TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

HUOLTOVARMUUSKESKUS

Kyberharjoitusskenaariot 2021

Skenaarioesimerkkejä harjoituksen järjestäjälle

Traficomin julkaisuja
2/2021

Skenaariot

1 Tietojen jakaminen sosiaalisessa mediassa
2 Firmware-haavoittuvuus
3 Palvelunestohyökkäyksellä kiristäminen
4 Sosiaalisen median käyttäjätilin salasanavuoto
5 Maksujärjestelmän tietovuoto
6 Hajoavat kovalevyt
7 Vanhat palvelimet
8 IPv4 – IPv6
9 Tietoliikenneprotokollan haavoittuvuus
10 Tietomurto
11 Alihankkija vaihtaa omistajaa
12 Kriittisten tietojen dokumentointi
13 Riippuvuudet ulkoisista toimijoista
14 Valtiollinen vakoilu
15 Laaja tietoliikennehäiriö
16 Tunnelointiohjelman häiriöt
17 Tietoja sähköpostilla väärään osoitteeseen
18 Emotet
19 Kielletyt laitteet
20 Laajamittainen epidemia

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-731-0
ISSN 2669-8757

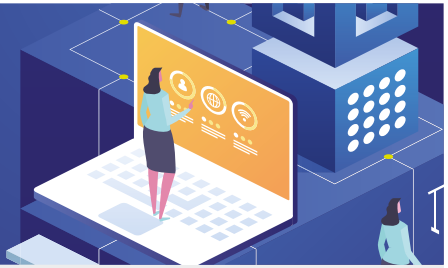
Kyberharjoitusskenaariot 2021

Tämä skenaariokokoelma kuvaa 20 erilaista kyberturvallisuuden poikkeamaa, joita voidaan käyttää kyberharjoituksen tapahtumankuvauksina. Kokoelma on laadittu yhteistyössä kumppaniyritysten asiantuntijoiden kanssa perustuen tosielämän kyberturvallisuuspoikkeamiin.

Skenaarioiden pohjalta voidaan suunnitella erilaisia harjoituksia, joissa skenaarion tapahtumia käydään läpi erilaisin menetelmin. Tapahtumakuvauksen lisäksi jokaiseen tapaukseen on kuvattu soveltamisohje sekä lisähaaste, jolla harjoituksen vaikeusastetta voi nostaa. Harjoitusta varten useampia skenaarioita voidaan myös yhdistää, jonka avulla harjoituksen haastavuutta voidaan myös lisätä.

Harjoituksen suunnittelussa voit käyttää apuna Kyberturvallisuuskeskuksen harjoitusohjetta: www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Skenaario 1
Tietojen jakaminen sosiaalisessa mediassa



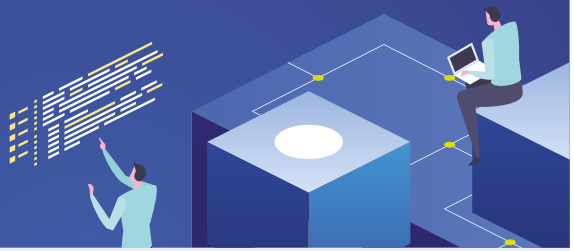
Organisaatiolla on pitkään ollut avoimen viestinnän kulttuuri ja työntekijät ovat mm. ”somettaneet” aktiivisesti työhön ja työyhteisöön liittyviä asioita.

Viime aikoina organisaation avainhenkilöt ovat saaneet henkilökohtaisilla some-kanavillaan paljon omituisia seuraajia ja tiedusteluja työasioihin liittyen. Kohdistettu tietojenkalastelu on lisääntynyt voimakkaasti. Henkilökunnan käyttämillä pikaviestikanavilla ei ole aktiivista käyttäjävalvontaa, vaikka siellä keskustellaankin työasioista. Kilpailijat ovat viime aikoina vieneet tarjouskilpailuja viime metreillä ja organisaation työntekijöitä on rekrytoitu kilpailijoiden palvelukseen paremmalla palkalla.

Soveltaminen: Skenaario soveltuu tietovuotoon, jossa organisaation työntekijät itse jakavat tarpeettoman paljon tietoa omasta työyhteisöstään ja työasioistaan niin, että se haittaa liiketoimintaa. Skenaariossa korostuvat organisaation sisäisen ja ulkoisen viestinnän säännöt ja rajoitteet, sekä ymmärrys liikesalaisuuden piiriin kuuluvasta tiedosta ja sen levittämisestä.

Lisähaaste: Organisaatiota vastaan on tehty rikosilmoitus yrityssalaisuuden loukkauksesta. On ilmennyt, että työntekijät ovat vuotaneet sosiaalisen median kanavilla NDA:n alaisia tietoja sopimuksiin liittyen.

Skenaario 2
Firmware-haavoittuvuus



Organisaation aktiiviverkkolaitteissa havaitaan vanhentuneita firmware-ohjelmistoja. Asiaa selvitettäessä ilmenee, että sisäverkossa on pitkään ilmennyt hitautta ja toimimattomuutta.

Kyseisen laitemerkin toimittaja on lisäksi ilmoittanut useista kriittisistä haavoittuvuuksissa eri tuotteissa, jotka pitää päivittää viipymättä.

Soveltaminen: Skenaario soveltuu organisaation tietoverkon tietoturvan (saatavuus) ja tietoverkon asianmukaisen dokumentaation tarkasteluun.

A) Miten tunnistaa laitteet, jotka tarvitsevat päivitystä
B) Missä laitteet ovat ja kuka niitä hallinnoi
C) Miten päivitys tehdään hallitusti, kuka sen tekee ja milloin

Lisähaaste: Organisaation verkkolaitteiden firmware-ohjelmistossa on ilmennyt nollapäivähaavoittuvuus. Varastossa olevat varalaitteet ovat samoja, kuin tuotantoverkon laitteet.

Skenaario 3
Palvelunestohyökkäyksellä kiristäminen

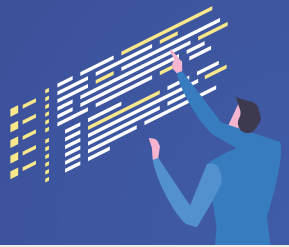
Yrityksen toimitusjohtaja saa kiristysviestin, jossa uhataan palvelunestohyökkäyksellä, jos hyökkääjälle ei makseta 5 bitcoinia kolmen päivän kuluessa. Kiristysviesti tulee toimitusjohtajalle lauantaiaamuna. Kiristysajankohta on organisaatiolle kriittinen, sillä yrityksen tarjoamien tuotteiden vuoden tärkein sesonki on juuri alkamassa.

Hyökkääjä vahvistaa uhkausta pienellä näytteellä ja saa organisaation verkkopalvelun hetkellisesti alas.

Soveltaminen: Skenaario soveltuu tietoverkon kapasiteetin ja varayhteysjärjestelyiden testaamiseen. Lisäksi skenaariolla voidaan harjoituttaa organisaation prosesseja, jotka liittyvät palvelusopimuksiin ja viranomaisten kanssa toimimiseen.

Lisähaaste: Verkkoyhteyksien palveluntoimittaja ilmoittaa, että verkkopesurikapasiteettiä ei laitepäivitysten takia ole lisättävissä viikkoon, mutta uuden sopimuksen puitteissa muista parannuksista voidaan neuvotella.

Skenaario 4
Sosiaalisen median käyttäjätilin salasanavuoto



Organisaation virallisen sometilin pääkäyttäjäoikeudet on liitetty työntekijän henkilökohtaiseen sometiliin. Työntekijä kirjautuu omilla tunnuksillaan haitalliselle sivustolle, jolloin myös yrityksen tunnukset joutuvat vääriin käsiin. Työntekijä ei itse huomaa käyttäjätunnusten vuotoa.

Organisaation sometilillä aloitetaan pian tapahtuneen jälkeen organisaation mainetta tahraava viestintäkampanja, joka uhkaa tulevaa yrityskauppaa.

Soveltaminen: Skenaariolla voidaan harjoitella yrityksen sisäistä ja ulkoista viestintää sekä maineen hallintaa. Harjoituksessa voidaan myös testata tietosuojaan liittyvien prosessien hallintaa.

Skenaariota voidaan käyttää myös käyttäjätunnusten hallinnan prosessien sekä organisaation sisäisten tapahtumapolkujen tunnistamiseen juurisyyharjoituksen muodossa.

Lisähaaste: Yrityksen työntekijä, jonka tilin kautta yritystili on kaapattu, ei ole tavoitettavissa viikkoon.

Skenaario 5
Maksujärjestelmän tietovuoto

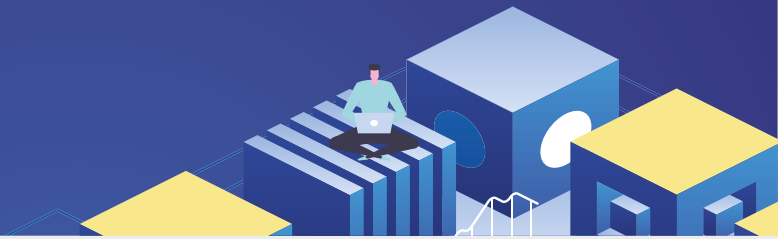
Organisaatio saa kiristysviestin, jossa uhataan maksujärjestelmässä olevien asiakastietojen julkaisulla.

Asiaa aletaan tutkimaan tarkemmin ja ilmenee, että maksetut laskut ovat ohjautuneen väärille ulkomaisille tileille jo jonkin aikaa. Tapahtumien alku näyttäisi sijoittuvan uuden maksujärjestelmän käyttöönottoon. Maksujärjestelmä tilattiin ulkopuoliselta konsultilta, jonka asiaan liittyvä toimeksianto on päättynyt kuusi kuukautta sitten.

Soveltaminen: Skenaario alkaa tilanteesta, jossa aletaan tekemään kiristykseen liittyvää uhka-arviota. Myöhemmin ilmenee, että kiristys oli ehkä vain hämäystä, jolla peiteltiin rahavirtojen ohjausta väärille tileille. Skenaarion tarkoituksena on harjoitella sopimuksiin ja turvalliseen tuotekehitykseen liittyviä prosesseja. Se ilmentää myös dokumentaation merkityksellisyyttä pitkän ajan jälkeen ongelmia selvitettäessä.

Lisähaaste: Tietosuojan piirissä olevia asiakastietoja julkaistaan Pastebinissä.

Skenaario 6
Hajoavat kovalevyt



Organisaatio suhtautuu epäilevästi pilvipalveluihin ja siksi se pitääkin yllä omia fyysisiä palvelimia kellarissa (on premise).

Eräänä aamuna töihin tullessa ylläpitäjä huomaa, että tiedostopalvelin on kaatunut ja alkaa selvittämään syytä. Ongelmaa selvitettäessä ilmenee, että myös muiden palvelinten RAID-levyjärjestelmissä on yksittäisiä kovalevyjä rikki. Muutama vuosi aiemmin organisaatio uusi lähes kaikki kovalevyt palvelimiinsa kertaheitolla. Nyt on ilmennyt, että kyseisessä tuotteessa on valmistusvirhe ja ne näyttävät hajoavan tietyn käyttötuntimäärän jälkeen. Valmistaja vahvistaa ongelmat.

Soveltaminen: Skenaariolla voidaan tarkastella tietoturvaan liittyvää tietojen eheyttä ja saatavuutta.

Aika ajoin on hyvä testata tallennusjärjestelmien vikasietoa, varatallennusjärjestelmiä sekä tiedon palauttamista. Näin tiedon saatavuus ja liiketoiminnan jatkuvuus voidaan taata paremmin.

Lisähaaste: Sama ongelma alkaa ilmenemään myös työntekijöiden työasemissa.

Skenaario 7
Vanhat palvelimet

Organisaatiolla on verkossa vanhoja palvelimia, joista on avoin yhteys internettiin. Osa palvelimista on täysin tarpeettomia ja unohdettuja, mutta osassa ajetaan ”mukavuussyistä” joitain ohjelmistoja, joita ehkä joku käyttää työasioissa. Ilmenee, että yksi tai useampi näistä palvelimista on joutunut tietomurron kohteeksi.

Operaattori ilmoittaa, että yrityksen hallitsemasta verkosta lähtee haittaohjelman aiheuttamaa liikennettä internettiin ja operaattori uhkaa sulkea yhteydet.

Soveltaminen: Skenaariossa tarkastellaan oman verkkoinfrastruktuurin ja -liikenteen tuntemusta sekä dokumentaatiota. Skenaariossa korostuvat verkkoon kytkettyjen laitteiden hallinta ja tunnistaminen. Myös oman verkkoliikenteen monitorointi ja tunteminen on olennaista, jotta voidaan erottaa epänormaalit tapahtumat normaalista verkkoliikenteestä.

Lisähaaste: Tutkittaessa ilmenee, että murrettu palvelin on aikanaan toiminut dokumentinhallinnan testipalvelimena, jossa on käytetty organisaation oikeaa tietoa sovellusten testaamiseen. Testaaminen on tehty konsulttiyhtiön toimesta, jonka toiminta on jo lopetettu.

Skenaario 8
IPv4 – IPv6

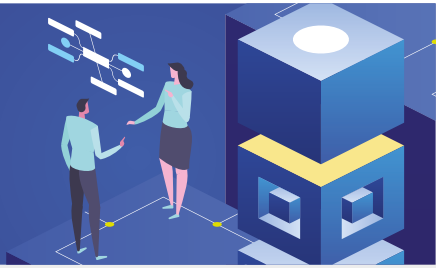
Organisaatiolla on perinteisesti ollut tiukat ja hyvin hallitut IPv4-palomuurisäännöt. Valkohattuhakkeri ilmoittaa, että kaikki automaatioverkon laitteet kommunikoivat verkkoon IPv6:lla ja löytyvät Shodanin avulla.

Soveltaminen: Skenaariossa korostuu oman verkkoliikenteen tunteminen ja verkkoon kytkettyjen laitteiden oikeiden asetusten tekeminen. Verkkoliikenteen perusasioiden ja tietoliikenneprotokollien ymmärtäminen auttaa organisaatiota tekemään asiat tietoturvallisesti.

Kysymyksiä tarkasteltavaksi: Voidaanko IPv6 ottaa pois käytöstä kaikista laitteista vai onko käytössä palveluita, jotka sitä ehdottomasti vaativat? Voiko muutokset tehdä vain palomuurilla? Miten vaikutuksia testataan?

Lisähaaste: Tuotantoverkon laajuuden ja monimukaisuuden vuoksi testiverkon pystyttäminen ei ole mahdollista. Muutokset joudutaan tekemään suoraan tuotantoverkkoon.

Skenaario 9
Tietoliikenneprotokollan haavoittuvuus



Mittaustietoa kentältä lähettävän IoT-laitteen tietoliikenneprotokolla osoittautuu niin haavoittuvaksi, että tietoliikenteen voidaan katsoa muuttuneen salaamattomaksi. Laitteita on käytössä satoja. Kaikkien laiteiden vaihtaminen ei kustannussyistä ole mahdollista.

Soveltaminen: Skenaariossa käsitellään IoT-laitteiden erityisominaisuuksiin liittyvää tietoturvaa. Lähtökohtaisesti IoT-laitteita ei ole suunniteltu tietoturva edellä. Erityisesti vanhoissa laitteissa saattaa olla suuriakin tietoturva-aukkoja, joiden paikkaaminen voi olla haastavaa.

Kysymyksiä tarkasteltavaksi: Onnistuuko laitteiden päivitys? Miten päivitys turvallisesti tehdään? Manuaalisesti vai esim. etäyhteydellä OTA-tyyppisesti (Over The Air)?

Lisähaaste: Skenaarion laitteiden käyttämää tietoliikenneprotokollaa ei voida tehdä tietoturvalliseksi. Keksi jokin muu keino.

Skenaario 10
Tietomurto

Organisaatiossa havaitaan tietomurto ja sen hallinnoimia arkaluontoisia asiakastietoja on vuotanut vääriin käsiin. Tekijän kiristää organisaatiota uhkaamalla julkaista tiedot jos lunnasvaatimusta ei täytetä.

Tietomurtoa tutkittaessa ilmenee, että tietoja viety usealla eri kerralla viimeisen kahden vuoden aikana. Haasteena lieneekin nyt on selvittää, että mitä on tapahtunut missäkin vaiheessa.

Soveltaminen: Skenaariossa käsitellään lokien hallintaa ja tutkimisen haasteita sekä organisaation teknistä kyvykkyyttä löytää tekijän jättämiä jälkiä omista tietojärjestelmistä. Skenaario myös testaa organisaation prosesseja ja toimintaa epäillyssä rikostapauksessa, jonka tekijä on ainakin toistaiseksi tuntematon.

Lisähaaste: Tietovuoto paljastuu medialle ja organisaatiolta odotetaan nopeita vastauksia kysymyksiin, kuka on teon takana ja mitä asialle aiotaan tehdä.

Skenaario 11
Alihankkija vaihtaa omistajaa

Organisaation käyttämä alihankkija, kuten pilvipalveluita tuottava yritys, myydään EU/ETA-alueen ulkopuolelle. Organisaation omiin asiakassopimuksiin on kirjattu, että tietoja säilytetään EU:n tietosuoja-asetuksen (GDPR) piirissä.

Soveltaminen: Skenaariossa käsitellään organisaation kriittisen tiedon hallintaa ja EU:n tietosuoja-asetuksen vaikutusta. Tietosuojan osalta myös organisaation käyttämät VPN-ratkaisut, AV-virustuotteet, kommunikointialusta voivat myös joutua tarkastelun alle.

Lisähaaste: Ilmenee, että pilvipalvelun ostaja on vihamielisiä pyrkimyksiä omaava valtio (tai muu epäilyttävän valtion vaikutuksen alla oleva taho). Kauppa tapahtuu pikaisella aikataululla.

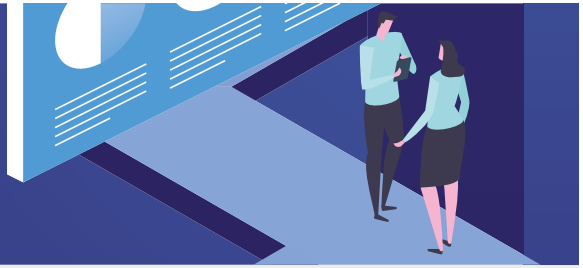
Skenaario 12
Kriittisten tietojen dokumentointi

Organisaation koko tietoverkko ja sen ylläpito on yhden henkilön käsialaa. Verkkoa 40 vuotta rakentanut asiantuntija ei ole pitänyt kirjallista dokumentointia toiminnastaan, vaan tieto on lähinnä hänen päässään. Henkilö joutuu sairaalaan pitkäksi aikaa.

Soveltaminen: Skenaariossa käsitellään dokumentaation tekemistä ja sen turvallista säilyttämistä ja saatavuutta. Organisaation toiminnan kannalta kriittisiä tietoja sekä toiminteita kannattaa jakaa. Turvaamalla tiedon saatavuus ja eheys kasvatetaan samalla organisaation resilienssiä.

Lisähaaste: Verkkoa ylläpitävä henkilö menehtyy sairaalassa, eikä hänen muistissa olevia tietoja ehditty dokumentoimaan.

Skenaario 13
Riippuvuudet ulkoisista toimijoista



Pilvipalvelussa on käyttökatko. Syyksi ilmoitetaan konfiguraatiovirhe. Yhteyksien palautuessa huomataan, että kaikki varmuuskopiot ovat korruptoituneet. Käyttökatko keskeytti myös juuri alkaneen varmuuskopioinnin, jonka seurauksena tuotantopalvelimen tiedostojärjestelmä koki häiriöitä ja osa tiedoista muuttui käyttökelvottomaksi.

Palvelun tarjoaja ilmoittaa, että heillä on tärkeämpiä asiakkaita etusijalla ja että tässä tapauksessa varmuuskopioiden palauttamiseen menee viikko.

Soveltaminen: Skenaariossa ilmenee oman verkonhallinnan ulkopuolinen ongelma. Tapahtuma ilmentää organisaation liiketoiminnan jatkuvuuden riippuvuutta ulkoisista tekijöistä, joihin ei aina välttämättä voida vaikuttaa. Miltä osin organisaation pitäisi pyrkiä tietojärjestelmien osalta omavaraisuuteen? Mitkä ovat niitä liiketoiminnan kannalta kriittisimpiä osa-alueita, joita ilman organisaatio ei pärjää? Pitääkö sopimuksia tarkentaa?

Lisähaaste: Palveluntarjoaja ilmoittaa, että organisaation varmuuskopiot eivät ole enää palautettavissa.

Skenaario 14
Valtiollinen vakoilu

Organisaation palkkaaman konsultin työntekijä on vieraillut ulkomailla työkannettava mukanaan. Konsultin kannettava tietokone kävi tullissa takahuoneessa verhojen takana ”räjähdeskannauksessa”, joka konsultin mukaan kesti luvattoman kauan.

Kannettavalla tietokoneella oli organisaation sopimuksia kolmannen osapuolen kanssa tehdyistä kriittistä yrityskaupoista. Kyseinen yrityskauppa on herättänyt kiinnostusta usean eri valtion taholta.

Soveltaminen: Skenaariossa käsitellään luottamuksellisen tiedon käsittelyä sekä fyysistä turvallisuutta. Organisaatioilla on usein haasteena valvoa, miten heidän omistamaansa tietoa käsitellään kumppaneiden tai alihankkijoiden toimesta.

Lisähaaste: Konsultti kertoo asiasta vasta jälkikäteen, kun organisaatio on jo tehnyt sitovia sopimuksia kolmannen osapuolen kanssa.

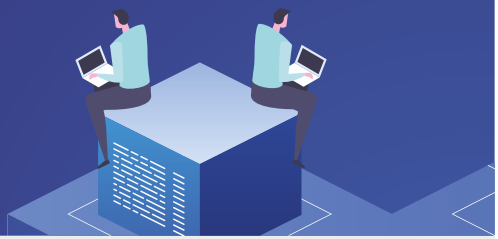
Skenaario 15
Laaja tietoliikennehäiriö

Laajamittainen häiriö usean eri toisiinsa kytkeytyvän toimialan tuotantoverkoissa. Seurauksena palveluiden kaatuminen (palvelunestotila). Asiaa tutkittaessa ilmenee viitteitä tietomurroista pitkällä aikavälillä.

Soveltaminen: Skenaariossa käsitellään tapausta, jossa eri toimijoiden infrastruktuurit leikaavat toisiaan ja häiriöt vaikuttavat suoraan toimitusketjujen toimintaan. Keskiöön nousee yksittäisten toimijoiden oma sisäinen kybertilannekuva, tiedon jakaminen ja siitä muodostuva yhteinen kybertilannekuva. Laajassa häiriössä myös viranomaisten toiminnan tunteminen saa tärkeän merkityksen.

Lisähaaste: Laaja häiriötila vaikuttaa palveluntarjoajien resursseihin, eikä kaikkia voida palvella heti.

Skenaario 16
Tunnelointiohjelman häiriöt



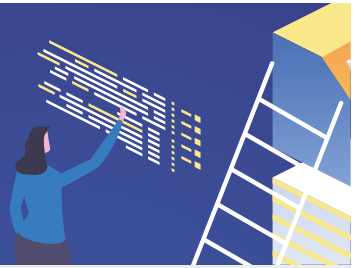
Organisaation käyttämässä VPN-ohjelmistossa ilmenee pakotetun päivityksen jälkeen epävakautta tai se ei käynnisty lainkaan.

Organisaation toiminnan kannalta kriittiset verkon sisäiset ohjelmistot eivät toimi tai niiden välittävään tietoon ei voi luottaa. Organisaation työntekijöistä muutoinkin yli puolet joutuu päivittäin tekemään töitä etäyhteyden välityksellä.

Soveltaminen: Skenaariossa käsitellään organisaation ohjelmistojen hallintaa ja esimerkiksi päivitysten toimivuuden varmistamista ennen niiden asentamista. Skenaariolla voidaan myös testata, mikä on organisaation kyky palata hallitusti ohjelmistojen hallinnassa aikajanalla taaksepäin.

Lisähaaste: Organisaation tuotantoyksikön henkilöstö ei pysty ohjaamaan etäsijoitettuja tuotantolaitteita turvallisesti, koska VPN-yhteyttä ei saada toimimaan lainkaan.

Skenaario 17
Tietoja sähköpostilla väärään osoitteeseen

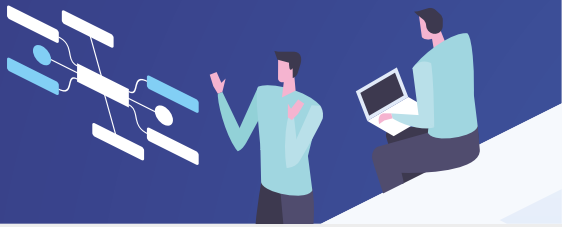


Organisaation tietohallinto lähettää tahattomasti työntekijöiden käyttäjätunnukset ja salasanat sähköpostilla väärään osoitteeseen organisaation ulkopuolelle. Asiaa selvitettäessä ilmenee, että samainen tietohallinnon työntekijä on aiemminkin lähettänyt arkaluontoisia tietoja samaan osoitteeseen, koska luuli sen kuuluvan toiselle henkilölle.

Soveltaminen: Skenaariossa tarkastellaan tahattoman sisäisen tietovuodon käynnistämää prosessia organisaatiossa. Tapahtumaa voi soveltaa miettimällä työntekijöiden oma-aloitteisuutta tietovuodon ilmoittamisessa, jos vuotanut tieto olisikin vähemmän sensitiivistä. Ilmoittaisivatko työntekijät tietovuodosta yhtä matalalla kynnyksellä, ja mitä he mainitsisivat ilmoituksessa?

Lisähaaste: Asiaa selvitettäessä ilmenee, että työntekijä on lähettänyt viestin omassa sähköpostiohjelmassa oikeaan osoitteeseen, mutta mitä ilmeisimmin sähköpostipalvelimella on haittaohjelma, joka muuttaa kohdeosoitteen.

Skenaario 18
Emotet

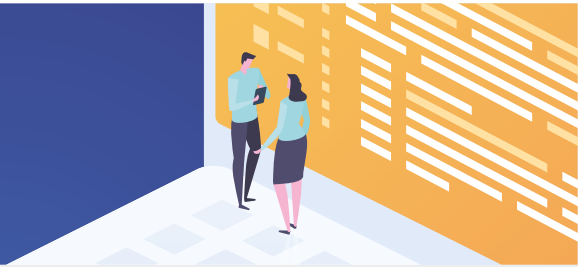


Ainakin yhdeltä organisaation työasemalta havaitaan epämääräistä verkkoliikennettä, jonka epäillään liittyvän Emotet-haittaohjelmaan.

Soveltaminen: Skenaariossa käsitellään organisaation havainnointikykyä ja kykyä löytää poikkeamia verkkoliikenteestä. Myös haittaohjelmatartunnan tekninen selvityskyky ja sen tutkinnan dokumentointi sekä työasemien uudelleen asennus ja toiminnan jatkuvuuden takaaminen korostuvat.

Lisähaaste: Havaintoja alkaa tulemaan kasvavaan tahtiin useilta työasemalta.

Skenaario 19
Kielletyt laitteet

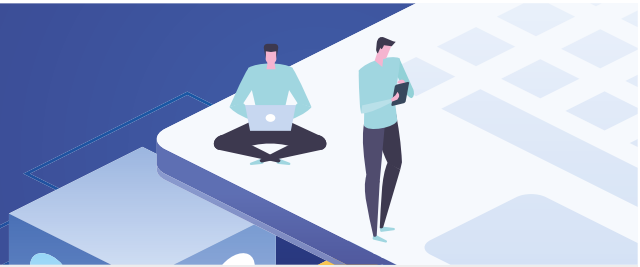


Organisaatiolla on turvallisuussopimus erään valtion viraston kanssa, joka liittyy organisaation tuottamiin palveluihin. Viranomaistaholta tulee kielto käyttää tietyn tuotemerkin tuotteita/laitteita. Organisaation toiminta ja sen tuottamat palvelut nojaavat vahvasti tämän tuotemerkin laitteiden käyttöön. Toiminnan jatkaminen edellyttää tuotteiden vaihtoa.

Soveltaminen: Skenaario haastaa organisaation liiketoiminnan jatkuvuuden ja sen käyttämän laitevalikoiman. Miten toiminnan resilienssiä parannetaan esimerkiksi hajauttamalla laitehankintoja ja käyttämällä usean toimittajan tuotteita? Voiko kieltoon perustuvasta laitteiden käytön lopettamisesta saada kompensaatiota valtiolta? Entä voiko yritys joutua maksamaan sopimussakkoa laitetoimittajalle sopimusten ennenaikaisesta päättämisestä?

Lisähaaste: Myös muihin toimijoihin kohdistuu samoja vaateita. Korvaavien laitteiden voimakkaasti kasvaneen kysynnän takia toimitusajat venyvät pitkiksi.

Skenaario 20
Laajamittainen epidemia



Laajamittainen epidemia pakottaa organisaatiot etätyökäytänteisiin, kun kokoontumista rajoitetaan. Organisaatioiden pitää järjestää nopeasti kaikille etätyövälineet ja antaa ohjeistus tietoturvalliseen etätyöskentelyyn.

20/20

Soveltaminen: Skenaario nostaa esiin jatkuvuudenhallintaan ja viestintään liittyviä asioita. Organisaatioiden toiminnan ja resurssien pitää olla joustavia ja normaaleille työskentelytavoille pitää olla kriisiaikana vaihtoehtoiset suunnitelmat.

Lisähaaste: Epidemia puhkeaa rajuna ja organisaation johtoryhmä joutuu ensimmäisenä eristyksiin, eikä voi hoitaa työtehtäviä kunnolla.

Yhteistyössä:

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus