SUOMALAISEN YRITYKSEN KYBERTURVALLISUUS MUUTTUNEESSA MAAILMASSA

Maailmantilanteesta riippumatta yritysten kyberturvallisuus on paikallista. Tämä tarkoittaa, että Venäjän hyökkäys Ukrainaa vastaan voi johtaa taistelukenttien kyberhyökkäysten leviämiseen tietoverkkoihin ja verkkopalveluihin myös Suomessa. Kyberhyökkäykset voivat levitä suomalaisiin yrityksiin tai muihin kohteisiin tarkoituksella kohdennettuina tai kohdistamattomina. Globaalit tietoliikenneyhteydet mahdollistavat sen, että ajallisesti hyökkäys voi kohdistua yrityksiin Ukrainassa ja Suomessa samana päivänä.

Kun organisaatiot pohtivat kyberturvallisuuttaan Ukrainan sodan aikana, on myös yksittäisten ihmisten hyvä varmistaa säännöllisesti, että heidän tietokoneensa, mobiililaitteidensa ja ohjelmistojen päivitykset ovat ajan tasalla ja että kaikki salasanat ovat turvallisia ja kaikki tärkeät tilit on suojattu kaksivaiheisella todennuksella. Tie yritykseen voi löytyä työntekijän omien laitteiden kautta.

Olemme jo pitkään eläneet tietojenkalastusyritysten kulta-aikaa ja vallitseva tilanne todennäköisesti vain pahentaa jo ennestään vaikeaa tilannetta. Tietojenkalasteluhyökkäykset voivat lisääntyä hyökkääjien pyrkiessä huijaamaan ihmisiä napsauttamaan linkkejä, jotka antavat hyökkääjille pääsyn tietokonejärjestelmiin. Sen jälkeen hyökkääjä voi varastaa tietoa, tuhota sitä tai salata sen.

Sodan suorana vaikutuksena yrityksiin kohdistuvaan kyberuhan luonteeseen on esimerkkinä Ukrainassa viime viikolla löydetty "pyyhkijä"-haittaohjelma, joka poistaa pysyvästi tiedot tartunnan saaneista tietokoneista. Sitä löytyi pääasiassa Ukrainasta, mutta samana päivänä myös jo Latviasta ja Liettuasta. Sodan myötä kynnys tuhoamiselle on alentunut. Hyökkäyksen tarkoituksena on tuhota, hyökkääjällä ei ole tarvetta kerätä rahaa rikollisilla keinoilla. Tämä asettaa tietojen varmuuskopioinnin merkityksen aivan uudelle tasolle.

Eräänä tilanteeseen räätälöitynä uhkana on mainittu väärennetyt lahjoitussivustot ja ihmisten houkuttelu erilaisiin vetoaviin asioihin. Pyrkimys on aina saada ihminen toimimaan hyökkääjän tahtomalla tavalla. Usein kyse on tunteisiin vetoamisesta tai kiireen tunteen luomisesta. Tällaisessa tilanteessa ihminen unohtaa helposti varovaisuuden ja klikkaa linkkiä tai avaa liitetiedoston.

Laajat palvelunestohyökkäykset ovat niin ikään viime päivinä olleet paljon esillä ja näyttääkin siltä, että niiden avulla tavoitellaan medioiden, finanssialan toimijoiden ja muiden keskeisten organisaatioiden toiminnan häiriintymistä. Tällaisten hyökkäysten tavoitteena on aiheuttaa yleistä sekasortoa ja evätä kansalaisten pääsy verkkopalveluihin.

Hyökkäystapoja on muitakin, mutta puolustajan toimet niitä vastaan ovat pääsääntöisesti samanlaisia uhasta riippumatta. Ja ne lähtevät ihan perusasioista maailmanpoliittisesta tilanteesta huolimatta. Tässä oppaassa listataan erilaisia toimia kyberturvallisuuden parantamiseksi. Niistä kukin yritys voi poimia itselleen sopivia tai toteutettavissa olevia toimia.

Suomalaiseen yhteiskuntaan on kohdistettu vaikuttamista jo ennen sotaa. Sodan käynnistyminen todennäköisesti kiihdyttää eri tahojen ponnistuksia vaikuttaa suomalaiseen päätöksentekoon ja mielipiteisiin. Myös käynnissä olevasta sodasta verkossa ja sosiaalisessa mediassa liikkuu myös todella paljon disinformaatiota. Tällaisina aikoina on erityisen tärkeää, että yritykset ja kansalaiset hyödyntävät luotettavia tiedonlähteitä eivätkä osallistu epäluotettavan tiedon levittämiseen.

Varautumisen perusasioita

Ole valpas

Älä koskaan avaa sähköpostin liitettä tuntemattomalta henkilöltä ja ole tarkkana tuntemiltasi ihmisiltä tulleiden viestien kanssa. Jos saat yllättävän tai odottamattoman liitteen tai kysymyksen sisältävän sähköpostin, soita lähettäjälle ja varmista sähköpostin aitous. On aina turvallisempaa kirjoittaa URL-osoite itse osoitekenttään kuin napsauttaa linkkiä.

Jos sinua yritetään saada antamaan tietoa yrityksestä tai sen työntekijöistä, varmista asia tarvittaessa esimieheltä tai johdolta. Ajattele ennen kuin klikkaat, suuri osa kyberhyökkäyksistä alkaa yksinkertaisella tietojenkalasteluviestillä. Älä välitä epäilyttäviä viestejä eteenpäin.

Valitse vahva salasana

Salasanan tulee olla 12–15 merkin pituinen ja siinä on oltava erikoismerkkejä tai symboleja. Jokaisella verkkotililläsi pitäisi olla eri salasanat. Voit seurata niitä kaikkia käyttämällä hyvämaineista salasanojen hallintaohjelmaa, kuten Applen, Googlen tai Microsoftin tarjoamia.

Pidä virustorjuntaohjelmistosi ajan tasalla

Varmista, että virustorjuntaohjelmisto on määritelty päivittymään automaattisesti. Tämä auttaa vaikeuttamaan hakkereiden pääsyä tietokoneellesi, kannettavalle tietokoneellesi tai älypuhelimellesi sekä varoittaa sinua epäilyttävistä verkkosivustoista ja latauksista.

Käytä vain luotettuja Wi-Fi-verkkoja

Ilmainen Wi-Fi näyttää kätevältä, mutta hakkerit voivat myös käyttää sitä siepatakseen Internet-viestintääsi. Ennen kuin liityt ilmaiseen verkkoon, varmista, että Wi-Fi-yhteys kuuluu yritykselle, jonka tunnet ja johon luotat. Jos olet epävarma, käytä henkilökohtaista Wi-Fi-hotspotia tai älypuhelimen verkkoyhteyttä. Käytä tarvittaessa VPN-ohjelmistoa verkkoliikenteen suojaamiseksi.

Älä luovuta henkilökohtaisia tietojasi ja someta harkiten

Ole erityisen varovainen kaikista pyynnöistä antaa tietoja, kuten syntymäaikasi, sosiaaliturvatunnuksesi tai pankkitilisi. Sama koskee tietoa, jonka julkaiset verkossa sosiaalisessa mediassa. Pidä henkilötiedot yksityisinä.

Koulutus

Kouluta henkilökuntaasi tai hanki ulkopuolinen kouluttaja. Henkilökunnan osaaminen ja valppaus ovat merkittävässä asemassa yrityksen varautumisessa. Parempi välttää vahinko kuin korjata sitä. Etä- ja hybridityön tietoturva on niin ikään tärkeää pitää mielessä.

Kriittiset tiedot ja varmuuskopiointi

Arvioi mikä on toiminnan kannalta kriittistä tietoa ja miten se on suojattu ja varmuuskopioi se.

Varmuuskopiointitoimenpiteet tulee tehdä säännöllisesti ja kokeilla säännöllisin väliajoin, että palautus toimii. Muista myös säilyttää varmuuskopiot offline-tilassa ja tarkistaa ne säännöllisesti varmistaaksesi, ettei niitä ole myrkytetty haittaohjelmilla.

Jos teet kopioinnin ulkoisella kovalevyllä, älä pidä kovalevyä kytkettynä tietokoneeseen, vaan vain kopioinnin ajan. Muutoin hyökkäys voi levitä tietokoneen ja tietoverkon kautta kovalevyyn tuhoten tai kryptaten varmuuskopion.

Käteinen

Jos verkkoyhteys pankkiisi ei ole tilapäisesti käytettävissä tai pankkikortit eivät toimi, voi olla hyvä pitää käteistä rahaa. Katkos voi olla lyhytaikainen, mutta sitä ei voi etukäteen tietää.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen sivuille (https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille) on koottu kattava kattaus käytännön ohjeita ja neuvoja oman tietoturvan suojaamiseksi.

Lisäkeinoja kyberhyökkäyksen onnistumisen todennäköisyyden vähentämiseksi ja yrityksen selviämiseksi onnistuneesta hyökkäyksestä

Ota monivaiheinen tunnistautuminen kaikissa järjestelmissä, palveluissa ja sosiaalisen median tileillä. Käytä luotettavia sovelluksia monivaiheisen tunnistautumisen mahdollistamiseksi kuten Microsoft Authenticator tai Google Authenticator. Varmista, että kaikki etäkäyttö organisaation verkkoon ja järjestelmänvalvojan käyttö edellyttää vähintään kaksivaiheista todennusta.

Varmista, että ohjelmistojen päivitykset ovat ajan tasalla.

Varmista, että organisaation IT-henkilöstö tai palveluntarjoaja on poistanut käytöstä kaikki portit ja protokollat, jotka eivät ole välttämättömiä liiketoiminnalle.

Jos yrityksesi käyttää pilvipalveluita, varmista, että IT-henkilöstö tai vastuuhenkilö on tarkistanut tai varmistanut palvelun ja käytössä on tarkoituksenmukaiset kontrollit ja tietoturva-asetukset.

Varmista, että organisaation koko verkko on suojattu palomuureilla sekä virus-/haittaohjelmien ajantasaisella torjuntaohjelmistolla. Varmista, että yrityksesi on valmis reagoimaan tietoverkkoihinne tunkeutumisen tapahduttua.

Selvitä miten organisaatio voi suojata kriittiset verkossa toimivat järjestelmät ja palvelut palvelunestohyökkäyksiltä. Tee suunnitelma siitä miten toiminta järjestetään palvelunestohyökkäyksen kestäessä.

Nimeä jatkuvuusryhmän jäsenet, joilla on roolit ja oikeudet toimia kyberhyökkäyksen aikana. Varmista avainhenkilöiden tavoitettavuus eri vuorokauden aikoina. Liiketoiminnan jatkuvuus voi tarkoittaa sen selvittämistä, miten toimitte ilman tietolaitteita ja pääsyä verkkoon. Joissain organisaatioissa tämä tarkoittaa paperia ja kynää.

Testaa varmuuskopiointimenettelyjä varmistaaksesi, että kriittiset tiedot voidaan palauttaa nopeasti, jos organisaatioon kohdistuu kiristysohjelma tai muu kyberhyökkäys, Varmista, että varmuuskopiot on eristetty verkkoyhteyksistä.

Vähennä hyökkääjien mahdollisuuksia tunnistamalla altistukset, haavoittuvuudet ja virheelliset määritykset, jotka voivat tarjota hyökkääjille mahdollisuuksia saada jalansijaa tietoverkossasi ja käytä korjaavia päivityksiä. Seuraa viranomaisten sivustoja ja varoituksia. Kyberturvallisuuskeskuksen sivuille on koottu laaja joukko käytännönläheistä materiaalia yritysten tietoturvan kehittämiseksi. (https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille).

Jos mahdollista, suorita neuvotteluhuoneharjoitus varmistaaksesi, että kaikki osallistujat ymmärtävät roolinsa tapahtuman aikana. Harjoituksen ei tarvitse olla muodollinen, avoin keskustelu valitun skenaarion pohjalta usein antaa paljon.

Ota tarvittaessa yhteyttä kyberpalvelujen tarjoajaan kartoittaaksesi tilannetta ja palvelujen tarvetta etukäteen.

Ajatuksia yritysjohdolle

Yritysjohtajilla ja yritysten hallituksilla on tärkeä rooli sen varmistamisessa, että yrityksen työntekijät ymmärtävät kyberturvallisuuden merkityksen ja omaksuvat oikeat toimintatavat.

Kyberturvallisuus ja yrityksen hallituksen vastuu – opas: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Lähes jokaisessa organisaatiossa tietoturvaparannuksia punnitaan suhteessa kustannuksiin ja liiketoiminnan riskeihin. Kohonneessa kyberuhkaympäristössä ylimmän johdon tulee tehdä selväksi koko organisaatiolle, että tietoturvallisuuden varmistaminen on tärkeää lähitulevaisuudessa. Digitaalisessa ajassa jokaisella työntekijällä on rooli siinä.

Yrityksellä kaikkien työntekijöiden on hyvä tietää milloin ilmoittaa mahdollisista kybertapauksista johdolle. Johto voi tarvittaessa ilmoittaa asiasta viranomaisille. Näin yritys voi parantaa mahdollisuuksiaan tunnistaa ongelma nopeasti ja auttaa muita suojautumaan uusilta hyökkäyksiltä.

Johdon on hyvä osallistua toimintasuunnitelman valmisteluun. Johdon on hyvä osallistua mahdolliseen neuvotteluhuoneharjoitukseen yhdessä muiden avainhenkilöiden kanssa.

Rajalliset resurssit huomioiden turvallisuuden ja jatkuvuuden investoinnit tulisi keskittää liiketoiminnan kriittisiä osia tukeviin järjestelmiin. Ylimmän johdon tulee varmistaa, että tällaiset järjestelmät on tunnistettu ja varmistettu että kriittisiä liiketoimintoja voidaan tavalla tai toisella jatkaa kyberhyökkäyksen jälkeen.

Selvitä yrityksesi mahdollinen vakuutusturva kyberhyökkäystilanteessa.

Jos mahdollista, suunnittele, varaudu ja harjoittele pahimman varalle. Johdon vastuulla on liiketoiminnan suojaaminen ja toiminnan jatkuvuuden varmistaminen.

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

KESKUS-
KAUPPAKAMARI

Alvar Aallon katu 5 C, PL 1000 | 00100 HELSINKI | +358 9 4242 6200
kauppakamari.fi

Linkit:

Kyberturvallisuuskeskuksen työntekijöiden ja yksityishenkilöiden tietoturvaohjeet https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille

Kyberturvallisuuskeskuksen ohjeet ja oppaat yrityksille

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Pienyritysten kyberturvallisuusopas

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Keskuskauppakamarin tietosuoja ja tietoturvaopas yrityksille

https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf

Helsingin seudun kauppakamarin opas yritystietojen turvaamisesta.

https://view.24mags.com/helsinki.chamber/yritysturvallisuus-pida-yritystiedot-turvassa#/page=1

Liittyvät artikkelit:

https://kauppakamari.fi/blogi/onko-yrityksesi-varautunut-kyberrikollisuuteen-ja-vakoiluun/

https://kauppakamari.fi/tapahtumat/yritysjohdon-kyberjohtamisen-ohjelma/

https://kauppakamari.fi/tiedote/korona-aiheiset-huijausviestit-lisaantyneet-tarkista-oikea-tieto-aina-virallisista-lahteista/

https://kauppakamari.fi/tiedote/keskuskauppakamari-tarjoaa-tietosuojaoppaan-ja-tietoturvaoppaan-yritysten-tueksi/

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency