Petri Launiainen
Gestion Communications Oy
5. lokakuuta 2020

Kybertilanteiden viestintä

Miten kybertilanteiden viestintään ja maineriskiin voi varautua?

Asiakkaiden, liikekumppanien ja sidosryhmien luottamus on jokaisen organisaation, niin yksityisen liikeyrityksen kuin valtion virastonkin, menestyksellisen toiminnan ehdoton edellytys. Ilman luottamusta ei synny luottamuksellisia kumppanuuksia eikä asiakassuhteita.

Miten organisaatio voi menettää tärkeiden sidosryhmiensä luottamuksen? Tapoja on tietenkin monia, mutta yksi nopeimmista ja tehokkaimmista tavoista on olla suojaamatta hallussaan olevia tärkeitä tietoja kuten asiakastietoja, henkilötietoja, liikesalaisuuksia ja muita arkaluontoisia tietoja. Jos näitä tietoja anastetaan tai niiden tietoturva muutoin vaarantuu, syntyy niin sanottu kybertilanne*, joka ei välttämättä ole mennyt kriisikynnyksen yli, mutta joka on ehdottomasti poikkeuksellinen tilanne. Syyttävä sormi osoittaa aina organisaatiota, jonka haltuun tärkeät tiedot on annettu. Vaikka tietoturvapalvelut olisikin ostettu palveluntuottajalta, luottamus itse organisaatioon vaarantuu.

Kybertilanteet ovat erityisen hankalia ja haitallisia organisaatioille kolmesta syystä. Ensinnäkin lähes kaikilla organisaatioilla on henkilötietoja tai asiakastietoja hallussaan. Toiseksi organisaatioiden toiminta on enemmän ja enemmän tietoverkoissa tapahtuvaa. Kolmanneksi kybertilanteissa tärkeiden sidosryhmien luottamus vaarantuu tilanteiden luonteen vuoksi todella nopeasti. Kybertilanteet ylittävät kriisikynnyksen nopeammin ja helpommin kuin moni muu poikkeuksellinen tilanne.

* kybertilanne on tilanne, jossa organisaation tietoturvaan kohdistuu uhka tai rikollinen teko ja joka saattaa aiheuttaa organisaatiolta teknisiä tai muita toimenpiteitä uhan estämiseksi tai rikoksen selvittämiseksi.

Iso osa yrityksistä on varautunut huonosti tietoturva-asioihin. Huonoiten varautuneita ovat pk-yritykset ja parhaiten varautuneita ovat isot yritykset. Kokemukseni mukaan kybertilanteen aiheuttamaan mainehaittaan tai kybertilanteen aiheuttamaan viestintätarpeeseen on varauduttu organisaatioissa vielä huonommin kuin tietoturva-asioihin ylipäätään.

Kybertilanteiden eli tietomurtojen ja muiden tietoturvaa vaarantavien tilanteiden mahdollisuus on tiedossa kaikissa organisaatioissa. Näin ollen kybertilanne ei ole koskaan varsinaisesti odottamaton tilanne. Ja juuri tämä lisää sen vahingollisuutta organisaatiota kohtaan tunnetulle luottamukselle.

Niin oudolta kuin se kuulostaakin, niin hyvin hoidettu kybertilanne on usein mahdollisuus organisaatiolle vahvistaa itseään kohtaan tunnettua luottamusta. Kybertilanteen aikana organisaatiolla on loistava tilaisuus hoitaa tilanne vastuullisesti ja arvojensa mukaisesti. Lopputuloksena pitäisi olla kriisistä aiheutuvan näkyvyyden hyödyntäminen parhaalla mahdollisella tavalla. Tämä edellyttää yrityksen perusrakenteiden ja arvojen olevan vakaalla pohjalla. Kriisin aikana ei perustavaa laatua olevia virheitä saada enää kunnolla korjattua.

Miksi ja miten kybertilanteen viestintään pitäisi varautua?

Lainsäädännössä on organisaatioille asetettu velvoitteita, joiden vuoksi tietoturvaloukkauksista pitää ilmoittaa sekä viranomaisille että asiakkaille.

Tietoturvasäännösten mukaan rekisterinpitäjän ja henkilötietojen käsittelijän tulee suojata henkilötiedot niihin liittyvää riskiä vastaavasti. Mikäli luonnollisten henkilöiden oikeuksille tai vapauksille riskin aiheuttava tietoturvaloukkaus pääsee kuitenkin tapahtumaan, pitää siitä ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa. Tietoturvaloukkauksesta pitää ilmoittaa myös rekisteröidylle henkilölle mikäli henkilön oikeuksille ja vapauksille aiheutuu todennäköisesti korkea riski.

Arvopaperimarkkinalaissa on puolestaan säädetty pörssiyhtiöiden sisäpiirisäännöksien lisäksi myös jatkuvasta tiedonantovelvollisuudesta koskien tietoja, jotka voivat vaikuttaa olennaisesti yhtiön arvopaperin arvoon.

Kybertilanteet eroavat muista poikkeuksellisista tilanteista monellakin tavalla, mutta erityispiirteenä on näiden monimutkaisten tilanteiden selittäminen sidosryhmille ja medialle. Esimerkiksi kybertilanne kääntyy kansan kielessä ja mediassa nopeasti tietomurroksi vaikka mitään tietoja ei olisikaan anastettu. Ja organisaation maineen kannalta on tietenkin selkeä ero siinä, onko tietoja päätynyt rikollisille vai onko niitä ainoastaan yritetty anastaa.

Sijoittajia ja rahoittajia kiinnostaa miten kybertilanteisiin on varauduttu ja miten mahdollisen tilanteen aiheuttama mainehaitta on huomioitu organisaatiossa. Näillä kun on suora vaikutus yrityksen liiketoimintaan ja sen jatkuvuuteen. Tutkimuksen mukaan 60 % pk-yrityksistä USA:ssa on ajautunut kybertilanteen jälkeen konkurssiin.

Kybertilanteet ovat usein puhtaasti rikollista toimintaa. Esimerkkeinä tästä ovat muun muassa vuonna 2015 suomalaisen yrityksen Affecton tytäryhtiölle aiheutunut lähes miljoonan euron tappio sekä Konecranesin tytäryhtiön 17,2 miljoonan euron tappiot. Vuonna 2019 tehdyn tutkimuksen mukaan juuri kyberrikoksen aiheuttamat kriisitilanteet huolettavat yritysjohtajia tulevaisuudessa eniten.

Rahallisia seuraamuksia yrityksille voi tulla myös GDPR:n velvoitteiden rikkomisista. Ensimmäiset sakot on määrätty Suomessakin. Euroopassa sakkoja on määrätty tähän mennessä noin 360 tapauksessa yhteensä 500 miljoonaa euroa.

Kybertilanteisiin voi varautua etenkin tietoturvaa parantamalla. Mutta sen lisäksi organisaation kannattaa varautua kybertilanteen viestintään ja sitä seuraavan mahdollisen kriisitilanteen viestintään. Viestintä on kybertilanteen hoitamisen näkyvin osa ja sen onnistuminen on kriittinen tekijä tilanteesta selviämisen kannalta. Saattaa syntyä niin sanottu ”lawful but awful” -tilanne, jossa on toimittu täysin oikein, mutta tilanne näyttää silti pahalta ulkopuolisen silmin katsottuna.

Kybertilanteet ja informaatiovaikuttaminen

Kybertilanteissa saattaa olla mukana elementtejä informaatiovaikuttamisesta, jotka pitää tunnistaa mahdollisimman nopeasti. Pelkkä medialukutaito ei riitä vaan vaikuttavan tahon motiivit pitää tunnistaa, jotta tilanteeseen voidaan reagoida oikein.

Informaatiovaikuttamisella tarkoitetaan toimintaa, jolla

pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn. Vaikuttamisen keinoja ovat esimerkiksi väärien tai harhaanjohtavien tietojen levittäminen ja painostaminen sekä sinänsä oikean tiedon tarkoitushakuinen käyttö. Kyse on strategisesta toiminnasta, jonka tavoitteena on saada kohde tekemään itselleen haitallisia päätöksiä ja toimimaan omaa etuaan vastaan.

Informaatiovaikuttamista on havaittu valtioiden välillä jo pitkään. Usein infovaikuttamisoperaatioissa käytetään tietoverkkoja ja tietoteknisiä keinoja hyväksi. Hyvänä esimerkkinä kybertilanteen ja infovaikuttamisen symbioosista on taannoinen sijoitusyhtiö BlackRockin toimitusjohtajan väärennetty kirje sijoittajille, jossa toimitusjohtaja lupasi yhtiönsä panostavan ilmastonmuutoksen vastustamiseen huomattavasti.

Vuoden 2016 presidentinvaalit USA:ssa olivat malliesimerkki siitä, miten tietoverkkoja, sosiaalisen median palveluntuottajan asiakastietoja hyödyntämällä ja informaatiovaikuttamisella voi vaikuttaa laajoihin yhteiskunnallisiin asioihin.

Yritysten odotetaan ratkovan entistä enemmän yhteiskunnallisia ongelmia ja senpä vuoksi ne saattavat jatkossa olla useamminkin erilaisten haktivistien maalitauluna esimerkiksi vastuullisuus- ja ympäristökysymyksissä.

LÄHTEET

Affectolta huijattiin miljoona euroa
Tapaus on jo toinen suomalaisyritykseen kohdistunut petos lyhyessä ajassa
https://www.hs.fi/talous/art-2000002846856.html

Fake BlackRock communications are a master class in spoofing and social engineering
https://www.cnbc.com/2019/01/16/fake-blackrock-communications-are-a-master-class-in-spoofing.html

Finlex Arvopaperimarkkinalaki
https://finlex.fi/fi/laki/ajantasa/2012/20120746#O3L6

GDPR Enforcement Tracker
https://www.enforcementtracker.com/?insights

GDPR-sakko kolmelle Suomessa
https://www.tietopiiri.fi/gdpr-sakko-kolmelle-suomessa/

Informaatiovaikuttamiseen vastaaminen: Opas viestijöille. Valtioneuvoston kanslian julkaisuja 2019:11
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161512
VNK_11_2019_Informaatiovaikuttamisen%20vastaaminen_web.pdf?
sequence=1&isAllowed=y

Miksi PK-yritykset ovat erityisen herkkiä kyberhyökkäyksille?
https://blog.f-secure.com/fi/miksi-pk-yritykset-ovat-erityisen-herkkia-kyberhyokkayksille/

Tietosuojavaltuutetun toimisto
https://tietosuoja.fi/tietoturvaloukkaukset