Huoltovarmuuskriittiset alat varautuvat harjoittelemalla hybridiuhkia vastaan – nämä asiat sinunkin tulee tietää

Mediatiedote 10.5.2023

Hybridi- ja kyberuhat ovat nousseet otsikoihin entistä näkyvämmin Venäjän hyökkäyssodan alettua. Esimerkiksi Traficomin Kyberturvallisuuskeskuksen mukaan viime kuukausina valtionhallinto ja huoltovarmuuskriittiset toimijat ovat olleet entistä useammin kyberhyökkäysten kohteena. Erityisesti kohdistettujen kyberhyökkäysten määrä, joissa kohdeorganisaatio on tarkkaan valittu, on kasvanut.

Maamme kriittisestä infrastruktuurista ja huoltovarmuudesta vastaavat toimijat ovat ottaneet tilanteen jo pitkään tosissaan ja lisäävät valmiuttaan harjoittelemalla. Juuri nyt on tärkeää tiedostaa se, mistä vaikuttamisessa on oikeasti kysymys ja miten sitä vastaan voi puolustautua, muistuttavat monialaisen teknologiayritys Instan kyberturvallisuusasiantuntijat.

Ketju on yhtä vahva kuin sen heikoin lenkki

Installa huolehditaan paitsi puolustussektorin, myös kriittisestä infrastruktuurista ja huoltovarmuudesta vastaavien toimijoiden turvallisuudesta. Vuosien varrella tutuiksi ovat tulleet niin kyber- kuin hybridiuhat. Insta on järjestänyt kriisijohtamisharjoituksia esimerkiksi vesilaitoksille, vakuutusyhtiöille sekä useille valtionhallinnon organisaatioille, ja viime aikoina esille ovat nousseet erityisesti hybridiuhat.

– Hybridivaikuttamisen keinoja ovat esimerkiksi kyberhyökkäykset, informaatiovaikuttaminen, fyysinen vaikuttaminen sekä sotilaalliset operaatiot. Vaikuttamiskeinot ovat usein tehokkaita ja haitallisia niiden taustalla olevan toimijan suurien resurssien vuoksi, kertoo Instan turvallisuusasiantuntija **Erik Salli**.

Esimerkkinä hybridivaikuttamisesta voidaan mainita Ukrainaan ennen helmikuuta 2022 Venäjän kohdistamat laajat kyberhyökkäykset ja informaatio-operaatiot. Koska hybridivaikuttaminen tapahtuu usein välillisesti, kansalaisten ja eri toimijoiden kautta, on ketju yhtä vahva kuin sen heikoin lenkki. Isokin organisaatio vai lamaantua pienestä syystä.

– Usein hybridiuhkia käytetään kattoterminä kaikille vaikuttamiskeinoille, mutta todellisuudessa kysymys on eri menetelmien yhdistämisestä vaikuttamiseksi kansalliseen päätöksentekoon, Salli tiivistää.

Mitä uhkien torjuminen edellyttää

Simuloitu johtamisharjoitus on paras tapa valmistautua tositilanteisiin, tunnistaa turvallisuuden pullonkaulat ja minimoida vahingot. Installa onkin havaittu se, että kiinnostus harjoituksia kohtaan on lisääntynyt kaikilla sektoreilla. Vaikka Suomen kokonaisturvallisuus ja yhteistyö on kansainvälisesti poikkeuksellisen hyvällä tasolla, ratkaisevaa on se, ettemme tyydy nykytilaan – varautumisen ylläpitäminen ja kehittäminen tulee olla jatkuvaa.

– Harjoituskenaariot on suunniteltava huolella, organisaation lähtötaso ja resurssit huomioiden. Simulaatioharjoituksessa päästään kuvaamaan eri vaikuttamiskeinoja yhtäaikaisesti, jolloin harjoitus kuvastaa organisaation todellista valmiutta kohdata vastaava tilanne, muistuttaa toistasataa harjoitusta vetänyt Instan projektipäällikkö **Joel Muujärvi**.

Instan fasilitoimia harjoituksia voidaan järjestää kustannustehokkaasti ja yhtä aikaa myös suurille joukoille. Esimerkiksi puolen päivän pituisilla verkostoharjoituksilla yli 50 vesilaitosta pääsi peilaamaan toimintaansa tositilanteeseen sekä selvittämään esimerkiksi sen, ovatko niiden kyberturvallisuustyökalut ja -osaaminen ajan tasalla sekä miten uhkiin on mahdollista varautua.

Hybridivaikuttamisen näkökulmasta edessä ovat yhä kriittisemmät ajat. Seuraavan kahden vuoden aikana Suomessa järjestetään useat vaalit, ja globaali vastakkainasettelu autoritaaristen ja demokraattisten maiden välillä on lisääntynyt. Siksi Installa kannustetaan paitsi yrityksiä, myös kansalaisia panostamaan tietoturvaan sekä varautumaan poikkeustilanteisiin.

Instan kriisi- ja valmiusjohtamisen ratkaisut vahvistavat organisaation johdon ja henkilöstön osaamista poikkeus- tai kriisitilanteissa. Harjoitellut toimintatavat kasvattavat turvallisuutta ja auttavat häiriötilanteen nopeassa hallinnassa. Näin voidaan myös minimoida kriisitilanteiden mahdollisesti synnyttämiä aineellisia ja aineettomia vahinkoja.

Lisää aiheesta:

www.insta.fi/asiakastarinat/vesilaitokset-varautuvat-harjoittelemalla (20.4.2023)

www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara (21.4.2023)

Lisätiedot:

Insta

Turvallisuusasiantuntija Erik Salli, p. 020 771 7936, erik.salli@insta.fi

insta.fi | Twitter | LinkedIn | YouTube

Media: media@insta.fi

Insta on turvallisen ja kestävän tulevaisuuden ratkaisija. Olemme edelläkävijä ja luotettava kumppani teollisuuden, puolustuksen, ohjelmistokonsultoinnin ja kyberturvallisuuden asiakkaillemme. Yhdistämällä huippuosaamisen ja älykkään teknologian kehitämme turvallisuutta ja suorituskykyä yhä nopeammin muuttuvassa digitalisoituvassa maailmassa. Ihmiset, osaaminen ja vastuullisuus ovat toimintakulttuurimme perusta. Vuonna 2022 perheyhtiömme liikevaihto oli 153,4 miljoonaa euroa ja henkilöstömäärämme noin 1 100. Lisätietoja: www.insta.fi