Salpakari / Viitaila
Riskienhallinta / KTK

10.10.2016

Dnro:
976/04/2016

Valtiovarainministeriö

Lausuntopyyntö 14.9.2016, VM136:09/2013

Viestintäviraston lausunto VAHTI 3/2016 Tietoturvapoikkeamien hallinta - ohjeluonnokseen 14.9.2016

Viestintävirasto kiittää mahdollisuudesta esittää lausuntonsa VAHTI 3/2016 Tietoturvapoikkeamien hallinta - ohjeluonnokseen 14.9.2016 ja tuo esille seuraavat ehdotukset:

1 Kohta 3.3.5

"Kokouksen koollekutsujana toimii usein Kyberturvallisuuskeskus." -kohta pitäisi muuttaa "Kokouksen koollekutsujana toimii Viestintäviraston Kyberturvallisuuskeskus.".

2 Kohta 3.3.8

Ensimmäisessä virkkeessä tarkoitetaan varmaankin tieto**suoja**valtuutettu tieto**turva**valtuutetun sijaan.

3 Kohta 5.1.4.5 Haittaohjelmatilanteet

"Kiristyshaittaohjelmia vastaan voi suojautua rajaamalla käyttäjien käyttöoikeuksia, pitämällä virustorjunnan ajan tasalla sekä huolehtimalla varmuuskopioiden ajantasaisuudesta ja palautusjärjestelyjen säännöllisestä testaamisesta."

Tässä kohdassa tulisi huomioida, että varmuuskopiot tulee fyysisesti erottaa suojattavasta järjestelmästä. Varmuuskopiointi toiselle loogiselle levypartiolle tai toiselle, järjestelmään yhteydessä olevalle verkkolevyasemalle, ei välttämättä estä järjestelmän saastumista.

4 Kohta 5.1.4.7 Tietojen kalastelu (phishing)

"Tärkein suojauskeino tietojenkalasteluyrityksiin on käyttäjien tietoturvakoulutus. Tiedot, joita useimmiten yritetään viedä, ovat käyttäjätunnuksia ja salasanoja, mutta hyökkääjä saattaa olla kiinnostunut myös muista tiedoista."

Tässä kohdassa voisi olla esimerkkejä: "kuten organisaatiorakenteesta, maksuprosesseista, organisaation käytössä olevista järjestelmistä, henkilöiden vastuista, loma-ajoista ja sijaisjärjestelyistä"

5 Kohta 5.2 Todistusaineiston turvaaminen

"Todistusaineiston käsittelyssä on olennaista turvata aineiston eheys ja aikaleimat."

Tässä kohdassa tulisi korostaa ennakkotoimintaa esimerkiksi seuraavasti "Tämän vuoksi onkin tärkeää, että järjestelmien käyttämät kellot synkronoidaan mahdollisen tapahtuman selvittämisen helpottamiseksi."

6 Kohta 6.1. Tekniset toipumistoimenpiteet

"Toipumisvaiheessa tehtävät toimenpiteet voivat vaihdella paljonkin riippuen siitä, minkälaisesta poikkeamasta on ollut kysymys. Poikkeaman seurauksena voidaan joutua mm.:

- palauttamaan tietoja varmuuskopioista
- korjaamaan haavoittuvuuksia
- päivittämään järjestelmiä tai asentamaan niitä kokonaan uudelleen
- vaihtamaan salasanoja tai
- tiukentamaan tietoturvavaatimuksia"

Tässä kohdassa voitaisiin lisäksi mainita tilanne, että poikkeaman seurauksena voidaan olemassa olevia laitteita joutua vaihtamaan tai hankkimaan kokonaan uusia laitteita, jos vanhojen kapasiteetti tai yhteensopivuus aiheuttaa ongelmia nykyjärjestelmässä.

7 Kohta LIITE 2

TLP-protokollasta julkaistiin ensimmäinen laajaan valmisteluun perustuva määrittely CERT:ien yhteistyöjärjestö FIRST:n toimesta. Keskeisin muutos tietoturvayhteisössä liittyy TLP:AMBER-luokan määrittelyyn.

Uusi Amber-luokan määrittely kuuluu seuraavasti: "Tieto voidaan jakaa muille tiedonvaihtoryhmän jäsenille, tiedot vastaanottavan henkilön edustaman organisaation sisäisesti sekä organisaation sidosryhmissä tiedon edellyttämiin toimenpiteisiin ryhtymiseksi välttämättömille henkilöille. Tiedon luovuttaja voi tarvittaessa asettaa luokituksen yhteydessä lisärajoituksia tai -vapauksia tiedon käsittelylle. "Yksilöity tarve tietää"."

Liitteen kuvaukset voisi varmistaa yhdenmukaiseksi Viestintäviraston sivuilta löytyvän dokumentin (https://www.viestintavirasto.fi/attachments/cert/certtiedostot/julkaisu_003_2016_J.pdf) mukaiseksi.

Pääjohtaja Kirsi Karlamaa

Riskienhallintapäällikkö Juha Salpakari