CySec Ice Wall Oy

Lausunto

29.01.2021

Asia: VN/ 797/2021

Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Lausunto

Organisaatioiden tietoverkkoihin tulee suunnitella ja toteuttaa kyvykkyys tutkia ja todistaa verkon tapahtumat autenttisten todisteiden pohjalta esim. esitutkintaan saattamiseksi. Lokit eivät ole autenttisia tietoverkon todisteita. Myös syyttömyys ja se että mitään ei ole tapahtunut pitää voida yksityiskohtaisesti todistaa.

Ehdotamme että lisätään teksti:

”Tietomurtojen selvittämiseksi tarvitaan useamman vuoden autenttiset ja täydelliset todisteet, sillä keskimäärin tietomurto on lähes vuoden kohteen verkossa. Tämän vuoksi tietoverkkoihin lisätään tutkittavuus- ja todistettavuusjärjestelmä kattamaan ao. verkon kriittiset kohdat. Prosessi, ohjeistus, valvonta ja johtaminen järjestetään autenttisten tietoverkon todisteiden saattamiseksi analyysiin ja edelleen esitutkintaan asti.

Järjestelmät ml. verkot, käyttäjät ja pääkäyttäjät eriytetään keskenään ja toisistaan siten, että vaarallisia työyhdistelmiä ei missään tilanteessa muodostu, ja em. ryhmillä ei ole mitään vaarallista työyhdistelmää oman organisaationsa tutkittavuus- ja todistettavuusjärjestelmäänsä eikä niissä oleviin autenttisiin todisteisiin.

Varautuminen aloitetaan prioriteettijärjestyksessä siten, että ensin alkaa keruu ja säilöntä riittävän pitkäksi ajaksi. Näin autenttiset todisteet ovat olemassa ko. asennuksesta alkaen. Osana varautumista koulutetaan, harjoitellaan ja todennetaan osaamisen osalta katkeamattomat autenttisten todisteiden kirjaus- ja käsittelykäytännöt.

Analyysin, esitutkinnan ja tutkinnan työkalujen kehitys tietoverkkojen primääridatan (raakadata) visuaalisointiin, automaattiseen analysointiin, koneoppimisen- ja tekoälyjärjestelmien opettamiseen mahdollistetaan lakimuutoksella, joka mahdollistaa organisaatioiden esitutkintaan tarkoitetun primääridatan hyödyntämisen kehitystyössä. Esim. tekoäly voi oppia oikein vain, mikäli täysin muuttamaton primääridata autenttisena todisteena on käytettävissä. Tätä varten kehitetään kansallinen prosessi, käytännöt, lupamenettelyt, valvonta ja lainvalmistelu.”

Tutkittavuus- ja todistettavuuskyvykkyys

Kyvykkyys sisältää katkeamattoman kirjausketjun (audit trail), katkeamattoman käsittelyketjun (chain-of-custody) sekä prosessin ja tämän mukaisen tietojärjestelmän. Näiden saavuttamiseksi järjestelyjen fyysinen turvallisuus, tekninen arkkitehtuuri ja koulutus tulee olla suunniteltu tietoverkon autenttisen sähköisen todisteen teorian mukaiseksi. Erityisesti järjestelmien keskinäiset, ihmisten keskinäiset sekä laitteiden ja ihmisten väliset toiminnot tulee järjestää uudelleen siten, että kaikki vaaralliset työyhdistelmät poistetaan.

Tietoverkossa kulkevan informaation keruu pitää olla täydellistä, luotettavaa ja turvallisesti toteutettua, jotta saavutetaan autenttisuuden perusvaatimus - alkuperäisyys. Vastaavasti säilytys tulee toteuttaa siten että autenttisuus säilyy, sekä riittävän pitkältä ajalta etukäteen. Tietojen käsittely tapahtuu fyysisesti erillisessä todisteverkossa.

Kriittisiin julkisen hallinnon organisaatioiden toimintoihin tulee prioriteettijärjestyksessä lisätä em. kyvykkyys ja kriittiset tietovarastot tulee varustaa em. kyvykkyydellä.

Käsittely varautumisesta aina mahdolliseen esitutkintaan saattamiseksi suoritetaan Network Evidence Reference and Discovery -mallin mukaisella prosessilla, jolla voidaan todistaa kirjaus- ja käsittelyketjujen katkeamattomuus.

Tietoverkon autenttisten todisteiden (primääridatan) tutkittavuus- ja toistettavuusjärjestelmä vertaantuu vastaavaan kyvykkyyteen kirjanpidossa. Kirjanpitolaki, asetukset ja Kilan ohjeet luovat perustan kirjanpidon / taloushallinnon käyttöön siten, että audit trail on aina todennettavissa.

Toteutus suunnitellaan järjestelmä- ja käyttäjätasolla siten että vaarallisia työyhdistelmiä ei synny tuotantoverkon, hallintaverkon ja itsenäisen todisteverkon kesken ml. henkilökunta, käyttäjät ja muut osapuolet.

Kaikki tuotantoverkkojen tietojen omistajat (engl. data owner) tulee nimetä, kouluttaa ja ohjeistaa johtamaan oman organisaationsa osalta autenttisten todisteiden käyttö analysoinnista aina esitutkintaan saattamiseksi. Tietojen omistajat päättävät, valvovat ja johtavat – mutta eivät itse osallistu – analyysit ja toimenpiteet aina esitutkintaan saattamiseksi. Käytössä on yksi-yli-yhden -periaate eli kaikkia toimenpiteitä suorittaa kaksi henkilöä.

Tietoverkko ja tietomurrot

Tietoverkko on ihmisen rakentama eikä siihen ole sisäänrakennettu tietoturvaa, lokit ovat laitevalmistajien ja ohjelmoijien subjektiivisia näkemyksiä siitä mitä on tapahtunut ja kaikkia tietoverkosta tapahtuvia hyökkäyksiä ei voida estää, sillä havainnointi- ja estojärjestelmät ovat jopa satoja päiviä jäljessä hyökkääjiä.

Tietomurrot ovat sisällä kohteen verkossa keskimäärin 280 päivää! Näin kertoo Digital Guardianin Ponemon Instituutin ja IBM:n tutkimusta kuvaava artikkeli: Average time to identify and contain a data breach (2020) https://digitalguardian.com/blog/what-does-data-breach-cost-2020.

Tietojemme mukaan Suomessa kukaan ei ole tehnyt havainnointi- ja estojärjestelmästä SLA-sopimusta, jossa luvataan estää kaikki tietomurrot. Kaikki em. järjestelmien toimittajat ovat kiertäneet jopa kysymyksen havaitsetteko tietomurrot ja estättekö kaikki hyökkäykset?

Isoja tietomurtoja on Suomessa tapahtunut 90-luvulta lähtien lukuisia. Niitä on salattu julkishallinnon ja yksityisten yhtiöiden etujen suojelemiseksi. Emme nimeä yhtään salattua tietomurtoa, toteamme vain, että sekä idästä että lännestä on tehty tietomurtoja Suomeen.

Suomessa toimiva pörssiyhtiön henkilö totesi, että heiltä viedyillä suunnittelukuvilla aloitti idässä aivan uusi toimija kilpailun. Yritys laski menettäneensä useita satoja työpaikkaa Suomessa.

Arvioimme yhdessä että Suomesta menetettiin jopa 1500 työpaikkaa, kun huomioidaan välilliset vaikutukset – tämä siis yhdessä tietomurrossa.

Asiantuntijoiden lausunnot

Eri organisaatioiden kyberturva-asiantuntijat ovat yhtiöllemme lausuneet seuraavaa:

Kyberturva-asiantuntija: ”Kun yrität tutkia tietoverkkorikollisuutta, on usein ongelma: Tutkittavaa tietoa ei ole. Sinulla pitäisi olla koko verkkoliikenne tallennettu. Lokitiedot eivät riitä.”

Kyberturvajohtaja: ”Ulkoministeriön tietomurto olisi selvitetty muutamassa viikossa, jos olisi ollut tällainen järjestelmä käytössä.”

Kyberturvatutkija: ”Näyttää siltä, että kaikkia tapahtumia ja tietovuotoja ei havaita, koska puolustajilla ei ole käytettävissä yksityiskohtaista verkkodatahistoriaa. Analyysikyky on tietysti myös ongelma.”

Asiantuntija F-Secure, Traficom-seminaarissa 11/2019: ”Kyllä kaikki tietoverkon rikkomukset saataisiin selville kaiken tallentavalla järjestelmällä. Tällaista vaan ei ole!” Tähän muuten vastattiin, että kyllä sellainen on, ja vieläpä kotimainen ja patentoitu.

Strateginen kyberturvakysymys tänään kuuluu, kumpi tie valitaan: ”Tarttis tehrä jotain?” vai ”Kyllä se siitä?”. Suosittelemme edellistä, jälkimmäisestä on jo runsaasti kokemusta.

Sairaanhoitopiirit

Sairaanhoitopiireihin tehdyissä haastatteluissamme selvisi, että (kyber)turvallisuuden johtaminen on jakaantunut kolmeen erilliseen osaan: IT vastaa verkosta ja palvelimista sekä käyttäjien järjestelmistä, turvallisuusjohtaja vastaa fyysisestä henkilöturvallisuudesta ja sairaalainsinööri vastaa lääkintälaitteista ja niiden turvallisuudesta. Lisäksi lääkäri vastaa potilaasta ja sairaanhoitaja esim. lääkkeen antamisesta.

Erään SHP:n juristitaustainen hallintojohtaja totesi haastattelijalle tulokset kuultuaan tämän tarkoittavan sitä, että kukaan ei todellisuudessa vastaa mistään! Hän tarkoitti käsittääksemme tällä sitä, että kolmelle taholle jaettu vastuu kadottaa todellisen vastuun. Lähde: H. Kamppuri – SHP haastattelut.

Osaaminen

Suomessa on syytä kehittää uusia kotimaisia kyberturvatuotteita, -palveluita ja tätä kautta osaamista. Tätä mitataan suoraan alan patenttien ja liikevaihdon määrällä.

Toimittaessa pelkästään ulkomaisilla tieto- ja tietoturvajärjestelmillä osaaminen on siirtynyt Suomesta pois eikä siirry kotimaiseksi osaamiseksi. Lisäksi tänne ei hakeudu osaajia, koska täällä ei kehitetä merkittävästi uutta. Esim. tuotannonohjaus- ja terveydenhuoltojärjestelmien osaaminen on siirtynyt voimakkaasti pois Suomesta 2000-luvulla. Samalla kyky tunnistaa kyberturva-loukkauksia on vakavasti heikentynyt.

Nykyisellään Suomessa opetetaan sertifiointikursseja ja taidot ovat opetettuja (’hauki on kala’ -oppiminen). Todellinen oppiminen edellyttää soveltamista ja uuden luomista aidolla autenttisella esitutkintakelpoisella materiaalilla.

Kyberturvallisuutta ajatellaan lähes pelkästään horisontaalisena ongelmana, kun pitäisi ottaa rinnalle vertikaalinen ajattelu.

Tavoitteista puuttuu mittarit, ehdotamme esim.

1. Kaikkien kriittisten palvelimien tietoliikenneyhteydet tulee varustaa kyvykkyydellä yhdistää tutkittavuus- ja todistettavuusjärjestelmä. Tämä on tehtävä varautumisvaiheessa, jotta mahdollisen tutkinnan alkaessa voidaan nopeasti palata tutkimaan vanhoja tietoliikennetapahtumia.

2. Muutetaan lainsäädäntö niin että se mahdollistaa primääridatan käyttämisen kotimaisessa kyberturvatuotekehityksessä

Luuppala Harri

Kamppuri Heikki
CySec Ice Wall Oy - Toimitusjohtaja