Teemu Kumpulainen

Varjoista valoon: Järjestelmien kartoitus ja matka hallintaan

Abstract:

Kyberturvan ensimmäinen kenttätehtävä alkaa laitteistojen ja järjestelmien kartoituksesta. Ilman tiukkaa vaatimusta toimituksissa, ajansaatossa laitoksiin on kertynyt eri valmistajien komponentteja, ohjelmistoja sekä eri tasoisia järjestelmän sisäisiä verkkoja. IT näkökulmasta kaikkea tätä voisi kutsua ”Shadow IT” eli varjo IT nimellä.

Kysymys kuuluukin kuinka voin suojata jo kytkettyjä järjestelmiä eri uhilta ja kuinka uskallan kytkeä vanhoja järjestelmiä IT:en?

Pelkotilat ja kysymykset vähenevät, kun laitteistot saadaan kartoitettua, riskit, uhat ja vastatoimet määriteltyä sekä vastuuhenkilöt nimettyä.

Laitekannan sekä järjestelmien kartoitukseen ei ole yhtä valmista ratkaisua vaan työkalut, tapa, henkilöstö sekä tarvittavat tiedot tulee määritellä kokonaisuutena.

Laitteistojen skannaaminen

Aktiivinen, passiivinen vai manuaalinen keräys?
Kuka kerää ja saadaanko laitteista kerättyä kaikki tarvittavat tiedot?
Miten saadaan ylläpidettyä motivaatiota puuduttavaan tiedonkeruuvaiheeseen?
Jokaisessa tavassa on hyvät puolet ja puutteet.
Laitetietojen lisäksi täytyy pystyä keräämään ohjelmistotiedot Windows ja linux pohjaisista käyttöjärjestelmistä.

Aktiivisella skannauksella saadaan irti laitetiedot. Jotta aktiivisella skannauksella saadaan irti tarpeeksi laadukasta dataa, on kohdelaitteen tuettava tietoa antavia protokollia ja lisäksi niihin pitää olla verkon kautta pääsy.

Passiivisella monitoroinnilla nähdään, kuinka laite on ohjelmoitu kommunikoimaan ja ketkä ovat sen kommunikointipartnerit. Passiivinen tiedonkeruu vaatii tietenkin laitteen, jonka läpi tieto kulkee. Lisäksi tiedon olisi hyvä olla salaamatonta, jotta pakettien sisällöstä saadaan irti lisätietoja.

Manuaalisella kartoituksella saadaan kerättyä operointipohjaista, kirjoittamatonta tietoa, mikä on erittäin hyödyllistä jatkovaiheissa. Laitosta ja kabinetteja kierrettäessä tulee tarkkailtua myös fyysistä suojausta sekä hallitsemattomia ja virrattomia laitteita. Tähän työhön vaaditaan monesti mukaan kunnossapito- tai automaatiohenkilö, kenellä on valtuudet avata sähkökaappeja ja liikkua tuotannossa.

Laitteistotietojen keruu semi-automaattisesti ja manuaalisesti voi olla tekijälle tai tekijöille puuduttavaa. Tehtävän ”epäseksikkyyttä” voi piristää perustamalla yhteisö, tarinallistamisella ja pelillistämisellä. Näistä muutama esimerkki.

Laitteistotietojen jatkokäsittely

Jatkokäsittelyvaiheina on datan yhdistäminen eri tietolähteistä. Eri lähteistä luettuna samasta laitteesta voi syntyä duplikaatteja, sekä eri ohjelmistojen keräämät nimikkeet saattavat erota toisistaan, jolloin niitä pitää manuaalisesti yhdistellä ja muokata.

Kun tiedot on saatu järjesteltyä, tulee päätettäväksi, missä tiedot säilytetään (CMDB) ja tukeeko se tarvittavia tietomalleja. Tarvittaessa tiedot voi koota väliaikaisesti, vaikka exceliin.

Ryhmittelyn jälkeen voidaan aloittaa järjestelmien ja laitteistojen erottelut ja paloittelusuunnitelmat verkkopohjaista segmentointia varten. Segmentointityöpajoissa korostuu ja huomataan kerätyn datan riittävyys ja laatu, sekä vastuussa olevien henkilöiden operointi ja järjestelmä tuntemus.

Keywords: OT cybersecurity, Asset discovery and inventory, Champions, Data correlation, Segmentation

***Corresponding Author: Corresponding Author:** E-mail: teemu.kumpulainen@konecranes.com

1 Introduction

Puhevuorossa käydään läpi tietojenkeruu ja sen muutama jatkovaihe. Esityksen läpivientinä käytetään

esimerkkinä omakohtaisia kokemuksia vaiheiden läpiviennistä.

2 Extended abstracts

3 Bibliography

Kumpulainen Teemu

16 kokemus komponenttivalmistajan ja OT palvelun tarjoajan puolelta sisältäen vianhakua, suunnittelua sekä palveluiden rakentamista tuotantoympäristöihin.

Nykyään päivätöissä Konecranesin Globaalissa organisaatiossa OT tietoturvan erikoisasiantuntijana.

Ohjaavina sanoina työelämässä toimivat, “yksinkertainen on kaunista ja toimivaa” sekä ”ihmislähtöinen kyberturva”.

Authors may use any established style for formatting the references and for citing references in the text. The style should be consistent throughout the paper. The list of references should only contain papers cited in the text.