Lauri Partinen ktkt23sp

Windows toimialueen koventaminen

Windows toimialueen koventaminen
Käyttöjärjestelmät

2024

SISÄLLYS

1 JOHDANTO

Windows-toimialueen koventaminen tarkoittaa keinoja, joilla vähennetään toimialueen haavoittuvuuksia, rajoitetaan luvatonta pääsyä ja minimoidaan riskejä. Windows-toimialueita hallinnoidaan Active Directoryn avulla. Toimialueet keskittävät hallinnan käyttäjille, tietokoneille ja resursseille. Toimialueen koventaminen parantaa tietoturvaa ja vähentää riskiä joutua kyberhyökkäyksen kohteeksi. Se auttaa pitämään yrityksen tiedot ja palvelut turvassa.

2 ACTIVE DIRECTORY

Active Directory (AD) on hakemistopalvelu, joka auttaa hallitsemaan, verkottamaan, todentamaan, ryhmittelemään, organisoimaan ja suojaamaan yrityksen toimialueverkkoja (Carlson 2024)**.** Active Directoryn käyttö mahdollistaa tietokoneen pääsyn tietokoneen sisäisiin resursseihin. Näitä ovat esimerkiksi verkkotulostin, verkon tiedoston jakaminen, pilvipalveluiden käyttö tai sähköpostin lähettäminen. Useimmille käyttäjille annetaan sähköpostiosoite ja salasana, joka on linkitetty Active Directoryn-tiliobjektiin. Active Directory käyttää Light Directory Access Protokollaa varmistaakseen turvallisen sisäänpääsyn ja onko käyttäjä osa ryhmää. Active Directoryssä on paljon erilaisia ryhmiä, jotka mahdollistavat erilaisia rooleja ja valtuuksia käyttäjilleen. Nämä pitää tuntea hyvin, jotta haitallisen hyökkääjien pääsyn riskiä voitaisiin vähentää.

Active Directory on hierarkia, jota kutsutaan tyypillisesti puuksi (yksi toimialue) tai metsäksi (useita toimialueita), joka tallentaa tietoja, joita kutsutaan objekteiksi (Carlson 2024)**.** Toimialueen yläosassa on toimialueen ohjain, jota käytetään Active Domain Services kopion isännöintiin. Laajemmissa toimialueissa Active Directory Domain Services sisältää mahdollisuuden replikoida muutoksia toimialueen ohjaimiin toimialueen tai usean toimialueen sisällä. Ohjain mahdollistaa myös järjestelmänvalvonnan sisältäen käyttäjätili ja verkon resurssien kontrolloinnin.

Active Directory Domain Service -tietovarasto on tietokanta, joka tallentaa ja käsittelee tiedot käyttäjille, palveluille ja sovelluksille. Toimialueita käytetään

tyypillisesti ryhmittelemään ja hallitsemaan yrityksen objekteja. Näitä ovat esimerkiksi sääntöjen soveltaminen ja rooli- ja laajuuskäytännön mahdollisuuden lisääminen, joka kattaa kenellä on pääsy mihinkin tai kuka voi tehdä muutoksia tai päivityksiä Directoryyn.

Toimialueiden puut yksi toimialue ja metsät useampi toimialue. Luovat osoita toimialueiden välille, mikä mahdollistaa tarkemman hallinnan, miten tietoja replikoidaan eri toimialueiden kesken. Tätä käytetään erityisesti suurimmissa yhtiössä, joilla on useita liiketoiminta yksiköitä ympäri maailmaa. Yhtiöt haluavat rajoittaa pääsyä ja varmistaa, että käytännöt olisivat vaatimuksien mukaisia. maailmanlaajuinen luettelo, jossa voidaan hakea ja tehdä kyselyitä kaikissa toimialueissa mahdollistaa erilaisten luottamustasojen laatimisen toimialueiden ja metsien välille.

Active Directory mahdollistaa objektien ryhmittelyn organisaatioyksikköihin. Organisaatioyksikköjä käytetään jäsentämiseen ja hallinnan helpottamisen, joka mahdollistaa rooli lähestymistavan. Esimerkiksi sinulla voi olla järjestelmänvalvoja, joka on vastuussa Pohjois-Amerikasta ja toinen järjestelmänvalvoja, joka on vastuussa EMEA:sta (Carlson 2024)**.** Tämän avulla oikeuksien rajoittaminen ja oikeuksien laajuutta pystyy kontrolloimaan, jotta järjestelmävalvojan oikeudet kuuluvat omille alueilleen.

Active Directory Tiered access model sisältää teknisiä ohjausobjekteja, jotka vähentävät etuoikeuksien eskaloitumisriskiä. Se koostuu loogisesta rakenteesta, joka erottaa Active Directoryn resurssit luomalla rajat turvallisuustarkoituksiin (Krupakar 2023)**.** Ensisijainen tavoite on suojata Active Directoryn tärkeimmät identiteetit. Saman verkkotunnuksen jäsenet voivat suorittaa normaaleja tehtäviä esimerkiksi sähköpostin selailua ja käyttää sovelluksia. Se sisältää kolme eri tasoa nolla, yksi ja kaksi. Nollatasoon sisältyy järjestelmänvalvojan tunnukset, verkkotunnukset ja ryhmät. Ykköstasossa on verkkotunnuksen jäsensovellukset ja palvelimet. Kakkostasossa on loppukäyttäjien laitteet esimerkiksi myyntihenkilöstö ja henkilöstöpalvelu.

Porrastetun pääsymallin toteutus perustuu Etuoikeutettujen valtuustietojen estämisestä rajojen ylittämisestä vahingossa tai tarkoituksella. Teknisten

kontrollien implementointi Group policy Objectissa on tärkeää, jotta tilanteilta vältyttäisiin. Group policy object yhdistää suojausoikeudet, jotka voivat estää sisäänpääsyn tai luvan päästä käsiksi tietoihin.

Active Directoryssa on kaksi luottamussuhdetyyppiä toimialueiden välisen luottamustason määrittämiseen, jotka ovat yksisuuntainen ja transitiivinen luottamus, johon sisältyy alitoimialueet.

Azure Active Directory (Azure AD) on pilvipohjainen identiteettipalvelu, joka voi synkronoida Active Directory -tietovarastosi ja laajentaa ominaisuuksia mahdollistaakseen muita pilvipalveluita, kuten kertakirjautumisen ja monivaiheisen todennuksen (Carlson 2024)**.** Azurea hyödynnetään yhteyden muodostamiseen ja todentamiseen esimerkiksi Office 365 palvelussa.

Active Directorylla on merkittävä rooli tietoturvamurtojen ennaltaehkäisyssä. Huono hallinta ja virheellinen konfigurointi voivat mahdollistaa hyökkääjän pääsyn kriittisiin järjestelmiin, jonka avulla hyökkääjä pystyy asentamaan haittaohjelman, joka voi aiheuttaa yritykselle toimintakatkoja. Taloudelliset vahingot voivat olla merkittäviä ja yrityksen työntekijöiden tiedot voivat olla vaarassa. Tämän takia Active Directoryn käyttö tulee olla mahdollisimman turvallista, jotta pahinta mahdollisinta skenaariota ei pääse tapahtumaan, jossa hyökkääjä saa käyttöönsä järjestelmänvalvojan oikeudet. Jos hyökkääjä saa järjestelmänvalvojan oikeudet haltuunsa. Useissa tapauksissa se tarkoittaa Active Directoryn uudelleenrakentamista, joka tulee yritykselle todella kalliiksi.

3 KOVENTAMISTEKNIIKAT

Hyökkääjät käyttävät monia eri hakkerointitekniikoita, joilla he yrittävät päästä uhriin käsiksi. Näitä keinoja ovat esimerkiksi pääsynhallintaan liittyvät haavoittuvuudet ja virhekonfiguraatiot järjestelmässä. Erityisen tärkeää yrityksen järjestelmän koventamisen näkökulmasta on luoda tietoturvastrategia, joka perustuu vankkaan riskienarviointii ja liiketoiminnan kyberresilienssiin.

Kerberoasting on yleisesti käytetty jälkikäyttötekniikka, jonka avulla hyökkääjät saavat etuoikeuden pääsyn Active Directoryyn. Hyökkääjä hyödyntää Kerberos Ticket Granting Service (TGS) -palvelua pyytääkseen salattua salasanaa, minkä jälkeen hyökkääjä murtaa sen offline-tilassa erilaisten raakavoimatekniikoiden avulla (Krupakar 2023). Hyökkäyksistä tekee erityisen vaarallisen vaikea havaittavuus, koska pyyntö tehdään hyväksytyn käyttäjän kautta. Hyökkäyksen esto tapahtuu kaksivaiheisen todennuksen kautta tai nollaamalla Kerberos key distribution center -palvelutilin salasanan säännöllisesti.

Lan Manager Hash:ssä käyttäjätilin salasanaa ei tallenneta selkokielisenä; sen sijaan se tallentaa salasanat hash-esitystyypillä (Krupakar 2023). Kun käyttäjä luo tai muokkaa salasanaa alle 15 merkkiseksi, Windows luo Lan manager hash:in ja Windows nt hash:in, jotka voidaan tallentaa Active Directoryyn. Lan manager hash on heikompi ja alttiimpi hyökkäyksille kuin NT hash.

Server message block mahdollistaa turvallisen tiedonsiirron verkossa. Erityisesti Microsoftin palvelut käyttävät protokollaa tiedosto- ja tulostusviestintään. SMB-allekirjoituksen määrittäminen ryhmäkäytännön kautta on ratkaisevan tärkeää Man in the Middle (MiTM) -hyökkäysten havaitsemiseksi, jotka voivat johtaa SMB-liikenteen muokkaamiseen siirron aikana (Krupakar 2023). Se varmistaa tietojen eheyden palvelimelle ja asiakkaalle.

Lightweight Directory Access Protocol (LDAP) mahdollistaa resurssien paikantamisen ja todentamisen verkossa (Krupakar 2023). Käynnistääkseen mukautettuja LDAP-pyyntöjä hakkerit käyttävät man in the middle hyökkäyksiä. Tämän varalta LDAP-allekirjoitus on tunnistautumisen ja turvallisuuskerroksen ominaisuus, joka hyväksyy vain LDAP-pyynnöt.

4 SALASANAKÄYTÄNNÖT

Windows toimialueen koventamisessa kriittistä on salasanojen suojaus ja turvallisuus. Salasanan suojaus on tärkeää käsitellä tietoturvaloukkausten ja salasanan uudelleenkäytön vuoksi. Organisaatioiden salasanojen nollaus tai

päivittäminen on haastava operaatio, jonka organisaatiot yleensä laiminlyövät. Salasanojen vaihtamiseen ja muokkaamiseen on erilaisia ratkaisuja. Yksi tekniikka on lisätä monivaiheinen tunnistus active directoryyn, johon valitset vaihtoehdon, ettet vaihda salasanaa usein. Toinen ratkaisu on Microsoftin tarjoama gMSA, joka vaihtaa salasanat 30 päivän välein.

Salasanakäytännöt. Hyökkääjät käyttävät erilaisia yrityksen salasanan vaarantamistekniikoita, joita ovat esimerkiksi tunnistehyökkäykset ja salasanojen ruiskuttaminen. Yrityksien kannalta tiukka salasanakäytäntö on elintärkeää, jotta tämänkaltaisilta hyökkäyksiltä vältyttäisiin mahdollisimman hyvin. Salasanakäytännöt liittyvät salsananojen ominaisuuksiin esimerkiksi salasanan pituus, monimutkaisuus ja vaihtuvuus. Asetuksissa salasanapolitiikkaa voi vaihtaa kolmella eri asetuksella: salasanojen historian varmennus, salasanojen minimi pituus ja monimutkaisuus vaatimukset. Salasanojen historiasta tulisi asettaa, että ei voi laittaa uudeksi salasanaksi 10–15 aikaisempaa salasanaa. Salasanan tulisi olla vähintään 10–14 merkkiä. Salasanan tulisi monimutkaisuudeltaan käyttää isoja kirjaimia, pieniä kirjaimia, numeroita ja erikoismerkkejä.

5 TYÖKALUT KOVENTAMISESSA

Microsoft security compliance toolkit (MSCT) on paikallisten ja toimialuetason käytäntöjen toteuttamiseen ja hallintaan tarkoitettu työkalu. Käyttäjän ei tarvitse huolehtia monimutkaisista syntakseista ja komentosarjoista, sillä kehitetys suojauksen peruslinjaukset ovat valmiina ohjelmassa loppuympäristöä varten.

Policy analyser on yksi ominaisuus complaince toolkitissä, jonka avulla voit vertailla ryhmäkäytäntöjä ja tarkastaa nopeasti epäjohdonmukaisuudet, ylimääräiset asetukset ja tehtävät muuutokset. Erityisesti kun ryhmäkäytäntöobjekteja on paljon eri tasoilla complaince toolkit ratkaisee tarvittavat asetukset puolestasi.

Active directorylla on merkittävä rooli tietoturvamurtojen ennaltaehkäisyssä. - huono hallinta ja virheellinen konfigurointi mahdollistaa hyökkääjän pääsyn

kriittisiin järjestelmiin ja palveluihin. Jatkuva seuranta ja päivitykset ovat tärkeitä yrityksen toimintaedellytyksien kannalta.

6 LÄHTEET

Carson, J. 2024. Active Directory and hardening: An ethical hacker´s guide to reducing AD risks. Delinea. WWW-dokumentti. Saatavissa: https://delinea.com/blog/active-directory-security-guide-to-reducing-ad-risks [viitattu 22.11.2024].

Krupakar, J. 2023. Active Directory Hardening. Medium. WWW-dokumentti. Saatavissa: https://medium.com/@john245461/active-directory-hardening-c804f3c3e63e [viitattu 22.11.2024].