jamk

Puolustautumissuunnitelma

Ryhmä 13

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

Hyökkäykset ja puolustusmenetelmät TTC6040 - 3009
11.12.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

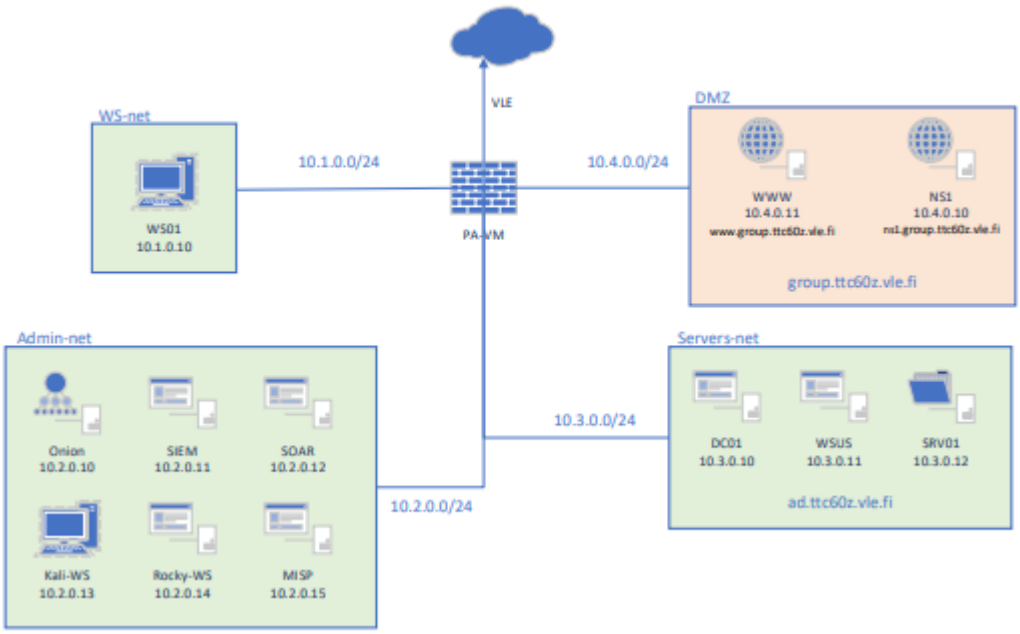
Kuviot

1 Johdanto

Tässä harjoitustyössä keskitytään DefendByVirtual yrityksen puolustautumissuunnitelman toteuttamiseen. Käymme läpi muun muassa seuraavia aihealueita:

- Ympäristön ja yrityksen kehityskohteet kyberpuolustus näkökulmasta
- Kehityskohteiden priorisointi
- arkkitehtuurien, teknologioiden ja toimitapojen yhteydet
- Ihmiset, teknologiat ja prosessit
- Lisäkovennukset ja kontrollit

Harjoitus perustuu DefendByVirtual yrityksen VLE ympäristöön, jota on kuvattu kuviossa 1.



Kuvio 1. VLE

2 Ympäristön kyberpuolustuksen kehittäminen

Tässä luvussa keskitymme VLE-ympäristön kehittämiseen muun muassa kovennuksilla, kontrolleilla, ja monitoroinnin parantamisella. Kehityskohteet pohjautuvat vahvasti aiemmin toteutettuun Uhka-arvioon, jossa on noussut ilmi kontrolleja mahdollisia hyökkäystaktiikoita vastaan. Parannuskohteiden porrastamiseksi ja toteutuksen mahdollistamiseksi olemme luokitelleen kehityskohteet 3 prioriteettiluokkaan. Prioriteetti 1 (0-3kk), keskitason prioriteetit 2 (3-6kk), pitkän aikavälin prioriteetit 3 (6-12kk).

2.1 Lyhyen aikavälin prioriteetit (0-3kk)

Teknologiat:

- **Verkkosegmentointi ja liikenteen hallinta:**
  - PA/VM-palomuurin sääntöjen vahvistaminen.
- **WS-net:**
  - Ota käyttöön 2 vaiheinen tunnistautuminen
  - Työasemien pääsynhallinta: Poista paikalliset admin-oikeudet
- **SRV01:**
  - Otetaan käyttöön tiivistefunktiot tiedostojen manipulointia vastaan
- **Admin-net:**
  - Varmista että hallintaverkkoon on pääsy vain MFA:ta käyttäen
- **DMZ ja Servers-net:**
  - Suojaa verkkosivut (WWW) ja DNS-palvelin (NS1) DDos-palveluilla. Esimerkiksi cloudflare
  - Kovennetaan DC01 lisää, varmistetaan palvelinsovellusten tietoliikenteen salaaminen
  - 2-vaiheinen tunnistautuminen sivuston administrator-paneeliin ja palvelimelle ssh-yhteydelle.

Prosessit:

- Kehitä monitorointityökalujen kuten ElasticSIEM sääntöjä vastaamaan ajankohtaisia uhkia.
- Varmista, että lokitiedot tallennetaan varmennettuun paikkaan, jossa niiden manipulointi estetään

Ihmiset:

- **Toteuta henkilöstön peruskoulutus, erityisesti:**
  - Phishing-hyökkäysten tunnistus ja sosiaalisen manipuloinnin riskit
  - Käyttämään MFA:ta tehokkaasti
- **IT-henkilöstön kouluttaminen**
  - Mahdollistetaan esimerkiksi sertifikaattien hankkiminen työn kautta
  - Mahdollistetaan esimerkiksi 10–15 % työajan käytöstä kouluttautumiseen

2.2 Keskitason prioriteetit 2 (3-6kk)

Teknologiat:

- **DNS ja palvelinvarmuudet:**
  - DNSSEC käyttöönotto NS1:ssä
  - Kovennetaan WWW- ja SRV01 palvelimet seuraamaan CIS Benchmark -ohjeita
- **Harjoitukset ja testaukset:**
  - Suoritetaan hyökkäyssimulaatioita ja arvioidaan olevien tietoturvakontrollien tehokkuutta
- **Sähköpostin suojaaminen:**
  - Lähettäjän luotettavuuden analysointi

Prosessit:

- Suunnitellaan, dokumentoidaan ja päivitetään poikkeamien hallintaprosessi
- Auditoidaan käyttöoikeudet kaikissa järjestelmissä ja varmistetaan niiden asianmukaisuus
- Asetetaan järjestelmäkohtaiset tarkistuslistat kovennuksia varten

Ihmiset:

- Koulutetaan IT-henkilöstöä tai palkataan uutta henkilöstöä suorittamaan hyökkäysten simulointi-testejä ja analysoimaan niiden tuloksia
- Järjestetään tai ostetaan kyberturvaharjoitus

2.3 Pitkän aikavälin prioriteetit 3 (6-12kk)

Teknologia:

- **Zero Trust -malli:**
  - Implementoidaan Zero Trust -periaatteet koko infrastruktuuriin. Kaikki yhteydet validoidaan ja autentikoidaan, ja pääsyt myönnetään vain tarpeen mukaan.

Prosessit:

- Laaditaan organisaatiolle kattava tietoturvastrategia
- ISO 27001 sertifiointi
- Dokumentaatioiden laajentaminen. MITRE D3FEND- ja OWASP- työkalujen käyttö suojausten suunnittelussa

Ihmiset:

- Vahvistetaan organisaation tietoturvakulttuuria jatkuvilla koulutuksilla.
- Tarjotaan edistyneempiä koulutuksia IT-henkilöstölle tietoturvan strategisista työkaluista (esim. Zero Trust -mallin hallinta ja SIEM:n analytiikka).
- Järjestetään koko henkilöstölle vuosittainen tietoturvatietoisuuspäivä

3 Arkkitehtuurin, teknologioiden ja toimintatapojen yhteen nivoutuminen

Tietoturvan rakentaminen ei voi tapahtua erillisinä osina. Arkkitehtuurin, teknologioiden ja toimintatapojen tulee toimia saumattomasti yhteen, jolloin jokainen osa tukee toisiaan. Tässä mallissa yhdistetään ihmiset, teknologia ja prosessit luomaan kokonaisvaltainen turvallisuusratkaisu.

3.1 Verkkosegmentointi ja arkkitehtuuri

VLE ympäristö on jaettu selkeisiin segmentteihin: WS-net, Admin-net, DMZ ja Servers-net. Tämä varmistaa kriittisten palveluiden kuten Active Directoryn (DC01) suojaamisen pääverkosta. Näiden segmenttien väliseen liikenteeseen sovelletaan ”Zero Trust” -periaatteita, eli liikenne validoidaan aina.

Segmenttien keskiössä toimii PA/VM-palomuuri liikenteen ohjaajana. Palomuurisäännöt integroivat teknologian ja prosessit estämällä asiattoman pääsyn ja valvomalla segmenttien välistä liikennettä, sekä verkon ulkoa tulevaa liikennettä.

3.2 Teknologiat ja automaatio

Ympäristössä on käytössä SIEM ja SOAR järjestelmät, jotka keräävät ja analysoivat tietoturvalokeja kaikista segmenteistä. SOAR automatisoi hälytyksiin vastaamista ja mahdollistaa nopean reagoinnin uhkiin. Tietoturvateknologiat tukevat ympäristön arkkitehtuuria, esimerkiksi Servers-netissä on käytössä eheysvalvonta, joka varmistaa tiedostojen eheyden.

Ympäristössä on myös käytössä Security Onion, joka valvoo verkkoliikennettä ympäristössä. Työkalu toimii yhdessä Wazuh ja ElasticSIEM järjestelmien kautta ja tarjoaa kokonaisvaltaisempaa kuvaa ympäristön tapahtumista.

3.3 Ihmiset ja toimintatavat

Henkilöstö on jaettu eri rooleihin: käyttäjät (WS-net), ylläpitäjät (Admin-net) ja verkkopalveluiden hallinnoijat (DMZ). Selkeät pääsy- ja käyttöoikeusprosessit määrittävät, kuka pääsee mihinkin verkkoon ja millä oikeuksilla. Prosesseja voidaan tukea vähimmäisoikeuksien periaatteella, sekä monivaiheisella tunnistautumisella.

3.4 Ihmiset, teknologia ja prosessit

Tietoturvan onnistuminen yrityksessä riippuu kolmen peruspilarin tasapainosta, jotka ovat ihmiset, teknologiat ja prosessit. Näiden kaikkien tulee toimia yhdessä, jotta voidaan varmistaa tietoturvallisuuden ja CIA (confidentiality, integrity, availability) kolmion toteutuminen.

Ihmiset:

- **Koulutus ja valvonta:**
  - Peruskäyttäjät koulutetaan tunnistamaan yleisiä uhkia kuten phishing
  - IT-henkilöstölle tarjotaan kehittyneitä koulutuksia, kuten Red Team -harjoituksia, sertifiointeja ja Zero Trust -mallien hallintaa.
- **Vastuunjako**
  - Poikkeamatilanteiden (incident response) vastuu jaetaan eri tiimien kesken esimerkiksi. SOC-tiimin jako 3 tasoon
    - **Taso1:** vastaa SIEM-hälytyksistä, niiden tutkimisesta ja eskaloinnista 2 tasolle. ¨
    - **Taso2:** Tutkii 1 tasolta eskaloituja tapauksia syvällisemmin. Suorittaa mutkikkaampien tapausten monitorointia ja analyysiä. Proaktiivinen hyökkääjien metsästys. Vastaa palautumisesta
    - **Taso3:** Vastaa vielä haastavammasta ja syvällisemmästä tutkimuksesta, suorittaa uhkien metsästystä ja uhkien tutkimista. Analysoi haittaohjelmia.

Teknologia:

- **Teknologia toimii mahdollistajana, mutta sen käyttöönotto vaatii strategiaa:**
  - **Proaktiiviset kontrollit**: IDS/IPS, SIEM:n analytiikka, SOAR:n automaatio.
  - **Reaktiiviset mekanismit**: Poikkeamien hallintaprosessit ja palautusjärjestelmät

- **Yhteistyö järjestelmien välillä:**
  - Esimerkiksi SOAR automatisoi SIEM:n keräämien hälytysten pohjalta uhkiin vastaamisen.

Prosessit:

- **Prosessit määrittävät, kuinka ihmiset ja teknologia toimivat yhdessä:**
  - Esimerkiksi lokitietojen tarkastelu ja poikkeamien dokumentointi ovat selkeitä ja säännöllisiä rutiineja
- **Prosessien testaus:**
  - Järjestetään säännöllisiä tietoturvasimulaatioita varmistaaksemme, että teknologia ja henkilöstö toimivat odotetusti

4 Huomioitavat osa-alueet

Ympäristöön on suoritettu kattavasti kovennuksia erilaisten ohjeistusten ja suositusten perusteella, sekä laajat hallintasuunnitelmat esimerkiksi ISO 27000 standardiperheen mukaisesti. Tästä huolimatta jokainen ympäristö on haavoittuvainen, oli se, kuinka turvattu tahansa. Tästä voimme tehdä johtopäätöksen, että aina löytyy parannettavaa ja nyt keskitymmekin jatkossa huomioitaviin kehityskohtiin.

WWW-palvelin:

- Wordpress-järjestelmään tulee asentaa tietoturva-laajennuksia, kuten palomuuri (esim. Wordfence) ja epäilyttävän liikenteen tunnistukseen käytettäviä ratkaisuja.
- Säännölliset turvallisuustarkastukset kolmannen osapuolen toimesta voivat varmistaa, ettei OWASP Top 10 -haavoittuvuuksia pääse syntymään.
- Varmuuskopiointi
- Disaster Recovery -suunnitelma on dokumentoitava ja testattava vähintään kerran vuodessa.

Admin-net:

Admin-net sisältää yrityksen keskeisimmät tietoturvatyökalut ja järjestelmät, joten niiden turvallisuus on prioriteetti.

- SIEM ja SOAR ovat kriittisiä työkaluja uhkien tunnistamisessa ja hallinnassa, joten niiden konfiguraatiot on tarkistettava.
- mahdolliset haavoittuvuudet SIEM-työkaluissa (esim. lokidatan manipulointi) voivat johtaa harhaanjohtaviin hälytyksiin.

Servers-net

- Disaster Recovery -suunnitelma on dokumentoitava ja testattava vähintään kerran vuodessa.
- Varmuuskopiot

- Implementoidaan DLP (Data Loss Prevention) -ratkaisut kriittisiin tiedostoihin Servers-netissä. Tämä estää tietojen luvattoman kopioinnin tai siirtämisen ulkoisiin medioihin
- säännölliset haavoittuvuusskannaukset AD-ympäristössä (esim. BloodHound, PingCastle)
- CIS 18 turvakontrollien noudattaminen

Kolmannen osapuolen hallinta:

- Tarkista alihankkijoiden ja yhteystyökumppaneiden tietoturva käytännöt
- Hyödynnetään esimerkiksi Vendor Guidelines arviointia
- Sopimusvelvoitteet: Sisällytä sopimuksiin tietoturvaa koskevat ehdot, kuten vastuut tietovuodoista ja raportointivelvoitteet.
- Valvominen ja Auditointi: Suorita säännöllisiä auditointeja palveluntarjoajien tietoturvakäytännöistä ja varmista, että ne pysyvät ajan tasalla uusien uhkien suhteen.

5 Pohdinta

Harjoitustyössä perehdyimme puolustautumissuunnitelman toteuttamiseen, joka perustuu aiemmin tehtyyn uhka-arvioon. Saimme hyödyllistä käytännön kokemusta siitä, kuinka erilaiset dokumentaatiot tukevat toisiaan ja kuinka hyödynnämme esimerkiksi uhka-arviota puolustautumissuunnitelman toteuttamista.

Perehdyimme syvällisemmin uhka-arviossa ilmenneisiin hyökkäyksen torjumismenetelmiin ja loimme suunnitelman niiden toteuttamiseksi ympäristöön. Otimme huomioon myös muut tietoturvallisuutta parantavat toimenpiteet kuten henkilöstön jatkuva kouluttaminen ja tietoturvakulttuurin parantaminen sekä erilaiset järjestelmien ja tietojen varmuuskopioinnit palauttamista varten.

Lähteet