TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

HUOLTOVARMUUSKESKUS

Kyberharjoitusskenaariot 2020

Skenaarioesimerkkejä harjoituksen järjestäjälle

Traficomin julkaisuja
121/2019

Skenaariot

1 Henkilötietojen tietovuoto
2 Automaatiojärjestelmän häirintä
3 Pitkäkestoinen hyökkäys
4 Salasanavuoto
5 Julkinen tietokantavuoto
6 Laskutushuijaus
7 Tuntematon USB-laite
8 Tuntematon laite verkossa
9 Saastunut ohjelmistokomponentti
10 Yritysvakoilu
11 Yrityskauppa
12 Käytöstä poistettu monitoimilaite
13 Domain-kaappaus
14 Ohjausdatan manipulointi
15 Palveluntarjoajaan kohdistuva palvelunesto
16 Kryptolouhintaa palvelimilla
17 Organisaatio haktivistiryhmän tähtäimessä
18 Valkohattuhakkeri ilmoittaa haavoittuvuudesta
19 Tuntematon tietoliikenne
20 Pitkäkestoinen sähkökatko

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-453-1
ISSN 2669-8749

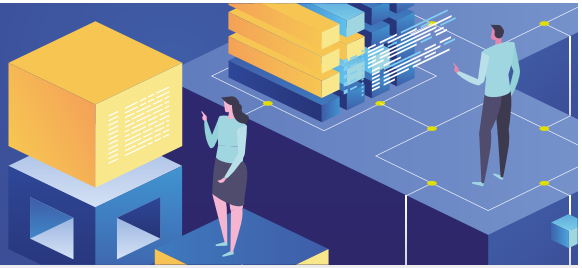
Kyberharjoitusskenaariot 2020

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

Skenaarioiden pohjalta voidaan suunnitella erilaisia harjoituksia, joissa skenaarion tapahtumia käydään läpi eri menetelmin. Tapahtumakuvauksen lisäksi jokaiseen skenaarioon on kuvattu soveltamisohje ja lisähaaste, jolla harjoituksen vaikeusastetta voidaan nostaa. Harjoituksen haastavuutta voi myös nostaa yhdistämällä useampia skenaarioita.

Harjoituksen suunnittelussa suosittelemme käyttämään Kyberturvallisuuskeskuksen harjoitusohjetta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Skenaario 1
Henkilötietojen tietovuoto



Tunnetun lehden toimittaja soittaa ja kertoo, että verkossa on esitystenjakopalvelussa ladattavissa organisaation sisäinen PowerPoint-esitys, johon on liitetty Excel-taulukko.

Taulukkoa muokkaamalla siitä paljastuu henkilöstöä koskevia arkaluontoisia tietoja, muun muassa palkka- ja työsuhdeasioihin liittyviä yksityiskohtia.

Tiedostoa on ladattu sivuston mukaan 127 kertaa.

1

Soveltaminen: Skenaario soveltuu tietovuotoon ja tietosuojaan liittyvien prosessien harjoitteluun. Skenaariossa korostuu myös ulkoisen ja sisäisen viestinnän merkitys. Taustalla on vahingossa verkkoon ladattu dokumentti, jota ei ole sanitoitu huolellisesti.

Lisähaaste: Vuotaneet tiedot sisältävät erittäin arkaluontoisia tietoja työntekijöistä, kuten terveystietoja. Joukossa on myös asiakkaiden liikesalaisuksiina pidettäviä tietoja.

Skenaario 2
Automaatiojärjestelmän häirintä

Automaatiojärjestelmän keskitetyssä hallintajärjestelmässä on ollut haavoittuvuus. Tuntematon hyökkääjä on onnistunut murtautumaan tuotantolaitteiston hallintaverkkoon. Hyökkääjä on muuttanut tuotantolinjaston parametreja hieman, mistä seuraa tuotteiden valmistuksessa laatuongelmia.

Hyökkäys huomataan kasvaneiden asiakasvalitusten ja tuotepalautusten kautta, kun laatuongelman syytä aletaan selvittää. Hyökkäys on jatkunut yli kuusi kuukautta.

2

Soveltaminen: Skenaario soveltuu tuotantojärjestelmien valvontaan liittyvien prosessien testaamiseen sekä jo tapahtuneen hyökkäyksen jälkiselvitysten arviointiin. Hyökkääjä on tehnyt pieniä muutoksia, minkä johdosta hyökkäystä ei ole heti havaittu.

Lisähaaste: Parametrimuutoksia on ollut useita. Hyökkääjä sabotoi laitteita niin, että niihin tulee huoltoa ja tuotannon seisokkia aiheuttavia vaurioita. Tuotteissa ilmenevät laatuongelmat aiheuttavat henkilövahinkoja.

Skenaario 3
Pitkäkestoinen hyökkäys

Harjoituksen vuoksi tehdyssä lokianalyysissa tulee ilmi seikkoja, jotka aiheuttavat kumppaniyrityksen tietoturva-asiantuntijassa ihmetystä.

Tarkempi lokianalyysi osoittaa, että organisaation verkkoon on tunkeuduttu jo vuotta aiemmin, ja hyökkääjät ovat hiljalleen keränneet ja siirtäneet omalle palvelimelleen organisaation tietoja, mm. henkilöstöön ja taloushallintoon liittyviä dokumentteja.

Aktiivisia vastatoimia ei ole aloitettu, eikä hyökkääjä tiedä tulleensa havaituksi.

3

Soveltaminen: Skenaario soveltuu tietomurron alkutoimien suunnitteluun. Skenaariossa korostuvat hallittu ja suunniteltu vaste havaittuun vakavaan poikkeamaan. Skenaarion osana voidaan harjoitella viranomaisten kanssa toimimista aktiivisen hyökkäyksen torjunnassa.

Lisähaaste: Hyökkääjä havaitsee, että hänet on huomattu, ja alkaa tuhota yrityksen tietoja ja peittää jälkiään poistamalla lokitietoja ja käytettyjä tunkeutumistyökaluja.

Skenaario 4
Salasanavuoto

Organisaation johtaja soittaa tietohallinnon päivystykseen illalla ja kysyy, miksi hänen matkapuhelimeensa on tullut tekstiviestitse useita monivaiheisen tunnistautumisen kertakäyttökoodeja.

Johtaja kertoo olevansa parhaillaan mökillä kalastamassa, ja ettei ole parhaillaan kirjautumassa mihinkään.

Autentikaatiopyynnöt vaikuttavat saapuvan organisaation VPN-järjestelmästä.

4

Soveltaminen: Skenaariossa kuvattujen tapahtumien perusteella voidaan epäillä, että ainakin toimitusjohtajan salasana on joutunut vääriin käsiin. Onnistuneen hyökkäyksen selvittäminen edellyttää salasanavuodon tutkimista ja epäilyttävien kirjautumisyritysten lähteen selvittämistä.

Lisähaaste: Toimitusjohtaja kertoo välittäneensä saamiensa ohjeiden mukaan kertakäyttökoodin tekstiviestillä ”asiakaspalvelulle”. Tapauksesta on viikkoja aikaa.

Skenaario 5
Julkinen tietokantavuoto

Organisaation viestintä saa kyselyn tunnetun lehden toimittajalta internetin keskustelupalstoilla leviävistä mahdollisista organisaation asiakastiedoista. Selvityksen jälkeen ilmenee, että tiedot ovat peräisin yrityksen tietokannasta.

Tietokantaa ylläpitää palveluntoimittaja. Tietokantaa hyödyntää organisaatio itse sekä kaksi organisaation asiakasta. Kaikilla kolmella on tietokantaan täydet oikeudet.

5

Soveltaminen: Skenaario alkaa tilanteesta, jossa tietojen lähde tunnetaan, mutta vuotokohta on epäselvä. Skenaarion avulla voidaan harjoitella monen käyttäjän järjestelmän suojaamiseen liittyviä seikkoja. Skenaariossa korostuu myös yhteisen tietoturvapolitiikan ja -ohjeiden noudattaminen monen toimijan ympäristössä.

Lisähaaste: Tietokantapalvelimien lokit ulottuvat vain kolmen viikon päähän, mutta data vaikuttaa vanhemmalta. Muut tietokantaa käyttävät tahot käyttävät EU:n ulkopuolisia maita palvelujen toteuttamiseen.

Skenaario 6
Laskutushuijaus

Taloushallinnosta huomataan, että 250 000 euron maksu on jäänyt saamatta. Erääntyneestä laskusta huomautettaessa asiakas toimittaa kopion maksamastaan laskusta.

Laskussa on väärä tilinumero, joka johtaa ulkomaalaiselle pankkitilille. Laskun saatteena on yrityksen sähköpostitililtä lähetetty viesti, jossa kerrotaan uudesta tilinumerosta.

Tietohallinnon selvityksissä ilmenee, että hyökkääjä on saanut haltuunsa pilvipalveluna käytetyn sähköpostin tunnukset, ja lähettänyt ”korjattuja” virheellisiä tilinumeroita useille asiakkaille.

6

Soveltaminen: Skenaario kuvaa BEC-huijauksen (Business Email Compromise), jossa hyökkääjä on onnistunut tunkeutumaan sähköpostijärjestelmään ja lähettää valelaskuja asiakkaille yrityksen nimissä. Hyökkäysmenetelmää edeltää tietojenkalasteluhyökkäys, jossa käyttäjätunnukset saadaan haltuun.

Lisähaaste: Laskuja on lähetetty kymmenille eri asiakkaille. Hyökkääjät ovat olleet sähköpostijärjestelmässä pitkään, ja ovat todennäköisesti saaneet käsiinsä yrityssalaisuuksia.

Skenaario 7
Tuntematon USB-laite

Työntekijä huomaa työpisteensä näytön takana sijaitsevassa USB-keskittimessä tuntemattoman laitteen.

Laite on kytketty langattoman näppäimistön vastaanottimen ja USB-keskittimen väliin. Laitteessa ei ole merkintöjä, eikä työntekijä tunnista sitä.

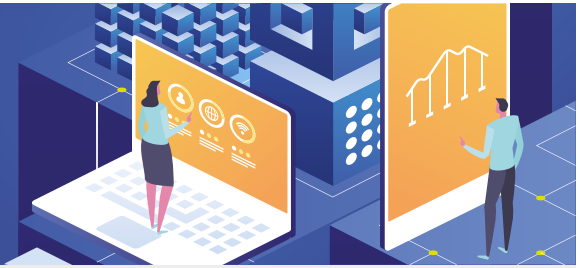
Työntekijä ei koske laitteeseen, vaan ilmoittaa asiasta tieto-hallinnolle ja pyytää toimintaohjeita.

7

Soveltaminen: Skenaariossa voidaan arvioida fyysisen turvallisuuden ja kulunvalvonnan merkitystä kybertoimintaympäristön suojaamiselle. Vakoilulaitteen käsittelyssä korostuu todistusaineiston säilyttäminen. Laitteen on voinut asentaa paikalleen joko yrityksen oma työntekijä tai muu tiloissa liikkuva henkilö, kuten siivooja tai huoltomies.

Lisähaaste: Työntekijä irrottaa laitteen ja vie sen kotiinsa tutkittavaksi. Työntekijä purkaa laitetta ja vioittaa sitä. Toimitilojen kameravalvonta tai kulunvalvonta ei ole toiminut tapahtuma-aikaan.

Skenaario 8
Tuntematon laite verkossa



Tuotantojärjestelmien käyttäjiltä tulee ilmoituksia, että tuotantodatassa on virheitä. Myös viimeisimmissä varmuuskopioissa havaitaan ongelmia.

Samaan aikaan organisaation tiloista löytyy tuntematon laite, joka on kytketty verkkoon sellaisen työaseman läheisyyteen, jolla työskentelee pääkäyttäjäoikeuksilla varustettuja työntekijöitä.

Kukaan ei tunnista laitetta. Laitteessa on useampi antenni, ja siinä olevat ledit vilkkuvat tiuhaan.

8

Soveltaminen: Skenaariossa korostuvat verkkoon kytkettyjen laitteiden hallinta sekä vieraiden laitteiden varalta valvominen. Lisäksi skenaariossa on fyysisen turvallisuuden ulottuvuus. Laitteen liittyminen havaittuun ongelmaan on epäselvää, skenaariossa voidaan myös soveltaa mahdollisuutta siihen, että laite on luvallisesti kytketty.

Lisähaaste: Laitteen päällä on pölykerros, joten se on ollut paikallaan selkeästi pitkään. Tuotantodatasta otetut varmuuskopiot on tarkoituksella korruptoitu. Laitteesta löytyy 4G-modeemi, jonka avulla organisaatiolta varastetaan dataa ohi verkon kontrollien.

Skenaario 9
Saastunut ohjelmisto-komponentti

Ohjelmistokehittäjä on ottanut vahingossa käyttöön haittaohjelmalla saastuneen ohjelmistokomponentin. Ohjelmistokomponentti on osa organisaation tuotetta. Haittakoodia ei ole havaittu organisaation omissa prosesseissa.

Tuote on julkistettu, ja siinä oleva haittakoodi mahdollistaa luvattoman pääsyn tuotetta käyttävien asiakkaiden järjestelmiin. Haitallinen koodi on ollut ohjelmistossa useamman kuukauden, ja se on jaeltu useille asiakkaille. Asiakasyritys havaitsi haittakoodin tietoturvaohjelmiston päivityksen jälkeen, ja raportoi siitä heti organisaatiolle.

9

Soveltaminen: Skenaariossa käsitellään tuotantoketjun laadun ja turvallisuuden varmistamista. Skenaarion keskeinen piirre on tuotteen valmistajan vastuu asiakkaille toimitettujen tuotteiden päivittämisestä turvallisiksi.

Lisähaaste: Asiakas ei ilmoita suoraan organisaatiolle haittakoodista, vaan puhuu asiasta ensin julkisuudessa. Tuotteen päivittäminen verkon yli on vaikeaa tai mahdotonta. Ohjelmistokomponenttiin ei ole saatavilla korjaavaa päivitystä, koska sitä ei enää ylläpidetä.

Skenaario 10
Yritysvakoilu

Työntekijän työsuhde on päättynyt. Vaikka henkilön käyttöoikeudet onkin poistettu yrityksen omista järjestelmistä, kriittisestä pilvipalvelusta niitä ei ole huomattu poistaa.

Työntekijä siirtyy vastaaviin tehtäviin kilpailevaan yritykseen ja varastaa tietoja entisen työnantajansa pilvipalvelusta, hyödyntäen niitä uudessa tehtävässään.

Entisen työntekijän toimet huomataan sattumalta auditoinnin yhteydessä tapahtuvassa käyttöoikeuksien ja lokien tarkastelussa.

10

Soveltaminen: Skenaariossa käsitellään käyttöoikeuksien hallintaa, palveluiden ulkoistamiseen liittyviä haasteita ja toimintaa selkeässä rikostapauksessa, jossa epäilty on tiedossa.

Lisähaaste: Väärinkäytökseen syyllistynyt tekijä ei ole organisaatiosta lähtenyt, vaan siihen saapunut työntekijä. Kilpailijalta varastettua tietoa on käytetty oman organisaation eduksi.

Skenaario 11
Yrityskauppa

Yrityskaupan jälkeen yritysten verkot yhdistetään nopealla aikataululla. Hiljattain ostetun yrityksen verkot eivät olleet tarpeeksi tietoturvallisia, minkä seurauksena emoyhtiön verkkoon pääsee haitallista liikennettä.

Tänä aamuna verkonvalvonta huomaa huomattavan määrän ulospäin menevää tuntematonta liikennettä. Yrityksen kriittiset järjestelmät ovat vaarassa, ja tuntematon hyökkääjä on saanut jalansijan verkkoon.

Juuri ostetun yrityksen verkko on puutteellisesti dokumentoitu.

11

Soveltaminen: Skenaariossa käsitellään ongelmaa, joka johtuu kahden erilaisen turvallisuuskulttuurin yhdistämisestä ja isoista, nopeista muutoksista verkkoinfrastruktuurissa.

Lisähaaste: Ostetussa yrityksessä ei ole tehty minkäänlaista verkonvalvontaa. Ostetun yrityksen palvelut on tuotannollisista syistä saatava nopeasti mukaan organisaation emoverkkoon. Aikaa kunnolliselle turvallisuusauditoinnille ei ole.

Skenaario 12
Käytöstä poistettu monitoimilaite

Yrityksen tulostamiseen ja skannaukseen käytetty monitoimilaite uusitaan. Vanha monitoimilaite myydään edelleen käytettyjä toimistotarvikkeita välittävän yrityksen kautta. Monitoimilaitteen kiintolevyä ei ollut tyhjennetty tietoturvallisesti.

Keltaisessa mediassa julkaistaan uutinen, jossa paljastetaan yrityksen luottamuksellisia dokumentteja löytyneen internetin keskustelupalstoilta.

Yksittäinen kansalainen on ostanut käytetyn laitteen ja tutkinut sen kovalevyn, jolta löytyneitä skannattuja ja kopioituja dokumentteja on jaettu verkossa.

12

Soveltaminen: Skenaariossa käsitellään tiedon turvalliseen hävittämiseen liittyviä asioita. Lisäksi skenaariossa käsitellään tapausta, jossa yrityksen sisäisiä dokumentteja vuotaa julkisuuteen.

Lisähaaste: Skannausten joukossa on runsaasti henkilökunnan arkaluontoisia tietoja, kuten terveystietoja. Osa työntekijöistä on kopioinut henkilökohtaisia papereitaan, joista ilmenee arkaluontoisia tietoja. Osassa tiedoista on työntekijän rikokseen viittaavaa sisältöä.

Skenaario 13
Domain-kaappaus

Asiakas soittaa maanantaina puolen päivän aikaan tiedustellakseen, miksi kiireiseen sähköpostiin ei ole vastattu. Organisaatiossa paljastuu, että sen verkkotunnuksen DNS-asetuksiin on tehty muutoksia, joiden seurauksena sisään tuleva sähköposti ja verkkoliikenne ohjautuu vieraalle toimijalle.

Hyökkääjä on onnistunut saamaan muutosoikeudet yrityksen domaintietoihin. IP-osoite, johon domain on asetettu osoittamaan sijaitsee ulkomailla.

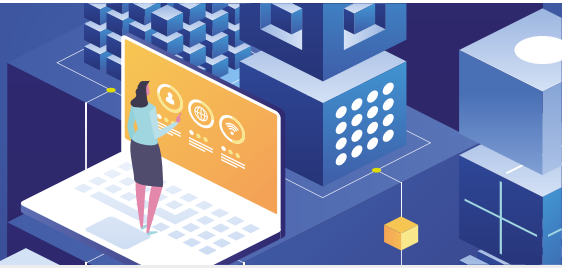
Sähköpostipalvelimelta ilmenee, että viimeinen sisään tullut sähköpostiviesti on torstai-aamupäivältä.

13

Soveltaminen: Skenaariossa ilmenee oman verkonhallinnan ulkopuolinen ongelma. Nimipalvelinasetusten muutos edellyttää kykyä nopeaan reagointiin. Organisaatio menettää kykynsä toimia oman verkkotunnuksensa alla.

Lisähaaste: Nimipalvelimen hallinnan muutosta varten tarvittavan tilin salasana on murrettu. Hallintatili on kuitenkin yrityksen oman domainin alla, jota hyökkääjä hallitsee. Salasanan palautussähköposti päätyy hyökkääjän haltuun.

Skenaario 14
Ohjausdatan manipulointi



Tuotantolaitoksen valvonta- ja ohjausjärjestelmän tuottama valvontainformaatio ei vastaa todellisuutta.

Koska laitosta operoidaan edelleen normaalisti, laitoksessa tapahtuu katastrofaalinen vikatilanne, jonka seurauksena tapahtuu onnettomuus. Onnettomuudesta seuraa henkilövahinkoja, ja tieto tapahtuneesta kulkeutuu joukkotiedotusvälineisiin.

Tuntematon hyökkääjä kiristää johtoa uhkaamalla toistaa hyökkäyksen muissa laitoksissa. Hyökkääjä vihjailee, että hänellä on sisäpiirin pääsy organisaation järjestelmiin.

14

Soveltaminen: Skenaariossa käsitellään ohjausjärjestelmien luottamuksellisuuden häiriötä sekä toimintaturvallisuuden kontrolleja tuotantojärjestelmissä.

Lisähaaste: Onnettomuus tapahtuu samanaikaisesti useissa tuotantolaitoksissa. Henkilövahingot johtavat kuolemiin ja vakaviin vammautumisiin. Onnettomuuden seurauksena tapahtuu vaarallisen aineen vuoto, joka vaarantaa lähialueen asutusta.

Skenaario 15
Palveluntarjoajaan kohdistuva palvelunesto

Organisaation ulkomailla olevat työntekijät ilmoittavat, että organisaation verkkosivuille ei pääse. Suomessa verkkosivut toimivat, mutta hitaasti. Mediassa on uutisoitu toiseen organisaatioon kohdistuneesta massiivisesta palvelunestohyökkäyksestä.

Asiaa selvitettäessä ilmenee, että hyökkäyksen varsinainen kohde käyttää samaa palveluntarjoajaa kuin organisaatio. Palveluntarjoaja käyttää palveluiden tuottamiseen jaettuja palomuureja ja kuormantasaajia, jotka ovat lamaantuneena palvelunestohyökkäyksen vuoksi. Palveluntarjoaja ei vastaa yhteydenottoihin eikä viesti tilanteesta ulospäin.

Soveltaminen: Skenaariossa on käsillä tapaus, jossa jaettu infrastruktuuri pettää toiseen toimijaan kohdistuneen hyökkäyksen vuoksi. Skenaariossa voidaan käsitellä mm. SLA-sopimuksien sisältöä, sovittuja palvelutasoja ja -aikoja sekä ulkoistamiseen liittyviä riskejä.

Lisähaaste: Palvelunestohyökkäys on poikkeuksellisen pitkäkestoinen, ja aiheuttaa palveluntarjoajalla massiivisia ongelmia. Organisaation etäyhteydet eivät ole käytössä. Palveluntarjoaja pitää organisaatiota matalan prioriteetin asiakkaana.

Skenaario 16
Kryptolouhintaa palvelimilla

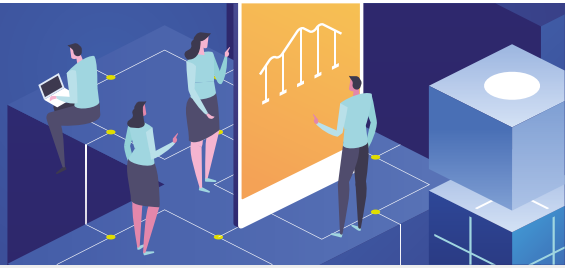
Maanantaina töihin tullessa asiakaspalvelun inbox on täynnä viestejä siitä, että organisaation palvelut toimivat hitaasti. Organisaation controller huomaa myös, että automaattisesti skaalautuvien pilvipalveluiden kustannukset ovat kasvaneet valtavasti viikonlopun aikana, ja välittää tiedon tietohallintopäällikölle.

Tutkittuaan tilannetta tietohallinto huomaa, että organisaatiolle kriittisissä järjestelmissä on havaittu kryptovaluuttaa louhiva haittaohjelma. Haittaohjelma rampauttaa palveluiden toimintakykyä ja kuluttaa palvelinten resursseja.

Soveltaminen: Skenaariossa tapahtunut haittaohjelmasaastuminen ei vaaranna yrityksen tietoja, mutta kuluttaa sen resursseja. Saastumisen juurisyiden selvittäminen edellyttää työtä. Taustalla on tietoturva-aukko, jonka kautta saastuminen on tapahtunut.

Lisähaaste: Automaattisesti skaalautuvat pilvipalvelut aiheuttavat ison rahallisen kustannuksen. Pilvipalveluntuottaja vaatii, että lasku maksetaan, vaikka syy on rikollisessa toiminnassa. Haittaohjelma on kuluttanut resursseja kuukausien ajan matalammalla intensiteetillä.

Skenaario 17
Organisaatio haktivisti-ryhmän tähtäimessä



Organisaation tietoturvapäällikkö saa viranomaisilta tiedustelutietoa, että varteenotettava haktivistiryhmä on keskustellut internetfoorumilla laajamittaisesta kyberhäirintäkampanjasta organisaatiota kohtaan.

Ryhmän motivaatio hyökkäykseen perustuu sosiaalisessa mediassa levitettyihin vääriin tietoihin organisaatiosta.

Ryhmä on tunnettu pitkäkestoisista kampanjoistaan, joilla aiheutetaan runsaasti vahinkoa uhriorganisaatioille. Sillä epäillään olevan kytköksiä valtiollisiin toimijoihin.

17

Soveltaminen: Skenaarion taustana on julkisesti levitetyt virheelliset tiedot organisaation epäeettisestä tai laittomasta toiminnasta. Skenaariossa on vahva kriisiviestinnällinen näkökulma. Kyberhyökkäyksiin varautuminen edellyttää toimenpiteitä.

Lisähaaste: Organisaatio on juuri ulkoistamassa keskeisiä toimintojaan pilveen. Osa väitteistä joita organisaatiosta esitetään, pitävät paikkansa. Organisaatio on juuri ostanut yrityksen ulkomailta, ja integroi sen toimintoja parhaillaan omiinsa.

Skenaario 18
Valkohattuhakkeri ilmoittaa haavoittuvuudesta

Tuntemattoman nimimerkin takaa operoiva henkilö ilmoittaa organisaation asiakaspalvelun sähköpostilaatikkoon löytäneensä organisaation tuotteesta vakavan haavoittuvuuden.

Valkohattuhakkeri on antanut organisaatiolle 90 päivää aikaa julkaista korjauksen haavoittuvuuteen ja viestiä tilanteesta ennen kuin haavoittuvuus tulee julkiseksi.

Alustavan arvion mukaan haavoittuvuuden korjaamisessa menee ainakin neljä kuukautta.

18

Soveltaminen: Skenaariossa käsitellään tilannetta, jossa tuote-haavoittuvuuden julkistusaikataulu on kireämpi kuin korjaamiseen vaadittava aika. Skenaario edellyttää haavoittuvuuskoordinaatiota hakkerin ja viranomaisten kanssa.

Lisähaaste: Tieto valkohattuhakkerin yhteydenotosta on viipynyt asiakaspalvelussa kuukauden, ja tulee ilmi sattumalta kahvipöytä-keskustelussa. Haavoittuvuus on konkurssiin menneen alihankki-jan toimittamassa komponentissa.

Skenaario 19
Tuntematon tietoliikenne

Organisaatiossa testataan uutta tietoturvaohjelmistoa verkon valvontaan. Testaamisen yhteydessä ohjelmisto havaitsee erikoista tietoliikennettä, jota ei tunnisteta. Salatulta vaikuttavaa liikennettä tulee useammalta työasemalta sekä muutamalta palvelimelta ja sen kohteena on ulkomainen palvelin.

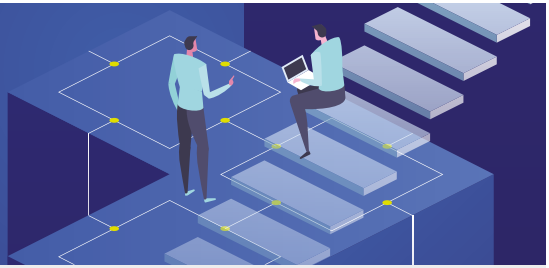
Liikenne käyttää useita eri protokollia (UDP, TCP, ICMP). Liikennettä tulee purskeittain välillä suuria määriä, ja välillä pienempiä, säännöllisen kokoisia paketteja.

Työasemien haittaohjelmaskannaus ei tunnista haitallisia ohjelmia työasemilta.

Soveltaminen: Skenaario alkaa epäselvästä tilanteesta, jossa merkit viittaavat haittaohjelman toimintaan. On kuitenkin mahdollista, että liikenne on asianmukaista, mutta huonosti dokumentoitua. Asian selvittäminen edellyttää oman organisaation toimintaan syventymistä.

Lisähaaste: Lokitiedoista ilmenee, että ulkomaiseen palvelimeen on ollut liikennettä jo monta kuukautta. Asiaa selvitettäessä ilmenee, että kyseinen palvelin on raportoitu yhdeksi valtiollisen haittaohjelmakampanjan komentopalvelimista.

Skenaario 20
Pitkäkestoinen sähkökatko



Syysmyrsky katkoo puita ja aiheuttaa laajoja sähkökatkoja alueelle. Myös paikallinen muuntaja on hajonnut. Organisaatio siirtyy varavirran käyttöön, mutta sen riittävyys on vain muutamia tunteja. Tuotantojärjestelmien sähkönsaanti on turvattu akustolla, mutta kiinteistön muuhun toimintaan ei riitä sähköä.

Ulkoistetut palvelut toimivat, mutta organisaation oma tietotekninen infrastruktuuri lakkaa toimimasta muutaman tunnin kuluttua ilman tietoa siitä, milloin toiminta saadaan takaisin normaalitilaan.

20

Soveltaminen: Skenaario nostaa esiin jatkuvuudenhallintaan, viestintään ja kriittisiin järjestelmiin liittyviä vaikutuksia. Skenaariota voi käyttää väistötilaharjoituksen taustana, jolloin työskentely siirretään pois päätiloista.

Lisähaaste: Syysmyrsky aiheuttaa vaurioita organisaation käytössä olevalle kiinteistölle. Myrsky aiheuttaa liikenne-esteen, jolloin pääsy toimitiloihin estyy. Myrsky pimentää tukiasemia estäen mobiiliyhteyksien käytön.

Yhteistyössä

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

kyberturvallisuuskeskus.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus