7/2022

Kybersuosituksia mediayrityksille

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI

Dokumentin tarkoitus ja sisältö

Tämän dokumentin tavoitteena on auttaa media-alan yrityksiä kyberturvallisuutta parantavien toimenpiteiden suunnittelussa ja toteutuksessa. Suositukset on tuottanut Mediapooli. Käytännön toteutuksesta vastasi 490 Innovations Oy alan asiantuntijoiden tukemana.

Dokumentissa käsitellään varsin vapaamuotoisesti kyberturvallisuuteen liittyviä osa-alueita. Mukana on paitsi tietoturvaan ja tietosuojaan liittyviä suosituksia, myös esimerkiksi sisältöjen eheydestä huolehtimiseen ja informaatiovaikuttamiseen liittyviä suosituksia. Suurin osa suosituksista keskittyy riskien ennaltaehkäisyyn. Lisätietolinkit tukevat teemoihin perehtymistä.

Dokumentti on jaettu viiteen osaan:

1. Yleisiä kyberturvallisuudesta huolehtimiseen liittyviä periaatteita
2. Teemoja, joihin erityisesti media-alan yrityksissä on hyvä kiinnittää huomiota
3. Eri työntekijäryhmille relevantteja ohjeita
4. Toimintaohjeita, kun riski on toteutunut
5. Muuta tukimateriaalia

Materiaali on tarkoitettu yritysten oman toiminnan kehittämisen tueksi. Sekä varautumiseen että eri toteutuneisiin tilanteisiin luodut toimintaohjeet kannattaa käydä läpi yrityksen omista lähtökohdista käsin ja työstää omaan toimintaan sopiviksi esimerkiksi työpöytäharjoitusten avulla. Sisältöön liittyvää palautetta voi lähettää Mediapoolin valmiuspäällikölle (www.mediapooli.fi/yhteystiedot/).

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI

Sisällys

Ohje. Siirtyäksesi tietylle sivulle, paina ctrl ja klikkaa otsikkoa.

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI

Osa 1

Yleisiä kyberturvallisuuteen liittyviä periaatteita

Kyberturvallisuus vaatii systemaattista johtamista

Ei projekti vaan prosessi

- Kyberturvallisuuden kehittäminen ei ole määräaikainen projekti. Kyberturvallisuuden kehittämisen tulee olla jatkuva prosessi. Uhkia ja niihin liittyviä toimenpiteitä on työstettävä säännöllisesti. Muuten sekä pienten että suurten kyberongelmien riski kasvaa.

Hallitus ja johto ovat avainasemassa

- Kun yrityksen hallitus ja johto pitävät kyberturvallisuutta merkityksellisenä, ottavat sen kaupallisten tavoitteiden rinnalla osaksi yrityksen strategisia tavoitteita ja osallistuvat turvallisuuden kehittämiseen, syntyy hyviä tuloksia.

Myös raha ratkaisee

- Varautuminen maksaa. Kyberhyökkäyksiin varautuminen vaatii sekä sisäisiä henkilötyötunteja että panostuksia tekniikkaan ja ulkoisiin palveluihin. Mutta varautumattomuus voi maksaa vielä enemmän.

Projektilla liikkeelle

- Jos kyberasiat ovat jääneet yrityksessä muiden kiireiden jalkoihin, kannattaa toteuttaa projektimainen kehityspyrähdys ennen jatkuvan prosessin käynnistämistä. Esimerkki kehittämisprojektista löytyy osasta 5.

Varautunut palkitaan

- Kyberturvallisuuden kehittäminen kehittää organisaation toimintaa myös laajemmin. Se auttaa koko organisaatiota ymmärtämään yrityksen tehtävän merkityksellisyyttä ja ohjaa kaikkia tekemään työtä yhteisten tavoitteiden hyväksi. Harjoitukset kasvattavat ymmärrystä koko organisaation toiminnasta.
- Ja kun pahantahtoinen toimija kolkuttelee yrityksen digitaalisia ovia tai pääsee niistä joskus sisälle, varautunut palkitaan. Mitään isoa vahinkoa ei päässyt tapahtumaan.

Valmiussuunnittelu ja osaaminen avainasemassa

Hyvin suunniteltu kestää

- Vaikka henkilöstön tietoisuus erilaisista riskeistä olisi erinomainen, aina joskus tapahtuu vahinkoja ja kyberhyökkääjä pääsee tunkeutumaan yrityksen käyttämiin järjestelmiin. Tällöin ratkaisevaa on, että hyökkäys havaitaan nopeasti ja vahingot minimoidaan. Vahingot jäävät pieniksi, jos erilaisiin hyökkäyksiin ja niiden havaitsemiseen on varauduttu jo suunnitteluvaiheessa.

Toimintakin on suunniteltava

- Kun kriisi on päällä, ei ole aikaa aloittaa toiminnan suunnittelua. Poikkeustilanteita varten pitää miettiä valmiiksi, mitä tehdään erilaisissa häiriötilanteissa, miten vastuut jaetaan, minkälaista yhteistyötä tehdään muiden yritysten ja viranomaisten kanssa ja miten tilanteesta viestitään yleisölle, asiakkaille ja sidosryhmille.

Organisaation osaaminen ratkaisee

- Erilaiset ohjeet ja tarkistuslistat ovat yksi keino huolehtia siitä, että yrityksen kaikki työntekijät ovat tietoisia heille relevanteista kyberturvallisuutta parantavista toimenpiteistä.
- Organisaatiossa pitäisi olla riittävää teknistä syväosaamista, jotta löydetään luovia ratkaisuja ennakoimattomiin ongelmiin.

Osaaminen syvenee harjoituksissa

- Ohjeet ja suunnitelmat unohtuvat helposti. Uhkia tunnistavilla ja niitä ratkaisevilla harjoituksilla on suuri merkitys.
- Harjoituksissa riskit ja puutteet valmiudessa havaitaan konkreettisten tilanteiden kautta. Samalla harjoittelijoiden ymmärrys kasvaa. Harjoituksissa sovitut asiat jäävät mieleen ja opitun pohjalta ohjeita ja suunnitelmia voidaan parantaa.

Valmiina havaitsemaan ja viestimään

Viestinnällä öljyä tai hiekkaa organisaation rattaisiin

- Kun ongelmatilanteisiin liittyvä viestintä toteutetaan ennakkosuunnitelman mukaisesti, tilanne pystytään hoitamaan nopeasti ja kaikki tietävät, missä mennään ja mitä seuraavaksi on tehtävä.
- Jos viestintä ei toimi, tekeminen hidastuu ja sirpaloituu.
- Ongelman nopean ratkaisun lisäksi viestinnän avulla voidaan merkittävästi pienentää tilanteesta syntyviä vahinkoja.
- Kriisitilanteiden jälkeen on tärkeä arvioida viestinnän onnistumista ja päivittää suunnitelmaa havaittujen puutteiden osalta.

Valpasta ei yllätetä

- Kun yritys kerää tilannekuvaa sekä omista järjestelmistä että ulkoisista lähteistä, yllätetyksi tulemisen mahdollisuus pienenee.
- Pieni ennaltaehkäisevä korjausliike voi säästää suurelta ongelmalta.

Osa 2

Suosituksia mediayrityksille

Ole huolellinen perusasioissa

Anna käyttöoikeuksia vain niitä tarvitseville

- Mitä laajempi joukko voi käyttää tiettyä järjestelmää, sitä suurempi on riski väärinkäytöksille. Käyttäjäoikeuksien hallinta kannattaa suunnitella huolellisesti. Näin minimoidaan sekä oikeutetun käyttäjän että käyttäjätunnukset anastaneen hyökkääjän mahdollisuudet aiheuttaa vahinkoja.

Käytä monivaiheista tunnistusta laajasti

- Monivaiheiseen tunnistamiseen on tarjolla useita erilaisia menetelmiä. Näitä kannattaa käyttää kaikissa tärkeissä järjestelmissä. Jos käyttäjällä on esimerkiksi oikeus julkaista sisältöä mediatalon nimissä, on riittävän vahva tunnistaminen paikallaan. Myös pääsy mediatalon käyttämiin lähdekoodiarkistoihin kannattaa varmistaa monivaiheisen tunnistuksen avulla.

Tarkista kriittisiä järjestelmiä käyttävien taustat

- Suojelupoliisi tekee turvallisuusselvityksiä sekä valtion viranomaisille että yksityisille yrityksille. Selvitys on paikallaan, kun henkilöllä on työnsä puolesta laajat mahdollisuudet nähdä luottamuksellista tietoa tai halutessaan vahingoittaa tai manipuloida julkaisutoiminnan kannalta keskeistä teknistä järjestelmää tai julkaistavia sisältöjä.

Turvaa varmuuskopiot

- Kannattaa varmistaa, että kenelläkään ei ole mahdollisuutta tuhota kriittisten järjestelmien varmuuskopioita.

Pidä koodi ja pilvialustat hallinnassa

Koodausmaailma elää jatkuvassa muutoksessa

- Mediayrityksissä tehdään ja teetetään paljon koodia. Palveluita muutetaan ja kehitetään jatkuvasti. Toteutuksissa käytettävät ulkoiset koodikirjastot päivittyvät usein. Koodia muutetaan usein myös siksi, että löydetään tietoturvaa uhkaava haavoittuvuus.
- Ulkoisten koodikirjastojen haavoittuvuuksia kannattaa seurata automaattisten työkalujen avulla (esim. npm, OWASP) ja erilaisia kehitystyökaluja kannattaa muutenkin hyödyntää laajasti.
- Kun riski havaitaan, korjaukset on syytä tehdä viipymättä.

Kun asetukset ovat kohdallaan, pilvipalvelut ovat turvallisia

- Pilvipalveluita käytettäessä on tärkeä huolehtia kaikkien palvelun osien tietoturva-asetuksista. Monimutkaiseen eri palvelukomponenteista muodostuvaan kokonaisuuteen jää helposti aukkoja, joita hyökkääjä voi hyödyntää.

Huolehdi tietoliikenneyhteyksien laadusta

Media-ala ei toimi ilman yhteyksiä

- Jos yhteydet eivät toimi, mediasisältöjen tuottaminen ja julkaiseminen on käytännössä mahdotonta. Tietoliikennekatkos näkyy välittömästi asiakkaille ja tuo yritykselle yleensä taloudellisia menetyksiä ja negatiivista julkisuutta.

Varmennettu yhteys ja riittävä SLA

- Mediayhtiön keskeisen toimipisteen tietoliikenneyhteys kannattaa hankkia varmennettuna. Yhteyden SLA:n (Service Level Agreement), joka määrittää mm. yhteydelle sallitun katkosajan ja korjausmenettelyt ongelmatilanteissa, tulee olla riittävän vaativa.
- Kiinteän yhteyden rinnalle kannattaa harkita toiselta operaattorilta hankittua 5G-yhteyttä ja varmistaa, että varmentava tukiasema ei hyödynnä samaa kiinteää tietoliikenneyhteyttä kuin kiinteä pääyhteys.

Pilviyhteyksiin riittävä nopeus ja redundanssi

- Pilvipalveluiden osalta kannattaa varmistaa, että yhteyden kaistanleveys on riittävä ja että redundanssista eli vaihtoehtoisista reiteistä on huolehdittu.
- Yhteys voidaan toteuttaa erillistä operaattorilta hankittua yhteyttä käyttäen tai hyödyntäen internetin sisäisiä välitysmekanismeja.

Laadukkaat kotitoimistoyhteydet

- Poikkeustilanteissa, kuten koronaepidemian aikana, toimitustyötä on pystyttävä tekemään kotoa käsin. Yrityksen kannattaa huolehtia siitä, että erityisesti AV-sisältöjä tekevillä työntekijöillä on käytössään laadukas laajakaista – mieluiten langallinen ja langaton.
- Ulkoantenni parantaa langattoman yhteyden laatua.

Varmista varajärjestelmillä

Tunnista järkevä varautumisen taso

- Täydellisen varajärjestelmän rakentaminen ei yleensä ole taloudellisesti järkevää. Varajärjestelmissä kannattaa keskittyä yrityksen ja yhteiskunnan kannalta kaikkein kriittisimpien toimintojen varmistamiseen.
- Varajärjestelmän ei välttämättä tarvitse olla käytettävissä välittömästi pääjärjestelmän vikaantumisen jälkeen. Eri palveluille voidaan hyväksyä eri mittaisia katkoksia. Näin varautumisen kustannuksia voidaan laskea

Minimoi riippuvuudet

- Varajärjestelmän tulee olla mahdollisimman riippumaton pääjärjestelmästä. Sen tulee olla toimintakykyinen, vaikka kansainväliset yhteydet olisivat poikki tai kansainväliset palvelut eivät olisi käytettävissä.

Paras ratkaisu voi löytyä yhteistyön kautta

- Jokainen yritys rakentaa omat tekniset pääjärjestelmänsä omista lähtökohdistaan.
- Varajärjestelmän kohdalla paras ratkaisu voi löytyä yhteistyön kautta. Kaikilla mediayhtiöillä on samankaltaiset tarpeet tavoittaa yleisönsä kaikissa tilanteissa.

Hyvä suunnitelma ratkaisee

- Varajärjestelmän rakentaminen ja ylläpitäminen on usein kallista. Varautumissuunnittelu sen sijaan on kohtuullisen edullista.
- Suunnittelemalla ja harjoittelemalla erilaisten ongelmatilanteiden ratkaisemista tunnistetaan, missä varajärjestelmiä oikeasti tarvitaan ja missä riittävät suunnittelu ja hyvä osaaminen.

Valvo eheyttä ja brändisi käyttöä

Uhat kasvavat tekniikan kehittyessä

- Kehittyvä mediatekniikka mahdollistaa yhä huomaamattomammat ja laadukkaammat väärennökset. Laadukkaasti tuotetun väärennöksen jakaminen mediatalon nimissä tai julkaistun sisällön hienovarainen muuntelu ovat riskejä, joihin kannattaa varautua.
- Valesivustojen toteuttaminen on jo nyt yleistä. Mediayhtiön sivustolta näyttävälle sivulle voidaan ohjata käyttäjiä esimerkiksi sosiaalisen median kautta. Myös mediatalon omiin julkaisukanaviin saattaa päätyä ei-toivottua sisältöä.
- Verkkosivustojen mainonta on usein kolmansien osapuolten toimittamaa. Näiden toimijoiden luotettavuutta ja tietoturvaa on syytä seurata.

Väärinkäytökset tulisi havaita nopeasti

- Epäilyttävistä sisällöistä saadaan yleensä tieto yleisöpalautteen kautta. Tämä on kuitenkin varsin hidas ja epävarma tapa havaita väärinkäytöksiä.
- Julkaisukanavien eheyttä voi edistää käyttämällä tietorakenteita, jotka estävät kontrolloimattomien muutosten tekemisen. Tässä voidaan hyödyntää Ledger-tietokantoja, sähköisiä allekirjoituksia ja muita vastaavia teknologioita.
- Kannattaa myös harkita yhteistyötä alan yritysten kesken. Valesivustojen etsintää ja mediasisältöjen käytön seurantaa laajemminkin voi olla järkevä tehdä yhteisen teknisen ratkaisun kautta.

Suunnittele ja harjoittele

Varautumissuunnittelu kasvattaa organisaation osaamista

- Hyvän suunnitelman avulla palautuminen ongelmasta tapahtuu nopeasti.
- Todellinen ongelmatilanne harvoin toteutuu juuri suunnitellulla tavalla, mutta suunnitelmassa on todennäköisesti ainakin osaratkaisuja, joita voidaan hyödyntää.
- Teknisen varautumisen lisäksi organisaation sisäistä ja organisaatioiden välistä toimintaa ohjaavat suunnitelmat varmistavat, että ongelmaan reagoidaan nopeasti ja hallitusti.
- Varautumissuunnittelu nostaa organisaation osaamista ja tietoisuutta erilaisista riskeistä ja auttaa minkä tahansa ongelman ratkaisemista.
- Liian laajoja suunnitelmia ei kannata tehdä. On parempi luoda yksinkertaisia suunnitelmia ja panostaa säännölliseen harjoitteluun organisaation osaamistason nostamiseksi.

Harjoittelu testaa valmiutta ja tuottaa uusia ratkaisumalleja

- Harjoittelun avulla voidaan testata organisaation valmiutta reagoida erilaisiin ennalta odotettuihin tai odottamattomiin tilanteisiin.
- Harjoitus nostaa esiin myös uusia ratkaisumalleja, joiden avulla ongelmatilanne voidaan ehkä ratkaista aikaisempaa helpommin, nopeammin tai edullisemmin.
- Harjoittelu on luonteva väline myös yritysten välisen yhteistyön kehittämiselle ja kaikille yhteisten haasteiden ratkaisemiselle.
- Kriisitilanteessa, jossa jonkin yrityksen kriittinen resurssi ei ole käytettävissä, voi apu löytyä toisesta yrityksestä.

Älä tee yksin

Vertaisyrityksillä on samoja haasteita

- Varautumiseen liittyvissä kysymyksissä kannattaa tehdä yhteistyötä myös kilpailijoiden kesken.
- Joitakin tilanteita varten kannattaa ehkä rakentaa yhteinen varautumisratkaisu tai yhteisiä komponentteja, joita jokainen hyödyntää omalla tavallaan. Jos yhden yrityksen tuotantoresurssi on kriisitilanteessa käyttökelvoton, toinen yritys voi ehkä tarjota väliaikaisesti omia välineitään.
- Yritysten asiantuntijoiden välinen keskustelu auttaa siirtämään tietoa hyvistä varautumismalleista yritysten välillä. Näin kaikkien yritysten järjestelmät voidaan turvata paremmin ja kustannustehokkaammin.

Varautumista tukevia organisaatioita

- Mediapoolista ja Digipoolista saat lisätietoja alan yritysten huoltovarmuuteen liittyvästä toiminnasta ja erilaisista harjoituksista, joita järjestetään yritysten ja viranomaisten kesken.
- Kyberturvallisuuskeskus pystyy auttamaan yrityksiä monin tavoin. Julkisten oppaiden lisäksi tarjolla on myös yrityskohtaista ohjausta ja neuvontaa. Kannattaa tutustua Kyberturvallisuuskeskuksen palveluihin heidän verkkosivustonsa kautta.
- Huoltovarmuuskeskus osallistuu huoltovarmuuskriittisten järjestelmien varmistuksista aiheutuviin kustannuksiin. Tuki harkitaan aina tapauskohtaisesti.

Osa 3

Kiteytyksiä ja muistilistoja eri työntekijäryhmille

Tässä osassa esitetyt tekstit on tarkoitettu pohjamateriaaliksi, jota yritykset voivat käyttää sellaisenaan tai työstää omiin prosesseihinsa sopiviksi.

Kaikki työntekijät

Vahva salasanakulttuuri on turvallisuuden perusta

- Käytä pitkiä salasanoja tai salalauseita ja kaksivaiheista tunnistusta - myös somessa
- Käytä eri palveluissa eri salasanoja
- Aseta myös kotireitittimeen turvallinen salasana
- Varmista, että kukaan ei saa salasanojasi haltuunsa

Ole huolellinen laitteiden käytössä

- Pidä laitteesi ja sovelluksesi päivitettyinä
- Käytä vain yrityksesi hyväksymiä sovelluksia
- Anna puhelinsovelluksille vain välttämättömät oikeudet (kamera, mikrofoni, sijainti,…)
- Suojaa tärkeät puhelinsovellukset pin-koodilla
- Vain työasioita työkoneella - kotiasiat kotikoneella
- Älä kytke tietokoneesi usb-porttiin mitään varmistamatonta muistia tai laitetta
- Vältä julkisia langattomia verkkoja, muista VPN

Ole terveen epäluuloinen

- Lähetä luottamuksellinen tieto salattuna
- Mieti, mitä jaat ja kenelle
- Älä klikkaa mitään epäilyttävää
- Sähköposti tai viesti tutulta voi olla huijarin lähettämä
- Oikealta näyttävä sivusto voi olla valesivusto. Tarkista verkkosivun osoite.
- IT-tuki ei kysy salasanoja tai pankkitunnuksia
- Kiitos, kun ilmoitat epäilyttävät havaintosi [yhteystieto]

Osallistu yrityksesi turvallisuuskoulutukseen

Lue lisää

- Kyberturvallisuuskeskuksen oppaita yksityishenkilöille
- Digiturvallinen elämä(DVV)
- Ohjeita turvalliseen etätyöhön

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI

Hallitus ja johto (1/2)

Varmista, että kyberriskien hallinta on organisoitu ja resursoitu

- Kyberturvallisuus on vahvasti mukana riskienhallinnassa, strategisissa tavoitteissa ja budjetissa
- Sovittuja kyberturvallisuusperiaatteita noudatetaan kaikkien teknisten järjestelmien suunnittelussa, hankinnassa ja käytössä
- Reaaliaikaista tilannekuvaa kyberuhkista ja hyökkäyksistä ylläpidetään ja siitä viestitään suunnitellusti
- Yritysjohto osallistuu kyberriskien ja kriittisten järjestelmien tunnistamiseen ja priorisoimiseen
- Yritysjohto osallistuu varatekniikan ja palvelutasojen priorisointiin ja kustannusoptimointiin
- Yrityksen kyberturvallisuutta koordinoi nimetty henkilö

Varmista, että vakaviin ongelmatilanteisiin on varauduttu

- Yrityksellä on toiminta- ja johtamismalli kriisi- ja häiriötilanteita varten
- Kyberhäiriöiden käsittelyyn osallistuvat henkilöt on nimetty
- Sisältöjen tuotanto ja jakelu pystytään turvaamaan riittävällä tasolla kaikissa kanavissa ja kaikissa tilanteissa
- Yrityksen brändin ja sisältöjen väärinkäytön varalle on valvontamekanismit ja toimenpidesuunnitelmat
- Nopeaan sisäiseen ja ulkoiseen viestintään eri tilanteissa on varauduttu

Hallitus ja johto (2/2)

Varmista, että kaikkien työntekijöiden työroolia vastaavasta osaamisesta huolehditaan

- Eri työroolien vaatima kyberturvallisuusosaaminen on tunnistettu ja dokumentoitu
- Tarvittavasta koulutuksesta on huolehdittu
- Organisaation osaamista ja valmiutta kehitetään säännöllisten harjoitusten avulla
- Yrityksessä on riittävästi syvää teknistä osaamista, jotta löydetään ratkaisuja myös odottamattomissa tilanteissa

Varmista riittävä yhteistyö vertaisyritysten ja huoltovarmuusorganisaation kanssa

- Yhteistyöstä sekä normaalioloissa että poikkeustilanteissa on sovittu
- Normaalin kaupallisen toiminnan ylittävistä vastuista ja kustannuksista on sovittu sopimuksin
- Yritys osallistuu alan yhteisiin harjoituksiin

Varaudu siihen, että kyberhäiriöiden määrä kasvaa

Lue lisää

- Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa (KTK)
- Kyberturvallisuus ja yrityksen hallituksen vastuu (KTK)
- Ohjeet eri työntekijäryhmille

Kyberturvallisuusvastaava (1/2)

Varmista tekniset perusvaatimukset ja käytännöt

- Kyberarkkitehtuuri on määritelty, sitä ylläpidetään ja siinä on huomioitu verkkojen segmentointi, sovellusturvallisuus ja tietojensuojelu
- Kriittisimmät järjestelmät on tunnistettu ja suojattu
- Suojattava tieto on tunnistettu ja salattu
- Riskejä ja niihin liittyviä toimenpiteitä kuvaavaa dokumentaatiota päivitetään säännöllisesti
- Organisaatiolla on ohjeet, millä tavalla laitteiden, palveluiden ja järjestelmien tiedot ja riippuvuudet kuvataan ja miten niitä ylläpidetään.
- Yritykselle relevantit riskienhallintakriteerit on määritelty

Varmista, että vakaviin ongelmatilanteisiin ja on varauduttu

- Ks. eri työntekijäryhmien ohjeet tähän liittyen
- Tunnistettuja häiriötilanteita varten on olemassa toimenpide- ja viestintäsuunnitelmat
- Yrityksellä on kriteerit, joiden ylitys laukaisee toimenpiteet kyberhäiriöön reagoimiseksi
- Häiriötilanteissa tarvittavat yhteystiedot ja ohjeet löytyvät useasta eri paikasta/järjestelmästä
- Puhelimessasi on kaikkien häiriötilanteissa relevanttien henkilöiden yhteystiedot

Kyberturvallisuusvastaava (2/2)

Varmista tilannekuva, testaa ja arvioi

- Huolehdi siitä, että tilannekuvaa kerätään eri lähteistä ja että siitä viestitään hallitusti
- Hyödynnä ulkopuolisia asiantuntijoita riskien arvioinnissa ja valmiustason testaamisessa
- Testaa yrityksen kybervalmiutta aika-ajoin esimerkiksi Kybermittarilla

Varmista suunnittelemalla ja tekemällä yhdessä eri työntekijäryhmien kanssa, että heille sovittuja kyberturvallisuustoimenpiteitä toteutetaan

Lue lisää

- Ohjeet eri työntekijäryhmille
- Kaikki listatut lähteet ovat relevantteja

Toimittaja

Ota perustaidot haltuun

- Noudata kybersuosituksia erityisen huolellisesti
- Opiskele/kertaa toimittajan digiturvakurssi
- Paneudu lain tietosuojavaatimuksiin

Suojaa itsesi ja lähteesi

- Käytä tiedon salausta laajasti, jotta erityistä suojaa vaativa tieto ei erotu joukosta
- Minimoi mahdollisuudet tiedonhankintasi seuraamiseen/jäljittämiseen
- Hyödynnä Signal-sovellusta ja salattua sähköpostia
- Jos matkustat riskimaihin, kertaa erityisohjeet

Varaudu vaikuttamisyrityksiin

- Verkossa näkemääsi saatetaan manipuloida
- Suunnitelmallisen disinformaation määrä kasvaa – muista lähdekritiikki
- Salaa, jos mahdollista, henkilötietosi (osoite, …)
- Jos sinua uhkaillaan, kiristetään, maalitetaan tai lahjotaan, ilmoita työnantajallesi ja poliisille

Varaudu identiteettivarkauteen

- Seuraa nimesi käyttöä verkossa
- Toimi heti, jos havaitset identiteettivarkauden

Varmista kodin tietoliikenneyhteydet

- Toimitustyön on jatkuttava myös poikkeusoloissa
- Live-tuotantoja varten tarvitset nopean kiinteän laajakaistan ja varmistavan mobiiliyhteyden

Lue lisää

- Mediapoolin julkaisut
- Poliisi: Rikosilmoitus

Päätoimittaja

Varmista perusasioiden noudattaminen

- Kaikki työntekijät noudattavat yleisiä kyberturvallisuusohjeita
- Toimittajat noudattavat toimittajien suosituksia ja suorittavat toimittajan digiturvakurssin
- Monivaiheista tunnistamista käytetään kaikilla julkaisualustoilla, sometileillä ja myös Microsoftin palveluissa

Jos median käyttämästä tekniikasta vastaa emoyhtiö/konserni/ulkoinen tuottaja

- Varmista, että kyseinen palveluntuottaja huolehtii kyberturvallisuudesta. Voit käydä läpi esimerkiksi tässä ohjeistuksessa esitettyjä listoja.
- Varmista, että ongelmatilanteiden käytännöistä yrityksesi ja palveluntuottajan välillä on sovittu

Jos media hankkii itse tekniikkansa:

- Nimeä työntekijä, joka hankkii kohtuullisen kyberturvallisuusosaamisen ja hyödyntää työssään esim. tämän ohjeistuksen materiaalia
- Hanki yrityksen tueksi ulkoinen tietoturva-asiantuntija/yritys

Varaudu poikkeustilanteisiin

- Hyödynnä soveltuvin osin hallitukselle ja johdolle annettuja erityisohjeita
- Varmista, että puhelimessasi on kaikkien häiriötilanteissa relevanttien henkilöiden yhteystiedot
- Varmista, että ainakin Osan 4 kuvaamiin tilanteisiin on varauduttu

HR-vastaava

Huolehdi yhdessä johdon ja kyberturvasta vastaavien kanssa riittävästä osaamisesta

- Eri työroolien vaatima kyberturvallisuus-osaaminen on tunnistettu ja dokumentoitu
- Tarvittavasta koulutuksesta on huolehdittu
- Kybersuositukset ovat esillä/helposti saatavilla ja lisätietoa on helppo löytää
- Yrityksessä on riittävästi syvää teknistä osaamista myös odottamattomien ongelmien ratkaisuun

Hallitse henkilö- ja henkilötietoriskejä

- Kriittisimpiä järjestelmiä operoivien henkilöiden taustat tarkistetaan
- Henkilötietojen tallennus ja käsittely omissa ja/tai palveluntarjoajan järjestelmissä täyttää ainakin lainsäädännön minimivaatimukset (GDPR)

Varmista aktiivinen harjoitustoiminta

- Häiriötilanteissa toimimista harjoitellaan systemaattisesti
- Harjoitustarpeet on tunnistettu ja niiden toteuttamiseen on harjoitussuunnitelma
- Harjoitustoimintaa kehitetään

Lue lisää

- Tämän suosituksen muut ohjeet
- KTK:n opasmateriaalia
- Kyberharjoitusohje
- Digiturvallinen elämä (DVV)
- Mediapoolin julkaisut

Taloudesta vastaava

Taloustiedot kiinnostavat rikollisia ja vakoilijoita

- Noudata turvaohjeita erityisen huolellisesti
- Huolehdi siitä, että taloustietojen käsittelyä varten on turvalliset käytännöt (käyttöoikeudet, hyväksymiskäytännöt, tietojen lähettäminen/siirto, varmuuskopiot,…) ja niitä noudatetaan
- Varmista, että kaikki taloushallintoa tukevat palveluntarjoajat huolehtivat kyberturvallisuudesta kaikessa toiminnassaan (systemaattiset käytännöt, sertifikaatit, …)
- Jos hankit taloushallinnon palveluita, huomioi palveluiden hankkijoille ja juristeille listatut suositukset

Varmista käsittelemiesi tietojen oikeellisuus

- Varo rikollisten lähettämiä valelaskuja tai maksumääräyksiä. Sähköposti, joka näyttää tulevan toimitusjohtajalta, voi olla rikollisen lähettämä.
- Varmista datan/tekniikan/palvelun toimittajan kanssa, että analytiikkadata on aitoa ja manipuloinnilta suojattua

Juristi

Varmista, että kyberturvallisuus huomioidaan kaikissa palvelusopimuksissa

- Toimittajat täyttävät palvelun kriittisyyttä vastaavat kyberturvallisuusvaatimukset, ml. GDPR
- Ohjelmistojen toimittajilta edellytetään turvallisten ohjelmistonkehitysmenetelmien käyttöä
- Palvelutoimittajia koskeviin kybertuvallisuusvaatimuksiin on vakioidut sopimuspohjat
- Toimittajasopimuksissa sovitaan kyberuhka- ja häiriötietojen jakamisesta

Huolehdi poikkeustilanteisiin liittyvistä sopimuksista

- Normaaliajan toiminnan ylittävistä velvoitteista on sovittu mediayhtiöiden, operaattoreiden, palvelutoimittajien ja yhteiskunnan välisin sopimuksin
- Kilpailuoikeudelliset seikat huomioidaan silloin, kun varautumiseen liittyy yhteiskunnan tukea

Lue lisää

- Kyberturva ICT-sopimuksissa (HVK)
- Johdon ja hankinnan ohjeet

Viestinnästä vastaava

Varaudu poikkeustilanteisiin

- Osallistu harjoituksiin
- Tee tunnistettuihin häiriötilanteisiin sopivia viestipohjia
- Kirjaa eri häiriötilanteita varten sekä sisäisen että ulkoisen viestinnän kohderyhmät ja viestintäkanavat
- Säilytä kriisiviestinnässä tarvittavia tietoja eri formaateissa, jotta ne löytyvät myös esimerkiksi tietojärjestelmän kaaduttua

Ylläpidä kyberteemoihin liittyvää sisäistä viestintää

- Yrityksen kyberohjeiden toistuva viestintä
- Tilannekuva ja ajankohtaiset riskit
- Harjoitukset ja muut sisäiset kyberaktiviteetit

Lue lisää

- Kriisiviestintä kyberkriisissä
- Kybersää
- Kyberharjoitusohje

Palveluiden hankkija

Huomioi kyberturvallisuus sopimuksissa

- Käytä yrityksen vakioituja sopimuspohjia
- Edellytä turvallisten ohjelmistonkehitysmenetelmien käyttöä
- Sovi kyberuhka- ja häiriötietojen jakamisesta
- Sitouta toimittaja oman palvelunsa jatkuvaan monitorointiin ja kyberturvan kehittämiseen
- Huomioi mahdolliset B2B-asiakkaiden asettamat kyberturvallisuusvaatimukset

Ole tarkkana hankintaprosessin aikana

- Varmista, että palvelun toimittaja täyttää palvelun kriittisyyttä vastaavat vaatimukset
- Arvioi toimittajia sovittuja riskien arviointikriteereitä käyttäen
- Varmista ennen hyväksymistä, että palvelun toimittajan todelliset prosessit vastaavat luvattua
- Varmista, että palvelun toimittaja noudattaa GDPR:n vaatimuksia ja mm. tuhoaa tarpeettomat tiedot

Huolehdi mainosten turvallisuudesta

- Varmista, että mainosten/mainosalustan toimittaja valvoo aktiivisesti sisältöjensä ja järjestelmiensä turvallisuutta, aitoutta ja eheyttä

Lue lisää

- Kyberturva ICT-sopimuksissa (HVK)
- Turvallinen tuotekehitys (KTK)
- Ohjeita pilvipalvelujen turvallisuudesta (KTK)
- Muiden työroolien erityisohjeet

Tekniikan kehittäjä ja ylläpitäjä (1/3)

Varmista tärkeät järjestelmät

- Varmista kriittisimmät järjestelmät varajärjestelyin
- Suunnittele, miten teknisiä pää- tai varajärjestelmiä käynnistetään/palautetaan käyttöön
- Muista varaosat, varalaitteet, elinkaaren ja tuen kesto sekä mahdolliset kielletyt maat
- Pilvipalvelussa varmista, että kaikki palvelun osat toteutetaan ja konfiguroidaan tietoturvallisesti
- Tee soveltuvin osin yhteistyötä vertaisyritysten ja huoltovarmuusorganisaation kanssa
- Hyödynnä operaattorien osaamista ja tekniikkaa

Kehitä turvallisesti

- Ota haltuun turvallisen kehityksen menetelmät
- Hyödynnä ohjelmistojen kehitystä tukevaa automatiikkaa

Varmista tietoliikenne

- Toimitilan tietoliikenne: korkean SLA:n varmennettu yhteys, varalla eri operaattorin 5G
- Pilvipalveluiden yhteyksiin riittävästi redundanssia
- Laadukkaat etätyöyhteydet (erit. live-tuotanto)

Huolehdi media-alan erityiskohteista

- Media-arkistojen manipulointi estetään/havaitaan
- Suorien tv- ja radiosisältöjen tuotanto ja jakelujärjestelmät pystytään palauttamaan tai korvaamaan nopeasti kaikissa tilanteissa
- Yksinkertainen verkkojulkaisu ja tarvittava reititys toimivat jopa ilman kansainvälisiä yhteyksiä
- Mediasisällöille on kaikissa tilanteissa (myös ilman kansainvälisiä palveluita) riittävästi CDN-kapasiteettia

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI

Tekniikan kehittäjä ja ylläpitäjä (2/3)

Pidä järjestelmät ja ohjelmistot ajan tasalla

- Tarkasta säännöllisesti, että ohjelmistot, laitteet ja palvelut ovat ajantasaisia ja päivitykset on tehty
- Tarkista säännöllisesti, että pääsyvaltuutukset (erityisesti suojattavat kohteet) ovat ajan tasalla
- Tee muutoksia suojattaviin kohteisiin sovittujen käytäntöjen mukaisesti, huolellisesti ja testaten
- Seuraa automatiikkaa hyödyntäen (esim. npm, OWASP) koodisi ulkoisiin riippuvuuksiin liittyviä haavoittuvuuksia. Päivitä nopeasti.

Huolehdi tilannekuvan rakentamisesta

- Kerää lokeja kaikista tärkeistä kohteista
- Seuraa ulkopuolisia tietolähteitä ja kerää tietoa järjestelmistäsi tunnistaaksesi haavoittuvuudet
- Hyödynnä automatiikkaa lokien ja muiden tietolähteiden monitoroinnissa
- Raportoi poikkeavista kirjautumisyrityksistä ja muista poikkeamista sovitun käytännön mukaisesti
- Toteuta ja ylläpidä järjestelmää, joka monitoroi yrityksen brändin ja sisältöjen (väärin)käyttöä

Huolehdi kyberturvan perusrakenteista

- Ylläpidä kyberarkkitehtuuria
- Tunnista ja kirjaa sovitulla tavalla kunkin osajärjestelmän tiedot, riippuvuudet ja vaikutukset, ja ylläpidä tietoja
- Ylläpidä uhkaprofiilia ja päivitä sitä säännöllisesti
- Varmista, että tärkeät tietovarannot on tunnistettu ja salattu
- Säädä tunnistamisen vahvuus kohteen riskin mukaan
- Varmista, että kaksi-/monivaiheista tunnistamista käytetään kaikilla alustoilla

Tekniikan kehittäjä ja ylläpitäjä (3/3)

Hallitse toimittajayhteistyötä

- Varmista, että palvelun toimittaja täyttää palvelun kriittisyyttä vastaavat vaatimukset
- Edellytä turvallisten ohjelmistonkehitysmenetelmien käyttöä
- Arvioi palveluiden toimittajia sovittuja riskien arviointikriteereitä käyttäen
- Varmista ennen hyväksymistä, että palvelun toimittajan todelliset prosessit vastaavat luvattua

Harjoittele

- Osallistu harjoituksiin ja niiden organisoimiseen
- Harjoittelua/testausta pitää tehdä säännöllisesti, esimerkiksi vuosittain per kriittinen järjestelmä
- Ota tekniikan toimittajat mukaan harjoitteluun

Lue lisää

- KTK:n opasmateriaalia
- Turvallinen tuotekehitys (KTK)
- Ohjeita pilvipalvelujen turvallisuudesta (KTK)
- Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa (KTK)
- Näin keräät ja käytät lokitietoja (KTK)
- Opas tietomurtojen havaitsemiseen (KTK)
- Tilannekuva ja verkostot (KTK)
- EBU:n kyberohjeistuksia
- OWASP Dependency-Check
- Muiden työroolien erityisohjeet

Osa 4

Toimintaohjeita, kun riski on toteutunut

Tässä osassa esitetyt kuvaukset eivät ole valmiita ja kaiken kattavia suunnitelmia eri tilanteisiin. Ne on tarkoitettu pohjamateriaaliksi, jota yritykset voivat hyödyntää omassa varautumissuunnittelussaan ja varautumisharjoituksissaan.

Median sometili on kaapattu

Hahmota tilanteen vakavuus

- Harmiton teinipila vai vakava median uskottavuutta murentava ja/tai sen brändiä hyödyntävä rikos?

Toimenpiteet

- Jos käytössä on rinnakkainen tili pääkäyttäjän oikeuksin, poista kaapatun tilin oikeudet
- Varoita käyttäjiä (ks. Viestipohjat)
- Ilmoita väärinkäytöksestä Kyberturvallisuuskeskukselle ja poliisille
- Palauta tilin hallinta (Meta, Twitter)
- Jos et pysty palauttamaan tilin hallintaa itse tai oman organisaatiosi kautta, ota yhteyttä Kyberturvallisuuskeskukseen

Viestipohjia

- Esimerkkipohja: ”[median] [somealusta] –tili on kaapattu. Kanavassa jaetut viestit voivat olla valheellisia tai sisältää haitallisia linkkejä. Lisätietoa verkkosivulla [media.fi] (huom. ei hyperlinkkiä tähän, koska se on riski).”

Varautuminen

- Noudata kaikille yhteisissä suosituksissa listattuja keinoja, kuten pitkät salasanat, kaksivaiheinen tunnistaminen ja mobiililaitteiden pin-suojaus
- Vaihda salasanoja säännöllisesti varsinkin, jos tilillä on useita käyttäjiä
- Luo varatili, jolla on pääkäyttäjän oikeudet
- Luo tavallisen käyttäjän varatili
- Tarkista säännöllisesti tilin asetukset ja oikeudet

Median tai toimittajan somekanava täyttyy asiattomista viesteistä

Esimerkkejä

- Aktivistiryhmä on ottanut median kohteekseen
- Automatisoidut botit generoivat kanavaan viestejä

Toimenpiteet

- Sulje somekanavasta ne osat, joita pitkin viestit tulevat (kommentointi, chat, …)
- Poista asiattomia viestejä lähettävä tili tai estä sen viestit
- Tiedota tilanteesta muita viestintäkanavia käyttäen
- Ilmoita väärinkäytöksestä Kyberturvallisuuskeskukselle ja poliisille

Viestipohjia

- Esimerkkipohja: ”[median] [somealusta] on asiattoman viestikampanjan kohteena. Lisätietoa verkkosivulla [media.fi] (huom. ei hyperlinkkiä tähän, koska se on riski).”

Varautuminen

- Perehdy eri somekanavien rajausominaisuuksiin ja harkitse niiden käyttöä jo ennakoivasti

Median tai toimittajan identiteetti on varastettu

Esimerkkejä

- Käyttäjiä ohjataan valesivustolle
- Median tai toimittajan nimissä esitetään valeuutisia tai muokattuja sisältöjä
- Median uutisesta jaetaan muokattua versiota
- Yrityksen työntekijän nimissä lähetetään sähköpostia tai muita viestejä

Toimenpiteet

- Ilmoita väärinkäytöksestä Kyberturvallisuuskeskukselle ja poliisille
- Varoita käyttäjiä (viestipohjat)
- Hyödynnä tarvittaessa Take down –palveluita
- Jos on tapahtunut tekijänoikeusrikkomus, ole yhteydessä tekijänoikeusjärjestöihin

Viestipohjia

- Esim.:”[median] nimissä on julkaistu valesivusto verkko-osoitteessa www… (älä aktivoi linkkiä). Älä missään tapauksessa klikkaa sivustolle johtavaa linkkiä somessa tai missään internetissä. Turvallisimmin käytät palveluamme, kun avaat verkkoselaimen ja kirjoitat mediamme verkko-osoitteen osoite-kenttään.”

Varautuminen

- Skannaa säännöllisesti (automaattisesti) yritykseen ja toimittajiin liittyviä verkkosisältöjä ja tunnista mahdolliset väärinkäytökset
- Mieti valmiiksi, miten ja missä kanavissa eri tilanteissa viestitään. Luo useita viestipohjia.

On tapahtunut tietomurto tai tietovuoto

Esimerkkejä

- Yrityksen julkaisukanavassa esitetään murtautujan sisältöä
- Yrityksen julkaisukanavan sisältöä muokataan huomaamattomasti
- Murtautuja saa haltuunsa työntekijöiden töissä käyttämiä tilejä
- Murtautuja saa haltuunsa yrityksen tai työntekijöiden suojattavia tietoja

Toimenpiteet

- Poista virheellinen sisältö
- Palauta kaapatut tilit
- Ilmoita väärinkäytöksestä Kyberturvallisuuskeskukselle , tietosuoja-valtuutetulle ja tarvittaessa poliisille
- Varoita tarvittaessa käyttäjiä
- Toteuta muut suunnitellut toimenpiteet

Viestintä

- Viesti asiasta yrityksen viestintäohjeiden ja mahdollisten valmiiden pohjien mukaisesti

Varautuminen

- Järjestetään harjoitus/harjoituksia, joissa käydään läpi mahdollisia tilanteita ja suunnitellaan niihin liittyviä toimenpiteitä ja viestintää sekä ennaltaehkäisevää varautumista
- Kirjataan harjoituksen tulokset ja muutetaan tulosten pohjalta yrityksen toimintaa ja ohjeistusta

Lue lisää

- https://www.suomi.fi/oppaat/tietovuoto
- https://www.suomi.fi/oppaat/tietomurto

Mediaan kohdistuu palvelunestohyökkäys

Esimerkkejä

- Median verkkosivut toimivat hitaasti. Erityisesti kuvat ja videot eivät lataudu normaalisti.
- Verkkosivuston jotkin osat eivät toimi

Toimenpiteet

- Selvitä onko kyseessä palvelunestohyökkäys vai tekninen vika
- Selvitä hyökkäyksen tekotapa ja käynnistä sellaiset ennalta suunnitellut toimenpiteet, jotka parhaiten hillitsevät juuri kyseisen hyökkäyksen vaikutuksia
- Tee yhteistyötä operaattorin kanssa ennalta sovittujen mallien pohjalta
- Ilmoita väärinkäytöksestä Kyberturvallisuuskeskukselle ja poliisille

Viestipohjia

- Esim. ”[Median] verkkosivuihin kohdistuu palvelunestohyökkäys. Sivusto toimii normaalia hitaammin. Käyttäjien tiedot eivät ole vaarassa.”

Varautuminen

- Varautuminen palvelunestohyökkäyksiin kannattaa suunnitella erityisammattilaisten kanssa osana muuta julkaisualustan suunnittelua.

Lue lisää

- KTK:n neuvoja
- EBU:n suosituksia

Osa 5

Muuta tukimateriaalia

Tästä osasta löytyy yleistä tukimateriaalia yritysten oman kehittämistyön tueksi sekä lisätietolinkkejä.

Esimerkki kehitystyön käynnistämisprojektista

1. Käynnistetään kyberturvallisuuden ”perushuolto”

- Yrityksen johto nimeää vastaavan koordinaattorin
- Koordinaattori kokoaa tuekseen sopivan tiimin
- Tiimi toteuttaa yhden tai useamman työpöytäharjoituksen. Näissä tunnistetaan riskejä ja mitataan valmiuden tasoa.
- Tiimi muokkaa tässä esitettyjä kybersuosituksia ja eri tilanteisiin liittyviä toimintaohjeita omalle yritykselle sopiviksi
- Tiimi tunnistaa mahdollisia syvempää kehittämistyötä vaativia teemoja ja ehdottaa toimenpiteitä näiden edistämiseksi
- Tiimin tukena on todennäköisesti järkevää käyttää ulkopuolisia asiantuntijoita
- Tiimi varmistaa yhdessä johdon kanssa, että sovitut toimenpiteet toteutetaan

2. Organisoidaan kohdassa 1 tunnistettujen puutteiden korjaaminen. Esimerkiksi:

- Parannetaan teknisten järjestelmien turvallisuutta
- Hankitaan lisää kyberturvallisuusosaamista
- Järjestellään yrityksen sisäisiä prosesseja ja vastuita uudelleen
- Lisätään yhteistyötä vertaisyritysten ja varautumisesta huolehtivien viranomaisten kanssa

3. Organisoidaan kyberturvallisuuden ylläpito ja kehittäminen jatkuvaksi prosessiksi

- Työtä on jatkettava pitkäjänteisesti

Lue lisää

- Kyberharjoitusohje
- Suositukset hallitukselle ja johdolle

Pienmedian kyberturvallisuuden vastuulista

Vastuu	OK?	Vastuuhenkilö/kontakti
Kyberturvallisuusasioiden koordinointi		
Teknisten järjestelmien suojaus		
Henkilöstön ohjeet ja koulutus		
Säännöllinen harjoittelu		
Viestintä ja viestipohjat		
Palvelutoimittajien kyberturvallisuus		
Yhteistyö operaattorin/operaattorien kanssa		
Yhteistyö viranomaisten ja vertaisyritysten kanssa		
Konsernin tai palvelutoimittajan tukiorganisaatio, joka auttaa varautumisessa ja häiriötilanteissa		

Harjoituksen toteutusesimerkki (1/3)

Harjoitus voi olla hyvin pieni (tunnistetaan pienellä joukolla kahvikupin ääressä riskejä) tai laaja yritystenvälinen harjoitus (esim. Tieto –harjoitukset). Tässä on kuvattu esimerkki keskisuuresta harjoituksesta, joka sopii yrityksen sisäiseen valmiuden kehittämiseen. Lue myös Kyberturvallisuuskeskuksen Kyberharjoitusohje.

Askel 1. Yrityksen johto nimeää projektiryhmän

- Onnistunut harjoitus edellyttää valmistelua, harjoituksen käytännön toteuttamista ja jälkikäteen tapahtuvaa tulosten arviointia. Näitä tehtäviä varten nimetään projektiryhmä, johon tarvitaan vähintään kaksi henkilöä: Harjoituksen johtaja ja asiantuntija. On suositeltavaa, että harjoituksen organisointiin osallistuu useampia henkilöitä.

Askel 2. Projektiryhmä määrittelee yhdessä johdon kanssa harjoituksen tavoitteen ja osallistuvat organisaation osat

- Projektiryhmä määrittää yhdessä yrityksen johdon kanssa harjoituksen tavoitteen ja ne organisaation osat, joista osallistujat tulevat. Tavoitteen tulee olla sellainen, että sen saavuttamisessa tarvitaan kaikkien harjoitukseen osallistuvien työrooleja. Tavoitteena voi olla esimerkiksi häiriöstä toipuminen. Tällöin jokainen harjoitukseen osallistuja tarkastelee mitä omassa työroolissa on tehtävä, jotta toipuminen olisi nopeaa ja häiriöstä aiheutuvat vahingot pieniä. Tavoitteena voi olla myös esimerkiksi yritysten välisen yhteistyön kehittäminen, teknisen järjestelmän testaaminen vikatilanteessa, kriisiviestinnän kehittäminen, jne.

Harjoituksen toteutusesimerkki (2/3)

Askel 3. Projektiryhmä valmistelee harjoituksen

- Valitaan skenaario, eli mitä on tapahtunut ja miten tilanne etenee.
- Nimetään osallistujat
- Määritellään harjoituksen ajankohta ja kesto
- Luodaan harjoituksessa tarvittava materiaali ja työvälineet
- Sovitaan selkeät roolit projektiryhmän jäsenten kesken (johtaminen, tulosten kirjaaminen)
- Tehdään osallistujille yksinkertaiset ohjeet, joissa kerrotaan perustiedot harjoituksesta ja annetaan valmistautumisohjeet
- Pyydetään tarvittaessa asiantuntija-apua sekä valmisteluun että toteutukseen (esimerkiksi tekninen harjoitus, jossa käytetään oikeita järjestelmiä)
- Esimerkkiskenaarioita:
  - Yrityksen jokin avainresurssi ei ole käytettävissä joko satunnaisen ongelman tai aktiivisen vahingonteon seurauksena (fyysinen tila, tietoliikenneyhteys, oma järjestelmä, kumppanin palvelu)
  - Joku ulkoinen taho esiintyy yrityksen nimissä tai jakaa muokattua mediasisältöä (valesivustot, muokattu media, jakelukanavan tai päätelaitteen haltuunotto)
  - Yrityksen vihamieliseksi muuttunut oma työntekijä pyrkii hyödyntämään oikeuksiaan ja aiheuttamaan vahinkoa
  - Sairaus tai muu tekijä estää suurta osaa työntekijöistä tekemästä työtään
  - Katso lisää Kyberharjoitusskenaariot 2021

Harjoituksen toteutusesimerkki (3/3)

Askel 4. Projektiryhmä toteuttaa harjoituksen

- Toteutus toteutetaan suunnitelman mukaisesti. Harjoituksen alussa kerrataan harjoituksen tavoite ja menettelytavat. Harjoituksen tapahtumat ja osallistujien kommentit kirjataan mahdollisimman tarkasti muistiin. Harjoituksen jälkeen osallistujilta kysytään palautetta harjoituksen toteutuksen onnistumisesta.
- Jos kyseessä on kokousmainen työpöytäharjoitus, puheenjohtaja keskusteluttaa sovitut teemat sovitussa aikataulussa antaen kaikille osallistujille mahdollisuuden kertoa näkemyksensä. Teknisessä harjoituksessa, jossa luodaan tekninen vikatilanne, asiantuntijat ratkovat ongelmaa todennäköisesti epämuodollisemmin.
- Yllätyksiin kannattaa varautua. Harjoittelijoiden näkemykset voivat ohjata ratkaisua ennalta odottamattomaan suuntaan. Tällaisissa tilanteissa joustavuus todennäköisesti maksimoi harjoituksesta saatavan hyödyn.
- Harjoitukseen osallistujilta kannattaa kerätä palautetta harjoituksen onnistumisesta sekä harjoituksen aikana että sen jälkeen. Palautteen avulla harjoitusosaaminen kehittyy ja osallistujien motivaatio kasvaa.

Askel 5. Projektiryhmä raportoi harjoituksen tulokset

- Miten harjoitus edisti asetettua tavoitetta? Kuinka hyvä organisaation valmius oli? Mitkä ovat harjoituksen perusteella tärkeimmät kehityskohteet? Miten valmiuden kehittämis- ja harjoitustoimintaa kannattaa jatkaa? Osallistujilta saatu palaute ja harjoituksen toteutustapojen jatkokehittäminen.

Yhteistyö operaattorin kanssa

- Sovi eri tietoliikenneyhteyksien laadusta ja SLA:sta (Service Level Agreement) huolellisesti kunkin yhteyden kriittisyys huomioiden
- Sovi häiriötilanteisiin liittyvistä toimenpiteistä (esimerkiksi palvelunestohyökkäys, reititys poikkeustilanteissa)
- Sovi tietoliikenteen monitorointiin ja poikkeamien havaitsemiseen liittyvistä toimenpiteistä
- Lisäksi operaattorit tarjoavat erilaisia turvallisuutta parantavia palveluita, joihin kannattaa tutustua osana kyberturvallisuuden kehittämistä

Ohjeita Signal-sovelluksen turvalliseen käyttöön

- Lataa sovellus virallisesta sovelluskaupasta
- Varmista, että Signalista on käytössä viimeisin versio
- Varmista, että Signal-tiliin ei ole linkitetty tuntemattomia laitteita (Settings -> Linked Devices)
- Signal-tiliä ei tule linkittää tietokonesovellukseen, eli sitä tulee käyttää vain täysin päivitetyllä laitteella
- Kytke Registration Lock -asetus päälle (Settings -> Account -> Registration Lock). Tämä asetus estää Signal-tilin siirtämisen toiselle SIM-kortille ilman Signalin PIN-koodin syöttämistä.
- Varmista, että Signal-viestit eivät näy puhelimen lukitusruudulla (Settings -> Notifications -> Notification Content -> None Name or Content TAI Name only)
- Ota käyttöön Disappearing Messages –toiminto, jos on pienintäkään vaaraa, että laite voisi päätyä vääriin käsiin: valitse keskustelun otsikko -> Disappearing Messages -> esimerkiksi 1 viikko tai 1 päivä, tilanteesta riippuen.

Signal

Kyberturvallisuuteen kannustavia lauseita

Kyberhuolellinen voi olla huoleton

Kyberviisaan eurotkin ovat turvassa

Vaarassa ovat toimittajan kone, mieli ja kieli

Harjoitus tuottaa kybermestareita

Huolellisuus palkitaan kriisin aikana

Vahinkoja ei voi estää, mutta haittoja voi

Usein kumppani päästää pahiksen sisään

Hyvä viestintä on kriisin paras lievittäjä

Jokainen kuitti voi auttaa hyökkääjää

Mistä ei ole sovittu, siitä lipsutaan

Sateeseen varaudutaan poutasäällä

Kyberturvallisuus on yhteistyötä

Lisätietoa

Kyberturvallisuuskeskus

- Linkkejä oppaisiin
- Kyberturvallisuuskeskuksen oppaita yksityishenkilöille
- Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa
- Kyberturvallisuus ja yrityksen hallituksen vastuu
- Kyberharjoitusohje
- Turvallinen tuotekehitys
- Ohjeita pilvipalvelujen turvallisuudesta
- Näin keräät ja käytät lokitietoja
- Opas tietomurtojen havaitsemiseen
- Tilannekuva ja verkostot
- Kybersää
- Palvelunestohyökkäys

Huoltovarmuuskeskus

- HVK:n julkaisut
- Ohjeita turvalliseen etätyöhön
- Kyberturva ICT-sopimuksissa
- Suosituksia kyberhäiriötilanteessa

Muut

- Mediapoolin julkaisut
- Digi-ja väestötietovirasto: Digiturvallinen elämä
- Poliisi: Rikosilmoitus
- EBU:n kyberohjeistuksia
- Sometilien palautus (Meta, Twitter)
- https://www.suomi.fi/oppaat/tietovuoto
- https://www.suomi.fi/oppaat/tietomurto
- Kriisiviestintä kyberkriisissä
- OWASP

HUOLTOVARMUUSORGANISAATIO
MEDIAPOOLI