivat organisaation tieto- ja viestintätekniikan ulkopuolella (esim. yrityksen hallinnoimat sovellukset tai loppukäyttäjän laskentasovellukset), käyttämällä riskipohjaista lähestymistapaa. Yritysten on pidettävä yllä rekisteriä näistä sovelluksista, joilla tuetaan kriittisiä liiketoimintoja tai liiketoimintaprosesseja.

Ohje 18- Tieto- ja viestintätekniikan muutoksenhallinta

62. Yritysten on laadittava ja toteutettava tieto- ja viestintätekniikan muutoksenhallintaprosessi sen varmistamiseksi, että kaikki tieto- ja viestintäteknisten järjestelmien muutokset rekisteröidään, arvioidaan, testataan, hyväksytään, valtuutetaan ja toteutetaan hallitusti. Kiireelliset tai hätätilanteessa tehtävät tieto- ja viestintätekniset muutokset on voitava jäljittää, ja niistä on ilmoitettava jälkikäteen asianomaiselle resurssien omistajalle jälkianalyysia varten.

63. Yritysten on määritettävä jatkuvasti, vaikuttavatko nykyisen toimintaympäristön muutokset nykyisiin turvatoimenpiteisiin tai vaativatko ne muiden toimenpiteiden käyttöönottoa niihin kuuluvien riskien lieventämiseksi. Näiden muutosten on noudatettava yritysten virallista muutoksenhallintaprosessia.

Ohje 19 – Liiketoiminnan jatkuvuuden hallinta

64. Yritysten liiketoiminnan jatkuvuutta koskevan käytännön osana hallinto-, johto- tai valvontaelin on vastuussa yrityksen tieto- ja viestintätekniikan toiminnan jatkuvuutta koskevan käytännön laatimisesta ja hyväksymisestä. Tieto- ja viestintätekniikan toiminnan jatkuvuutta koskevasta käytännöstä on tiedotettava asianmukaisesti yrityksessä, ja sitä on sovellettava kaikkiin asianomaisiin työntekijöihin ja tarvittaessa palveluntarjoajiin.

Ohje 20 – Liiketoiminnan vaikutusanalyysi

65. Vakaan liiketoiminnan jatkuvuuden hallinnan osana yritysten on tehtävä liiketoiminnan vaikutusanalyysi, jossa arvioidaan määrällisesti ja laadullisesti yritysten altistuminen vakaville toimintahäiriöille sekä niiden mahdollinen vaikutus käyttämällä sisäisiä ja/tai ulkoisia tietoja ja skenaarioanalyysia. Liiketoiminnan vaikutusanalyysissa on myös otettava huomioon määritettyjen ja luokiteltujen liiketoimintaprosessien ja liiketoimien sekä yrityksen toimintojen, tehtävien ja resurssien (esim. tietoresurssien ja tieto- ja viestintäteknisten resurssien) kriittisyys sekä niiden keskinäiset riippuvuudet ohjeen 4 mukaisesti.

66. Yritysten on varmistettava, että niiden tieto- ja viestintätekniset järjestelmät ja palvelut on suunniteltu ja mukautettu liiketoiminnan vaikutusanalyysin mukaisesti esimerkiksi siten, että tietyillä kriittisillä komponenteilla on varajärjestelmä, joka estää kyseisiin komponentteihin vaikuttavien tapahtumien aiheuttamat häiriöt.

Ohje 21 – Liiketoiminnan jatkuvuuden suunnittelu

67. Yritysten yleisissä liiketoiminnan jatkuvuutta koskevissa suunnitelmissa on otettava huomioon olennaiset riskit, jotka voivat vaikuttaa haitallisesti tieto- ja viestintäteknisiin järjestelmiin ja palveluihin. Suunnitelmilla on tuettava tavoitteita liiketoimintaprosessien ja liiketoimintojen sekä yrityksen toimintojen, tehtävien ja

resurssien (esim. tietoresurssien ja tieto- ja viestintäteknisten resurssien) luottamuksellisuuden, luotettavuuden ja käytettävyyden suojelusta. Yritysten on koordinoitava kyseisten suunnitelmien laadintaa tarvittaessa asiaankuuluvien sisäisten ja ulkoisten sidosryhmien kanssa.

68. Yritysten on otettava käyttöön liiketoiminnan jatkuvuutta koskevia suunnitelmia, jotta varmistettaisiin, että ne pystyvät reagoimaan asianmukaisesti mahdollisiin vikaskenaarioihin palautusaikatavoitteen (enimmäisaika, jossa järjestelmä tai prosessi on palautettava häiriön jälkeen) ja palautuspistetavoitteen (enimmäisaika, jonka tiedot voivat olla kateissa, jos poikkeama tapahtuu ennalta määritetyllä palvelutasolla) mukaisesti.

69. Yritysten on käsiteltävä liiketoiminnan jatkuvuutta koskevissa suunnitelmissaan useita erilaisia skenaarioita, myös äärimmäisiä mutta uskottavilta tuntuvia skenaarioita ja kyberhyökkäysskenaarioita, ja arvioitava kyseisten skenaarioiden mahdollista vaikutusta. Näiden skenaarioiden perusteella yritysten on kuvattava, miten tieto- ja viestintäteknisten järjestelmien ja palvelujen jatkuvuus sekä yritysten tietoturva varmistetaan.

Ohje 22 – Reagointi- ja palautussuunnitelmat

70. Liiketoiminnan vaikutusanalyysin ja uskottavilta tuntuvien skenaarioiden perusteella yritysten on laadittava reagointi- ja palautussuunnitelmat. Näissä suunnitelmissa on yksilöitävä, minkä ehtojen perusteella suunnitelma voidaan ottaa käyttöön ja mihin toimiin on ryhdyttävä, jotta varmistetaan vähintään yritysten kriittisten tieto- ja viestintäteknisten järjestelmien ja palvelujen luotettavuus, käytettävyys, jatkuvuus ja toimintakunnon palauttaminen. Reagointi- ja palautussuunnitelmien tavoitteena on oltava yritysten operaatioiden palautustavoitteiden täyttäminen.

71. Reagointi- ja palautussuunnitelmissa on otettava huomioon sekä lyhyt- että tarvittaessa pitkäaikaiset palautusvaihtoehdot. Suunnitelmilta edellytetään vähintään seuraavaa:

    a) Niissä on keskityttävä tärkeiden tieto- ja viestintäteknisten palvelujen, liiketoimintojen, tukiprosessien, tietoresurssien ja niiden keskinäisten riippuvuuksien toimintakunnon palauttamiseen, jotta voidaan estää haitalliset vaikutukset yrityksen toimintaan.

    b) Ne on dokumentoitava ja toimitettava liiketoiminta- ja tukiyksiköiden saataville, niiden on oltava heti käytettävissä hätätilanteessa, ja niissä on määritettävä selkeästi tehtävät ja vastuut.

    c) Niitä on päivitettävä jatkuvasti sen mukaisesti, mitä on opittu häiriöistä, testeistä, uusista tunnistetuista riskeistä ja uhista sekä muuttuneista palautustavoitteista ja prioriteeteista.

72. Suunnitelmissa on myös otettava huomioon muita vaihtoehtoja, jos palauttaminen ei ole toteuttamiskelpoista lyhyellä aikavälillä kustannusten, riskien, logistiikan ja ennakoimattomien olosuhteiden vuoksi.

73. Reagointi- ja palautussuunnitelmien osana yritysten on otettava huomioon ja toteutettava jatkuvuutta koskevia toimenpiteitä, joilla lievennetään yritysten tieto- ja viestintäteknisten palvelujen jatkuvuudelle ratkaisevien tärkeiden palveluntarjoajien vikoja (EIOPAn hallintojärjestelmää koskevien ohjeiden ja pilvipalvelujen tarjoajille ulkoistamisesta annettujen ohjeiden mukaisesti).

Ohje 23 – Suunnitelmien testaus

74. Yritysten on testattava liiketoiminnan jatkuvuutta koskevia suunnitelmiaan ja varmistettava, että niiden kriittisten liiketoimintaprosessien ja liiketoimien sekä yrityksen toimintojen, tehtävien ja resurssien (esim. tietoresurssien) ja tieto- ja viestintäteknisten resurssien ja niiden keskinäisten riippuvuuksien (myös palveluntarjoajien tarjoamien) toimintaa testataan säännöllisesti yrityksen riskiprofiilin perusteella.

75. Liiketoiminnan jatkuvuussuunnitelmia on päivitettävä säännöllisesti testitulosten, voimassa olevien uhkia koskevien tietojen ja aiemmista tapahtumista opitun perusteella. Niihin täytyy sisällyttää kaikki palautustavoitteiden merkitykselliset muutokset (myös palautusaikatavoite ja palautuspistetavoite) ja/tai muutokset liiketoimintaprosesseissa ja liiketoimissa sekä yrityksen toiminnoissa, tehtävissä ja resursseissa (esim. tietoresursseissa ja tieto- ja viestintäteknisissä resursseissa).

76. Liiketoiminnan jatkuvuutta koskevien suunnitelmien testauksessa on osoitettava, että niillä pystytään säilyttämään liiketoiminnan kannattavuus, kunnes kriittiset toiminnot on palautettu ennalta määritetylle palvelutasolle tai vaikutusten sietokykyä koskevalle tasolle.

77. Testitulokset on dokumentoitava, ja kaikki testeistä johtuvat havaitut puutteet on analysoitava, käsiteltävä ja raportoitava hallinto-, johto- tai valvontaelimelle.

Ohje 24 – Kriisiviestintä

78. Häiriö- tai hätätilanteessa ja liiketoiminnan jatkuvuuden suunnitelmien toteutuksen aikana yritysten on varmistettava, että niillä on käytössään tehokkaat kriisiviestintämenettelyt, jotta kaikille asiaankuuluville sisäisille ja ulkoisille sidosryhmille, myös asianomaisille valvontaviranomaisille, kun sitä edellytetään kansallisissa säädöksissä, sekä asianomaisille palveluntarjoajille, tiedotetaan hyvissä ajoin ja asianmukaisella tavalla.

Ohje 25 – Tieto- ja viestintäteknisten palvelujen ja järjestelmien ulkoistaminen

79. Sanotun rajoittamatta EIOPAn ulkoistamisesta pilvipalvelujen tarjoajille antamia ohjeita yritysten on varmistettava, että tieto- ja viestintäteknisiä palveluja ja järjestelmiä ulkoistettaessa tieto- ja viestintäteknistä palvelua tai järjestelmää koskevat asiaankuuluvat vaatimukset täytetään.

80. Jos ulkoistetaan kriittisiä tai tärkeitä toimintoja, yritysten on varmistettava, että palveluntarjoajan sopimusvelvoitteissa (esim. sopimuksessa, palvelutasosopimuksissa, asianomaisten sopimusten irtisanomissäännöksissä) on vähintään seuraavat:

    a) asianmukaiset ja oikeasuhteiset tietoturvatavoitteet ja -toimenpiteet, mukaan lukien vaatimukset, kuten tietoturvan vähimmäisvaatimukset, yritysten tietojen elinkaarta koskevat eritelmät, tarkastus- ja käyttöoikeudet ja kaikki vaatimukset, jotka koskevat tietokeskusten sijaintia, sekä tietojen salaamista, verkon turvallisuutta ja turvallisuuden seurantaprosesseja koskevat vaatimukset

    b) palvelutasosopimukset, jotta voidaan varmistaa tieto- ja viestintäteknisten palvelujen ja järjestelmien jatkuvuus sekä suorituskykytavoitteiden saavuttaminen tavanomaisissa olosuhteissa sekä valmiussuunnitelmissa tarkoitettujen tavoitteiden saavuttaminen, kun palvelu keskeytyy

c) operatiivisten poikkeamien ja turvapoikkeamien käsittelymenettelyt, myös laajenemisen ja raportoinnin osalta.

81. Yritysten on valvottava sitä, millä tasolla nämä palveluntarjoajat noudattavat turvallisuustavoitteita, turvatoimenpiteitä ja suoritustavoitteita, ja pyrittävä saamaan varmistus siitä.

Noudattamista ja ilmoittamista koskevat säännöt

82. Tämä asiakirja sisältää ohjeita, jotka on annettu asetuksen (EU) N:o 1094/2010 16 artiklan nojalla. Kyseisen asetuksen 16 artiklan 3 kohdan mukaisesti toimivaltaisten viranomaisten ja yritysten on kaikin tavoin pyrittävä noudattamaan ohjeita ja suosituksia.

83. Toimivaltaisten viranomaisten, jotka noudattavat tai aikovat noudattaa näitä ohjeita, täytyy sisällyttää ne sääntely- tai valvontakehykseensä asianmukaisella tavalla.

84. Toimivaltaisten viranomaisten on kahden kuukauden kuluessa käännettyjen versioiden laatimisesta vahvistettava EIOPAlle, noudattavatko tai aikovatko ne noudattaa näitä ohjeita, sekä ilmoitettava perustelut, jos ne eivät noudata tai aio noudattaa ohjeita.

85. Mikäli vastausta ei saada määräaikaan mennessä, EIOPA katsoo, etteivät toimivaltaiset viranomaiset noudata ohjeita.

Tarkistuksia koskeva loppumääräys

86. EIOPA tarkistaa näitä ohjeita.