TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa

Ohje johdolle ja asiantuntijoille

Kyberturvallisuuskeskus

Traficomin julkaisuja

8/2022

Sisällysluettelo

Kansainvälinen tilanne vaikuttaa väistämättä myös digitaaliseen maailmaan ja kyberuhkilta varautumiseen. On tärkeää, että organisaatioiden johto ja asiantuntijat tarkastelevat kyberturvallisuuden suojauskäytäntöjään sekä ylläpitävät niitä aktiivisesti.

Tässä ohjeessa puhutaan organisaation digitaalisista palveluista. Niillä tarkoitetaan kaikkia tietojärjestelmiä ja tietoliikenneyhteyksiä, joita organisaatio käyttää sisäisesti omassa toiminnassaan ja joiden kautta organisaatio tarjoaa asiakkailleen palveluja.

Kyberhäiriöt ovat yleisiä digitaalisessa yhteiskunnassa. Organisaatioiden omiin järjestelmiin voidaan hyökätä, mutta ne voivat myös joutua välillisesti kohteeksi alihankkijoidensa, kumppaneidensa tai asiakkaidensa kautta kuin myös täysin sivullisena uhrina esimerkiksi haittaohjelmatartunnan levitessä hallitsemattomasti.

Tämä ohje on tarkoitettu kaikille suomalaisille organisaatioille kyberturvallisuuden vahvistamiseen. Ohjeet eivät rajoitu ainoastaan vuoden 2022 alun kansainvälisen tilanteen aiheuttamaan varautumistarpeeseen, vaan niiden avulla on mahdollista kehittää myös yleisemmin organisaation kyberturvallisuutta.

Lue myös:

Kyberturvallisuus ja yrityksen hallituksen vastuu (Ulkoinen linkki)

Pienyritysten kyberturvallisuusopas

Kyberturvallisuuden johtaminen

1 Huomioikaa muutokset kyberturvallisuuden uhkakuvassa

Kunkin organisaation tulisi tarkastella muuttuneen kyberturvallisuuden uhkakuvan vaikutuksia omaan toimintaansa. Vastuu kyberturvallisuudesta kuuluu viime kädessä johdolle.

Kyberturvallisuuskeskus kehottaa organisaatioita:

- varaamaan riittävät resurssit kyberturvallisuuden varmistamiseksi ja tarvittavien toimenpiteiden toteuttamiseksi. Tässä yhteydessä on huomioitava myös johdon tavoitettavuus kriittisten päätösten tekemiseksi.
- tarkastelemaan, mitkä ovat organisaatioiden ydintoimintojen kannalta suojattavat digitaaliset palvelut, ja ovatko niiden suojaustoimenpiteet ajantasaisia ja ylläpidettyjä. Toimenpiteissä tulee huomioida organisaation riskien- ja jatkuvuudenhallintaa sekä myös fyysisiä turvallisuusjärjestelyitä koskevat tarpeet.
- seuraamaan kyberturvallisuuden tilaa viranomaisten, erityisesti Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tiedotteiden ja tilannekuvatuotteiden välityksellä sekä oma-aloitteisesti.

Lisätietoa:

Tilaa uutiskirjeitämme!

Tutustu ohjeisiimme

Kyberturvallisuus ja yrityksen hallituksen vastuu (Ulkoinen linkki)

2 Määritelkää liiketoimintakriittiset ympäristönne

Organisaation johdon tulee määritellä sen toiminnan kannalta kriittiset prosessit sekä niiden vaatimat digitaaliset palvelut ja tieto-omaisuus. Organisaation

johdolla sekä sen palveluista vastaavilla asiantuntijoilla ja kumppaneilla tulee olla tästä kokonaisuudesta yhtenäinen käsitys.

Kyberhäiriötilanteella voi olla vaikutuksia yhtäaikaisesti useisiin organisaation tarvitsemiin palveluihin. Näiden palauttaminen tulee perustua etukäteen määriteltyyn, dokumentoituun sekä harjoiteltuun suunnitelmaan. Tässä yhteydessä tulee olla selvää myös, mikä on palveluiden keskinäinen tärkeysjärjestys.

Organisaatioiden johdon tulisi valmistautua siihen mahdollisuuteen, että sen toiminta voi keskeytyä esimerkiksi kiristyshaittaohjelman tai pelkästään tietojen tuhoamiseen tähtäävän tuhohyökkäyksen johdosta. Silloin ainoa toiminnan jatkuvuuden mahdollistava keino ovat ajantasaiset ja palautettavissa olevat varmuuskopiot.

Kyberturvallisuuden kontrollit

3 Suojatkaa liiketoimintakriittiset ympäristönne

Hyökkääjät pyrkivät etsimään ja löytämään organisaation toiminnan kannalta kriittiset digitaaliset palvelut sekä hankkimaan pääsyn niihin. Usein näissä tapauksissa hyödynnetään perustason tietoturvapuutteita.

Organisaatioiden tulee varmistaa, että se torjuu näitä uhkia huolellisella tietoturvatyöllä. Tämän tulee tapahtua kattavasti niin organisaation omissa kuin sen kumppanienkin vastuulla olevissa digitaalisissa palveluissa.

Seuraaviin kohtiin on koottu sellaisia oleellisia toimenpiteitä, joihin kehotamme organisaatioiden kiinnittämään huomiota.

Toimenpiteet eivät tietyssä suoritusjärjestyksessä, vaan kunkin organisaation tulee tarkastella ja priorisoida nämä omista lähtökohdistaan.

Lisätietoa:

Näin suojaudut tietomurroilta

3.1 Ottakaa käyttöön monivaiheinen tunnistautuminen

Kaikissa julkisesta verkosta tavoitettavissa ja kirjautumista vaativissa organisaation digitaalisissa palveluissa tulee aina olla käytössä vahva monivaiheinen tunnistautuminen (MFA, 2FA). Tämä koskee niin organisaation omia kuin ulkoistenkin kumppanien vastuulla olevia palveluita.

Mikäli monivaiheinen tunnistautuminen ei ole jostain syystä mahdollista, tulee kyseinen järjestelmä suojata jotenkin muuten estämällä sen suora käyttö julkisesta verkosta.

Lisätietoa:

Nasevia neuvoja tiliesi turvaamiseksi

3.2 Asentakaa tietoturvapäivitykset viipymättä

Tietoturvapäivitykset tulee asentaa viipymättä erityisesti kaikkiin julkisesta verkosta tavoitettavissa oleviin digitaalisiin palveluihin.

Aikaväli haavoittuvuuksien löytymisestä niiden laajamittaisen hyväksikäytön alkamiseen on lyhentynyt jatkuvasti. Enää ei riitä päivitysten asentaminen kerran kuukaudessa vaan organisaatiolla tulee olla kyky reagoida riskiarvionsa perusteella päivitystarpeisiin viimeistään muutaman päivän kuluessa.

Rikolliset pyrkivät yleisesti hyödyntämään myös päätelaitteiden haavoittuvuuksia. Siksi erityisesti käytössä olevien laitteiden käyttöjärjestelmät, toimisto-ohjelmistot sekä selaimet tulisi aina päivittää viipymättä. Kaikkein suositeltavinta on ottaa tässä yhteydessä käyttöön automaattiset päivitykset. Mikäli päätelaitteiden päivitykset ovat organisaation keskitetyssä hallinnassa, niin käyttäjät tulisi pakottaa ainakin kriittisten päivitysten asentamiseen viimeistään viikon kuluessa.

Organisaation tulee seurata kaikkia oman toimintaympäristönsä kannalta oleellisia haavoittuvuuksia sekä arvioida niiden merkitys sen oman toiminnan jatkuvuusriskien kannalta. Päivitysten seurannassa voi auttaa tieto siitä, että moni valmistaja julkaisee päivityksensä niin sanottuna päivitystiistaina. Se on yleensä joka kuukauden toinen tiistai.

Lisätietoa:

Kyberturvallisuuskeskus - Haavoittuvuudet

Vulnerability Notes Database (Ulkoinen linkki)

Mitre Common Vulnerabilities And Exposures (CVE) (Ulkoinen linkki)

NIST National Vulnerability Database (NVD) (Ulkoinen linkki)

ICS-CERT Alerts (automaatioympäristöt) (Ulkoinen linkki)

3.3 Varmistakaa tietoliikenteen turvallisuus

Organisaation tulee määritellä, mikä on sen verkoissa toiminnan kannalta tarpeellista ja normaalia tietoliikennettä. Estäkää organisaation tietoliikenneverkkojen palomuureilla kaikki tarpeeton tietoliikenne. Saapuvan liikenteen lisäksi myös organisaatiosta ulospäin lähtevä tietoliikenne tulee rajata ainoastaan toiminnan kannalta tarpeelliseen tietoliikenteeseen.

Erityistä huomiota tulee kiinnittää siihen, että organisaation verkosta ei ole mahdollista liikennöidä julkiseen verkkoon haavoittuviksi tiedetyillä tai rikollisten tyypillisesti hyödyntämillä tiedonsiirtoprotokollilla.

Julkisen verkon yli ei tule sallia mitään salaamattomia tai haavoittuvaksi tiedettyjä tiedonsiirtoprotokollia. Myös organisaation sisäverkossa tulisi siirtyä salattujen protokollien käyttöön kaikkialla, missä se on mahdollista.

Tietoliikenneturvallisuudessa tulisi huomioida myös palvelimet sekä päätelaitteet, jolloin niiden sovelluspalomuureilla sallitaan ainoastaan käytössä olevien sovellusten toiminnan kannalta tarpeellinen tietoliikenne. Tällä menettelyllä vaikeutetaan myös organisaatioon verkkoon mahdollisesti päässeen tunkeutujan etenemistä ympäristöstä toiseen. Tätä tavoitetta tukee myös organisaation verkon jakaminen osiin eli segmentointi.

Lisätietoa:

NCSC-UK - Preventing Lateral Movement (Ulkoinen linkki)

NCSC-IE - Ingress & Egress Filtering (Ulkoinen linkki)

Shadowserverin listaus rikollisten usein hyödyntämistä protokollista (Ulkoinen linkki)

NSA - Network Infrastructure Security Guidance (Ulkoinen linkki)

Tunnetko tunkeutumisen laajentamisen (osa 1)

Tunnetko tunkeutumisen laajentamisen (osa 2)

3.4 Suojautukaa haittaohjelmilta

Organisaatioon ympäristöön päätyvä haittaohjelma muodostaa merkittävän riskin organisaation toiminnan jatkumiselle. On ehdottoman tärkeää huolehtia kattavasta ja ajantasaisesta haittaohjelmatorjunnasta. Sen tulee kattaa organisaation kaikki digitaaliset palvelut, palvelimet sekä päätelaitteet.

Vain toimintakuntoiset tietoturvakontrollit voivat suojata organisaatiota. Tietoturvakontrollien toimintaa tulee tarkastella säännöllisesti. Erityisesti on huomioitava, että tietoturvatuotteet on asennettu kattavasti kaikkialle, konfiguroitu oikein, ja että ne päivittyvät tunnistetietojen osalta sekä ovat toimintakuntoisia.

Kaikki organisaatioon saapuvat ja sieltä lähtevät tiedostot tulee tarkastaa haittaohjelmien varalta. Myös organisaation eri integraatiorajapinnoissa tulee huomioida haitalliselta sisällöltä suojautuminen.

Päätelaitteilla tulee ottaa käyttöön mahdollisuuksien myös mukaan haitallisilta linkeiltä suojaavia kontrolleja.

Päätelaitteilta tai palvelimilta tuleviin hälytyksiin tulee reagoida välittömästi. Hälytyksen kohde tulee eristää organisaation verkosta sekä tutkia asia huolellisesti, koska usein hälytys voi olla tunkeutumisyrityksen ensimmäinen merkki. Vaikka hälytyksiä ei tulisikaan, tulee tietoturvatuotteiden valvontalokeja tarkastella säännöllisesti.

Kyberturvallisuuskeskus on kiinnostunut organisaatioihin tulleista haittaohjelmista ja näitä koskevista näytteistä. Voitte välittää meille näistä tietoa alla olevan ohjesivumme mukaisesti.

Lisätietoa:

Sähköpostin välittäminen ja näytteiden lähettäminen Kyberturvallisuuskeskukselle (Ulkoinen linkki)

Microsoft - Macro malware

3.5 Varautukaa palvelunestohyökkäyksiin

Palvelunestohyökkäykset ovat jokapäiväinen ilmiö internetissä. Palvelunestohyökkäyksessä tyypillisesti luodaan keinotekoisesti ruuhkaa palveluun esimerkiksi täyttämällä palvelun käyttämän nettiliittymän kaista tai aiheuttamalla jollekin palveluketjussa olevalle laitteelle niin paljon prosessointikuormaa, että palvelun toiminta estyy (distributed denial of service, DDoS). Pullonkaulaksi voi muodostua paitsi verkkopalvelin myös esimerkiksi palomuuri.

- Organisaation tulisi arvioida, mihin sen digitaalisiin palveluihin voisi kohdistua sen toimintaa haittaava palvelunestohyökkäys.
- Minkä palveluiden tulee toimia myös kuormitustilanteessa?

Kuinka kauan palvelunestohyökkäystä voidaan kestää toiminnan häiriintymättä liiaksi?

Palvelunestohyökkäyksen tehokas torjuminen voi vaatia sellaista asiantuntemusta ja laitteistoa, jota ei normaalisti ole käytettävissä. Jos palvelun toimivuus on organisaatiolle tärkeää, on poikkeustilanteisiin varautuminen otettava huomioon jo palvelun toteutusta suunniteltaessa — vähintään on tiedettävä, mistä ja minkälaisella aikataululla asiantuntija-apua on saatavilla.

Kyberturvallisuuskeskus on kiinnostunut organisaatioihin kohdistuvista palvelunestohyökkäyksistä. Voitte ilmoittaa niistä meille kotisivujemme ilmoituslomakkeella.

Lisätietoa:

Neuvoja palvelunestohyökkäyksen estämiseksi

3.6 Suojatkaa myös pilvipalvelut

Organisaatiolla on todennäköisesti käytössään myös erilaisia pilvipalveluita. Myös niiden osalta tulee varmistaa, että kaikki organisaation kannalta tarpeelliset tietoturvakontrollit on otettu käyttöön. Pilvipalvelujen oletusasetukset eivät aina ole organisaation tietoturvan kannalta riittäviä.

Ulkoisissa pilvipalveluissa niiden toimittaja vastaa tyypillisesti infrastruktuurin turvallisuudesta. On syytä kuitenkin muistaa, että vastuu tiedon suojaamisesta pilvipalvelussa on aina loppuasiakkaalla itsellään. Vaikka käytännön työn tekisikin joku muu, tulee organisaation itse johtaa siihen liittyvää tietoturvaa. Organisaation tulee määritellä ja ohjeistaa, miten sen tietoa tulee suojata, käsitellä ja minkälaisia tietoja suojaavia kontrolleja tulee pilvipalveluissa ottaa käyttöön.

Lisätietoa:

Kyberturvallisuuskeskus - Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Azure security best practices and patterns (Ulkoinen linkki)

AWS - Best Practices for Security, Identity, & Compliance (Ulkoinen linkki)

Google Cloud security best practices center (Ulkoinen linkki)

Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta

3.7 Varmistakaa etäyhteyksien turvallisuus

Lähes kaikki organisaatiot ovat joutuneet koronaviruspandemian aikana toteuttamaan uusia etäyhteysratkaisuja. Rikolliset hyödyntävät laajasti etäyhteyksiin liittyviä tietoturvapuutteita.

Koska jokainen etäyhteys väistämättä lisää myös organisaation kyberturvallisuusriskiä, tulisi organisaatioiden aivan ensin arvioida ovatko olemassa olevat etäyhteydet ylipäätänsä enää tarpeellisia. Seuraavat kysymykset ovat oleellisia:

- Onko organisaatio varmasti tietoinen kaikista etäyhteystavoista, joita sillä on käytössään sen oman henkilöstön tai kumppanien tarpeisiin?
- Ovatko kaikki etäyhteydet vielä toiminnan kannalta välttämättömiä?
- Tarvitseeko koko henkilöstö tai kaikki kumppanit vielä etäyhteyksiä vai riittäisikö niiden tarjoaminen esimerkiksi ainoastaan päivystysluonteista työtä tekeville tahoille?
- Jos käytössä on ulkoisten kumppanien etäyhteyksiä organisaation ympäristöön, huomioidaanko niiden yhteydessä riittävästi riski tätä kautta tulevasta tunkeutumisesta?
- Siltä osin kun etäyhteydet katsotaan välttämättömiksi, tulee niiden tietoturvallisuudesta varmistua. Seuraavat toimenpiteet ovat oleellisia:

- Varmistetaan, onko etäyhteysratkaisu ylipäätänsä riittävän turvallinen käyttötarkoitukseensa ja onko se valmistajan tietoturvapäivitysten piirissä.
- Etäyhteyden toteuttavan tuotteen haavoittuvuuksia seurataan ja päivitykset asennetaan viipymättä niin palvelimen kuin päätelaitteidenkin osalta.
- Etäyhteysratkaisu on konfiguroitu turvalliseksi (esim. monivaiheinen tunnistaminen) ja käyttöön otettu vain organisaation toiminnan kannalta välttämättömät toiminnallisuudet
- Etäyhteyksien käyttäjätilejä ylläpidetään aktiivisesti ja tarpeettomaksi käyneet (esim. työntekijöiden vaihtuessa) suljetaan välittömästi.
- Etäyhteyksien käyttöä valvotaan ja niistä kerätään kattavaa valvontalokia. Organisaatiolla tulee olla välitön pääsy omiin etäyhteyslokeihinsa, vaikka itse ratkaisu olisikin ulkopuolisen kumppanin ylläpidossa.
- Kaikki etäyhteydet on dokumentoitu ajantasaisesti.

Lisätietoa:

CISA & NSA - Selecting and Hardening Remote Access VPN Solutions (Ulkoinen linkki)

3.8 Huolehtikaa varmuuskopioista

Kaikista toiminnan kannalta tärkeistä tiedoista tulee ottaa säännöllisesti varmuuskopiot. Varmuuskopioihin tulee sisällyttää liiketoimintatiedon lisäksi myös erilaiset järjestelmäasetukset. Varmuuskopioiden avulla tulee kyetä palauttamaan toiminta myös tilanteessa, jossa organisaation koko tietotekninen ympäristö joudutaan asentamaan uudelleen.

Varmuuskopioiden suojaamiseen tulee kiinnittää myös huomiota. Ympäristöön tunkeutunut taho ei saa päästä turmelemaan varmuuskopioita tai varastamaan tietoa salaamattomien varmuuskopioiden avulla. Varmuuskopioiden osalta tulisikin noudattaa niin kutsuttua 321-sääntöä. Silloin tieto on tallennettu vähintään 3 paikkaan, se sijaitsee vähintään kahdella eri laitteella tai medialla ja 1 varmuuskopio on kokonaan erillisessä paikassa.

Varmuuskopioiden palauttamista tulee testata säännöllisesti. Näin varmistutaan, että niiden palauttaminen onnistuu ja myös tarvittavat järjestelmäasetukset on varmuuskopioitu.

Lisätietoa:

Edistyneet kiristyshyökkäykset yleistyvät – Varo joutumasta saaliiksi!

Offline backups in an online world (Ulkoinen linkki)

Small Business Guide: Cyber Security (Ulkoinen linkki)

CISA - Stop Ransomware (Ulkoinen linkki)

NCSC-UK - Mitigating malware and ransomware attacks (Ulkoinen linkki)

3.9 Tarkastakaa julkiseen verkkoon näkyvät palvelunne

Rikolliset etsivät jatkuvasti verkosta sellaisia organisaatioiden palveluita, joita he voisivat hyödyntää. Joskus organisaatio ei ole itse tietoinen mitkä kaikki sen palvelut ovat vapaasti tavoitettavissa internetistä.

Organisaation jokin vain sisäiseen käyttöön tarkoitettu palvelu saattaa päätyä julkiseen verkkoon epähuomioissa tai vaikkapa palomuurin konfiguraatiovirheen johdosta. Siksi onkin suositeltavaa aika ajoin tarkastaa vastaako organisaation oma käsitys todellisuutta.

Verkossa on erilaisia vapaasti käytettävissä olevia hakukoneita, joilla on varsin helppoa selvittää esimerkiksi mitä palvelimia organisaation verkkotunnukseen liittyy tai mitä palveluita ne tarjoavat.

Lisätietoa:

Shodan (Ulkoinen linkki)

DNSdumpster.com (Ulkoinen linkki)

3.10 Tarkastelkaa langattomien teknologioiden muodostamia riskejä

Organisaatioilla on usein käytössään myös erilaisia langattomia eli vapaasti eteneviin radioaaltoihin perustuvia tiedonsiirtotapoja. Silloin kun näitä hyödynnetään kriittisten toimintojen yhteydessä, tulee huomioida myös langattomuuteen liittyvien erityisten riskien hallitseminen.

Langattomiin teknologioihin liittyy aina kohonnut salakuuntelun ja signaalin vääristämisen riski sekä mahdolliset saatavuuskatkokset tahattoman tai tahallisten häiriöiden seurauksena.

Langattomat tietoliikenneverkot

Organisaatioiden tulisi huomioida langattomien tietoliikenneteknologioiden muodostamia riskejä niiden kriittisten prosessien yhteydessä:

- Mikään toiminnan kannalta tärkeä tietoliikenneyhteys ei saisi perustua pelkästään yhteen langattomaan teknologiaan. Käytössä tulisi aina olla myös jokin vaihtoehtoinen tapa. Liike- tai yrityksen toiminnalle kriittisiä toimintoja ei tulisi rakentaa niin sanottujen luvasta vapaiden radiolaitteiden varaan yhteiskäyttöisille taajuusalueille, joilla häiriöriski on merkittävästi suurempi kuin taajuusalueilla, joilla toiminta pohjaa taajuussuunnitteluun.
- Tietoliikenteen salaus ei saisi koskaan perustua pelkästään langattoman teknologian tarjoamaan radioliikenteen salaukseen, vaan sen päälle tulisi toteuttaa riittävän vahva päästä-päähän tyyppinen salaus.
- Päätelaitteiden liikkuvissa yhteyksissä tulisi huomioida, että julkinen WLAN-verkko tai ulkomaisen operaattorin matkapuhelinverkko ei välttämättä ole aina turvallinen. Mikäli näitä joudutaan harkinnan perusteella käyttämään, tulisi päätelaitteissa olla käytössä organisaation omassa hallinnassa oleva VPN-yhteys.

Sijainti- ja aikatietopalvelut

Satelliittipaikannuksen (GNSS) peruspalveluita ovat kaikille avoimet sijainti- ja aikatiedot. Näiden saaminen mielletään usein itsestään selviksi asioiksi, niistä on tullut lähes luonnonvakioita. Organisaatioiden tulisi selvittää minkälaisia vaikutuksia niiden toiminnalle aiheutuisi sijainti- ja aikatiedon luotettavuuden heikentymisestä tai pitkäaikaisesta eli vähintään päiviä kestävästä saatavuuden katkoksesta:

- Tarkka ja luotettava sijaintitieto on olennainen osa erimerkiksi älykkäiden liikenne- ja tilannekuvajärjestelmien kehitystä, joissa eri toimintojen

koordinointi pohjautuu henkilöiden tai laitteiden sijaintiin alueella. Esimerkiksi logistiikkayritykset optimoivat kaluston käyttöä sijaintitiedon perusteella. Ilmailussa, merenkulussa sekä rautateillä sijaintitieto on operatiivisessa toiminnassa olennaisessa toimintaa tukevassa tai avustavassa roolissa.

- Aikatietoa hyödynnetään laajasti mm. tietoliikenne-, tele-, televisio- ja energiansiirtoverkoissa eri järjestelmäosien toiminnan synkronointiin.

Sijaintitiedon osalta toimintavarmuutta voi parantaa tukeutumalla useampaan GNSS-järjestelmään kuten esimerkiksi eurooppalaisen Galileon ja amerikkalaisen GPS:n yhdistelmään sekä järjestelmien monitaajuusvastaanottoon. GNSS-vastaanoton häiriösietoisuutta voidaan mahdollisesti parantaa myös erilaisilla antenniratkaisuilla. Joissakin GNSS-vastaanottimissa on myös ohjelmallisesti toteutettuja ja erikseen päälle kytkettävissä olevia häiriönsietoa parantavia ominaisuuksia. Sijaintitietoa voi täydentää myös matkapuhelinverkkojen tarjoamalla paikannuksella.

Merenkulussa ja veneilyssä on tärkeää varmistaa tarvittavan kartta-aineiston ja manuaalisten navigointimenetelmien saatavuus.

Aikatiedon varmistamiseksi voidaan myös tukeutua useampaan GNSS-järjestelmään, mutta lisäksi langalliseen menetelmään tai paikalliseen kellojärjestelmään perustuva varajärjestelmä on suositeltava.

Lisätietoa:

Internetiin liitettyjen laitteiden turvallinen käyttö

Bluetoothin turvallinen käyttö älylaitteissa

Satelliittipaikannuksen nykytila ja kehitysnäkymät

Ilmoitus radiohäiriöistä

4 Havainnoikaa ja analysoikaa tapahtumia

Organisaatioiden tulee varmistaa kyvykkyys havaita kriittisiin ympäristöihin kohdistuvia tietoturvapoikkeamia. Lokitietoa tulee kerätä sellaisista laitteista, ohjelmistoista ja tietovarannoista, joita hyökkääjä voisi käyttää hyväkseen. Lokitietoa tarvitaan selvittämään, mitä, miksi ja milloin jotakin tapahtui.

Lokitus tulee ottaa käyttöön suojattavien kohteiden kriittisyyden perusteella. Mitä suurempi potentiaalinen vaikutus vaarantuneella suojattavalla kohteella on, sitä enemmän lokitietoja organisaation tulisi kerätä kohteesta.

Lokitiedot tulee suojata mahdollisen tunkeutujan vaikuttamiselta. Lokit tulee tallentaa turvallisesti johonkin muualle kuin itse valvottavaan ympäristöön niin, ettei tunkeutujan ole mahdollista muuttaa niitä.

Organisaation tulee seurata kerättyjä lokitietoja saadakseen selkeän yleiskuvan operatiivisen toiminnan ja kyberturvallisuuden tilasta. Erityisesti lokeista tulisi nyt etsiä merkkejä seuraavista asioista:

- Käyttäjätietokantojen ja hakemistopalveluiden kirjautusmislokeissa (esimerkiksi Active Directory tai Azure AD) näkyvistä epänormaaleista tapahtumista. Näitä voivat olla muun muassa uusien käyttäjätilien luonti, käyttöoikeuksien korottaminen tai kirjautumiset epänormaaleista maantieteellisistä paikoista, päätelaitteilla tai ajankohtina

- Palomuurilokeissa näkyvistä epänormaaleista osoitteista, protokollista, liikennemääristä tai ajallisesti tavallisuudesta poikkeavista tapahtumista.

Lisätietoa:

Näin keräät ja käytät lokitietoja

NCSC-UK - Logging made easy (LME) (Ulkoinen linkki)

5 Reagoikaa tapahtumiin ja häiriöihin

Organisaatiolla tulee olla kyvykkyys reagoida välittömästi sen kriittisiin toimintoihin kohdistuviin kybertapahtumiin tai -häiriöihin. Näihin tilanteisiin tulee olla tunnistettu soveltuvat henkilöt tai roolit.

Tämän toiminnan tärkeimpänä tavoitteena on rajoittaa organisaation toimintaan kohdistuvaa vaikutusta sekä mahdollistaa toiminnan palauttaminen normaaliksi. Kyberhäiriöiden reagoimisen varalle tulee olla suunnitelma, jota pidetään yllä ja joka kattaa koko häiriönhallinnan elinkaaren.

Lisätietoa:

Opas tietomurtojen havaitsemiseen

NCSC-UK - Incident management (Ulkoinen linkki)

6 Varmistakaa toiminnan jatkuvuus

Organisaatiolla tulee olla toiminnan jatkuvuutta koskevat suunnitelmat, joiden avulla toiminta voidaan säilyttää ja palauttaa, mikäli siihen kohdistuu kybertapahtuma tai -häiriö.

Jatkuvuussuunnitelmissa on tunnistettu ja dokumentoitu ne laitteet, ohjelmistot ja tietovarannot sekä toiminnat, jotka minimissään tarvitaan toiminnan ylläpitämiseksi.

Lisätietoa:

HVK - Jatkuvuudenhallinta (Ulkoinen linkki)

Turvaa digitaalinen toiminta häiriötilanteissa (Ulkoinen linkki)

7 Informoikaa henkilöstöä

Organisaation koko henkilöstöllä on tärkeä rooli sen kyberturvallisuuden varmistamisessa. Johdon tuleekin varmistaa, että sen henkilöstö on riittävän tietoinen kyberturvallisuuden merkityksestä organisaation toiminnalle. Tässä yhteydessä johtaminen ja viestintä ovat keskiössä.

Henkilöstölle tulee antaa koulutuksen ja viestinnän keinoin riittävät valmiudet arkipäiväisten kyberturvallisuusuhkien kohtaamiseen.

Organisaatioissa tulisikin toteuttaa vähintään seuraavat toimenpiteet:

Johto viestii selkeästi koko henkilöstölle kyberturvallisuuden merkityksen organisaation toiminnalle sekä johdon ehdottoman sitoutumisen asiaan.

Järjestää henkilöstölle säännöllisesti sen työtehtävien kannalta riittävää tietoturvakoulutusta, jotta se kykenee toimimaan turvallisesti huomioiden yleisimmät työssään kohtaaman tietoturvauhat kuten tietojen kalastelu, haitalliset liitteet sekä linkit.

Järjestää henkilöstölle kanava, jonka kautta se voi ilmoittaa havaitsemistaan tietoturvapoikkeamista tai niiden epäilyistä.

Lisätietoa:

Näin pidät huolta tietoturvasta kotona ja työpaikalla

8 Ilmoittakaa tietoturvaloukkauksista tai niiden epäilyistä

Kyberturvallisuuskeskus kannustaa organisaatioita ilmoittamaan sille matalalla kynnyksellä kaikista tapahtuneista tai epäillyistä tietoturvaloukkauksista.

Ilmoituksen voi tehdä mieluiten verkkosivun **lomakkeella** sekä myös sähköpostitse **cert@traficom.fi** . Mikäli kyseessä ei ole akuutti tietoturvapoikkeama, niin toivomme yhteydenottoa osoitteeseen **kyberturvallisuuskeskus@traficom.fi** .

Saatua tietoa hyödynnetään kansallisen kyberturvallisuuden tilannekuvan ylläpitämisessä. Tilanteen niin vaatiessa olemme yhteydessä myös ilmoittaneeseen tahoon.

Tietoturvaloukkaus on rikos ja siksi siitä tulisi aina tehdä poliisille rikosilmoitus. Mikäli kyseessä on myös henkilötietojen tietoturvaloukkaus, tulee asiasta ilmoittaa tietosuojavaltuutetulle. Keskeisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien pitää ilmoittaa verkko- ja tietojärjestelmässä olevista tietoturvapoikkeamista myös toimialojen valvoville viranomaisille (NIS-ilmoitusvelvollisuus).

Lisätietoa:

Kyberrikosten tutkinta (Ulkoinen linkki)

Ilmoita tietoturvapoikkeamasta (NIS-ilmoitusvelvollisuus) (Ulkoinen linkki)

Henkilötietojen tietoturvaloukkaukset (Ulkoinen linkki)

Sähköpostin välittäminen ja näytteiden lähettäminen Kyberturvallisuuskeskukselle

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISSN 2669-8757 (netti)
ISSN 2669-8749 (printti)