jamk

Harjoitustyö 2, Haavoittuvuuksien Hallinta

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Kyberturvallisuuden hallinta TTC6020-3007
29.10.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto 2
2 Haavoittuvuuksien hallinta taustaa 3
3 Toteutettavat standardit 4
3.1 8.8 Teknisten Haavoittuvuuksien hallinnan toteutus 4
3.1.1 Tarkoitus 4
3.2 8.19 Ohjelmistojen asentaminen tuotantoympäristöön 5
3.2.1 Tarkoitus 5
4 8.8 Teknisten Haavoittuvuuksien hallinnan toteutus 5
4.1 Haavoittuvuuksien tunnistaminen 5
4.2 Haavoittuvuuksien arviointi, käsittely ja korjaaminen 8
4.3 Haavoittuvuuksien seuranta ja dokumentointi 8
5 8.19 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin toteutus 9
5.1 Asennusten turvallisuus 9
5.2 Ohjelmisto elinkaaren hallinta 9
6 Pohdinta 10
Lähteet 11
Liitteet 12
Liite 1. Ohjelmistot 12
Liite 2. Haavoittuvuudet 12

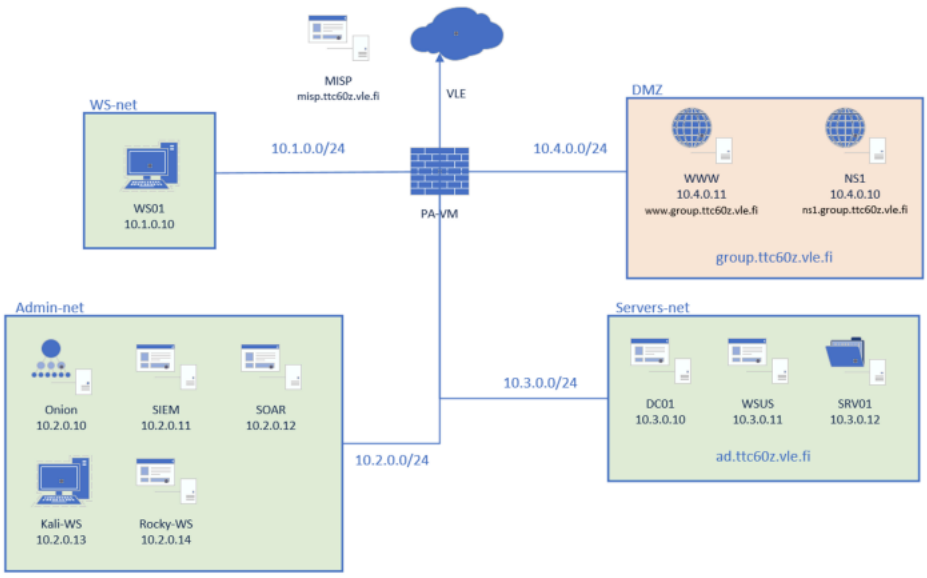
Kuviot

Kuvio 1. VLE 2
Kuvio 2. WS-netin skannauksen tulokset 6
Kuvio 3. WS-net:n CVE:t 6
Kuvio 4. CVSS-pisteytys 7
Kuvio 5. Admin-Net:n skannauksen tulokset 7
Kuvio 6. Servers-Net:n skannauksen tulokset 7
Kuvio 7. DMZ skannauksen tulokset 8

1 Johdanto

Tämän harjoitustyön tarkoitus on harjoitella ISO27001:2023 sekä ISO27002:2022 standardien mukaista haavoittuvuuksien hallintaa VLE ympäristössämme. Keskitymme standardien kappaleeseen 8. Teknologiset hallintakeinot. Haavoittuvuuksien hallinta on erittäin tärkeä osa organisaation tietoturvallisuutta, koska sen avulla pystytään hallitsemaan ja seuraamaan ohjelmistojen ja ympäristöjen mahdollisia haavoittuvuuk sia sekä niiden korjaamista ja seurausten pienentämistä. Harjoituksessa toteutamme haavoittuvuuksien skannauksia käyttäen Greenbone Vulnerability työkalua, toteutamme riskianalyysin ja laadimme suosituksia haavoittuvuuksien korjaamiseen ja lievittämiseen.

Harjoitus toteutetaan kuvitteellisen DefendByVirtual yrityksen VLE ympäristöön. (Kuvio 1)



Kuvio 1. VLE

2 Haavoittuvuuksien hallinta taustaa

Haavoittuvuuksien hallinta on keskeinen osa organisaation kyberjärjestelmän hallintaa, sillä haavoittuvuudet tekevät sen alttiiksi tietoturvauhille, kuten hakkereille. Hallinnan avulla voidaan pienentää järjestelmän hyökkäyspinta-alaa, jotta mahdollisilla hyökkääjillä ei ole niin paljoa mahdollisuuksia päästä järjestelmään. Haavoittuvuuksia voidaan hallita neljässä osassa, tunnistamalla, arvioimalla, selvittämällä ja jatkuvalla hallinnalla, kun niitä löytyy järjestelmän koneilla ja sovelluksissa. Haavoittuvuus tarkoittaa heikkoutta teknologiassa, jota hyväksikäyttäen hyökkääjä pääsee järjestelmän tietoihin käsiksi ilman tarvittavia valtuuksia. (What is Vulnerability Management? 2024.)

Haavoittuvuuksien löytäminen tapahtuu skannaamalla järjestelmää työkalulla, kuten Greenbone Vulnerability Manager (GVM). Skanneri etsii haavoittuvuudet sisäverkossa olevista järjestelmistä ja voi myös luokitella ne niiden kriittisyyden mukaan. (What is Vulnerability Management? 2024.)

Löytämisen ja haavoittuvuuksien tunnistamisen jälkeen ne voidaan luokitella perustuen riskiin. Riskiarvion saa usein suoraan työkalusta, jolla verkon skannaus tehdään. Haavoittuvuuksien hallinnassa riskejä luokitellaan esimerkiksi CVSS (Common Vulnerability Scoring System) -pisteytyksellä, joka luokittelee riskit niiden kriittisyyden mukaan. Arvioinnissa otetaan huomioon myös, miten haavoittuvuus kohdistuu liiketoimintaan ja miten vaikeaa se on toteuttaa hyökkääjän kannalta. Haavoittuvuuksien arvioinnilla organisaatio voi asettaa riskit selkeään tärkeysjärjestykseen. (What is Vulnerability Management? 2024.)

Seuraavaksi haavoittuvuudet tulee priorisoida ja yrittää korjata. Priorisoinnissa on useita vaihtoehtoja, liittyen siihen, miten haavoittuvuuksia tullaan käsittelemään jatkossa. Selvittäminen tarkoittaa haavoittuvuuden eliminoimista kokonaan, esimerkiksi päivityksellä. Lieventäminen tarkoittaa haavoittuvuuden mahdollisen hyväksikäytön estämistä muilla keinoin. Haavoittuvuus on olemassa, mutta sen vuoksi aiheutuvaa vahinkoa pyritään minimoimaan. Hyväksyminen tarkoittaa haavoittuvuuden jättämistä aloilleen. Haavoittuvuus voidaan hyväksyä, jos sen poistaminen tai minimoiminen maksaa organisaatiolle enemmän, kuin haavoittuvuuden mahdollisesti aiheuttama vahinko. (What is Vulnerability Management? 2024.)

Haavoittuvuuksien hallintaa on tärkeää ylläpitää ja varmistaa sen toiminta myös jatkossa. Haavoittuvuuksien jatkuva hallinta on prosessi, jota tulee tehdä jatkuvasti, jotta organisaation haavoittuvuudet ovat tiedossa ja organisaation reagointi näihin on ajantasaista. Skannaus ja valvonta tulisi olla tietyin väliajoin tapahtuvaa, jotta nouseviin tietoturvauhkiin voidaan varautua nopeasti. (What is Vulnerability Management? 2024.)

3 Toteutettavat standardit

ISO 27001:2023 ja ISO 27002:2022 ovat tietoturvan hallintajärjestelmän standardeja, jotka tarjoavat ohjeistuksia ja suosituksia tietoturvakäytäntöjen toteuttamiseen. Standardit painottavat riskien arviointia, hallintaa ja ennaltaehkäiseviä toimenpiteitä, joilla pyritään suojaamaan organisaation tietoja ja resursseja. Näissä standardeissa teknologisten haavoittuvuuksien hallinta ja ohjelmistojen turvallinen asentaminen tuotantoympäristöön ovat keskeisessä roolissa.

3.1 8.8 Teknisten Haavoittuvuuksien hallinnan toteutus

Käytettävien tietojärjestelmien teknisistä haavoittuvuuksista hankitaan tietoa. Organisaation altistuminen näille haavoittuvuuksille arvioidaan ja niihin liittyviin riskeihin vastataan asianmukaisilla toimenpiteillä. (SFS-EN ISO/IEC 27002:2022, 102). Haavoittuvuuksien hallinta on olennainen osa tietoturvan hallintaa, sillä hyödyntämättömät tai korjaamatta jääneet haavoittuvuudet voivat johtaa merkittäviin tietoturvariskeihin, kuten tietomurtoihin tai palvelunestohyökkäyksiin. ISO 27002 -standardin mukainen lähestymistapa haavoittuvuuksien hallintaan sisältää säännölliset skannaukset, riskianalyysit sekä suunnitellut korjaustoimenpiteet.

3.1.1 Tarkoitus

Estetään teknisten haavoittuvuuksien hyväksikäyttö. (SFS-EN ISO/IEC 27002:2022, 102). Tämä saavutetaan tunnistamalla ja arvioimalla järjestelmien haavoittuvuuksia, priorisoimalla ja varmistamalla, että riskitaso pysyy hyväksyttävällä tasolla.

3.2 8.19 Ohjelmistojen asentaminen tuotantoympäristöön

Toteutetaan menettelyt ja toimet, joilla hallitaan turvallisesti ohjelmistojen asentamista tuotantokäytössä oleviin järjestelmiin. (SFS-EN ISO/IEC 27002:2022, 120). Standardin mukaan organisaatioiden tulee varmistaa, että kaikki asennettavat ohjelmistot on testattu asianmukaisesti ennen tuotantokäyttöä ja että niiden päivitysprosessi on kontrolloitu. Tämä auttaa ehkäisemään virheiden tai haitallisten ohjelmien joutumista tuotantojärjestelmiin, mikä voisi vaarantaa liiketoimintaprosessit tai altistaa ympäristön hyökkäyksille.

3.2.1 Tarkoitus

Varmistetaan tuotantokäytössä olevien järjestelmien eheys ja estetään teknisten haavoittuvuuksien hyödyntämiseen. (SFS-EN ISO/IEC 27002:2022, 120). Tämä saavutetaan asettamalla selkeät säännöt ja ohjeet ohjelmistojen asentamiselle, kuten päivitysten validointi, testaus- ja hyväksymisprosessit, sekä käyttäjäoikeuksien rajoittaminen

4 8.8 Teknisten Haavoittuvuuksien hallinnan toteutus

DefendByVirtual yritykselle on luotu omaisuuserien luettelo, joka sisältää ohjelmistojen toimittajat, ohjelmistojen nimet, versionumerot, käyttötilanteet ja ohjelmistosta vastaavat henkilöt. Luettelon avulla pystytään toteuttamaan teknistä haavoittuvuuksien hallintaa. Luettelo on liitteenä Liite 1.

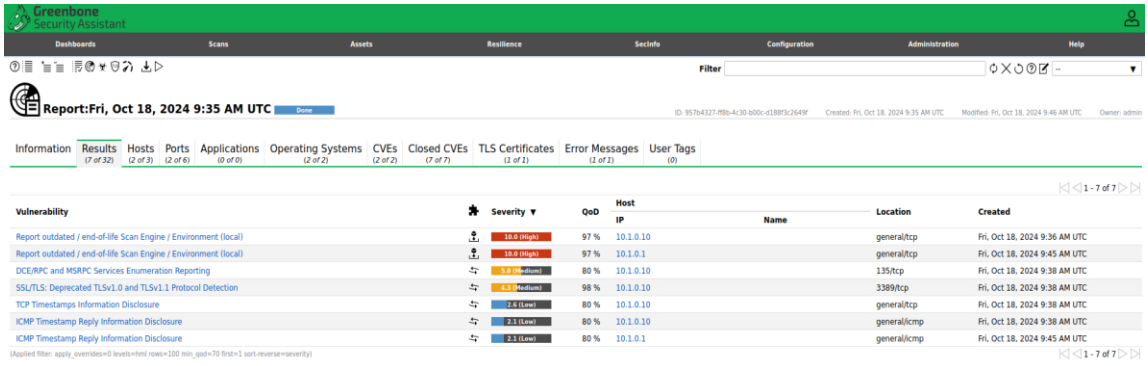
4.1 Haavoittuvuuksien tunnistaminen

Haavoittuvuuksien tunnistaminen on olennainen osa ISO 27002 standardin kohdan 8.8 toteuttamista. Toteutamme haavoittuvuuksien skannaamisen Greenbone Vulnerability Managemet (GVM) -työkalun avulla. GVM:n pääsee käsiksi Admin-verkon Kali-työasemalla.

Greenbone Vulnerability Management (**GVM**) on avoimeen lähdekoodiin perustuva haavoittuvuuksien hallintatyökalu, jonka avulla saadaan järjestelmän heikkoudet selville erilaisilla tietoturva skannauksilla. Se etsii järjestelmästä heikkoudet ja esittää ne selkeässä muodossa ylläpitäjille.

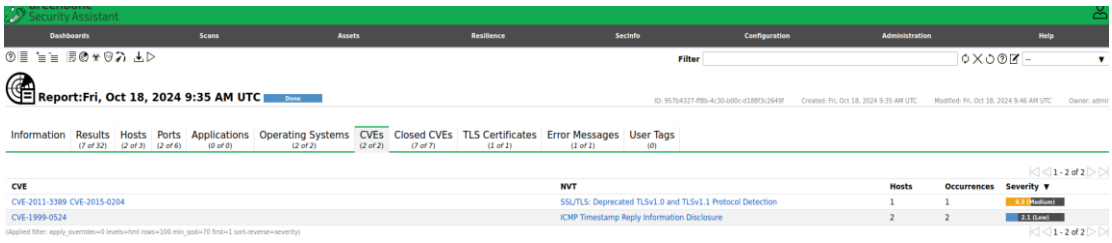
GVM käytöllä voidaan lyhentää aikaa, kun jokin haavoittuvuus on järjestelmässä, ja näin hallita järjestelmän haavoittuvuuksia tehokkaasti. GVM on Greenbonen nettisivujen mukaan maailmanlaajuisesti käytetyin järjestelmä haavoittuvuuksien hallintaan. GVM järjestelmällä saadaan organisaation haavoittuvuudet näkyviin, jonka jälkeen niitä voidaan korjata tai minimoida. (Protect Your IT Infrastructure from Hackers and Malware. 2024.)

Aloitimme skannaamalla WS-Net verkon GVM:llä. Skannauksissa Results-välilehdellä ylimmäisenä tuloksena näkyy tällä hetkellä vakaavuudella 10 oleva haavoittuvuus. Tämä ei sinänsä ole haavoittuvuus vaan kertoo, että käyttämämme GVM:n versio on vanhentunut, eikä sille ole enää valmistajan tukea. (Kuvio 2).



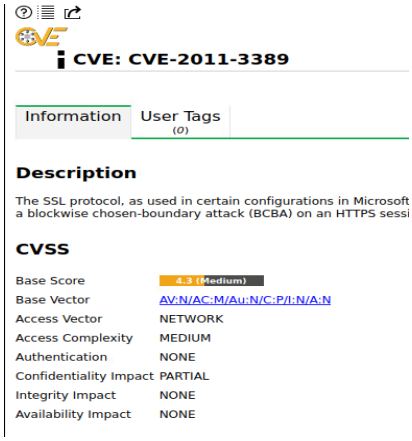
Kuvio 2. WS-netin skannauksen tulokset

CVEs -välilehdellä tarkastelimme järjestelmästä löytyviä CVE-tunnisteita (Kuvio 3). CVE on järjestelmä, joka antaa yksilöllisiä tunnisteita tietoturva-aukoille ja haavoittuvuuksille.



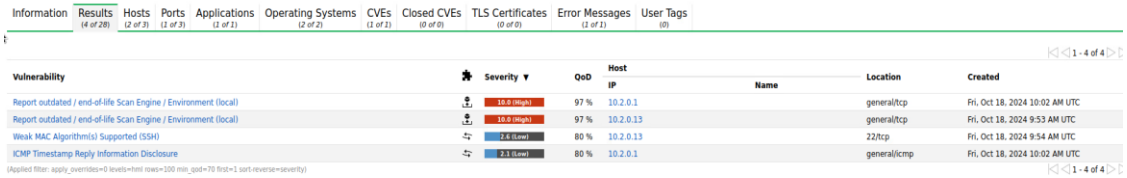
Kuvio 3. WS-net:n CVE:t

GVM laskee haavoittuvuuksien vakavuustasot valmiiksi skannauksen yhteydessä käyttäen CVSSV2-pisteytystä. Esimerkiksi haavoittuvuuden CVE-2011-3389:n CVSS-pisteytys on 4,3, joka vastaa keskitason haavoittuvuutta.

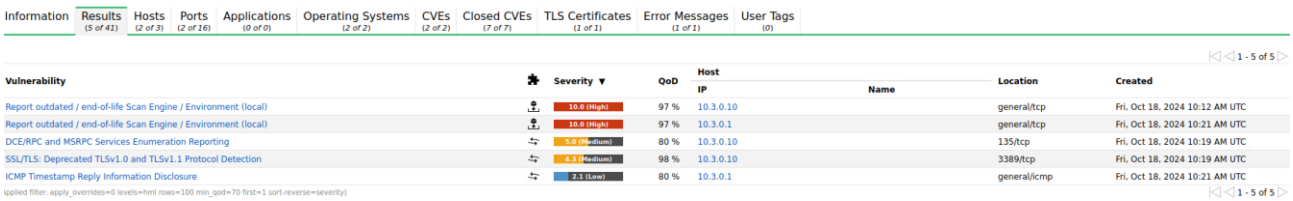


Kuvio 4. CVSS-pisteytys

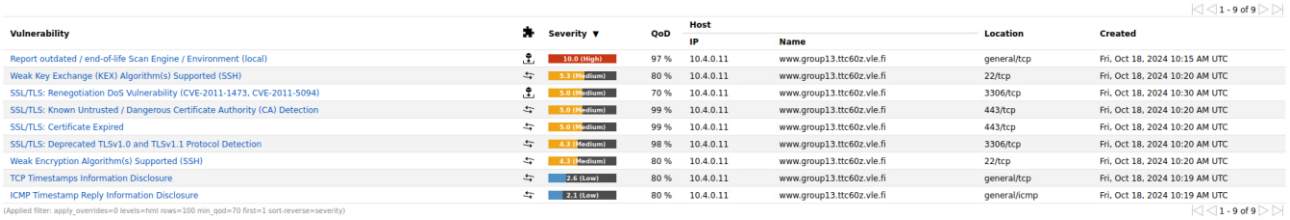
Skannasimme ympäristömme jokaisen verkon. Kuvioissa 5–7 on kuvakaappaus jokaisen verkon tuloksista.



Kuvio 5. Admin-Net:n skannauksen tulokset



Kuvio 6. Servers-Net:n skannauksen tulokset



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	10.4.0.11	www.group13.ttc60z.vle.fi	general/tcp	Fri, Oct 18, 2024 10:15 AM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	10.4.0.11	www.group13.ttc60z.vle.fi	22/tcp	Fri, Oct 18, 2024 10:20 AM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	10.4.0.11	www.group13.ttc60z.vle.fi	3306/tcp	Fri, Oct 18, 2024 10:30 AM UTC
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5.0 (Medium)	99 %	10.4.0.11	www.group13.ttc60z.vle.fi	443/tcp	Fri, Oct 18, 2024 10:20 AM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	10.4.0.11	www.group13.ttc60z.vle.fi	443/tcp	Fri, Oct 18, 2024 10:20 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	10.4.0.11	www.group13.ttc60z.vle.fi	3306/tcp	Fri, Oct 18, 2024 10:20 AM UTC
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	80 %	10.4.0.11	www.group13.ttc60z.vle.fi	22/tcp	Fri, Oct 18, 2024 10:20 AM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.4.0.11	www.group13.ttc60z.vle.fi	general/tcp	Fri, Oct 18, 2024 10:19 AM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	10.4.0.11	www.group13.ttc60z.vle.fi	general/icmp	Fri, Oct 18, 2024 10:19 AM UTC

Kuvio 7. DMZ skannauksen tulokset

4.2 Haavoittuvuuksien arviointi, käsittely ja korjaaminen

Löydettyjä haavoittuvuuksia arvioidaan käyttäen CVSS-pohjaista pisteytystä ja jaoteltu ympäristön verkkoihin. Otimme arviointiin mukaan haavoittuvuudet, jotka saivat CVSS-pisteytyksestä yli 4 pistettä, sekä CVE:t jotka näimme itse tarpeelliseksi korjata. Haavoittuvuudet, ympäristö, jota haavoittuvuus koskee, haavoittuvuuden vakavuus sekä korjaus- tai lievennysehdotukset ovat kuvattuna liitteessä 2.

4.3 Haavoittuvuuksien seuranta ja dokumentointi

Ympäristön haavoittuvuuksien seuranta on olennainen osa tietoturvaa, ja sen tehokkuus riippuu järjestelmällisestä lähestymistavasta. Haavoittuvuuksia tulee seurata järjestelmällisesti, koska versioiden vanhetessa järjestelmistä löytyy uusia haavoittuvuuksia, joita mahdolliset hyökkääjät voivat käyttää hyväkseen. Haavoittuvuuksia voidaan seurata esimerkiksi GVM-skannaustyökalulla, mutta siihen on myös muita tapoja. Skannauksia tulee tehdä järjestelmällisesti, mielellään mahdollisimman usein, jotta haavoittuvuudet eivät jää huomaamatta. Skannauksia tehdessä on tärkeää dokumentoida niiden tulokset, jotta organisaatiossa pysyy tieto haavoittuvuuksien kehityksestä ja niiden määrästä.

Skannaamisen lisäksi haavoittuvuuksien seurannassa on ajan tasalla pysyminen. Erilaisia haavoittuvuustietokantoja on paljon, ja on suositeltavaa seurata esimerkiksi National Vulnerability Databasea (NVD) ja tutkia siellä raportoituja haavoittuvuuksia, mitkä koskevat omaa ympäristöä. Laitteiden ja ohjelmistojen valmistajat julkaisevat tietoturvatiedotteita, joissa kerrotaan uusista tärkeistä päivityksistä ja korjauksista, joten niitä on hyvä seurata myös.

5 8.19 Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin toteutus

5.1 Asennusten turvallisuus

Järjestelmiin asennettaessa ohjelmistoja tulee noudattaa seuraavia säännöksiä.

1. Järjestelmiin asennettava ohjelmisto tulee olla onnistuneesti testattu.
2. Otetaan huomioon ohjelmiston mahdolliset ulkopuoliset ohjelmistot ja paketit, joita tulee tarkkailla ja hallita luvattomien muutosten estämiseksi.
3. Kun toimittaja asentaa tai päivittää ohjelmistoja, fyysinen tai ohjelmallinen pääsy annetaan vain tarpeen mukaan ja vain tarvittavin valtuuksin. Valvotaan toimenpiteitä asennuksen ajan.
4. Noudatetaan vähimmän oikeuden periaatteita. Yksilöidään minkä tyyppiset ohjelma asennukset on sallittuja ja mitkä kiellettyjä.

5.2 Ohjelmisto elinkaaren hallinta

Määritellään selkeät ohjeistukset ohjelmiston päivitykseen ja elinkaaren hallintaan. Näissä käydään läpi seuraavia ohjeita.

1. Vain koulutetut pääkäyttäjät päivittävät tuotantokäytössä olevat ohjelmistot, saatuaan valtuutuksen johdolta
2. Tuotantokäytössä olevat järjestelmät sisältävät vain hyväksyttyä koodia, ei kehityskoodia tai kääntäjiä
3. Ohjelmistojen lähdekirjastot päivitetään. Tuotantokäytössä olevia ohjelmistoja ja järjestelmädokumentaatiota hallitaan konfiguraationhallintajärjestelmällä.
4. Aina ennen muutosten toteuttamista määritellään palautusstrategia.

5. Ohjelmistojen kaikista päivityksistä ylläpidetään tapahtumalokia. Ohjelmistojen vanhat versiot arkistoidaan niin pitkäksi aikaa kuin mahdollista, kuin myös tarpeelliset tiedot, parametrit, menettely ja konfiguraatiot.

6. Kaikissa uuden version käyttöönottoa koskevissa päätöksissä otetaan huomioon muutoksen liiketoiminnalliset vaatimukset sekä version turvallisuus. Ohjelmistokorjaukset otetaan käyttöön, jos niillä voidaan poistaa tai vähentää tietoturvahaavoittuvuuksia.

7. Tarkkaillaan ja hallitaan ohjelmistojen ulkopuolisia ohjelmistoja ja paketteja.

8. Ylläpidetään tuotantokäytössä olevien ohjelmien versioita siten että toimittajien tuki säilyy. Jos on ohjelmistoja, joilla ei ole enää toimittajan tukea, otetaan huomioon sen niiden tuomat riskit. Päivitetään avoimenlähdekoodin ohjelmistoja viimeisimpään asianmukaiseen versioon.

6 Pohdinta

Harjoitustyön aikana keskityimme Iso 27001:2023 ja ISO 27002:2022 standardien mukaiseen haavoittuvuuksien hallintaan ja syvennyimme entisestään standardien hyödyntämiseen kyberturvallisuuden toteuttamisessa. Tehtävä kokonaisuuden hahmottaminen oli aluksi haastavaa pelkän tehtävän annon perusteella, mutta kun lähdimme taas pilkkomaan kokonaisuutta pienempiin osiin, saimme selkeämmän vision harjoituksen etenemisestä.

Aloitimme tehtävän standardien tutkimisella ja aloimme toteuttaa kohdan 8.8 mukaisia vaatimuksia. Pääsimme tässä yhteydessä tutustumaan haavoittuvuuksien tunnistamiseen GVM työkalulla, ja tämän jälkeen analysoimme paljastuneita haavoittuvuuksia. Tutustuimme skannausten suorituksen yhteydessä myös CVSS pisteytykseen. Harjoituksessa opimme, että skannausten tulosten perusteella on tärkeää käyttää systemaattista lähestymistapaa haavoittuvuuksien arvioinnissa. Kaikkia haavoittuvuuksia ei voida korjata välittömästi, joten priorisointi oli avainasemassa riskienhallinnassa.

ISO standardin kohtaa 8.19 tutkiessamme opimme myös paljon ohjelmistojen asennusten ja päivitysten testaus- ja hyväksyntäprosessin tärkeydestä. Tämä auttoi meitä ymmärtämään, että jopa pieni virhe ohjelmiston asennuksessa voi aiheuttaa tietoturvauhkan tai käyttökatkoksen. On siis tärkeää noudattaa tarkasti dokumentoituja asennusohjeita ja huolehtia siitä, että asennukset ja päivitykset suoritetaan asianmukaisesti.

Lähteet

Protect Your IT Infrastructure from Hackers and Malware. Greenbone sivusto. 2024. Viitattu 26.10.2024. https://www.greenbone.net/en/

SFS-EN ISO/IEC 27001:2023. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 4.8.2023. Viitattu 17.10.2024. https://janet.finna.fi/, SFS online

SFS-EN ISO/IEC 27002:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 18.11.2022. Viitattu 17.10.2024. https://janet.finna.fi/, SFS online

What is Vulnerability Management? Rapid7 artikkeli. 2024. Viitattu 26.10.2024. https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/

Liitteet

Liite 1. Ohjelmistot

Ohjelmistot

Liite 2. Haavoittuvuudet

Haavoittuvuudet