TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

HUOLTOVARMUUSKESKUS

Kyberharjoitusohje

Käsikirja harjoituksen järjestäjälle

Traficomin julkaisuja
26/2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISSN 2669-8757
26/2019

1 Johdanto

Tämän harjoitusohjeen on laatinut Liikenne- ja Viestintäviraston Kyberturvallisuuskeskus yhteistyössä Huoltovarmuuskeskuksen kanssa. Ohjeen käyttö ei edellytä kokemusta kyberharjoittelusta. Se on suunnattu organisaatioiden tietoturvasta ja tietohallinnosta vastuussa oleville tahoille, joiden tehtäviin organisaation kyberturvallisuudesta huolehtiminen kuuluu.

Kotimaisen kyberharjoitusohjeen tarve havaittiin Huoltovarmuuskeskuksen KYBER-2020-ohjelman aikana. Tietoa erilaisista harjoitustavoista on verkossa runsaasti tarjolla. Halusimme kerätä harjoitusten järjestämiseen liittyvät opit yhteen käytännönläheisellä tavalla.

Tässä ohjeessa kerromme, mistä kyberharjoituksessa on kyse, miten sellainen järjestetään ja miten säännöllisestä harjoittelusta saadaan kerättyä parhaat mahdolliset hyödyt organisaation oman varautumistyön tueksi.

Ohjeemme sisältää taustatietoja harjoittelun merkityksestä, käytännön neuvoja harjoituksen järjestämiseen ja kyberharjoitteluun liittyvän lyhyen sanaston. Lisäksi ohjeistamme, miten harjoittelutoimintaa voidaan tuoda osaksi organisaation vuosisuunnittelua.

Toivomme, että ohjeemme luomat raamit eivät rajoita vaan toimivat kyberharjoittelunne tukena ja moottorina, kun on aika viedä harjoitustoiminta keskusteluista käytäntöön.

Huoltovarmuuskriittisten organisaatioiden on mahdollista saada kyberharjoitustoimintaan yksilöllistä tukea ja apua Kyberturvallisuuskeskuksen harjoitustoiminnan tukipalvelulta. Yhteystiedot harjoitustoiminnan tukipalveluille löydät tämän ohjeen lopusta.

Kyberharjoitusohjeen avulla organisaatio voi

1. saada ohjeita ja neuvoja harjoitteluun liittyen
2. käynnistää oman kyberharjoitustoimintansa
3. suunnitella ensimmäisen oman harjoituksensa
4. parantaa jo olemassa olevaa harjoitusohjelmaansa
5. parantaa kykyään varautua tietoturvapoikkeamiin sekä -häiriöihin ja niistä toipumiseen.

2 Mikä on kyberharjoitus?

Kyberharjoitus on harjoitustapahtuma, jossa organisaatio mallintaa ja testaa varautumistaan erilaisiin kyberhäiriöihin. Harjoituksella tarkoitetaan organisaatiota kohtaavan tilanteen fiktiivistä mallintamista tarkoitukseen parhaiten soveltuvalla tavalla.

Kyberhäiriöt ovat organisaation tietoteknisessä toimintaympäristössä ilmeneviä poikkeustilanteita, joilla on vaikutuksia organisaation toimintaan. Kyberharjoituksen avulla kyberhäiriöitä simuloidaan, eli mallinnetaan. Näin luodaan kuvitteelliset olosuhteet, joissa häiriön vaikutuksia ja niistä toipumista voidaan testata.

Harjoitus voidaan mieltää organisaatiota kohtaavaksi ilmaiseksi kriisiksi, jonka ajankohta ja vaikutukset voidaan itse valita. Kriisitilanteista oppiminen on erittäin arvokasta, ja harjoituksen avulla tätä oppimisen tapaa voidaan soveltaa ilman, että kriisi haittaisi organisaation toimintaa. Harjoitus on usein edullinen tapa havaita puutteita, jotka liittyvät kriiseihin varautumiseen.

Erilaisia harjoituksia on järjestetty monissa organisaatioissa jo pitkään. Esimerkiksi paloturvallisuuden ylläpitämiseksi monissa toimitiloissa järjestetään pelastus- ja poistumisharjoituksia. Elintärkeitä taitoja on harjoiteltu ja opeteltu myös organisaatioiden ensiapukoulutuksissa.

Fyysisen maailman harjoituksista poiketen kyberharjoitus kohdistuu organisaation kybertoimintaympäristöön. Se tarkoittaa, että pitkälle verkottuneen toimintaympäristön häiriötilanteiden vaikutuksia arvioidaan tietojärjestelmiä pidemmälle - kyse ei siis ole pelkästä tietokoneiden toimintahäiriöharjoituksesta. Kyberharjoitus ei ole pelkkä IT-harjoitus.

Kyberhäiriöille on tyypillistä, että ne vaikuttavat myös muualla kuin varsinaisessa toimistoympäristössä, muun muassa tuotannon tai logistiikan häiriöinä. Kyberharjoituksessa voidaan esimerkiksi simuloida logistiikkakeskuksen tietojärjestelmän häiriö, jolla on vaikutuksia tavarantoimituksiin ja vastaanottoon.

Parhaimmillaan kyberharjoituksen avulla tietoteknisten häiriöiden laajat vaikutukset kirkastuvat kaikille osapuolille ja organisaation riippuvuus toimivista tietojärjestelmistä selkeytyy. Harjoitus voi tuoda esiin myös organisaation piilevät riippuvuussuhteet. Organisaation riskinhallintatyön ja monipuolisen varautumisen kannalta tällaiset opit olisivat erinomaisia.

Poikkeusoloissa toimintatapojen lisäksi harjoituksissa korostuvat myös viestintä ja johtaminen. Usein harjoituksessa päästäänkin sovittamaan yhteen organisaation eri toimintoja tosielämää muistuttavalla tavalla, jolloin ymmärrys eri osakokonaisuuksien yhteistoiminnasta vahvistuu. Erityisesti viestinnän merkitys kyberhäiriöiden hallinnassa on sosiaalisen median aikakaudella keskeinen.

Kyberharjoituksen voi järjestää itse tai harjoitus voi olla kolmannen osapuolen tuottama. Laajat yhteistoimintaharjoitukset, joihin osallistuu edustajia eri organisaatioista, ovat hyviä tilaisuuksia kehittää verkostomaista yhteistoimintaa ja luoda yhteyksiä eri organisaatioiden välille. Laajojen harjoitusten toteuttamisesta vastaavat erilaiset yhteistoiminta- tai koulutusorganisaatiot, kuten oppilaitokset tai valtion organisaatiot. Laajoihin yhteisharjoituksiin osallistuminen on erittäin hyödyllistä.

Jatkuva ja säännöllinen kyberharjoittelu on keskeinen osa modernin organisaation kyberturvallisuuden hallintaa. Jos organisaatiossanne ei vielä harjoitella, tämän oppaan avulla pääsette alkuun.

2.1 Miksi järjestäisin kyberharjoituksen?

Harjoittelu ei kannata vain harjoittelemisen vuoksi. Jos harjoitus on suunniteltu ja toteutettu organisaation tarpeiden mukaisesti ja opit muutettu toimintatavoiksi, organisaatio kehittyy varmasti.

Toimivatko häiriönhallintanne prosessit? Harjoitus on organisaatiolle erinomainen tapa varmistaa, että poikkeustilanteiden varalle sovitut toimintatavat ovat hyviä, tehokkaita ja tarkoituksenmukaisia. Harjoituksessa sovittuja tapoja voidaan aktiivisesti soveltaa niiden passiivisen tarkastelun sijaan. Harjoitus voi toimia myös uudistettujen prosessien testinä, jossa punnitaan toimivuutta tosielämässä.

Kyberharjoituksen avulla vahvuudet ja heikkoudet nousevat esiin. Etenkin kriisiohjeiden säännöllinen käsittely ja mieleen palauttaminen auttavat oikeassa tilanteessa. Muutamassa harjoituksessa poikkeamanhallintaohjeen olemassaoloa ei ole edes muistettu, vaikka sellainen oli olemassa!

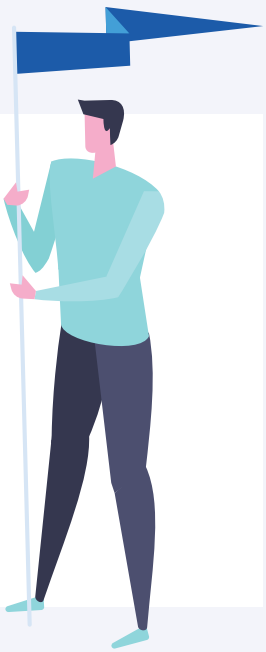
Monessa organisaatiossa oman harjoitusohjelman käynnistämistä lykätään jatkuvasti tulevaisuuteen. Tämä on ymmärrettävää, sillä harjoittelu voi tuntua vaativalta, vaikealta ja vain isoille organisaatioille kuuluvalta. Harjoittelun voi kuitenkin aloittaa pienellä ajalla ja vaivalla lähes tyhjästä.

Toimiva ja tasapainoinen harjoitusohjelma voi sisältää pieniä, helposti järjestettäviä harjoituksia ja monimutkaisempia toiminnallisia harjoituksia. Kevyillä työpöytäharjoituksillakin saadaan harjoittelun hyötyjä helposti käyttöön.

Ensimmäisen harjoituksen voi järjestää yksinkertaisena työpöytäharjoitteena. Yleensä nälkä kasvaa syödessä, mistä matka kohti monipuolisempia, haastavampia ja mielenkiintoisempia harjoituksia voi alkaa.

Harjoittelusta saatavia etuja ovat

- organisaation kriisinsietokyvyn parantuminen
- kasvanut ymmärrys tietojärjestelmäriippuvuuksista
- parantunut ymmärrys häiriötilanteiden laajoista vaikutuksista
- sisäisen ja ulkoisen viestinnän kehittyminen
- poikkeustilanteiden johtamisen kyvykkyyksien lisääntyminen
- harjoituksen tulosten analyysin kautta kehittyvät sisäiset prosessit
- parantunut yhteisymmärrys palveluntuottajien ja asiakkaiden kanssa
- vastuualueiden selkiytyminen
- luottamus epävarmuudesta selviämiseen kasvaa.



3 Erilaisia harjoitustyyppejä

Erilaisia kyberharjoitustyyppejä on lukematon määrä. Omaa harjoitusta suunniteltaessa on hyvä muistaa, että toteutustapoja on useita. Oikeastaan mikä tahansa prosessien hallittu tarkastelu voi käydä harjoituksesta. Tapahtumien simuloinnin yksityiskohtaisuus, harjoitusympäristö, tekniset vaatimukset ja ajankäyttö määrittävät eri harjoitustyyppejä. Omaan harjoitukseen voi poimia elementtejä monesta eri harjoitustyypistä tarpeen mukaan.

Sopivan harjoituksen valinta riippuu käytettävistä resursseista, harjoituksen tavoitteista ja harjoituksen kohdejoukosta. Tekniselle henkilökunnalle järjestettävä harjoitus poikkeaa johdon kriisinhallintaharjoituksesta niin toteutustavaltaan kuin tavoitteiltaankin. Tavoitteet ja osallistujat on hyvä määritellä ja valita ensin, harjoitusmenetelmä vasta niiden jälkeen.

Johdon kriisivalmiutta ja teknisen henkilökunnan osaamista ei voi kehittää samanlaisilla harjoituksilla. Harjoitustyyppi tulee valita sen perusteella, mitä halutaan harjoitella. Johtamisharjoituksia varten soveltuvia ovat esimerkiksi työpöytäharjoitus tai toiminnallinen harjoitus. Teknisesti taitava harjoittelijajoukko vaatii puolestaan teknisesti haastavamman tyypin. Harjoitustyyppejä yhdistelemällä voidaan tuoda yhteen johtamisharjoitus ja tekninen harjoitus. Tavoitteiden yhdistäminen ei ole vaivatonta, mikä näkyy monimutkaisemman harjoituksen suunnittelussa.

3.1 Työpöytäharjoitus

Sopii kyberhäiriöiden hallintaan, johtamiseen, prosessien läpikäyntiin ja arviointiin.

Toteutukseltaan kevyimpiä ja yleisimpiä harjoituksia ovat niin sanotut työpöytäharjoitukset, jotka perustuvat täysin kirjallisen materiaalin hyödyntämiseen. Työpöytäharjoituksessa ei mallinneta tapahtumaympäristöä. Yleensä harjoituksen tapahtumat ja niihin liittyvät tehtävät toimitetaan harjoittelijoille harjoituksen alussa.

Harjoituksen tavoitteena on löytää ja dokumentoida ratkaisuja ja vastauksia luotuihin tapahtumiin ja tehtäviin. Harjoituksen valmistelu on helppoa eikä vaadi pitkää ennakkovalmistelua. Järjestämiseen riittää, että harjoittelijat kutsutaan koolle ennalta sovittuun aikaan ja paikkaan ratkomaan pelissä eteen tulevia tehtäviä.

Työpöytäharjoitus ei yleensä sisällä ajastettuja syötteitä tai interaktiivisuutta, vaan harjoitustehtäviä ratkotaan rauhassa pohtien. Useista harjoitustehtävistä koostuva harjoitus voidaan aikatauluttaa vaikkapa siten, että ensimmäinen tunti pohditaan tilannetta 1 ja toinen tunti tilannetta 2. Yleensä lopputuloksena on kirjallinen vastaus kysymyksiin ja erillinen lista jälkikäteen selvitettävistä asioista.

Työpöytäharjoituksen tehtävä voi koostua esimerkiksi kuvitteellisesta nykytilanteen kuvauksesta ja siihen liittyvästä tehtävästä, joka on usein kysymyksen muodossa, esimerkiksi seuraavalla tavalla:

> ”Merkittävä laite- ja palveluntoimittaja ilmoittaa myyneensä koko liiketoimintansa maahan X.
> Aiheuttaako yrityskauppa muutoksia palveluiden luotettavuusarviointiin?”

Tällaisissa harjoituksissa ei ole keskeistä selvittää häiriön syytä tai pureutua teknisiin yksityiskohtiin, vaan laatia suunnitelmia poikkeustilanteiden varalta tai tarkistaa olemassa olevien suunnitelmien käyttökelpoisuus ja ajantasaisuus.

Työpöytäharjoitus tunnetaan myös nimellä ”paperiharjoitus” siksi, että sen järjestäminen ei edellytä teknistä ympäristöä. Pelin sisältö voidaan laatia etukäteen ja tulostaa paperiarkeiksi, jotka toimitetaan pelitiloihin. Pelin alkaessa pelitilanteen kuvaus otetaan esiin ja harjoitus voi alkaa. Myös teknistä ympäristöä tai sopivaa työkalua työpöytäharjoituksen järjestämiseen voi toki käyttää.

Työpöytäharjoitukset toimivat hyvin myös intensiivisempien harjoitusten ”esiharjoituksina”. Näin harjoittelijat voivat virittäytyä sopivaan tunnelmaan tai kerrata tulevassa harjoituksessa tarvittavia tietoja ja taitoja.

3.2 Juurisyyharjoitus (pre-mortem)

Sopii ongelmien ennakointiin ja riskienhallinnan suuntaamiseen.

Juurisyyharjoitus, joka tunnetaan myös nimellä pre-mortem, on harjoitustyyppi joka toteutetaan työpöytäharjoituksen tapaisesti. Harjoitus on toiminnallisesti kevyt ja helppo järjestää. Juurisyyharjoituksen tavoitteena on löytää riskien alkuperäisiä aiheuttajia, jotka toteutuessaan aiheuttavat kyberhäiriön.

Harjoittelevalle joukolle esitetään toteutunut kyberhäiriö, ja harjoittelijoiden tehtäväksi jää miettiä, mitkä tekijät omassa toimintaympäristössä saattaisivat aiheuttaa kuvatun kaltaisen lopputuloksen. Harjoitus pelataan ikään kuin keskeltä aloittaen, tapahtumien alkupistettä arvioiden.

Tunnistettuja riskejä voidaan käyttää tulevien harjoitusten skenaariotyön pohjana. Juurisyyharjoituksessa toteutuneena riskinä voidaan käyttää esimerkiksi tietovuotoa, jossa asiakasdataa on päätynyt julkisesti saataville. Harjoittelijoiden tehtäväksi jää kehitellä erilaisia tietoturvaloukkaustapahtumia, joiden seurauksena, tässä tapauksessa, tietovuoto on päässyt syntymään.

3.3 Toiminnallinen harjoitus

Sopii kriisijohtamiseen, kriisiviestinnän harjoitteluun ja yhteistoimintaharjoitteluun.

Toiminnallinen harjoitus on työpöytäharjoitusta realistisempi menetelmä. Muun muassa aikapaine on selkeästi tiukempi, sillä harjoituksessa käsitellään ajastettuja syötteitä. Ne tarjoillaan harjoittelijoille ennalta laaditun käsikirjoituksen perusteella, joka vie harjoituksen tarinaa eteenpäin.

Harjoituksen syötteet ovat yksittäisiä, harjoituksessa tapahtuvia asioita kuvaavia viestejä. Syöte voi olla mikä tahansa peliä edistävä informaatiokokonaisuus, esimerkiksi:

- sähköpostiviesti
- puhelu
- twiitti
- uutinen
- Facebook-kirjoitus
- harjoittelijalle pelikeskuksesta puhelimitse annettu tieto
- haastattelupyyntö.

Tässä harjoitustyypissä korostuu harjoittelijoiden kyky eläytyä tilanteeseen, kommunikoida ja viestiä keskenään sekä muodostaa ajankohtaista tilannekuvaa harjoituksen tapahtumien vaikutuksista organisaatioon.

Hyvässä harjoituksessa harjoittelijat saavat tapahtumista tietoa vähän kerrallaan, ja peliin liittyy useita tapahtumia monesta eri suunnasta. Esimerkiksi sosiaalisen median ja viestinnän haasteet on helppo tuoda peliin mukaan pelitapahtumia kommentoivilla uutisilla ja sosiaalisen median viesteillä. Myös median haastattelupyynnöt ja ”oikeat” haastattelut videointeineen antavat mahdollisuuden harjoitella ulkoista viestintää vaikeissa tilanteissa. Samalla ne lisäävät harjoituksen vaikeusastetta.

Tehokas ja dynaaminen pelikeskus on keskeinen osa toiminnallista harjoitusta. Pelikeskus on harjoittelijoista erillinen tila, jossa pelin suunnittelijat ohjaavat peliä. Keskuksen tehtävänä on johtaa peliä ja lähettää syötteet pelin aikana harjoittelijoille. Etukäteen suunniteltujen pääsyötteiden lisäksi ohjaajat voivat tuoda peliin ehdollisia syötteitä, joilla reagoidaan harjoittelijoiden ratkaisuihin ja päätöksiin. Uusia syötteitä voidaan tarvita myös tilanteessa, jossa harjoittelijat ohjaavat peliä ennalta arvaamattomaan suuntaan.

Suunnittelussa voi käyttää apuna harjoitussimulaattoria, joka kerää syötteet yhteen näkymään harjoittelijoiden käsille ja tarkasteltavaksi. Harjoitussimulaattoreista on kirjoitettu kappaleessa 6.7 Harjoituksen toimintaympäristön mallintaminen.

3.4 Tekninen harjoitus

Sopii teknisten valmiuksien korottamiseen, järjestelmiin perehtymiseen ja palautumistesteihin.

Tekninen harjoitus vaatii runsaita alkuvalmisteluita. Ajatuksena on viedä harjoituskokemus suoraan tietotekniseen ympäristöön luomalla siellä poikkeustilanne, jonka tunnistaminen, selvittäminen, korjaaminen ja dokumentointi muodostavat harjoituksen sisällön.

Teknisessä harjoituksessa voidaan simuloida erilaisia häiriö-, vika- ja uhkatilanteita hyvin realistisesti. Se voi myös perustua varajärjestelmien käyttöönoton testaamiseen, varmuuskopioiden palautukseen tai muuhun tapaan, jolla tuotantojärjestelmien toiminta poikkeustilanteissa varmistetaan.

Harjoituksen sisältönä voi olla esimerkiksi organisaation verkkoon kytketty tuntematon laite, joka liikennöi ulos organisaatiosta ”hyökkääjän” hallinnassa olevan tietokoneen kanssa. Harjoitusta varten tuotantoverkkoon liitetään haitallista laitetta simuloiva laite, joka tuottaa poikkeuksellista liikennettä. Harjoitus aloitetaan ilmoittamalla harjoitusjoukolle ensihavainto, jonka perusteella ongelman ratkaisemiseksi pitää tehdä oikeat toimenpiteet.

Harjoitusympäristö on merkittävässä roolissa, sillä tällä harjoitustyypillä voidaan päästä hyvin lähelle todellisia toimintamalleja ja prosesseja. Erilaisten laitteiden tai haitallisia ohjelmia simuloivien ohjelmien tekeminen tai tilaaminen vaatii toki paljon resursseja. Tekninen harjoittelu on suositeltavaa organisaatiossa, joissa on muilla harjoitustavoilla jo tarkasteltu poikkeustilanteen käsittelyä ja varmistettu siihen liittyvien prosessien toimivuus ja ajantasaisuus.

Teknisen harjoituksen voi toteuttaa myös täysin simuloidussa ympäristössä. Simuloiduissa ympäristöissä luodaan harjoittelijoille verkko, työasemat sekä palvelut, joissa ilmeneviä poikkeuksia tutkitaan yleisesti saatavilla tai käytössä olevilla työkaluilla. Muun muassa omien työkalujen puute sekä harjoitteluympäristön ja oman tuotantoympäristön erot voivat vaikuttaa harjoituskokemukseen, vaikka harjoitus olisikin todenmukainen. Harjoittelijoilta edellytetäänkin kykyä mukautua tilanteeseen ja toimia organisaation prosessien mukaan myös vieraassa tietoteknisessä ympäristössä.

3.5 Capture the flag -harjoitus

Sopii teknisen osaamisen kehittämiseen ja järjestelmiin tutustumiseen.

Capture The Flag- eli CTF-harjoitusten tavoitteena on etsiä tietoteknisistä järjestelmistä ”lippuja”, jotka kerryttävät kilpailijan tai joukkueen pistesaldoa. Liput voivat olla esimerkiksi tietynlaisia merkki- ja kirjainjonoja, jotka harjoittelija syöttää pisteytysjärjestelmään ne löydettyään. CTF-harjoituksissa lippuja voidaan piilottaa moneen eri paikkaan, mutta tyypillisesti harjoittelijoiden pitää päästä sisään suojattuun järjestelmään ja tehdä järjestelmän sisällä erilaisia selvityksiä, joiden perusteella liput paljastuvat.

CTF-harjoitukset ovat teknisiä harjoituksia, joissa pääosassa on harjoittelijoiden tai joukkueiden keskinäinen kilpailu. CTF-harjoituksia järjestetään erilaisten tilaisuuksien tai koulutusten yhteydessä sekä avoimina tilaisuuksina internetin ylitse.

Internetistä on vapaasti saatavilla erilaisia virtuaalikoneita, jotka on valmisteltu teknisten harjoitusten toteuttamista ajatellen. Niitä on mahdollista hyödyntää oman CTF-harjoituksen järjestämisessä. Vapaasti saatavilla olevia CTF-harjoituksia voi etsiä verkosta esimerkiksi hakutermeillä ”CTF challenge” tai ”capture the flag cyber exercise”.

CTF on helppo tapa aloittaa tekninen harjoittelu. Organisaatio voi kerätä oman joukkueensa ja osallistua CTF-kilpailuun tai -tapahtumaan. Harjoituksen järjestämisvastuu on muulla, mutta tekninen henkilökunta saa hyvää harjoitusta myös omien verkkojen haavoittuvuuksien tutkimista ja selvittämistä varten.

Organisaation omien prosessien tarkasteluun yleiset CTF-virtuaalikoneet tai -harjoitusalustat soveltuvat huonosti, mutta ne toimivat hyvin, kun oman teknisen henkilökunnan osaamista halutaan lisätä.

3.6 Suuret yhteisharjoitukset

Sopii verkostojen luomiseen, yhteistoiminnan vahvistamiseen ja tilannekuvan muodostamiseen.

Suomessa on jo pitkään järjestetty useita suuria yhteisharjoituksia aina viranomaisten keskinäisestä teknisestä harjoittelusta organisaatioiden välisten vuorovaikutusverkostojen luomiseen. Näissä harjoituksissa pelataan lähinnä toiminnallisen harjoituksen säännöillä yhdistäen siihen työpöytäharjoitusten piirteitä. Myös simuloitua internetympäristöä on käytetty. Näin harjoitukseen on tuotu teknisen harjoituksen sisältöä.

Omien sisäisten prosessien parantamisen sijaan yhteisharjoituksen tavoitteet liittyvät organisaation verkostojen ja arvoketjujen tarkasteluun. Yhteisharjoituksissa keskitytään luomaan yhteistä tilannekuvaa sekä sovittamaan yhteen oman organisaation ja yhteistyökumppaneiden toimintaa. Lisäksi usein halutaan harjoituttaa tiedonvaihtoa ja yleisen käsityksen rakentamista hyökkääjän motiiveista, toimintatavoista ja tavoitteista.

Jotkin yhteisharjoitukset keskittyvät tekniseen peliin, jolloin harjoittelevat joukot kilpailevat keskenään omaa peliympäristöään puolustaen ja pisteitä keräten.

Yhteisharjoitukseen osallistuminen ei yleensä edellytä organisaatioilta aiempaa harjoituskokemusta. Harjoituksen alussa järjestetään infotilaisuus, jossa harjoituksen tavoitteet, osallistujat ja käytännön seikat käydään läpi. Yhteisharjoituksen järjestäminen on usein hyvin työlästä, mutta osallistuminen vaatii vain harvoin organisaatiolta suuria panostuksia harjoituksen hyötyihin verrattuna.

Yhteisharjoitukset ovat pääsääntöisesti kutsutilaisuuksia. Jos organisaationne saa tilaisuuden osallistua yhteisharjoitukseen, se kannattaa käyttää, sillä yhteisharjoitukset ovat erinomaisia paikkoja tutustua myös eri harjoitusmenetelmiin.

Ennen harjoitusta organisaation kannattaa määritellä omat tavoitteensa ja valmistautua harjoitukseen mahdollisuuksiensa mukaan. Siten saadaan parhaat hyödyt yhteisharjoituksesta irti. Etenkin harjoitukseen lähetettävien henkilöiden roolit ja vastuut on syytä miettiä huolella ja katsoa, että roolit vastaavat tosielämän tarpeita.

4 Harjoituksen valmistelut

Harjoituksen elinkaari voidaan kuvata kolmen vaiheen kautta: valmistelu, toiminta ja jälkianalyysi. Erityisesti harjoituksen jälkeinen analyysi ja siitä saatujen oppien jalkauttaminen organisaation toimintaan on harjoituksen hyödyllisyyden kannalta keskeistä. Huolellinen suunnittelu taas varmistaa, että harjoitustapahtuman kulku ja yksityiskohdat on mietitty tarkkaan. Valmistelu ja jälkianalyysi vievät valtaosan harjoituskokonaisuudesta, mutta samalla ne valmistavat seuraavaan harjoitukseen. Valmistelu, toiminta ja jälkianalyysi muodostavatkin jatkumon – harjoituskierron.

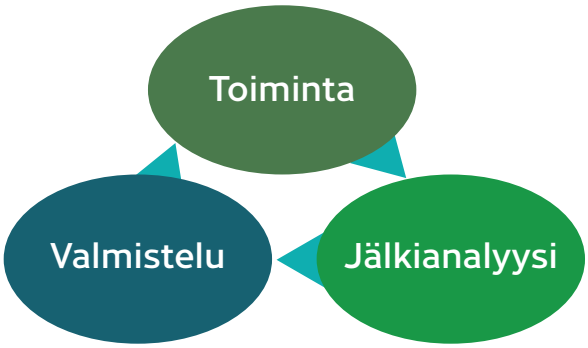
Valmisteluiden työläyteen vaikuttaa valittu harjoitustyyppi. Työpöytä- tai juurisyyharjoituksen järjestämiseen liittyvä valmistelu on kevyempää kuin toiminnallisen harjoituksessa, mutta tulosten analysointi on syytä resursoida hyvin.

Usein voi olla perusteltua järjestää vuodessa useita, kevyitä harjoituksia tiiviillä aikataululla kuin kuluttaa paljon aikaa ja vaivaa yhteen isoon harjoitukseen vuodessa.

Valmistelutyö on harjoituksen työläin vaihe. Vaikka harjoitus ostettaisiin palveluna, harjoituksen suunnittelutapaamisiin pitää varata kaikilta riittävästi aikaa. Harjoituksen suunnittelutapaamiset on hyvä varata reilusti etukäteen, vähintään kolme kuukautta ennen varsinaista tapahtumaa.

Harjoituksen suunnitteluun määritellyt henkilöt tulee sitouttaa harjoituksen valmisteluihin jo aikaisessa vaiheessa. Suunnitteluun pitää järjestää työaikaa, mikä tulee huomioida henkilöiden muiden tehtävien järjestelyissä. Suunnittelijoiden poissaolot suunnittelutapaamisista häiritsevät koko harjoituksen toteutusta, sillä heidän tulee hallita harjoituksen kokonaisuus.

Kaikkea ei voi suunnitella etukäteen, mutta harjoituksen raamit on hyvä määritellä niin tarkasti, että yllätyksiä sattuisi mahdollisimman vähän. Ulkopuolisen järjestäjän käyttäminen on usein hyvä ratkaisu, sillä harjoituksen suunnittelutyö lohkaisee ison palan organisaation omien työntekijöiden työajasta.



Suunnittelu muistuttaa pientä projektia. Jos suunnittelun hoitaa itse, työssä voi soveltaa seuraavaa esimerkkirunkoa:

Harjoituksen ideointipalaveri
- alustavat selvitystyöt
  - harjoituksen tavoite
  - harjoituksen laajuus
  - harjoituskohde
  - mahdolliset toteutusajankohdat
- suunnittelutyön alustava aikataulutaminen
- vastuunjako.

1. suunnittelutapaaminen:
- projektin käynnistäminen
- projektityöryhmän määrittely
- projektin resursointi
- harjoituksen tavoitteen päättäminen
- harjoitusmenetelmän valinta.

2. suunnittelutapaaminen:
- harjoituksen sisällön hahmottelu
- harjoituksen dokumentoinnin laatiminen
- osallistujien valitseminen ja kutsut
- tilojen varaaminen.

3. suunnittelutapaaminen:
- harjoituksen sisällön tai syötteiden työstö
- dokumentoinnin tarkastus ja viimeistely
- osallistujien varmistaminen.

Harjoituksen toteutus
- valmistautuminen
- harjoitus
- välitön palautetilaisuus (Hot Wash-up).

Harjoituksen jälkitoimet
- tarkkailijoiden raportoinnin viimeistely
- oppien läpikäynti osallistujaryhmien kesken
- oppien käytäntöön viemisen seuraaminen.

Projektin päättäminen ja kokonaisuuden arviointi

Uuden harjoituksen suunnittelu vuosikellon mukaisesti

Harjoituksen voi järjestää itse, missä etuina ovat pienemmät kustannukset ja mahdollisuus järjestää harjoituksia joustavasti omaan tahtiin. Ison osan harjoituksen suunnittelu- ja valmistelutyöstä voi myös ostaa ulkopuoliselta toimittajalta. Tällöin omaa aikaa säästyy, etenkin jos apuna on kokenut ammattilainen. Kuitenkin palvelujen käyttö vaatii tilaajalta vahvaa panosta, sillä harjoitus pitää suunnitella organisaation tavoitteiden ja toimintaympäristön mukaisesti. ”Avaimet käteen”-periaatteella yksilöllistä harjoitusta ei voi ostaa.

Suunnittelun aikana syntyy runsaasti kirjallista materiaalia, joka pitää laatia ja tallentaa niin, että se on helposti löydettävissä ja hyödynnettävissä myös jatkossa. Esimerkiksi harjoituksen palautekysely, erilaiset lomakepohjat tai harjoittelijoille laadittavat yleiset ohjeet voi olla uudelleenkäytettävissä lähes sellaisenaan.

4.1 Tavoitteen asettaminen

Harjoituksen kulkua suunnitteluvaiheesta jälkianalyysiin ohjaa päätavoite, joka kannattaa määritellä heti prosessin alkuvaiheessa. Se voi liittyä toiminnan tehostamiseen, turvallisuuteen, osaamisen kehittämiseen tai jonkin prosessin testaamiseen. Päätavoite johdetaan organisaation strategiasta ja riskienhallintatyöstä.

Tavoitteiden tulisi kuvastaa todellisia ja olemassa olevia tarpeita. Jos harjoitustoimintaa jatkuu pitkin vuotta, voidaan vuosikohtaiset päätavoitteet jakaa alatavoitteisiin, joille kullekin järjestetään oma harjoituksensa.

Päätavoite voi olla esimerkiksi ”kyberkriisinhallinta Major Incident Management -prosessin mukaisesti”, jonka alatavoitteiksi voidaan asettaa ”kriisiviestintäohjeiden soveltaminen”, ”varajärjestelmiin siirtymisen testaaminen” ja ”ajantasaisten yhteystietojen toteaminen”. Tavoitteiden perusteella voidaan ryhtyä suunnittelemaan esimerkiksi toiminnallista harjoitusta,

jossa simuloidaan kriisi, johon liittyy viestinnällisiä tarpeita sekä yhteydenpitoa palvelutuottajiin.

Jos tavoite on riittävän konkreettinen, jälkikäteen voidaan todeta, saavutettiinko se vai ei. ”Parannetaan prosessia x” -tyyppisissä tavoitteissa onnistumista tai epäonnistumista on vaikea todeta tai havaita.

Harjoituksen tavoitteet voivat liittyä esimerkiksi:

- kriisijohtamisen tai -viestinnän kehittämiseen
- teknisen valmiuden kohentamiseen
- häiriöistä toipumiseen
- uhkien havaitsemiseen
- raportointiin
- yhteydenpitomenetelmien ja varamenetelmien testaukseen
- häiriönhallintaprosessien testaamiseen
- teknisten järjestelmien testaukseen palvelu- ja laitetoimittajien kanssa työskentelemiseen tai vastuunjaon selkeyttämiseen.

Tavoitteet kannattaa kerrata jokaisessa harjoituksen suunnittelutapaamisessa, jotta ne pysyvät kirkkaana mielessä. Ne tulee myös tehdä selviksi harjoittelijoille, jotta kaikilla osapuolilla on yhteinen päämäärä.

4.2 Harjoitustyypin valintaan vaikuttavia tekijöitä

Mikä tahansa tilaisuus, jossa organisaation toimintaa testataan ja kehitetään, voidaan toteuttaa harjoituksena. Periaate on hyvä pitää mielessä harjoitustyyppiä valittaessa, kun harjoituksen tavoitteet, laajuus ja osallistujat on ensin päätetty.

Harjoitustyypit eivät sido harjoituksen suunnittelua, vaan eri tyyppien sopivia piirteitä ja ominaisuuksia voi vapaasti yhdistellä. Toiminnalliseen harjoitukseen voidaan lisätä esimerkiksi työpöytäharjoituksen ja teknisen harjoituksen piirteitä.

Monipolvista harjoitusta suunnitellessa ulkopuolisen avun käyttäminen kannattaa. Kaupallinen ja kokenut toimija keskittyy oleelliseen ja voi auttaa myös organisaation oman harjoitustoiminnan käynnistämisessä.

Harjoitus ei välttämättä aina vaadi fyysistä läsnäoloa. Harjoitus voidaan pelata myös niin, etteivät harjoittelijat saavu samaan paikkaan pohtimaan kysymyksiä. Erityisesti maantieteellisesti laajalla alueella toimivissa organisaatioissa etäyhteyden käyttö vähentää matkustamisen tarvetta. Osa voi olla harjoituksen aikana konsultoivissa ja ”tarvittaessa käytettävissä” -rooleissa ja osallistua peliin hetkellisesti puhelimen tai muun etäyhteyden avulla. Esimerkiksi juridinen apu voi olla joskus tarpeen.

Etäyhteys ja oman työn ohessa osallistuminen voi kuitenkin haitata keskittymistä. Siksi etäosallistujienkin pitäisi varata kalentereistaan riittävästi häiriötöntä harjoitusaikaa.

Jos halutaan harjoittaa iso joukko kerralla, jokaisesta erillään olevasta toimitilasta voidaan varata omat tilat etäosallistumista varten. Etäosallistumiseen voidaan käyttää muun muassa videoneuvottelua, pikaviestimiä, matkapuhelimia tai sähköpostia. Etäyhteyden käyttäminen on hyvä tapa testata organisaation viestivälineitä ja tarvittaessa varayhteyksiä, jos harjoituksessa tilanne estää ensisijaisten yhteydenpitovälineiden käytön.

5 Harjoituksen suunnittelu

Harjoitusta toteutettaessa organisaation johto, suunnittelijat, harjoittelijat ja tukitehtävissä toimivat henkilöt ovat keskeisessä asemassa. Mitä isommasta harjoituksesta on kyse, sitä enemmän tarvitaan ihmisiä eri rooleihin.

Johdon on tuotava selkeästi ilmi sitoutumisensa ja kiinnostuksensa harjoitukseen ja sen oppeihin. Jos johto ei selkeästi tue harjoitusta, suunnittelutyö kärsii, koska osallistujat voivat kokea, että heidän työaikaansa käytetään tarpeettomiin asioihin.

Jos harjoituksessa voidaan testata organisaation toiminnan jatkuvuutta poikkeavissa olosuhteissa ja havaitaan, että toimintakyky säilyy, tästä tiedosta hyötyy myös organisaation johto.

Seuraavaksi on kuvattu harjoituksen suunnittelun ja toteutuksen kannalta keskeiset tehtävät ja järjestelyt.

5.1 Suunnitteluryhmän kokoaminen

Suunnitteluun on hyvä varata ainakin kolme tai neljä tapaamiskertaa. Lisäksi harjoituksen tarinan ja syötteiden laatiminen vaatii erillistä suunnitteluaikaa. Harjoituksen suunnitteluryhmässä toimivien henkilöiden ei tulisi toimia harjoittelijoina, sillä heidän ennakkotietonsa pelitapahtumista vaikuttaisivat väkisinkin pelin kulkuun. Harjoituksen suunnitteluryhmää voidaan kutsua myös projektiryhmäksi.

Suunnitteluryhmällä on oltava johtaja, joka kutsuu suunnitteluryhmän kokoon ja vastaa harjoituksen johtamisesta. Hän myös toimii harjoituksen projektipäällikkönä. Ryhmässä on oltava myös harjoituksen sisällöstä vastaavia organisaation omia asiantuntijoita, jotka tuntevat organisaation toimintaa riittävän hyvin. Ryhmään voidaan pyytää myös ulkopuolisia asiantuntijoita, palvelutoimittajia tai muita kumppanien edustajia uutta näkökulmaa ja osaamistaan tuomaan.

Suunnitteluryhmässä jokaisen on tiedettävä roolinsa ja omat tehtävänsä. Ulkopuolisen harjoituskumppanin kanssa toimittaessa kumppani vastaa yleensä suunnittelutyön johtamisesta, suunnitteluryhmien tapaamisten järjestämisestä ja roolittaa suunnittelijat näiden vahvuuksien mukaan.

Esimerkki suunnitteluryhmän edustuksista ja rooleista:

- harjoituksen johtaja: tietoturvapäällikkö tai -johtaja tai ulkoinen kumppani
- skenaariosuunnittelutyön johtaja: tietoturva-asiantuntija tai ulkoinen kumppani
- harjoituksen sisäinen ja ulkoinen viestintä: viestintäasiantuntija tai -päällikkö
- tietohallinto, tietojärjestelmät ja ulkoiset toimittajat
- liiketoimintayksiköiden edustaja: key account manager tai vastaava
- palveluntuottaja: kumppaniyrityksen edustaja
- palveluntuottaja: tietoturvapalveluiden edustaja.

Tällaisella kokoonpanolla saadaan jo varsin hyvin selville, millainen harjoitus voisi hyödyttää organisaatiota eniten ja miten sitä kannattaa valmistella. Yllä oleva ryhmä on vain esimerkki, jota voi käyttää oman suunnittelun tukena.

5.2 Harjoittelijoiden valinta

Jos harjoituksen tavoitteena on kohentaa johtamista kriisitilanteessa, harjoittelijoiksi tarvitaan ainakin organisaation johto ja viestintä. Jos taas tavoite on parantaa tuotantojärjestelmän poikkeustilanteissa toimimista, harjoittelijoiksi valitaan tuotantojärjestelmän kanssa työskenteleviä ihmisiä. Tietoteknisen harjoituksen oikea harjoitusjoukko on organisaation tietotekninen henkilökunta esimiehineen.

Harjoitus voi sisältää tehtäviä, joihin tarvitaan organisaation henkilöstön useita eri edustajia. Viestinnän läsnäolo kaikissa harjoituksissa on suositeltavaa, sillä sen rooli kyberhäiriöiden hallinnassa on merkittävä - etenkin tapauksissa, joissa häiriön vaikutukset näkyvät organisaation ulkopuolelle. Myös sisäisiä häiriötilanteita harjoiteltaessa viestintä voi olla apuna laatimassa sopivia tiedotteita organisaation henkilökunnalle ja sidosryhmille.

Harjoittelijat, joiden rooli on vähäisempi, voivat hoitaa pelin tukitehtävät omalta työpisteeltään työtehtäviensä ohessa. Harjoittelijaa ei tarvitse kutsua paikalle koko ajaksi, jos hänen rooliinsa kuuluu esimerkiksi muutamaan kysymykseen vastaaminen. Olipa harjoittelijan rooli iso tai pieni, jokaiselle on syytä valita varahenkilö, joka osaa hoitaa alkuperäisen osallistujan tehtävät tämän poissa ollessa. Näin harjoitus ei pysähdy yllättäviin poissaoloihin.

Harjoituksen sisällön kannalta olennaiset ihmiset ovat usein mukana suunnittelemassa harjoitusta. Tavallisesti he eivät osallistu itse harjoitukseen harjoittelijoina. Suunnittelijoiden tilalle voi harjoituttaa esimerkiksi varahenkilöitä tai suunnittelijat voivat olla tavoitettavissa harjoituksen aikana vain puhelimitse. Tällaisessa roolissa suunnittelijan tulee keskittyä ratkaisemaan harjoituksessa esitettyjä ongelmia ainoastaan harjoittelijoiden kertomien faktojen valossa. Suunnitteluryhmän jäsen voi osallistua harjoitukseen pelaajana, mutta koska hän tietää harjoituksen käänteet ja yllätykset, hänen peliroolinsa tulisi muokata sen mukaan.

Harjoituksessa roolien määrä ei korvaa laatua. Jos mukaan kutsutaan liikaa osallistujia, itse harjoitustilanne voi muuttua kaoottiseksi. Esimerkiksi tekniselle henkilökunnalle järjestettävään harjoitukseen ei tarvita paikalle ylempää johtoa. Tosin päätöksentekoa edellyttävissä tilanteissa keskijohdon tai tiimiesimiesten saatavilla olo on tärkeää.

Harjoittelijoiden peliroolit liittyvät pääsääntöisesti heidän oikeaan työtoimenkuvaansa.

Harjoitukseen valittavilla pitää olla aikaa harjoitukselle. Tyypillisesti valmisteluineen ja purkuineen harjoitustapahtuma vie helposti koko päivän.

5.3 Harjoitukseen valmistautuminen

Harjoitustilanne on suurelle osalle poikkeuksellinen tapahtuma, siksi harjoittelijoille ei välttämättä ole itsestään selvää, miten harjoitukseen kuuluu valmistautua.

Harjoittelijoille pitää hyvissä ajoin tehdä selväksi, mitä tarvikkeita tai työntekovälineitä he tarvitsevat harjoitukseen mukaan. Jos harjoituksessa tarvitaan omaa tietokonetta, tulee tämä tehdä selväksi ja myös varmistaa verkkoyhteyksien riittävyys harjoitustilassa. Joskus on parempi ilman tietokoneen tuomaa häiriötä, sillä työsähköpostiin ja pikaviestimiin kilahtelevat viestit kaappaavat helposti harjoittelijan mielenkiinnon. Harjoituskutsussa tulee kuitenkin olla selkeästi ilmoitettuna, mitä harjoittelijat tarvitsevat harjoitukseen mukaan ja mitä välineitä harjoituksessa ei saa käyttää.

Tärkeintä on suhtautua harjoitukseen avoimesti ja myönteisesti sekä toimia harjoitusten tapahtumien mukaisesti. Harjoittelijat saattavat joskus pelata ”peliä vastaan” eli etsiä siitä porsaanreikiä, joiden avulla haastavat pelitilanteet voidaan kiertää.

Joskus harjoittelijat innostuvat ”ylipelaamaan” ja tekevät siirtoja, joita todellisuudessa ei edes harkittaisi jo valtavien kustannusten vuoksi. Esimerkiksi: Rajanylityksen valvontaan käytettävä järjestelmä toimii huonosti ja epäillään, että siihen on murtauduttu. Ongelma ratkaistaan sulkemalla maan ulkorajat, ettei järjestelmää enää tarvitsisi käyttää.

Tosielämässä ongelmaa ei tietenkään ratkaistaisi näin. Harjoittelussa on aina syytä pyrkiä realismiin sekä tapahtumissa että niiden ratkaisuissa.

Pelikeskuksen tehtävänä on suitsia ali- ja ylipelaamista. Keskuksesta voidaan viestittää harjoittelijoille, että valittu ratkaisu ei nyt onnistu, jolloin harjoittelijoiden tulee keksiä toinen. Harjoittelijoille on hyvä kertoa ennen harjoitusta sekä yli- että alipelaamisen riskeistä, jotta he tiedostavat oman toimintansa rajat sekä harjoituksen tarjoamat mahdollisuudet.

5.4 Tukitehtävät ja tarkkailijat

Harjoitukseen voidaan kiinnittää ihmisiä myös päivystäviin rooleihin muista organisaatioista tai yksiköistä. He eivät saavu harjoituspaikalle, mutta ovat valmiita vastaamaan harjoittelijoiden kysymyksiin harjoituksen aikana. Tyypillisesti näissä rooleissa toimivat esimerkiksi juristit, joilta pelaajat voivat tarvittaessa pyytää lainopillista tulkinta-apua. Päivystävä rooli sopii myös laite- tai palveluntoimittajalle, jonka kyvykkyyksistä ja vasteajoista voi nousta kysymyksiä harjoituksen aikana.

Tukirooleihin voidaan sijoittaa myös harjoittelijoiden esimiehiä ja ylempää johtoa, elleivät he ole harjoituksen varsinaisena osallistujajoukkona. Itsenäistä päätöksentekoa ja vaihtoehtoisia päätöksenteon malleja voidaan harjoituttaa myös poistamalla tukitehtävissä työskenteleviä harjoituksesta kesken harjoituksen.

Harjoituksissa kannattaa hyödyntää myös tarkkailijoita, joilla on tärkeä rooli harjoituksen jälkeisessä analyysityössä. Tarkkailija havainnoi, mutta ei puutu pelaajien toimintaan. Hän myös raportoi havaintonsa harjoittelijoille ja harjoituksen järjestäjille jälkeen päin. Tarkkailija voi olla henkilö joko organisaation sisältä tai ulkopuolelta.

Tehtävissä keskeistä on, ettei pelaajien toimintaan tai päätöksiin puututa. Käytännössä tarkkailijan ei kannata keskustella peliin osallistuvien henkilöiden kanssa. Tarvittaessa tarkkailija voi välittää tietoa pelikeskukselle harjoituksen sujumisesta ja mahdollisista ongelmatilanteista harjoituksen aikana. Tästä on sovittava etukäteen.

Tarkkailija kirjaa havaintonsa tarkkailijan muistioon. Jos mahdollista, voidaan käyttää useaa tarkkailijaa ja jakaa heille pelin eri osa-alueita seurattavaksi. Yksi voi keskittyä päätöksenteon ja toinen harjoituksen järjestelyjen arvioimiseen.

Pelin jälkianalyysivaiheessa tarkkailijat antavat välittömän palautteen harjoittelijoille ja harjoituksen järjestäjille. Myöhemmin he palauttavat puhtaaksi kirjoitettuna tarkkailumuistionsa, jonka perusteella tulevia harjoituksia voi kehittää. Muistion sijaan tarkkailijat voivat myös vastata harjoituksen jälkeen lähetettävään palautekyselyyn, jossa on yksilöity vastaajien roolit.

Tarkkailijan muistiota varten voidaan laatia lomake, johon merkitään tarkkailtavat osa-alueet kysymysten tai täytettävien kenttien muodossa. Näin voidaan suunnata tarkkailua. Lomakkeella voidaan kysyä esimerkiksi:

- ”Miten tilanteen johtamisvastuut jakautuivat?”
- ”Otettiinko viestintä huomioon oikea-aikaisesti ja riittävällä tavalla?”.

Tyhjentävää ja yleispätevää lomaketta ei voi eikä ole tarpeen laatia. Jokainen lomake pitää laatia tilannekohtaisesti harjoituksen tavoitteet, painopisteet ja harjoitteleva ryhmä huomioiden. Jos tarkkailija käyttää samaa lomakepohjaa vastaavissa harjoituksissa uudelleen, harjoittelun kehittymistä on mahdollista seurata.

5.5 Tilajärjestelyt

Onnistuneet tilajärjestelyt ovat iso osa hyvin sujuvaa harjoitusta. Harjoituksen tyyppi, sijainti ja osallistujien määrä määrittelevät pitkälti, millaisia tiloja tarvitaan. Yhtä kokonaisuutta suorittava joukko tarvitsee aina yhden huoneen: harjoittelijoille on varattava yksi huone ja mahdolliselle pelikeskukselle toinen. Esimerkiksi työpöytäharjoituksessa ei pelikeskusta tarvita, jolloin koko harjoitus voidaan hyvin toteuttaa yhdessä tilassa.

Jos eri tehtävissä toimivia harjoittelijaryhmiä on useita, heidät on syytä sijoittaa eri huoneisiin tai erottaa tiloja sermeillä. Neuvotteluhuoneen hyvä ilmanvaihto ja riittävät tilat takaavat, ettei pitkäkestoinen harjoitusistunto käy tarpeettoman raskaiksi. Harjoitustiloihin on varattava muistiinpanovälineitä, lehtiö- tai tussitaulu ja tarvittaessa virvokkeita.

Harjoittelijoiden kerääminen yhteen tilaan auttaa keskittymään harjoitukseen. Tilanne on usein todelliseen kriisitilanteeseen verrattuna keinotekoisen tuntuinen. Tyypillinen harjoitustilanteen kriisi kestäisi tosielämässä monta päivää, mutta harjoituksessa se voidaan typistää muutamaan tuntiin.

Harjoitustilat merkitään selkeästi esimerkiksi tekstillä ”HARJOITUS KÄYNNISSÄ” ja päivämäärällä. Myös harjoitustilan läheiset käytävät ja muut alueet, jossa harjoittelijat liikkuvat, merkitään huolellisesti väärinkäsitysten välttämiseksi. Harjoittelija saattaa keskustella harjoitukseen liittyvistä asioista puhelimessa käytävällä, jolloin ohikulkija voi kuulla osan puhelusta ja huolestua. Esimerkki harjoitushygienian merkityksestä: Harjoituksesta tietämätön työntekijä kuuli harjoittelijan puhelun, jossa todettiin kemikaalisäiliön kaatuneen varastossa. Tilanne johti todelliseen palohälytykseen.

Harjoittelijoille on tehtävä selväksi, missä tiloissa harjoitukseen liittyviä puheluita tai muita asioita saa puhua. Merkitseminen on erityisen tärkeää, jos harjoituksessa käytetään johtokeskuksia tai muita operatiivisia tiloja.

Toiminnallisessa harjoituksessa voidaan avata yksisuuntainen videoyhteys pelikeskuksesta harjoittelijoiden tilaan. Videolinkin kautta harjoittelijoita voidaan tarkkailla ja ohjata peliä harjoittelijoiden reaktioiden perusteella. Video- ja ääniyhteys voidaan toteuttaa esimerkiksi niin, että kannettavalla tietokoneella soitetaan videopuhelu, jossa pelikeskuksen puolen videokamera on peitetty ja mikrofoni mykistetty.

Harjoituksessa pidetään usein lounastauko. Lounaan ympärille voidaan rakentaa harjoitukseen ”aikahyppy” vaikkapa seuraavaan päivään, jolloin harjoituksen peliä voidaan edistää yli harjoitukseen rajatun ajan.

Jos harjoituksessa on paljon osallistujia, lounaalle olisi hyvä varata erillinen tila. Yleisessä lounasravintolassa harjoituksesta käyty keskustelu voi vuotaa pöydästä toiseen ja saada huhut liikkeelle.

6 Harjoituksen sisältö

Tavallisesti harjoituksen tapahtumat sijoittuvat nykyhetkeen ja nykyiseen toimintaympäristöön. Harjoituksissa toimitaan organisaation olemassa olevien rakenteiden ja arjen mukaan. Tarvittaessa voidaan luoda kuvitteellisia olosuhteita, joissa esimerkiksi harjoitellaan tulevaisuudessa tai poikkeavissa olosuhteissa. Tulevaisuuteen sijoittuvan harjoituksen lähtökohtana voi olla esimerkiksi todellisuudessa vielä suunnitteilla oleva ulkomaantoiminta, joka harjoituksessa on jo käynnissä.

Joskus harjoituksessa voidaan toimia täysin fiktiivisessä ympäristössä. Menetelmää voidaan käyttää esimerkiksi isoissa yhteysharjoituksissa, joissa jokaisen osallistujan on mahdotonta toimia todellisen työkuvansa mukaisesti. Tällöin harjoituksen tavoitteetkin voidaan asettaa ylemmälle tasolle, esimerkiksi verkostomaisen yhteistoiminnan kehittämiseksi.

6.1 Harjoitusskenaario

Harjoitusskenaario on harjoituksen kuvitteellisten olosuhteiden ja tapahtumien kertomus. Harjoituksessa skenaario perustuu tyypillisesti tietoturvaongelmaan ja sen taustoihin.

Organisaation oma riskienhallintatyö antaa hyvät eväät skenaarion rakentamiselle. Tunnistetuista riskeistä voidaan luoda skenaarioita, jotka perustuisivat riskien toteutumisista seuraaviin tapahtumiin. Vaihtoehtoisesti voidaan pitää lyhyt palaveri, jossa ideoidaan vapaasti erilaisia uhkia, jotka organisaatiota voisivat koskettaa. Myös teknologia-alan uutisia ja Kyberturvallisuuskeskuksen kybersäätä kannattaa hyödyntää skenaarioiden luomisessa.

Skenaarion laadinta alkaa tiiviillä ongelman kuvauksella, jossa määritellään skenaarion ydin. Esimerkiksi ”varastonhallintajärjestelmämme ei ole käytettävissä 72 tunnin ajan.” Tästä perusongelmasta rakennetaan harjoitusskenaario eli olosuhteet, joiden vuoksi ongelmat syntyivät, mutta myös seuraukset, joita ongelmat aiheuttavat. Näitä ongelmia harjoittelijoiden tulee ratkaista. Polku voi näyttää seuraavalta:
”Entinen työntekijämme on riitaantunut esimiehen kanssa. Työntekijällä on ollut pääsy varastonhallintajärjestelmän keskuspalvelimelle, johon hän on jättänyt haittaohjelman, joka tyhjentää palvelimen levyn keskiyöllä 1. maaliskuuta. Pelitapahtumat sijoittuvat 2. maaliskuuta aamulle.

Ensimmäiset työntekijät saapuvat logistiikkakeskukseen, mutta eivät pääse mm. tulostamaan lähetyslistoja tai tarkistamaan tilauksia. Logistiikkakeskuksen toiminta lamaantuu. Sisäänajoportti ruuhkautuu, koska kuljetusrekat eivät saa tarvitsemiaan tuotteita varastostamme. Häiriöitä aiheutuu myös lähialueen liikenteeseen.”

Toiminnallisessa harjoituksessa skenaariota ei tuoda heti harjoittelijoiden tietoon, vaan ensimmäinen syöte laaditaan perustuen esimerkiksi viestiin, jonka aamuvuorolaiset lähettävä tietohallintoon. Syötteet rakennetaan skenaarion mukaan, ja syötteiden tehtävä on tuoda skenaarion tapahtumat harjoittelijoiden tietoon harjoituksen kuluessa.

Työpöytäharjoituksessa skenaario voidaan kuvata harjoittelijoille harjoituksen alussa vaikkapa esimerkin tapaan. Tässä harjoitustyypissä osallistujat tunnistavat ja ratkaisevat skenaariosta nousevia ongelmia ja ongelmatilanteita.

6.2 Syötteet

Syötteet ovat informaatiota, jonka mukaan pelissä edetään. Syöte annetaan pelikeskuksesta pelaajille jollakin viestintävälineellä, syötteiden käyttö ja sisältö vaihtelevat pelityyppien välillä.

Käytännössä syöte on informaatiopaketti, joka tuo harjoittelijoille tietoa pelitapahtumista. Syöte voi olla:

- sähköpostiviesti
- valokuva
- kirje
- puhelu
- uutisartikkeli
- sosiaalisen median kirjoitus
- fyysinen esine
- tiedosto
- viranomaisilmoitus tai jokin muu skenaarion tapahtumia jollain tavalla kuvaava asia.

Syötteiden laatimisessa voi käyttää apuna esimerkiksi taulukkolaskentaohjelmaa, jolloin syötteet saadaan kerättyä helposti aikajärjestykseen. Taulukkoa voidaan käyttää pelin etenemisen seuraamiseen. Syötteet kannattaa rakentaa hierarkkisesti niin, että yhteen tapahtumaan liittyvät syötteet kerätään saman otsikon alle. Tämä selkeyttää harjoituksen suunnittelua ja auttaa tapahtumien hahmottamisessa.

Esimerkki syötetaulukon hierarkiasta:

Tapaus 1
Hyökkäys asiakastietokantaan

- Tapahtuma 1.1 - Tietomurto
  - Syöte 1.1.1 - Sähköposti
  - Syöte 1.1.2 - Puhelu
  - Syöte 1.1.3 - Haastattelupyyntö
- Tapahtuma 1.2 - Kiristys
  - Syöte 1.2.1 - Viranomaisilmoitus
  - Syöte 1.2.2 - Kiireellinen pyyntö

Tapaus 2
Kriittinen laiterikko

- Tapahtuma 2.1 - Tuotantojärjestelmän pysäytys
  - Syöte 2.1.1 - Puhelu
  - Syöte 2.1.2 - Sähköposti
- Tapahtuma 2.2 - Julkinen tiedote
  - Syöte 2.2.1 - Sähköposti

Taulukkoon kerätyt syötetiedot voivat sisältää muun muassa seuraavia asioita:

- järjestysnumero
- julkaisuaika
- tapahtuma, johon syöte liittyy
- syötteen kuvaus
- vastaanottaja
- lähettäjä
- syötteen tyyppi (sähköposti, puhelu, kirje, kuva...)
- syötteen sisältö (sähköpostiviesti, puhelun käsikirjoitus...)
- syötteen tila (pelattu, odottaa, hylätään)
- riippuvuudet toisista syötteistä.

Syötteet on valmistellaan etukäteen mahdollisimman valmiiksi, jotta ne voidaan lähettää viiveettä pelaajille. Pelikeskus seuraa koko harjoituksen ajan syötetaulukkoa, ja lähettää syötteinä toimivat viestit ennalta määriteltyyn aikaan tai reaktiona johonkin harjoittelijoiden tekemään

Klo	No.	Tapahtuma	Syötteen kuvaus	Lähettäjä	Vastaanottaja	Syötteen tyyppi	Syötteen sisältö	Tila
9:00	1	Pelin ohjaus	STARTEX	Pelikeskus	Kaikki harjoittelijat	Sähköposti	*** HARJOITUS *** HARJOITUS *** HARJOITUS *** Harjoitus on alkanut. Syötteet tullaan lähettämään tästä sähköpostiosoitteesta. *** HARJOITUS *** HARJOITUS *** HARJOITUS ***	Pelattu
9:30	2	Häiriö kirjaamossa	Haittaohjelma	Pelikeskus	Tietohallinto	Sähköposti	*** HARJOITUS *** HARJOITUS *** HARJOITUS *** From: jukkis@gmail.com To: atk-tuki@organisaatio.fi Subject: Kirjaamon kone jumissa - apua! Moi, Meillä näyttää olevan joku ongelma tän kirjaamon koneen kanssa, ei saada sitä auki, se näyttää jotain ihmeellistä kuvaa. Pääsiskö joku kattomaan tätä? Ollaan täällä Loimaan toimipisteellä. Mut saa kiinni numerosta 044 xxx xxxx. Sähköposti ei toimi, niin lähetän tän nyt omastani. Terveisin, Jukka Järvinen Kirjaamo *** HARJOITUS *** HARJOITUS *** HARJOITUS ***	Odottaa

päätökseen tai toimenpiteeseen. Syötteitä laadittaessa on hyvä huomioida, että yksittäisen syötteen käsittelyssä voi harjoittelijoilta kulua yllättävän paljon aikaa, joten tarkkaa aika-arviota yksittäisen syötteen käsittelylle on mahdoton antaa, mutta syötteiden käsittelyyn kuluva arvioitu aika pitää huomioida peliä suunnitellessa. Harjoittelijoiden oletettuja toimenpiteitä voi listata syötteen alle, minkä perusteella voi arvioida, kuinka paljon aikaa syötteiden väliin on syytä jättää. Syötteiden määrä on pidettävä kohtuullisena.

Harjoittelijajoukko koostuu usein eri toimialojen asiantuntijoista tai johtajista. Tällöin esimerkiksi tietohallinnolle voidaan kohdistaa yksi syöte ja viestinnälle toinen samanaikaisesti. Eri toimintoihin kuuluvat harjoittelijat voivat pelata rinnakkain tapahtumia, joissa tarvitaan erityisesti heidän asiantuntemustaan. Laadukkaasti suunnittelussa pelissä rinnakkain pelattavat syötteet liittyvät toisiinsa ja ohjaavat harjoittelijat tekemään yhteistyötä, mutta myös hoitamaan omaa tehtäväänsä.

Syötteiden laatimisessa vain mielikuvitus on rajana. Kriisijohtamisen harjoituksessa voidaan yhtenä syötteenä pelata esimerkiksi yhteydenottoja journalistien kanssa. Harjoittelijoiden luokse voidaan lähettää jopa toimittaja kameramiehen kanssa ottamaan reaaliaikainen haastattelu pelitilanteen tapahtumista. Erilaiset syötteet antavat mahdollisuuden harjoitella monenlaisia taitoja, joita kriisiin johtavan kyberhäiriön selvittämisessä vaaditaan.

6.3 Taustakuvaukset

Jos harjoitus sijoittuu todellisuudesta poikkeaviin olosuhteisiin, harjoitusskenaarion tueksi voidaan tuottaa taustakuvausmateriaalia (ns. ”state of the world”), eli lisätietoa harjoitusmaailmasta. Tyypillisesti harjoitus pelataan organisaation nykyisessä ja todellisessa toimintaympäristössä, tällöin taustakuvauksia ei tarvitse laatia.

Taustakuvauksissa voidaan käyttää esimerkiksi uutisia kiristyneestä poliittisesta, taloudellisesta, ympäristöllisestä tai sosiaalisesta tilanteesta, jotka eivät vaikuta pelin sisältöön suoraviivaisesti. Näin voidaan ohjata ja rajata harjoittelijoiden päätöksenteon vaihtoehtoja ja elävöittää peliä. Taustatietoa voi antaa harjoittelijoille jo etukäteen motivaation ja eläytymisen virittämiseksi.

Johdatuksena harjoitukseen toimii esimerkiksi etukäteen valmisteltu uutislähetys, joka esitetään harjoittelijoille juuri ennen harjoituksen alkua. Lähetyksessä voidaan uutisoida joko suoraan harjoittelevaa organisaatiota koskevista asioista tai olosuhteisiin liittyvistä taustatiedoista.

6.4 Harjoituksen viestintä

Harjoituksen keskeiset asiat toimitetaan harjoittelijoille sekä muulle organisaatiolle etukäteen valmisteltujen viestien välityksellä.

Harjoituksesta laaditaan yleinen tiedote, joka jaellaan organisaation sisällä. Tiedotteessa kerrotaan harjoituksen järjestämisajasta ja -paikasta sekä ilmoitetaan kutsutut osallistujat. Harjoituskutsu pitää lähettää riittävän ajoissa. Näin saadaan vahvistus harjoittelijoiden osallistumisesta ja heidän sitovat ilmoittautumisensa.

Viikko tai kaksi ennen harjoitusta harjoittelijoille lähetetään harjoitusohje, joka sisältää tiedot harjoituksen käytännön järjestelyistä, harjoituksen tavoitteet, osallistujat sekä harjoituspäivän aikataulun.

Harjoituksen jälkeen osallistuneille lähetetään kiitosviesti ja yhteenveto harjoittelusta sekä kerätystä palautteesta. Myös harjoittelevalle organisaatiolle on hyvä laatia lyhyt tiedote harjoituksen lopputuloksesta ja kerätystä palautteesta. Harjoituksesta kannattaa kirjoittaa myös julkinen tiedote, sillä harjoittelu vahvistaa organisaation julkista kuvaa kyberhäiriöihin vakavasti suhtautuvana toimijana.

Viestinnän merkitys korostuu erityisesti toiminnallisissa harjoituksissa, joissa keskeistä on harjoittelijoiden ja pelikeskuksen välinen viestintä. Pelikeskuksella tulee olla käytössään vähintään harjoitukselle varattu sähköpostilaatikko sekä puhelinnumero, joka toimii pelikeskuksen ”vaihteena”. Vaihteesta voidaan pyytää puhelimeen kuka tahansa, jonka kanssa harjoittelijat haluavat keskustella. Pelikeskuksen vastuulle jää pelata pyydetty rooli puhelimessa tai todeta, ettei pyydetty henkilö ole tavattavissa.

Pelikeskuksessa eri rooleja pelaaville voidaan vaihteen lisäksi varata omat puhelinnumerot, jolloin pelikeskuksen edustajat voivat keskustella eri harjoittelijoiden kanssa samanaikaisesti.

Harjoitukseen osallistuville viranomaisille voidaan järjestää oma yhteisnumero, josta saadaan tarvittaessa kiinni poliisi, Kyberturvallisuuskeskus tai muu viranomainen, jonka tukea harjoituksessa tarvitaan. Käytetyt puhelinnumerot ja sähköpostit kerätään pelin puhelinluetteloon, joka tulostetaan harjoittelijoiden käyttöön. Muita yhteystietoja ei harjoituksessa saa käyttää, siksi luetteloon kerätään myös harjoitukseen tukitehtävissä tai etäyhteydellä osallistuvien yhteystiedot.

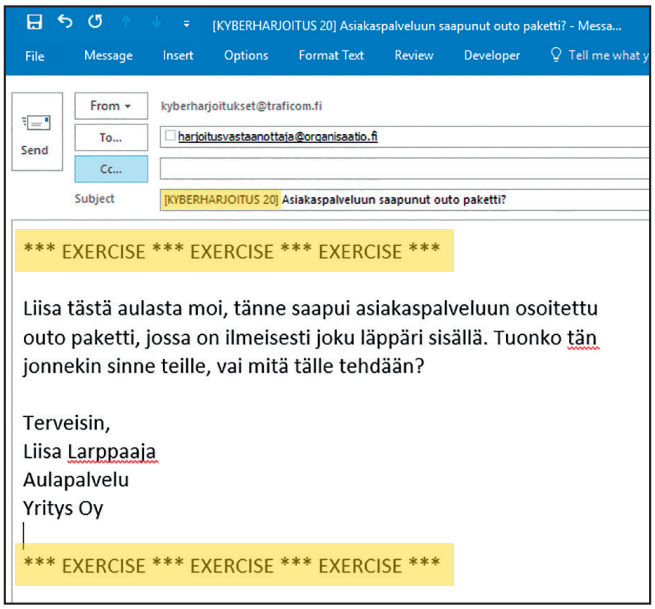
Pelikeskuksen sähköpostilaatikkoa on seurattava jatkuvasti harjoituksen ajan. Saapuneet sähköpostit on luettava ja niihin on vastattava viiveettä ja johdonmukaisesti. Jos syötteet välitetään harjoittelijoille sähköpostiviesteinä, sähköpostilaatikkoa käsittelevä pelikeskushenkilö voi myös lähettää syötteet.

6.5 Harjoitusmateriaalin merkitseminen

Harjoitukseen liittyvät viestit ja asiakirjat on merkittävä selkeästi, jotta ne tunnistetaan harjoitusmateriaaliksi. Esimerkiksi asiakirjojen ala- ja ylätunnisteisiin kannattaa lisätä HARJOITUS-merkintä punaisella fontilla.

Myös kuvitteellisia henkilötietoja sisältäviä asiakirjoja on hyvä käsitellä harjoituksessa tietosuojaa koskevan lainsäädännön mukaisesti. Tarpeettomat asiakirjat on syytä tuhota harjoituksen jälkeen niiden suojausluokituksen mukaisella tavalla, sillä harjoitukseen liittyvät dokumentit saattavat sisältää myös aidosti arkaluontoista tietoa.

Vakiintuneen käytännön mukaisesti sähköpostit voidaan merkata esimerkin mukaisella tavalla. Harjoitukseen liittyvät merkinnät korostettu:



Saapuneen viestin otsikko on merkitty harjoituksen tunnisteella. Näin harjoitukseen liittyvät viestit löydetään ja voidaan suodattaa helposti.

Viestin sisältökenttä aloitetaan harjoitusviestin selkeästi merkitsevällä tunnuksella, jossa voi lukea ”exercise” tai ”harjoitus”. Sisältökenttä myös päätetään harjoituksesta kertovalla tunnisteella.

Selkeä merkitseminen on tärkeää harjoitushygienian vuoksi. Asiayhteydestään irrotettuna harjoitukseen liittyvä viesti voidaan tulkita virheellisesti. Harjoitusviestin sisältökentässä on hyvä lukea selkeästi, keneltä viesti on tullut, sillä viestit lähetetään tyypillisesti pelikeskuksen sähköpostiosoitteesta.

6.6 Harjoituksen keskeyttäminen

Joissakin tapauksissa harjoitus on syytä keskeyttää. Näin voi käydä, jos organisaatiota kohtaa kesken harjoituksen todellinen kriisi. Tällöin voidaan käyttää tunnussanaa ”tosivaara”, jolla viestitään, että nyt käsiteltävä ongelma ei liity harjoitukseen.

Harjoituksen keskeyttämiseen liittyvät asiat merkitään harjoituksen dokumentaatioon. Keskeytettyä harjoitusta ei yleensä jatketa, sillä se häiritsee keskittymistä harjoituksen sisältöön. Tosielämän tapahtumat ja harjoitustapahtumat saattavat sekoittua harjoittelijoiden mielessä, ja harjoituksen lopputulos kärsii.

6.7 Harjoituksen toimintaympäristön mallintaminen

Harjoitusympäristön simuloinnilla tai mallintamisella tarkoitetaan tosielämässä olevien toimintojen ja resurssien esittämistä pelin kontekstissa mahdollisimman uskottavalla tavalla. Esimerkiksi medialähteitä tai sosiaalista mediaa voidaan mallintaa tarkoitukseen soveltuvilla ohjelmistoilla tai laatimalla niistä näköisversioita.

Julkisen viestimisen mallintaminen on melko suoraviivaista, sillä viestintä on pääsääntöisesti yksisuuntaista. Esimerkiksi lehdistötiedotteen laatimiseen ei työpöytäharjoituksessa tarvita teknisiä ratkaisuja. Toiminnallisessa harjoituksessa pelikeskus voi vastaanottaa harjoittelijoiden laatimia tiedotteita ja laatia syötteitä niiden perusteella.

Median, ja erityisesti sosiaalisen median mallintaminen, vaatii jo teknistä ympäristöä. Tähän käyttöön sopivat erilaiset harjoitussimulaattorit, joiden kautta on mahdollista viestiä sosiaalisessa mediassa ja mallintaa myös muuta viestintää. Myös erilaiset pikaviestin- tai julkaisuohjelmistot ovat mahdollisia, jos niitä osataan käyttää luovasti ja soveltaen.

Teknisessä harjoituksessa mallinnetaan tekninen toimintaympäristö, jossa harjoitustapahtumat pääasiassa toteutetaan. Markkinoilla on olemassa useita harjoitusalustoja, joissa palvelimet ja työasemat mallinnetaan alustan päällä. Usein alustoille on rakennettu valmiiksi useita erilaisia malliharjoituksia, joihin kannattaa tutustua.

Teknisen harjoituksen järjestäminen edellyttää simulointia erilaisilla järjestelmillä harjoitusympäristön luomiseksi, mutta myös toiminnallisessa harjoituksessa voi käyttää simulaattoria pelitarinan kuljettamiseksi. Simulaattoreilla voidaan varmistaa, että harjoittelijat saavat harjoituksessa tarvittavat tiedot käyttöönsä samanaikaisesti.

Markkinoilla on valmiita ratkaisuja juuri harjoituksen simulointiin. Yksinkertaisen harjoitussimulaattorin voi rakentaa vaikka ilmaisesta WWW-julkaisualustasta, johon luodaan ajastettuja syötteitä artikkeleina. Tosin tällaisesta ratkaisusta puuttuvat markkinoilla olevien harjoitussimulaattorien erityisesti harjoituskäyttöön suunnittelut ominaisuudet.

6.8 Teknisen harjoituksen tiimit

Isoissa yhteisharjoituksissa, joissa pelataan teknisessä ympäristössä, käytetään yleisesti värikoodeja eri tiimien roolien ja tehtävien määrittelyyn. Yleisimmät tiimivärit ovat punainen, sininen, valkoinen ja vihreä. Myös purppuraa, keltaista, harmaata tai muita värejä voi käyttää pelin ja tarpeen mukaan. Tiimien värikoodikohtaiset tehtävät määritellään yleensä harjoituksen

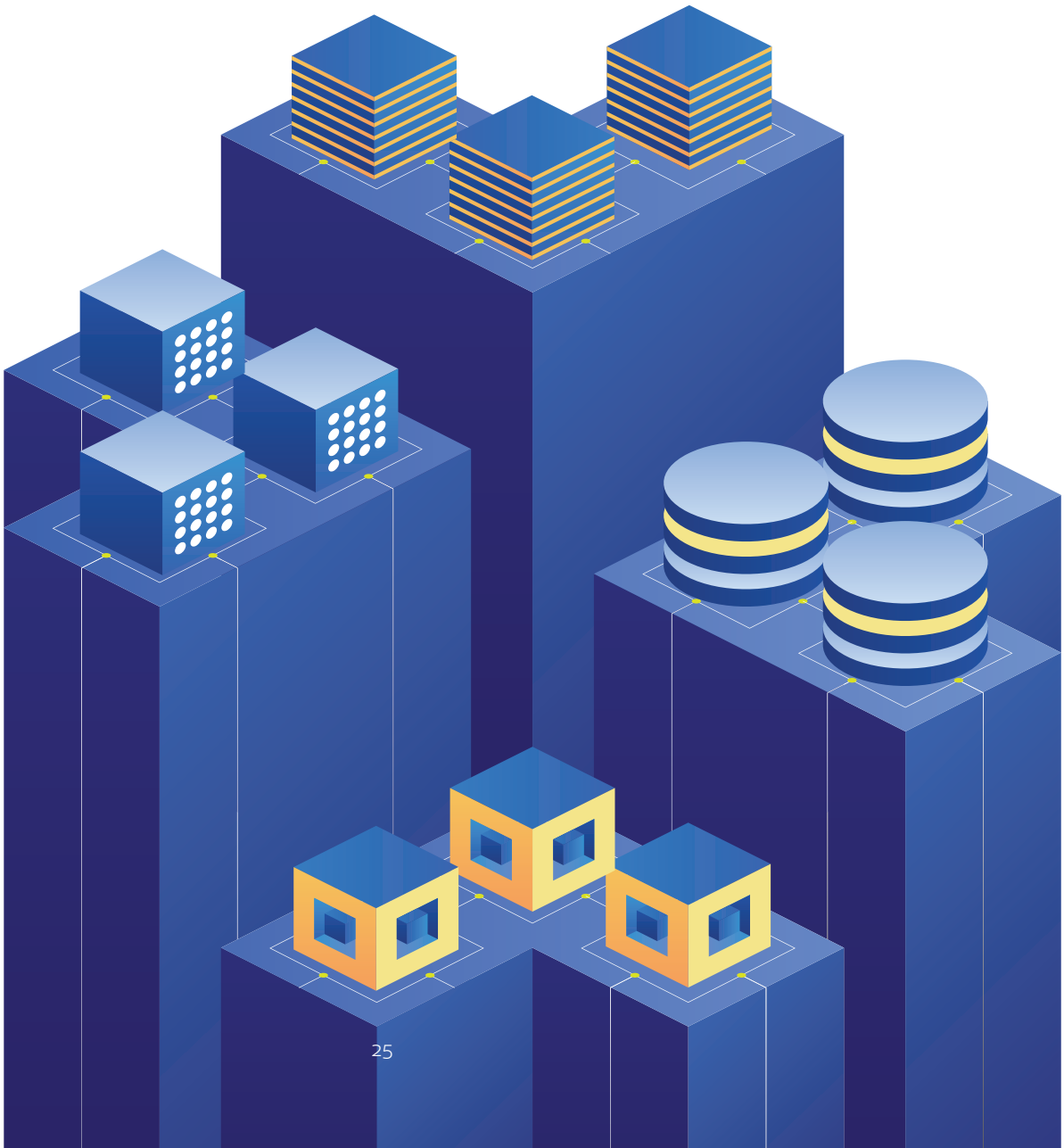
dokumentaatiossa, sillä punaista tai sinistä lukuun ottamatta värimäärittelyille ei ole vakioitua kansainvälistä tulkintaa.

Yleisen käytännön mukaisesti varsinaiset harjoittelijat tunnetaan sinisenä tiiminä. Laajoissa yhteisharjoituksissa sinisiä tiimejä voi olla useita. Näissä tilanteissa siniset tiimit voivat kilpailla keskenään pisteistä, joita onnistunut järjestelmien puolustaminen kerryttää.

Sinisen tiimin vastustajana on punainen tiimi. Punaisen tiimin tehtävänä on pyrkiä ennalta asetettuihin tavoitteisiinsa, esimerkiksi ottamaan haltuun ja hallitsemaan sinisen tiimin suojaamaa teknistä järjestelmää.

Punaisen tiimin tehtävänä on asettaa sinisselle tiimille haaste, joka mukautuu puolustajien toimien ja vastamenetelmien mukaisesti. Punainen tiimi koostetaan yleensä harjoituksen järjestäjistä tai näiden erikseen peliin kutsumista teknisistä asiantuntijoista.

Harjoituksen järjestäjät, harjoittelevien tiimien yhteishenkilöt, pelikeskusta tai muita pelin ylläpitäjiä edustavat henkilöt muodostavat valkoisen tiimin. Verkon ja peli-infrastruktuurin ylläpidosta ja pelinaikaisesta teknisestä tuesta vastaa vihreä tiimi.



7 Harjoituksen analysointi – opit hyötykäyttöön

Jos harjoitus on huolellisesti analysoitu, siitä saadaan parhaat hyödyt irti. Tässä työssä keskeinen rooli on tarkkailijoilla. Lopulta harjoituksen osallistujien, järjestäjien ja tarkkailijoiden huomiot yhdistämällä saadaan harjoituksesta monipuolinen kuva, jota voidaan käyttää jatkossa kehitystyön pohjana. Analyysivaihe kannattaa mieltää harjoituksen tärkeimmäksi vaiheeksi.

Kehityskohteiden tunnistamisen lisäksi analyysivaiheessa kirjataan konkreettiset toimenpiteet, joilla harjoituksen kehityskohteisiin puututaan. Toimet on syytä aikatauluttaa ja seurata, etteivät ne jää tekemättä.

Itse harjoitustapahtuma nostaa kriisien ja poikkeustilanteiden hallinnan tunnetta, mutta valitettavan usein nämä opit jäävät yksittäisten henkilöiden varaan. Harjoituksen oppien tuominen koko organisaation hyödyksi vaatii, että toimintaa todella muutetaan. On hyvä muistaa, että jo harjoituksen suunnitteluvaiheessa voidaan tehdä havaintoja, joiden perusteella organisaation toimintaa voidaan kehittää.

Harjoituksen tavoitteita asetettaessa arvioidaan, mikä toiminta harjoituksen aikana kehittyy. Oletus voi pitää paikkansa tai harjoitus voi tuoda esiin täysin uusia ja yllättäviä kehittymisen väyliä ja kohteita. Molemmat lopputulokset ovat

hyödyllisiä. Tavoitteiden tehtävänä on ohjata harjoituksen suunnittelua ei rajoittaa sen tuomia hyötyjä.

Harjoituksen päätyttyä järjestetään välitön palautetilaisuus, jossa harjoittelijat ja järjestäjät voivat tuoda ilmi ensivaiheen näkemyksensä ja huomionsa harjoituksen onnistumisesta. Samalla saadaan kerättyä näkemyksiä itse harjoituksen järjestämisestä ja purettua harjoitustilanteen aiheuttamaa jännitystä. Usein harjoittelijoilla on myös kysymyksiä, joita harjoituksen aikana ei ole pystynyt esittämään. Pelikeskuksen edustajan kannattaa varautua avaamaan harjoituksen toteutusta, tarinaa ja taustoja harjoittelijoille sekä perustelemaan harjoituksessa tehtyjä valintoja.

Osallistujilta ja järjestäjiltä on hyvä pyytää myös kirjallista palautetta. Vapaa teksti tai lomake, jolla voidaan myös mitata numeerisesti harjoituskokemuksen onnistumista, käyvät tähän tarkoitukseen hyvin.

Tarkkailijat välittävät palautteensa puhtaaksikirjoitettuna harjoituksen järjestäjälle. Jos palautetta varten on laadittu kyselylomake, sitä voidaan käyttää useamman kerran, jolloin samaan ”vastauspankkiin” saadaan tietoa harjoitusten välillä tapahtuneesta kehityksestä.

Yhteen kootut opit ja toimenpide-ehdotukset jaetaan harjoittelijoille tiedoksi. Kun osoitetaan, että harjoituksen avulla on löydetty kehityskohteita ja niiden perusteella tullaan muuttamaan käytäntöjä, se motivoi osallistumaan myös tuleviin harjoituksiin.

Kun opit on tuotu osaksi organisaation arkea, ne huomioidaan seuraavassa harjoituksessa. Esimerkiksi kehitetty prosessi on hyvä testata uudelleen toisissa olosuhteissa ja erilaisen haasteen edessä, jotta nähdään, oliko kehityssuunta oikea vai ei. Myös jo toimiva prosessi taipuu harjoitusskenaarioon, jonka avulla se voi muokkautua yhä paremmaksi.

Harjoittelun avulla etsitään heikkouksia prosesseissa ja toimintatavoissa, ei ihmisissä. On tärkeää, ettei harjoituksessa koeta vahvoja henkilökohtaisia epäonnistumisia. Harjoittelijoita pitää rohkaista toimimaan niin, että harjoituksessa voi turvallisin mielin kokeilla rohkeita ratkaisuja – kaoottisissakin tilanteissa.

Myönteiset kokemukset ovat tärkeitä harjoitusten jatkumolle. Erityisen hyvin suoriutuneiden harjoittelijoiden onnistumisia kannattaa nostaa esiin palautetilaisuuden yhteydessä.

7.1 Palautekyselyn suunnittelu

Kerätkää palautetta palautekyselyyn tarkoitetulla työkalulla. Muun muassa selainpohjaiset työkalut soveltuvat tähän hyvin. Työkalun avulla sama kysely voidaan helposti toistaa seuraavassakin harjoituksessa ja samalla arvioida harjoittelun kehittymistä. Kyselyn kautta palautteen antamiseen ja havaintojen koontiin saa myös lisää aikaa. Suullista palautetta se ei korvaa, mutta kirjallinen palaute sopii toisille paremmin.

Tavallisesti ulkopuolisen toimijan järjestämään harjoitukseen kuuluu palautekysely, jossa on kysymyksiä harjoituksen järjestelyihin ja organisaation häiriönhallintaan liittyen. Kyselyn päätavoitteena on kerätä tietoa itse kyberhäiriön selvittämisestä ja vasta toissijaisesti harjoitustapahtuman järjestämisestä.

Suullisen ja kriittisen palauteen antaminen harjoittelijajoukon edessä voi olla monelle mahdoton ajatus, mutta kirjallisesti sitä on helpompi antaa. Harjoitukseen kohdistuva kritiikki on syytä ottaa vastaan avoimin mielin, ja pyrkiä ymmärtämään, mihin palaute perustuu. Usein kritiikin taustalla oleva asia tai ilmiö voidaan seuraavassa harjoituksessa ottaa huomioon. Kriittinen palaute antaa mahdollisuuden parantaa harjoitustoimintaa, siksi se on positiivinen asia.

Harjoituksen eri osa-alueiden selkeät pistearviot helpottavat kokonaisuuden arviointia ja antavat mahdollisuuden raportoida harjoituskokemuksia myös eteenpäin selkeillä tunnusluvuilla. Harjoituksen palautekyselyn tulisi sisältää ainakin seuraavat osa-alueet:

Vastaajan rooli harjoituksessa
- järjestäjä, tarkkailija, harjoittelija, muut tuki tehtävät
- johto, tietohallinto, palveluntuotanto, muu yksikkö.

Harjoituksen käytännön järjestelyt
- tilajärjestelyt
- aikataulutus
- tiedottaminen
- tarjoilut.

Harjoituksen järjestämistapa
- Oliko harjoittelijajoukko valittu oikein?
- Oliko harjoitusmenetelmä sopiva?
- Oliko ohjeistus riittävä?

Harjoituksen pelillinen sisältö
- Oliko skenaario uskottava?
- Saatiinko harjoituksen aikana riittävästi tietoa tapahtumista?
- Olivatko taustakuvaukset uskottavia ja harjoitukseen soveltuvia?

Harjoituksen ammatillinen kehittävyys (subjektiivinen arvio)
- Voidaan esittää sarjana väittämiä: ”Koin harjoituksen hyödylliseksi” yms.
- Onnistuiko tilanteen johtaminen?
- Onnistuttiinko olemassa olevia häiriönhallinnan prosesseja kehittämään?

Halukkuus osallistua seuraaviin harjoituksiin
- ”Osallistun mielelläni jatkossakin harjoituksiin.”
- ”Suosittelen harjoituksia kollegoilleni.”
- ”Koin harjoittelun mielekkääksi.”

Avoin palaute harjoituksesta
- ruusuja, risuja, kehitysideoita, vapaa palaute.

Kun palaute on saatu, se koostetaan selkeäksi esitykseksi, josta poistetaan vastaajia yksilöivät tiedot, ja jaetaan harjoituksen osallistujille.

8 Harjoittelu osana kyber-turvallisuuden hallintaa

Organisaatiossa harjoitustoiminnan omistajuus vaikuttaa siihen, kuinka harjoittelua kehitetään. Kyberharjoittelu ei eroa merkittävästi muusta kriisitilanteiden harjoittelusta, joten jos organisaatiossa on jo olemassa kokemusta ja osaamista harjoittelusta esimerkiksi yritysturvallisuusyksikössä, kannattaa tätä hyödyntää kyberharjoittelun suunnittelussa.

Harjoitustoiminta on syytä viedä yksittäisistä tapahtumista keskeiseksi osaksi kyberturvallisuuden hallintaa. Näin voidaan jaksottaa ja testata organisaation jatkuvasti kehittyvää kyberturvallisuustoimintaa ja -kulttuuria. Harjoittelulla voidaan myös vahvistaa organisaation eri osastojen yhteistyötä.

Harjoituksia ei tarvitse toistaa samanlaisina muutaman kuukauden välein, vaan erilaisia harjoitustyyppejä voidaan koota vuoden mittaan sarjaksi, josta muodostuu selkeä kokonaisuus. Vuoteen voi esimerkiksi sovittaa muutaman työpöytäharjoituksen, yhden tai kaksi toiminnallista harjoitusta. Samalla voi harjoituttaa henkilökuntaa esimerkiksi tiiviimmin toistuvilla, simuloiduilla tietojenkalasteluhyökkäyksillä. Jos mahdollista, harjoitusvuoteen voi sovittaa myös yhden suurempaan yhteisharjoitukseen osallistumisen.

Kuinka laajasti organisaatio harjoittelee, riippuu tietenkin organisaation koosta ja resursseista. Pienemmissä organisaatioissa harjoittelumahdollisuudet ovat vähäisempiä kuin suuremmissa.

Harjoitusten järjestämisessä kannattaa hyödyntää myös yhteistyöverkostoja. Erilaiset yhteisöt, tiedonvaihtoverkostot tai asiantuntijaryhmät voivat toteuttaa harjoituksen, joka pelataan esimerkiksi yhteisen kokouksen tai seminaarin yhteydessä. Tapaamisissa voidaan myös valmistella harjoitus, jonka jokainen peluuttaa omassa organisaatiossaan. Lopulta tuloksia voidaan tarkastella ja vertailla yhdessä. Samanaikaisesti pelattava, organisaatiorajat ylittävä ja yhdessä suunniteltu kyberharjoitus avaa loistavia tilaisuuksia harjoitella yhteistoimintaa laajoissa häiriötilanteissa.

Strategisten tavoitteiden perusteella ohjataan yksittäisten harjoitusvuosien päätavoitteita, joista voidaan juontaa tavoitteet yksittäisille harjoituksille. Näin harjoittelu ei eristy muusta tietoturvatyöstä, vaan on keskeinen osa organisaation tietoturvatyötä.

Harjoittelua voidaan jakaa sisällöllisesti eri vuositeemoihin. Harjoitusteemojen ei tarvitse olla varsinaisesti kyberteemoja, sillä samoja harjoittelun menetelmiä voidaan käyttää myös erilaisten fyysisen maailman ja liiketoiminnan kriisien harjoitteluun. Usein kyberhäiriöihin liittyvien ongelmien vaikutukset ulottuvat kauas varsinaisista tietojärjestelmistä.

Parhaimmillaan säännölliseen harjoitteluun pääsee osallistumaan koko organisaatio. On selvää, että tietohallinto ja ylin johto harjoittelevat eri tavalla ja eri asioita, mutta molempien harjoittelu on merkityksellistä, tärkeää ja osa hyvin suunniteltua kyberturvallisuuden hallintaa.

8.1 Pitkäjänteinen suunnittelu

Seuraavan harjoitusvuoden suunnittelu kannattaa aloittaa hyvissä ajoin keräämällä seuraavalle vuodelle pääteemat, joihin liittyen organisaation kyberturvallisuustyötä halutaan kehittää.

Vuosikohtainen aihelista ja aikataulutus, jonka perusteella voidaan muodostaa harjoittelun vuosikello, voi olla isossa organisaatiossa esimerkiksi seuraavan kaltainen:

Maaliskuu 2020,
työpöytäharjoitus
- aihe: tuotantojärjestelmän pitkäkestoinen toimintahäiriö, varamenetelmien testaus
- harjoittelijat: tuotantopäälliköt, linjaesimiehet, viestintä.

Toukokuu 2020,
tekninen harjoitus
- aihe: hyökkääjän toimien tunnistaminen ja lokitus tuotantojärjestelmässä
- harjoittelijat: SOC, tietohallinto.

Kesäkuu 2020,
työpöytäharjoitus:
- aihe: keskeinen laitetoimittaja lopettaa toimintansa tai myydään ulkomaille
- harjoittelijat: johto, viestintä.

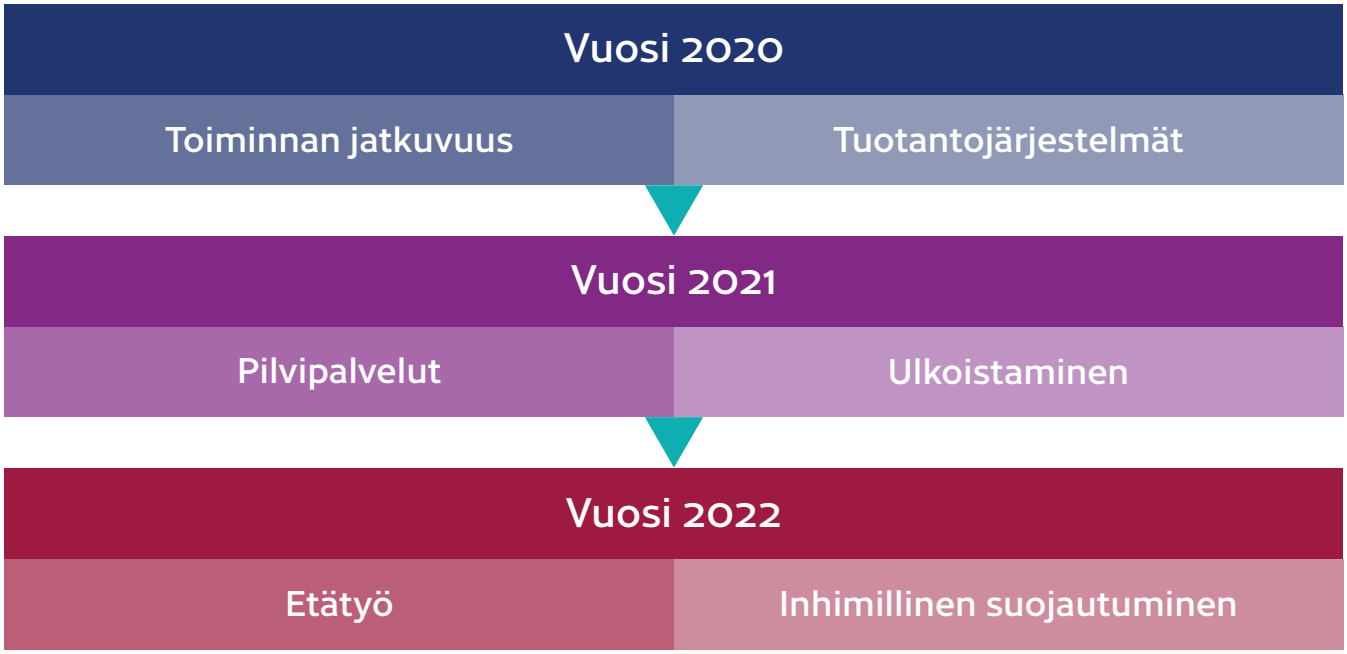
Syyskuu 2020,
tekninen harjoitus
- aihe: varmuuskopioiden palautusharjoitus
- harjoittelijat: tietohallinto.

Marraskuu 2020,
johdon toiminnallinen harjoitus
- aihe: tietomurto tuotantojärjestelmään, toimintahäiriö, sisäpiirin tietoturvauhka
- harjoittelijat: johto, major incident, management-tiimi, viestintä.

Esimerkissä X vuoden 2020 harjoituksissa keskitytään tuotantojärjestelmän toimintavarmuuden takaamiseen ja testaamiseen. Harjoituksilla on teemallinen yhteys, mutta ne harjoituttavat organisaation eri osia. Harjoitusvuoteen on kerätty työpöytäharjoituksia, teknisiä harjoituksia ja toiminnallisia harjoituksia. Yhteiseen teemaan perustuen harjoitukset tukevat toisiaan ja muodostavat selkeän kokonaisuuden. Osa harjoituksista on kevyitä ja nopeita järjestää, mutta toiset vaativat hieman enemmän aikaa. Kevyempien ja raskaampien harjoitusten vuorottelu antaa mahdollisuuden harjoitella monipuolisesti koko vuoden. Säännöllinen sykli pitää harjoituksessa käsiteltävät aiheet mielessä pitkin kalenterivuotta.

Vuoden kantavaksi teemaksi voidaan valita abstrahoitu kokonaisuus, kuten ”tietosuoja” tai ”tekninen tietoturva”. Organisaation oma riskienhallintatyö, toimintaympäristö ja sen muutokset antavat suuntaa teemoja valittaessa. Teemoille voidaan rakentaa ylivuotinen jatkumo, joka kytkee harjoitusvuosia toisiinsa luontevalla tavalla. Vuosittaiset teemat auttavat myös suuntaamaan tietoturvallisuustyötä, jolloin teeman mukaiset tietoturva-asiat nousevat paremmin esille.

Jokainen organisaatio laatii omat vuosikohtaiset tavoitteensa ja harjoitussyklinsä perustoimintansa ympärille. Yllä olevassa esimerkissä vuosikohtaisia teemoja on valittu kaksi, mutta valinnat pitää tehdä omien tarpeiden mukaisesti. Vuosikohtaisia teemoja voidaan edelleen purkaa tavoitteiksi, organisaation tietoturvastrategian linjausten mukaisesti.



9 Loppusanat

Toivomme, että tästä ohjeesta on apua oman organisaatiosi kyberharjoittelun suunnittelussa ja käynnistämisessä. Harjoittelun aloittaminen on helppoa ja yksinkertaista, sillä harjoitusmenetelmistä yksinkertaisimmat voidaan siirtää ideasta käytäntöön minuuteissa.

Yksinkertaisista asioista aloittamalla voidaan vähitellen siirtyä kohti monimutkaisempaa, jolloin isomman harjoituksen pirullisten skenaarioiden ja lennokkaiden juonien keksimisestä voi tulla tietoturvavuoden kohokohta.

Lisätietoja harjoittelun järjestämisestä voit hakea muun muassa seuraavista julkisesti saatavilla olevista teoksista:

- Handbook for planning, running and evaluating information technology and cyber security exercises (Center For Asymmetric Threat Studies, Swedish National Defence College, 2011)
- Exercise Guidance Basic Manual – An Introduction to the Fundamentals of Exercise Planning (Swedish Civil Contingencies Agency MSB, 2009)
- Manual and script for organizing cyber crisis exercises based on Cyber Crisis Exercise OZON (SURF Utrecht, 2017)
- Planning an Effective Incident Response Tabletop Exercise (Secureworks, 2018).

9.1 Yhteystiedot

Kyberturvallisuuskeskuksen harjoitustoiminnan tukipalvelut ovat huoltovarmuuskriittisten organisaatioiden käytössä. Jos olette kiinnostuneet järjestämään ensimmäisen kyberharjoituksennei, löytämään sopivan yhteistyökumppanin harjoitustoimintanne tueksi tai kaipaatte apua harjoituksen järjestämiseen, ottakaa yhteyttä harjoitustoiminnan tukeemme sähköpostitse kyberharjoitukset@traficom.fi

9.2 Keskeiset käsitteet

Harjoitushygienia
Toimintatapa, jolla varmistetaan, ettei harjoituksen sisältö leviä harjoittelevan joukon tai tilan ulkopuolelle. Kts. kappaleet 5.5. Tilajärjestelyt ja 6.4 Harjoituksen viestintä.

Harjoitusohjelma
Organisaation laatima vuosittainen ohjelma, jossa kuvataan organisaation harjoittelu yleisellä tasolla. Harjoitusohjelmaan kerätään vuoden aikana suunniteltavat ja pelattavat harjoitukset. Kts. kappale 8.1 Pitkäjänteinen suunnittelu.

Harjoitussimulaattori
Harjoitustapahtumien kuvaamista varten laadittu tietojärjestelmä, jolla harjoitustapahtumat tuodaan harjoittelijoiden tietoon. Kts. kappale 6.7 Harjoituksen toimintaympäristön mallintaminen.

Harjoitusskenaario
Harjoituksen tapahtumista ja taustakuvauksista koostuva kokonaisuus, joka kuvaa harjoituksen sisällön. Myös pelkkä ”skenaario”. Kts. kappale 6.1 Harjoitusskenaario.

Harjoitustiimit (esim. sininen ja punainen tiimi)
Eri värein erotellut harjoituksen osallistujat ja järjestäjät, jotka toimivat harjoituksessa eri tehtävissä. Käytetään erityisesti teknisissä harjoituksissa. Kts. kappale 6.8 Teknisen harjoituksen tiimit.

Harjoitustyyppi
Harjoitusta varten valittu pelitapa ja -tyyppi. Esim. työpöytäharjoitus, toiminnallinen harjoitus tai tekninen harjoitus. Kts. kappale 3 Erilaisia harjoitustyyppejä.

Harjoitusympäristö
Tekninen ympäristö, jossa harjoitus toteutetaan. Harjoitusympäristönä voi toimia joko tietojärjestelmä tai yrityksen toimintakenttä. Teknisen harjoituksen käsite. Kts. kappale 3.4 Tekninen harjoitus.

Hot wash-up
Harjoituksen jälkeen välittömästi järjestettävä palautetilaisuus. Kts. kappale 7 Harjoituksen oppien seuranta.

Jälkianalyysi
Harjoituksen jälkeinen harjoituksen oppien kerääminen, tarkastelu ja käytännön toimenpiteiksi purkaminen. Kts. kappale 7 Harjoituksen oppien seuranta.

Kyberharjoitus
Turvallisuusharjoitus, joka keskittyy tietojärjestelmien tai -turvallisuuden häiriötilanteisiin ja niistä seuraaviin laajoihin vaikutuksiin organisaatiossa. Kts. kappale 2 Mikä on kyberharjoitus?

Pelaaja
Harjoituksen varsinainen osallistuja, harjoittelija. Kts. kappale 5.2 Harjoittelijoiden valinta.

Pelikeskus
Tila, josta käynnissä olevaa peliä ohjataan ja kuljetetaan eteenpäin. Kts. kappale 5.5 Tilajärjestelyt.

Pre-mortem
Juurisyyharjoitus, harjoitus jossa aloitetaan seurauksista ja etsitään niille mahdollisia juurisyitä. Kts. kappale 3.2 Juurisyyharjoitus.

Simulointi
Kuvitteellisten harjoitustapahtumien kuvaaminen harjoituksessa. Kts. kappale 6.7 Harjoitusympäristön mallintaminen.

STARTEX, ENDEX
Harjoituksen käynnistys- ja lopetuskäskyt, sanoista ”start exercise” eli ”käynnistä harjoitus” ja ”end exercise” eli ”lopeta harjoitus”. Harjoitus aloitetaan ja päätetään STARTEX- ja ENDEX-viesteillä.

State of the world, harjoituksen taustakuvaus
Harjoituksen lähtötilannetta kuvaava taustakertomus, jolla voidaan luoda poikkeavat olosuhteet harjoitusta varten. Kts. kappale 6.3 Taustakuvaukset.

Syöte (inject)
Harjoituksen yksittäinen, tarinaa kuljettava tapahtuma, viesti tai muu harjoittelijoille välitetty informaatio. Kts. kappale 6.2 Syötteet.

Syötetaulukko
Pelin syötteistä koottu kokonaisuus, joka muodostaa harjoituksen pelillisen sisällön. Kts. kappale 6.2 Syötteet.

Tarkkailija
Harjoituksen osallistuja, jonka tehtävä on havainnoida harjoitusta ja kirjata havaintonsa muistiin. Kts. kappale 5.4 Tukitehtävät ja tarkkailijat.

Tosivaara
Harjoituksen keskeyttämiseen käytettävä sana, jolla viestitään todellisesta ongelmasta tai vaaratilanteesta. Kts. kappale 6.4 Harjoituksen viestintä.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000
traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus