Kyberturvallisuudenhallinta

Harjoitustehtävä 01

Aro Jesper, TTV21S1

Jalkanen Kalle, TTV21S2

Koivisto Ossi, TTV21S2

Salomäki Sini, TTV21S5

Harjoitustehtävä
Kyberturvallisuudenhallinta TTC6020-3006, Nevala Jarmo
20.2.2024
Tieto- ja viestintätekniikka, insinööri (AMK)

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Taulukot

1 Johdanto

Tässä harjoitustyössä muodostamme ISO standardin 27001 ja 27002 mukaisen omaisuuden hallinnan käytössä olevaan vle ympäristöön. Käymme läpi DefendByVirtual-yhtiön omaisuuserät, sekä mitä hallintakeinoja hyödynnetään omaisuuden hallinnassa. Lisäksi listaamme DefendByVirtualin käytössä olevat turvallisuus-/hallintatyökalut, sekä niiden tarkemmat kuvaukset, jotka sisältää turvallisuus-/hallintatyökalun nimen, version, käyttötarkoituksen sekä miksi ja miten työkalu liittyy ympäristöön.

1.1 5.9 Tietojen ja niihin liittyvät omaisuuserät

Taulukko 1 organisaation omaisuus

Omaisuus luokka:	**DefendByVirtualin omaisuuteen kuuluu:**
Tieto-omaisuus	- Koulutuspalvelu, sen sisältö sekä materiaali. - Tekninen asiantuntemus - Asiakastiedot - Käytetyt puolustusmekanismit sekä palvelut. - DefendByVirtualin omat puolustusmekanismit sekä omat tekniikat - Henkilöstön henkilökohtaiset tiedot
Ohjelmistot	- Windows 11 versio 10.0.22631 - Kali versio 2022.04 - Microsoft AD versio 88 - Palo Alto versio 10.1.3 - ElasticSIEM, versio 8.3.3, - Security Onion, versio 2.3.140 - Wazuh, versio 4.3.6 - Greenbone, versio 22.4 - Shuffle versio 1.0 - ITop versio 3.0.1 - TheHive versio 3.1.6-1 - Cortex versio 3.1.6-1 - Misp 2.4.161
Virtuaalikoneet	- WS01 - Onion - SIEM - SOAR - Kali-WS - Rocky-WS - MISP - WWW - NS1 - DC01 - WSUS - SRV01

Henkilöstö	- Matti Meikäläinen, Hallituksen puheenjohtaja - Jarmo Nevala, Toimitusjohtaja, Hallituksen varajäsen - Jarmo Viinikanoja, Liiketoimintajohtaja - Erkki Esimerkki, Tietoturvapäällikkö - Ossi Koivisto, Tietoturva-asiantuntija - Kalle Jalkanen, Tietoturva-asiantuntija - Sini Salomäki, Kouluttaja - Jesper Aro, Kouluttaja

Päivitetty 6.2.2024

2 5.10 Tietojen ja niihin liittyvien omaisuuserien hyväksyttävä käyttö

2.1 Käyttöoikeudet

Alla on listattuna DefendByVirtualin organisaatio, sekä kunkin ryhmän käyttöoikeudet yrityksen ympäristössä.

2.1.1 Johtotiimi

DefendByVirtualin johtotiimillä on pääsyoikeus ainoastaan WS-netin koneelle, joka on yhdistetty servers-netissä olevaan SRV01 tiedostopalvelimeen, verkkolevynä.

2.1.2 Hallitus

DefendByVirtualin hallituksella on oikeus päästä vain WS verkon koneille, joille servers-netin SRV01 tiedostopalvelin on jaettu verkkolevyksi.

2.1.3 Kyberturvallisuuspalvelut

DefendByVirtualin kyberturvallisuuspalveluihin ryhmään kuuluvat henkilöt saavat käyttää ws-net:issä olevaa työasemaa, joka käyttää myös servers-netissä olevaa SRV01 tiedostopalvelinta verkkolevynä. Heillä on myös oikeus Admin-net ympäristöön, sillä sen auditointi ja valmistelu kuuluu kyberturvallisuuspalveluiden henkilöstölle.

2.1.4 Koulutuspalvelut

Koulutuspalvelu ryhmään kuuluvat henkilöt saavat käyttää ws-net:issä olevaa työasemaa, joka käyttää myös servers-netissä olevaa SRV01 tiedostopalvelinta verkkolevynä. Heillä on myös oikeus Admin-net ympäristöön, sillä sitä käytetään koulutusmateriaalina ja esimerkkiympäristönä.

2.1.5 GNA

GNA vastaa ympäristöstä ja sen laitteista, joten heillä on pääsy kaikkiin aliverkkoihin ja laitteisiin, myös palomuuriin.

2.2 Kopioiminen ja säilyttäminen

DefendByVirtual organisaatiossa on tehty selkeä suunnitelma, kopioihin liittyvistä käytänteistä. Tehdessään kopion henkilöstön jäsenen tarvitsee ottaa kopio, joko cntr+c tavalla tai cp komennolla, eikä luoda uutta vastaavaa, näin varmistamme, että kopioitujen tiedostojen oikeudet pysyvät muuttumattomina alkuperäisistä.

Organisaation omaisuuden säilyttämiseen liittyvät käytännöt ovat taas valmistajien dokumentaation mukaiset. Olemme varmistaneet sisäisesti, että GNA huolehtii fyysistä laitteista ja yhteyksistä valmistajien ohjeistuksen mukaisesti.

DefendByVirtualin sisäinen ohjeistus on myös se, että tallenteiden kohdalla, tallennetiedostoihin tulee merkata: päiväys, paikka, palaverin/tapahtuman nimi. Tallenteita tulee säilyttää SRV01 laitteella erikseen ”Tallenteet[kuukausi/vuosi]” nimisessä kansiossa.

DefendByVirtual organisaatiossa tietojen tahatonta häviämistä pyritään välttämään, tämän takia SRV01 laitteella tulee tehdä raid 10 ratkaisu, jonka tarkoituksena on auttaa tiedostojen saatavuudessa ja palauttamisessa, jos fyysisiin levyihin ilmenee ongelmia. Toteutamme myös varmuuskopiota SRV01 palvelimesta, ajoitetusti kerran viikossa. Näin pystymme palauttamaan palvelimen nopeammin esim. tulipalon jälkeen. Varmuuskopiota säilytetään aina 2 kerrallaan (viime ja sitä edeltävä) ja itse varmuuskopio levyjä säilytetään organisaation tiloissa, kaukana SRV01 laitteesta,

2.3 Omaisuuserien ja tietojen omistajien tietojen ylläpito

Omaisuuseristä on luotu luettelo, jota tulee päivittää aina kun järjestelmään tehdään muutoksia. Tähän lukeutuu laitteet, sekä ohjelmistot. GNA vastaa luettelon luonnista ja ylläpidosta, sekä päivitetty listaus on aina toimitettava DefendByVirtualin tietoturvapäällikölle. DefendByVirtualin tietoturvahenkilöstö vastaa, että kaikkia tietoturvapolitiikoita ja -käytänteitä noudatetaan ja että ne ovat ajan tasalla. Tietoturvahenkilöstö tekee nämä yhteistyössä käyttöpalveluympäristöstä vastaavan GNA:n kanssa. Omaisuuserien käyttöä on seurattava ja raportoitava mahdollisista tietoturvariskeistä.

3 5.11 Omaisuuden palauttaminen

Omaisuuden palauttaminen kuuluu ehkäisevään hallintakeinotyyppiin, jonka tarkoituksena on määritellä miten henkilöstön ja muiden sidosryhmien tulisi palauttaa organisaatiolle kuuluva omaisuus työsuhteen tai sopimuksen päättyessä tai muuttuessa. Tämä ottaa osanaan kantaan organisaation omaisuuden suojaamiseen. (SFS-EN ISO/IEC 27002:2022, 30)

ISO27002:2023 ohjeistuksen mukaan ensinnäkin työsuhteen muutos- ja päättymisprosessin tulee olla määritelty ja siinä tulee olla ilmoitettuna selvästi organisaation niin fyysisen kuin sähköisenkin omaisuuden palauttaminen. Henkilön on myös mahdollista ostaa laitteistoa omaan käyttöön, missä tilanteessa on hyvä olla merkittynä, miten näissä tilanteissa tulee menetellä. Laitteiston lisäksi ohjeistuksessa on otettava huomioon tärkeitä tietoja koskevat menetelmät. Jos henkilöllä on yrityksen toiminnan kannalta oleellista tietoa itsellään, on se kirjattava ylös ja toimitettava organisaation haltuun. Irtisanoutunutta tai irtisanottua henkilöä tulee irtisanomisaikana sekä sen jälkeen estää pääsemästä kopioimaan yrityksen tietoja, mikäli siihen ei ole erillistä lupaa. (SFS-EN ISO/IEC 27002:2022, 31)

3.1 Työsopimus

DefendByVirtual organisaation henkilöstöhallinnosta vastaa johtotiimi. Työsopimuksiin on merkitty, jos ei vielä niin jatkossa kohta, jossa mainitaan omaisuuden molemminpuolisesta palauttamisesta työsuhteen päättyessä. Organisaation ohjeistuksen mukaisesti työntekijä ei saa tallentaa henkilökohtaisia tiedostojaan tai dokumenttejaan työ käytössä olevalle koneelle. Työntekijällä on

velvollisuus palauttaa organisaatiolle kuuluvan omaisuuden kuten tietokoneen, oheislaitteet, mahdollisen työpuhelimen sekä mahdolliset yrityksen toimintaa koskevat tiedot, kuten esimerkiksi sähköpostit ja yksityisissä tallennusalustoissa kuten pilvialustoilla (OneDrive, Google Drive, DropBox...) olevat tiedot, joita ei ole erikseen dokumentoitu. Yritys ei saa työsuhteen päätyttyä murtaa poistuneen henkilön salasanaoja päästäkseen käsiksi tietoihin vaan mahdolliset siirrot on tehtävä työsuhteen aikana, työntekijän suostumuksella. Työntekijällä on myös oikeus poistaa omia, ei yrityksen toiminnalle merkityksellisiä tietoja kuten esimerkiksi sähköposteja ennen työsuhteen päättymistä.

3.2 Omaisuuden lunastaminen

Työntekijällä on mahdollisuus lunastaa organisaation laitteita omaan henkilökohtaiseen käyttöön. Organisaatiossa on sovittu, että lunastus on mahdollinen, mikäli laitteen takuuaika on ummessa tai laite ei enää jostain muusta syystä sovi pitempiaikaiseen työkäyttöön. Kun lunastettava laite on tietokone, mobiili- tai muu tallentava laite työntekijä on velvollinen siirtämään tiedot yritykselle, mikäli tiedon sisältö on yrityksen toiminnalle merkityksellistä. Määritetyt toimenpiteet ovat laitteesta riippuvaisia.

3.2.1 Tietokone

Työsuhteen päättänyt on velvollinen keräämään tarvittavat tiedot talteen koneelta ja luovuttamaan yritystoiminnan kannalta merkittävät tiedot organisaation haltuun organisaation määrittämällä tavalla kuten esimerkiksi organisaation hallinnoimaan pilvitallennus alustaan. Tietokone tulee turva tyhjentää eli laitteen muisti on formatoitava ja ajettava läpi soveltuvalla tyhjennys työkalulla esimerkiksi Blanccolla. Vaihtoehtoisesti tietokoneen muistin voi vaihtaa uuteen ja vanha käytöstä poistunut tulee tuhota asian mukaisesti.

3.2.2 Mobiililaite

Mobiililaitteesta tallennetaan tarvittavat yhteystiedot ja muut yrityksen toiminnalle tarpeelliset tiedot. Puhelimesta otetaan talteen yrityksen omaisuudeksi lukeutuvat SIM-kortti/kortit, jotka tarvittaessa siirretään seuraavan työntekijän käyttöön tai tuhotaan. Työnantaja huolehtii SIM kortin tietojen päivittymisestä operaattorille. Lopuksi puhelin tulee alustaa ennen sen luovutusta työsuhteen päättäneelle henkilölle.

3.2.3 Fyysinen tallennusväline

Tallennusvälineen sisältö on työsuhteen päättäneen vastuulla siirtää organisaation haltuun yritystoimintaa koskevat tiedot. Työntekijä poistaa itse tarpeettomat tiedostot. Tallennusvälinne tulee turvatyhjentää ennen lunastusta.

4 Pohdinta

Mielestämme tehtävä tuki hyvin kurssin oppimistavoitteita, ja sen tekeminen oli mielekästä, Emme juurikaan kokeneet ongelmia, mutta koemme silti oppineemme paljon. Ainoa haasteemme oli varmaankin itse tehtävänannon selvittäminen, ja ryhmän sisäiset pohdinnat siitä, että haluammeko tehdä 5.9–5.11 vai laajemmin. Hetken puinnin jälkeen tulimme lopputuloksen että 5.9–5.11 käsittelee mielestämme tärkeimmät osuudet.

Lähteet

ISO/IEC 27002. 2022.Information security, cybersecurity and privacy protection — Information security controls. Oline SFS. Viitattu 19.2.2024.