Karelia-ammattikorkeakoulu
Tradenomi (AMK)
Tietojenkäsittely

Active Directoryn tietoturvallinen toteutus

Joona Häkli

Opinnäytetyö, Toukokuu 2024

www.karelia.fi

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Toukokuu 2024** **Tietojenkäsittelyn koulutus** Tikkarinne 9 80200 JOENSUU +358 13 260 600

Tekijä(t)
Joona Häkli

Nimeke
Active Directoryn tietoturvallinen toteutus

Toimeksiantaja

Tiivistelmä
Tässä opinnäytetyössä tarkastellaan yksityiskohtaisesti Active Directoryn (AD) tietoturvan toteutusta. Tavoitteena oli tunnistaa keskeiset elementit ja prosessit, jotka ovat tärkeitä luotettavan ja tietoturvallisen AD-ympäristön suunnittelussa ja ylläpidossa. Erityistä huomiota kiinnitettiin AD:n organisaatioyksikköjen (OU) rakenteelliseen suunnitteluun, Tier-mallin käytäntöihin, työasemien ja palvelinten suojausmekanismeihin sekä autentikointiprotokolliin, jotka kaikki muodostavat perustan organisaation tietoturvalle.

Menetelmänä oli kirjallisuuskatsaus ja aineistona käytettiin parhaiden käytäntöjen ohjeistuksia, Microsoftin ja CIS Center for Internet Securityn suosituksia ja luotettavia tietoturva-alan julkaisuja. Työssä keskityttiin nykyisiin tietoturvasuosituksiin ja alan standardien vertailuun. Työssä tarkasteltiin hallinnan kerrostamista, käyttöoikeuksien delegointia Tier-mallin mukaisesti sekä erilaisten suojausmekanismien ja autentikointiprotokollien tehokkuutta.

AD:n tehokas tietoturvallinen toteutus vähentää merkittävästi organisaation haavoittuvuutta tietoturvauhkia kohtaan. Selvitys osoitti, että AD:n turvallisuuteen panostaminen on äärimmäisen tärkeää tietoturvaloukkauksien ehkäisyssä. Lisäksi työn tulokset korostivat järjestelmällisen ja kokonaisvaltaisen lähestymistavan merkitystä tietoturvakäytäntöjen kehittämisessä ja toteuttamisessa organisaatioissa.

Kieli	Sivuja 33
suomi	

Asiasanat
Active Directory, tietoturva, kyberturvallisuus, järjestelmänhallinta

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2024
Degree Programme in Business Information Technology

Tikkarinne 9
80200 JOENSUU
FINLAND

Author (s)
Joona Häkli

Title
Secure implementation of Active Directory

Commissioned by

Abstract
This thesis examines in detail the implementation of security in Active Directory (AD). The goal was to identify key elements and processes that are important for designing and maintaining a reliable and secure AD environment. Special attention was paid to the structural planning of AD's organization units (OU), Tier-model practices, protection mechanisms of workstations and servers and authentication protocols, which all are fundamental for organization's security.

The methodology was based on a literature review, using best practice guidelines, Microsoft and CIS Center for Internet Security recommendations, and reliable security industry publications. The work focused on current security recommendations and a comparison of industry standards. The work studied management layering, delegating access rights according to Tier-model and the effectiveness of different protection mechanisms and authentication protocols.

Effective secure implementation of AD significantly reduces organization's vulnerability against security threats. The study showed that investing to AD's security is very important in preventing security breaches. In addition, the results of the work highlighted the importance of systematic and holistic approach in developing and implementing security practices in organizations.

Language
Finnish

Pages 33

Keywords
Active Directory, security, cybersecurity, systems management

Sisältö

Lyhenteet

AD	Active Directory
AES	Advanced Encryption Standard
ATA	Advanced Threat Analytics
BMR	Bare Metal Recovery
CIS	Center for Internet Security
DC	Domain Controller
DFS	Distributed File System
GPO	Group Policy Object
GSS	Generic Security Service
API	Application Program Interface
LDAP	Lightweight Directory Access Protocol
LAPS	Local Administrator Password Solution
NTLM	NT LAN Manager
OU	Organizational Unit
PAW	Privileged Access Workstation
PoLP	Principle of Least Privilege
PtH	Pass-the-Hash
PtT	Pass-the-Ticket
RDP	Remote Desktop Protocol
RFC	Request for Comments
SASL	Simple Authentication and Security Layer
SIEM	Security Information and Event Management
SSO	Single Sign-On
TGT	Ticket Granting Ticket
TPM	Trusted Platform Module

1 Johdanto

Tämä opinnäytetyö keskittyy Active Directoryn (AD) tietoturvan toteutukseen ja pyrkii tarjoamaan perusteellisen näkemyksen AD:n turvallisuusmekanismeista ja hallintatavoista. Opinnäytetyön päätavoite on esitellä laaja-alainen katsaus tietoturvan keskeisiin elementteihin, jotka liittyvät suoraan AD:n turvalliseen käyttöön. Erityisen tarkasti käsitellään OU-rakenteen (Organizational Unit) suunnittelua, Tier-mallin käyttöönottoa, työasemien ja palvelinten turvaamista erilaisilla suojausmekanismeilla sekä autentikointiprotokollia. Työssä analysoidaan myös, miten eri suojaukset ja menetelmät integroituvat yhtenäiseksi kokonaisuudeksi, jonka avulla voidaan rakentaa kestävä tietoturvarakenne koko organisaation käyttöön.

Active Directory on monimutkainen ja monipuolinen järjestelmä, joka vaatii huolellista suunnittelua ja ylläpitoa. Tämän vuoksi on ensiarvoisen tärkeää ymmärtää sen perusrakenteet, toimintaperiaatteet sekä tietoturvallisuuden kannalta kriittiset komponentit. Tässä työssä tarkastellaan näitä aspekteja syvällisesti, ja tarjotaan kattava yleiskuva siitä, miten AD:n eri osa-alueet toimivat yhteen luoden turvallisen ja hallitun IT-ympäristön. Työn tavoitteena on myös tarjota käytännön ohjeita ja parhaita käytäntöjä, jotka auttavat IT-ammattilaisia parantamaan organisaationsa tietoturvastrategioita.

Tietoturva on jatkuvasti kehittyvä kenttä, jossa uudet uhkat ja haasteet vaativat jatkuvaa valppautta ja sopeutumista. Active Directoryn kaltaiset keskeiset teknologiat ovat kriittisiä yritysten tietoturvan ylläpidossa, ja niiden suojauksen laiminlyönti voi johtaa merkittäviin riskeihin ja tietoturvaloukkauksiin. Tässä työssä pyritään osoittamaan, miten AD:n kattava ymmärrys ja sen mukainen suunnittelu ja hallinta voivat merkittävästi parantaa organisaation kykyä suojautua tietoturvariskeiltä. Analysoimalla ja esittelemällä AD:n tietoturvallisuuden perusteita, suunnitteluprosesseja ja parhaita käytäntöjä, tämä opinnäytetyö tarjoaa monipuolisia näkemyksiä ja työkaluja, jotka tukevat organisaation tietoturvan kehittämistä ja ylläpitämistä.

2 Active Directory

Active Directory (AD) on Microsoftin kehittämä monipuolinen hakemistopalvelu, joka on integroitu osaksi Windows Server -käyttöjärjestelmää. AD:n ensisijainen tehtävä on hallita käyttöoikeuksia ja pääsyä verkkoresursseihin laajassa yritysverkossa. Se tallentaa tietoa objekteina, kuten käyttäjät, ryhmät, tietokoneet ja palvelimet, jotka kaikki kategorisoidaan ja järjestetään niiden nimien ja attribuuttien perusteella. Active Directory sisältää useita palveluita, kuten Domain Services, Lightweight Directory Services ja Certificate Services. Nämä palvelut tarjoavat välttämättömiä toimintoja käyttäjähallinnasta tietoturvaan ja resurssien hallintaan. (Microsoft 2021b.)

AD on suunniteltu tukemaan monimutkaisia ja laajoja organisaatioita, tarjoamalla työkalut tehokkaaseen pääsynhallintaan ja identiteetinhallintaan. Sen avulla IT-henkilöstö voi hallita käyttöoikeuksia ja käyttäjäprofiileja keskitetysti, mikä helpottaa käyttäjätietojen ylläpitoa ja päivitystä. Active Directoryn rakenteellinen hierarkia mahdollistaa tarkan kontrollin käyttöoikeuksien ja ryhmäkäytäntöjen yli organisaatiossa. Tämä hierarkkinen ja delegoitu hallintamalli mahdollistaa turvallisuusvaatimusten täyttämisen samalla kun se tarjoaa joustavuutta toimintaympäristön muutosten hallinnassa. (Microsoft 2021b.)

Erityisesti AD:n mahdollisuus sopeutua eri käyttöympäristöihin ja integroitua muihin palveluihin tekee siitä toimivan työkalun IT-infrastruktuurin perustaksi. AD:n kyky integroida ja hallinnoida pilvipalveluita laajentaa sen soveltuvuutta nykyaikaisissa IT-ratkaisuissa. Tämä tehostaa organisaation kykyä vastata nykyajan liiketoiminnan haasteisiin. (Microsoft 2021b.)

3 Active Directoryn tietoturvan perusteet

3.1 Tietoturvan perusteet, pääsynhallintarajoitukset ja niiden käytännöt

AD:n tietoturvan perusteet sisältävät useita käytäntöjä, kuten vahvat autentikointimenetelmät, käyttöoikeuksien hallinnan vähimmän tarvittavan oikeuden periaatteella, palvelinkovennukset sekä järjestelmien ja tietojen säännöllisen tarkistuksen ja seurannan. On tärkeää suojata ympäristö ja sen kriittiset komponentit, kuten DC:t (toimialueen ohjauskone, Domain Controller) huolellisesti. (Microsoft 2023d.)

Monivaiheisen todennuksen käyttö mahdollisuuksien mukaan sekä tietoturvapäivitysten ajantasaisuus ovat myös tärkeässä roolissa. Verkkotopologian, kovennusten ja hallinnan delegoinnin Tier-mallin mukainen huolellinen suunnittelu on myös avainasemassa. Käytännöt tähtäävät organisaation tietoverkkojen, resurssien ja käyttäjätietojen suojelemiseen mahdollisilta uhilta ja hyökkäyksiltä. (Microsoft 2023d.)

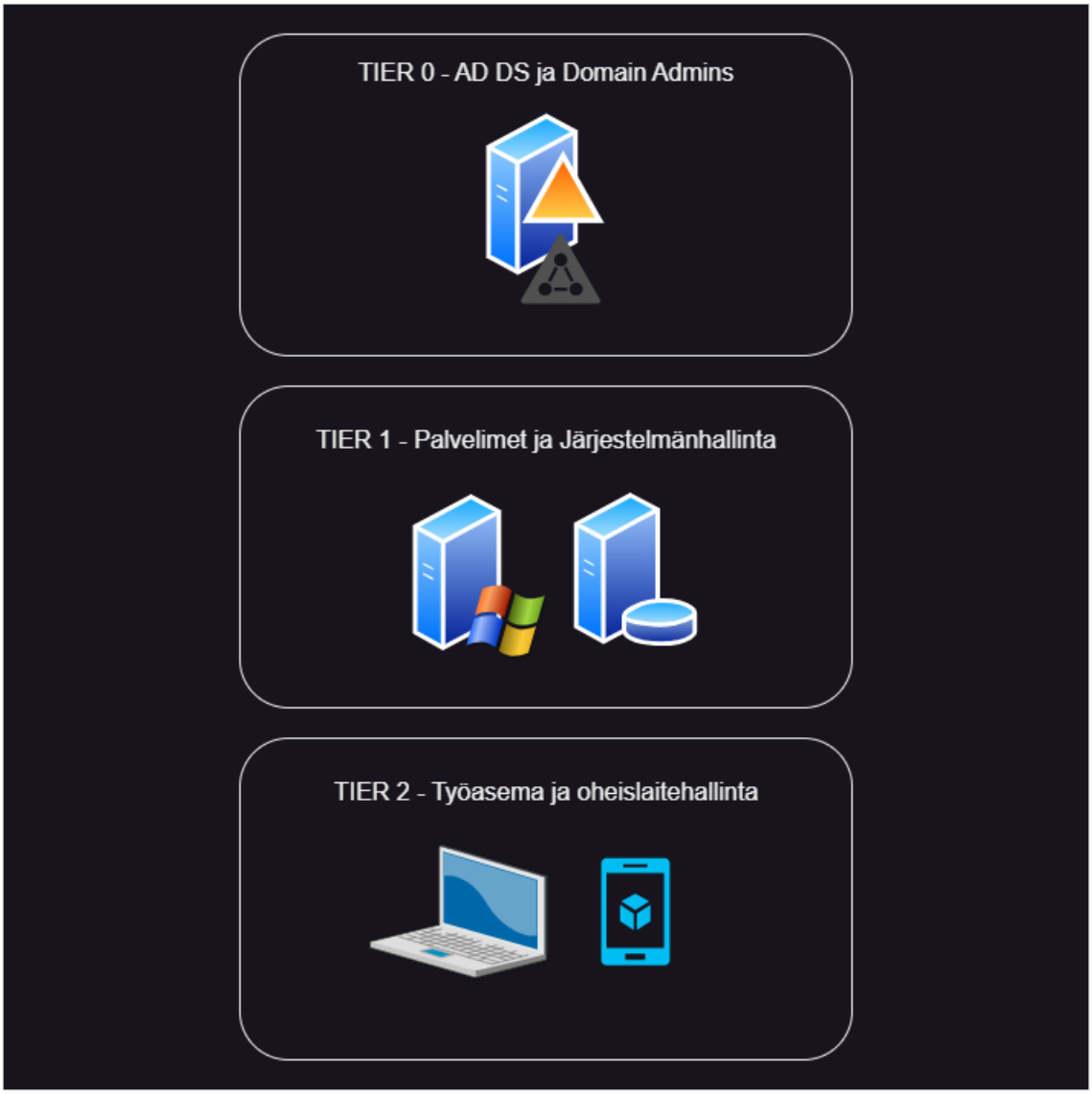
Pääsynhallinnan rajoitukset Active Directoryssa ovat keskeinen osa tietoturvallisuuden ylläpitämistä. Domain Controllerit (DC), jotka ovat keskiössä käyttäjätunnistuksessa ja resurssien hallinnassa, edellyttävät huomattavia turvatoimenpiteitä. Tämän vuoksi on välttämätöntä, että DC:t sijaitsevat turvallisissa tiloissa, joissa on pääsyvalvonta ja valvontakamerat turvaamassa laitteiston fyysistä koskemattomuutta. Verkkotason suojaus, kuten palomuurien ja tunkeutumisenestojärjestelmien (IDS/IPS) käyttö, lisää turvakerrosta estämällä luvattoman pääsyn ja liikenteen. (Microsoft 2023f.)

On myös suositeltavaa toteuttaa verkkoliikenteen eristäminen käyttämällä esimerkiksi virtuaalisia yksityisverkkoja (VPN) ja muuta eristystekniikkaa. Näin varmistetaan, että vain valtuutetut käyttäjät pääsevät käsiksi kriittisiin järjestelmän osiin. Tämä lähestymistapa ei ainoastaan paranna tietoturvaa, vaan myös tehostaa verkon hallintaa ja vähentää haavoittuvuutta tietoturvaongelmien edessä. On tärkeää ylläpitää korkeaa valmiutta ja reagointikykyä turvallisuusuhkiin, jotta voidaan nopeasti puuttua mahdollisiin

tietoturvaongelmiin ja minimoida niiden vaikutukset organisaation toimintaa. (Microsoft 2023f.)

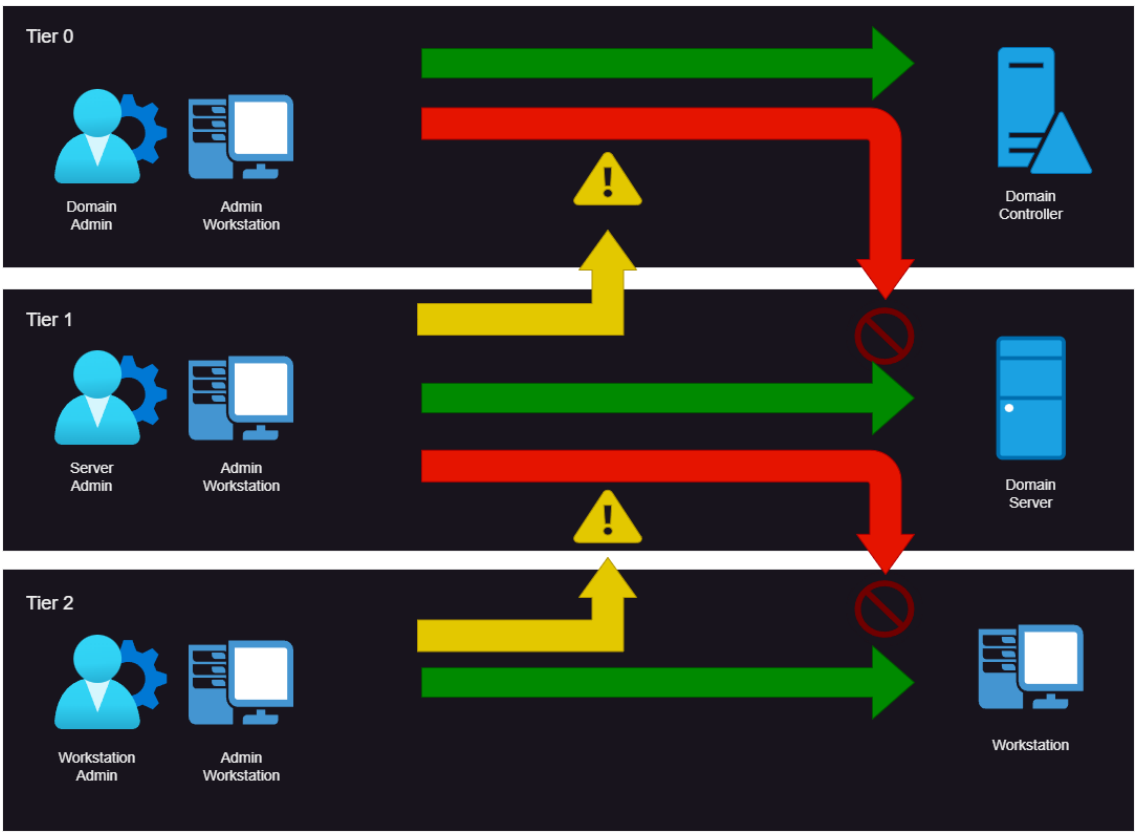
3.2 Pääsynhallinta ja tietoturvan kerrostaminen

AD:n tietoturvan perusta rakentuu pääsynhallinnan huolelliselle suunnittelulle ja kerrokselliselle (Tier-malli, kuvio 1.) lähestymistavalle tietoturvaan ja hallinnan delegointiin. Tämä lähestymistapa on keskeinen suojaamaan organisaation tärkeimpiä arvoja sisältäviä tietoja ja prosesseja.



Kuvio 1. Tier-tasojen kuvaus.

Tasojen määrittely on keskeinen osa hallinnollisten oikeuksien suojausstrategiaa. On olennaista harkita eri käyttöoikeustasojen potentiaalista vaikutusta mahdollisen hyökkääjän näkökulmasta. Jos yhdellä hallintatunnuksella on pääsy useampaan tasoon, se voi luoda suoran reitin hyökkääjälle siirtyä Tier-2-tason työasemilta sovelluspalvelimille (Tier-1) ja jopa hallitsemaan koko järjestelmää Tier-0-tasolla. Tämän riskin minimoimiseksi, kirjautumisoikeudet ja hallintapääsy tulee rajata niin, että ne ovat yksilöityjä kullekin tasolle. Esimerkiksi ylläpitäjä A, joka operoi kaikilla tasoilla 0-2, tarvitsee erilliset identiteetit jokaisen tason hallintaan, jotta voidaan asettaa tiukat pääsyrajoitukset tasojen välille. Dokumentaatiossa vihreä väri kuvaa käyttäjän sallittua kirjautumista, kun taas punainen osoittaa alhaisemman tason kirjautumisen, joka on estetty. Keltainen väri merkitsee kirjautumista korkeammalta tasolta, kuten verkkokirjautumista, joka ei anna oikeutta paikalliseen kirjautumiseen tai hallinnointiin ylemmän tason palveluissa. (Kuvio 2.)



Kuvio 2. Tier-pääsynhallinta.

3.2.1 Tier-rakenteen implementointi ja hyöty tietoturvalle

Tier-rakenne tarjoaa strategisen mallin AD:n turvallisuuden hallintaan (Heidecker, D. 2024). Tämä malli on osa laajempaa yrityksen pääsynhallintamallia, joka kattaa paitsi perinteiset AD-ympäristöt kuin myös pilvipalvelut ja etäkäyttöoikeudet. Malli sisältää ”Zero Trust” -periaatteet, jotka perustuvat oletukseen, että järjestelmään on jo murtauduttu, jolloin jokainen käyttöpyyntö vaatii vahvistuksen ja käyttöoikeudet myönnetään aina mahdollisimman suppeina. Mallissa korostetaan myös tarvetta vahvistaa erityisesti niitä polkuja, joita hallinnoidaan ja ylläpidetään etuoikeutetun pääsyn kautta, koska ne tarjoavat suurimman hallinnan liiketoiminnalle kriittisissä järjestelmissä. (Microsoft 2024b.)

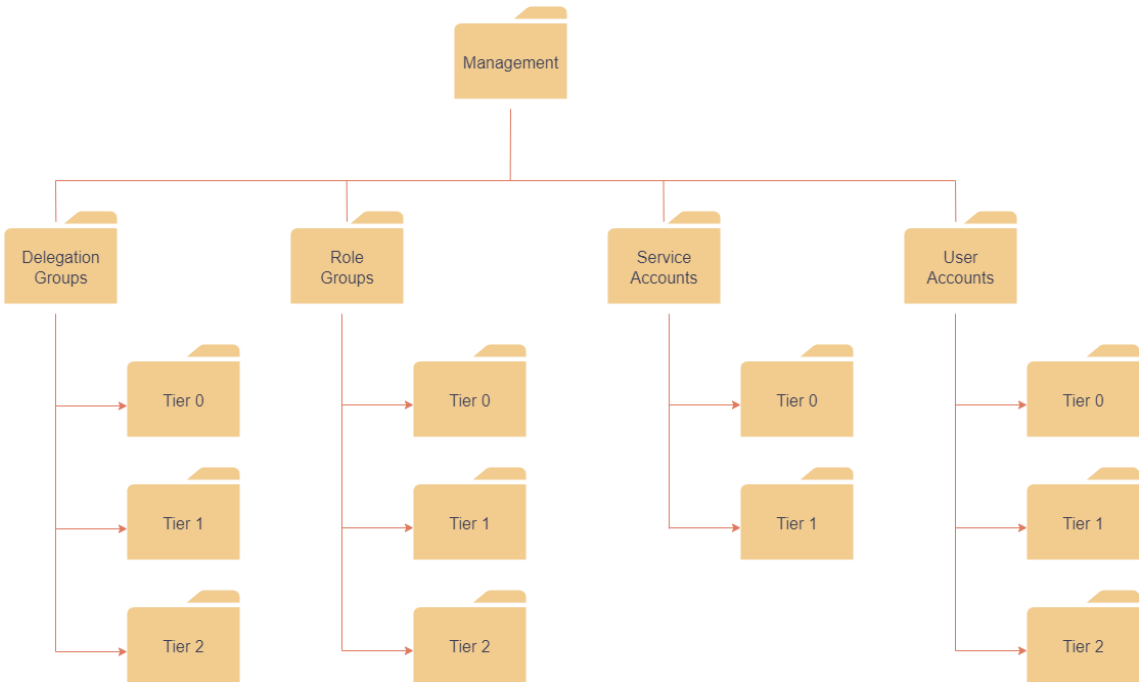
3.2.2 OU-rakenteen suunnittelu hyödyntäen Tier-mallia

Tier-malli AD:n tietoturvassa jakaa resurssit kolmeen tasoon: **Tier 0** -taso sisältää korkeimman tason hallintaresurssit, kuten Domain Controllerit. **Tier 1** sisältää esimerkiksi sovellus- ja tietokantapalvelimet ja **Tier 2** työasemat, mobiililaitteet, tulostimet ja muut loppukäyttäjän oheislaitteet. Tämän erottelun tavoitteena on estää tietoturvahyökkäysten leviäminen tai hyökkääjän pääsy yhdeltä tasolta toiselle, suojaten erityisesti korkeimman tason resursseja. Malli korostaa kriittisten hallintatunnusten suojaamista rajoittamalla niiden käyttöä ja soveltamalla tiukkoja turvallisuuskäytäntöjä. (Heidecker 2024.)

OU-rakenteen suunnittelu hyödyntäen Tier-mallia keskittyy erottamaan käyttäjien ja resurssien hallintaoikeudet turvallisuustasojen mukaan. Tier-malli mahdollistaa tietoturvallisen ja tehokkaan infrastruktuurin käytön ilman, että tarvitaan uusia työkaluja, kun olemassa olevien oikeaoppinen käyttö riittää. Se vahvistaa tietoturvaa eristämällä käyttöoikeudet ja -valtuudet, mikä tekee organisaation tärkeimpien resurssien suojaamisesta vahvempaa ja vähentää järjestelmien haavoittuvuutta. (Löfgren 2024.)

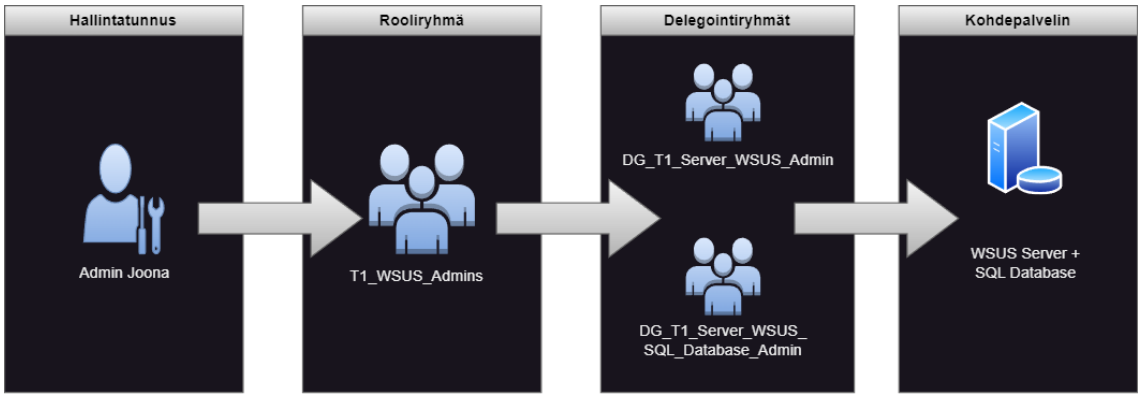
3.2.3 Management-organisaatioyksikkö

Management-organisaatioyksikkörakenteessa on erityisesti eroteltu hallinnolliset käyttäjät ja ryhmät suojaustasojen mukaan (kuvio 3). Tällöin oikeuksien delegointi on mahdollista eri tasoilla. Rakenteessa on neljä pääluokkaa: Delegation Groups eli delegointiryhmät, Role Groups eli rooliryhmät, Service Accounts eli palvelutunnukset ja User Accounts eli käyttäjätunnukset. Palvelutunnuksia käytetään sovellusten ja järjestelmien ajamiseen estäen samalla niiden kirjautuminen paikallisesti. Delegointiryhmillä hallinnoidaan eri järjestelmien oikeuksia ja rooliryhmät on jaettu hallintatehtävien mukaan. Tämä järjestely mahdollistaa hallinnan delegoinnin tarkasti pienimpien tarvittavien oikeuksien periaatetta (The Principle of Least Privilege (PoLP)) noudattaen ja samalla parantaen turvallisuutta. (Kinzer 2022.)



Kuvio 3. Management OU-rakenne.

Käyttöoikeuksien antaminen hallintatunnuksille tehdään lisäämällä käyttäjän hallintatunnus rooliryhmän jäseneksi. Rooliryhmä lisätään puolestaan tehtävän vaatimiin delegointiryhmiin jäseneksi, joiden kautta hallintatunnuksille annetaan käyttöoikeudet tarvittaviin resursseihin (kuvio 4).



Kuvio 4. Hallintaoikeuksien periytyminen.

3.3 Työasemien ja palvelinten suojausmekanismit

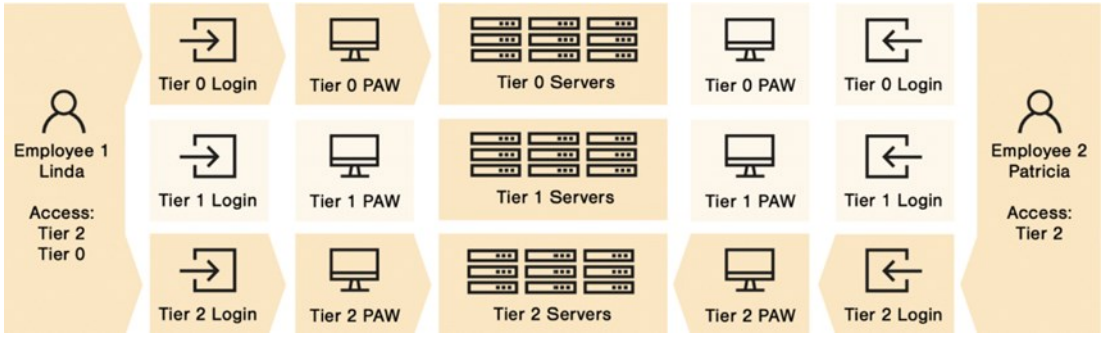
Artikkelissa "Using Tiered Administration for Group Policy Management" keskustellaan siitä, kuinka hallinnollista eriyttämistä voidaan soveltaa ryhmäkäytäntöjen hallintaan suojausmekanismien vahvistamiseksi. Artikkelissa painotetaan, että on tärkeää tiedostaa ja hallita sitä, ketkä voivat muokata ja linkittää ryhmäkäytäntöobjekteja (Group Policy Object, GPO) rajoittaen pääsyä tietyille hallinnollisille tasoille (Tier 0, Tier 1, Tier 2) riippuen siitä, mihin resursseihin GPO:t soveltuvat (esim. DC:t, palvelimet, työasemat). Tämä auttaa minimoimaan haittaohjelmien leviämistä ja parantamaan AD:n turvallisuutta. (Mar-Elia 2022.)

3.3.1 Privileged Access Workstation (PAW)

Privileged Access Workstations (PAW) ovat tietoturvallisia työasemia, jotka on erityisesti suunniteltu arkaluontoisia tehtäviä varten, kuten järjestelmänvalvojien käyttöön. PAW:n perusidea on luoda eristetty ja turvattu ympäristö, joka suojaa kriittisiä hallinnollisia tehtäviä ja prosesseja. (Delinea 2023.)

Käyttämällä PAW-työasemia organisaatiot voivat tehokkaasti erottaa korkean tason käyttöoikeuksia vaativat tehtävät muista käyttäjätilin tehtävistä (kuvio 5) vähentäen

siten riskejä, jotka liittyvät haittaohjelmien leviämiseen ja hyökkääjien pääsyyn arkaluontoisiin tietoihin. PAW:t auttavat varmistamaan, että vain valtuutetut käyttäjät pääsevät käsiksi herkkiin järjestelmiin ja dataan, mikä on keskeinen osa nykyaikaisia tietoturvasuosituksia. (Delinea 2023.)



Kuvio 5. Tier-mallin mukainen kirjautuminen hyödyntäen PAW-työasemia. (Delinea 2023.)

3.3.2 Local Administrator Password Solution (LAPS)

Local Administrator Password Solution (LAPS) tarjoaa automatisoidun ratkaisun paikallisten Administrator-tilien salasanojen hallintaan, parantaen AD-ympäristön tietoturvan tasoa. Se vähentää riskiä, joka liittyy kiinteiden tai yleisesti jaettujen salasanojen käyttöön. LAPS:in avulla yksittäiset salasanat luodaan automaattisesti kullekin koneelle ja tallennetaan turvallisesti AD-ympäristöön. Täten ne ovat vain valtuutettujen käyttäjien saatavilla. Tämä prosessi minimoi mahdollisuuden, että hyökkääjät voisivat hyödyntää staattisia salasanoja päästäkseen käsiksi järjestelmiin. (Microsoft 2023a.)

3.3.3 BitLocker-levynsalaus

BitLocker on Microsoftin kehittämä salausohjelmisto, joka suojaa tietoja kiintolevyllä käyttämällä levyn täyttä salausta. Se estää tietojen luvattoman käytön tai lukemisen. BitLocker salaa koko aseman sisällön ja vaatii oikean salauksen purkamiseen tarvittavan salasanan työaseman käynnistyksen yhteydessä. BitLocker tarjoaa vahvan suojan

tiedoille, tehden siitä keskeisen työkalun tietoturvan ylläpitämiseen erityisesti kannettavissa laitteissa. Kun tietokoneet ovat AD:n hallinnassa, BitLockerin avaimet voidaan tallentaa turvallisesti AD:n tietokantaan. Tämä keskitetty hallinta minimoi riskin menetetystä datasta, vaikka laitteita katoaisi tai ne varastettaisiin. (Rossevelt 2023.)

4 Active Directoryn toiminnallisuustaso ja autentikointimekanismit

4.1 Toiminnallisuustason kehitys- ja turvallisuusvaikutukset

AD:n toiminnallisuustasoilla on merkittävä vaikutus autentikointimekanismien ja tietoturvan kehitykseen organisaatioissa. Toiminnallisuustasot määrittävät, mitä ominaisuuksia ja toimintoja on käytettävissä AD-ympäristössä. Ne perustuvat domain-controllereiden käyttöjärjestelmäversioihin. Esimerkiksi Windows Server 2012 toi mukanaan ominaisuuksia, kuten merkittäviä parannuksia Kerberos autentikointiin (turvallinen todennusprotokolla) ja yhdistelmäautentikoinnin, joka edellyttää Windows Server 2012 -tason domain-toiminnallisuutta. (Microsoft 2021c.)

Tietoturvan kannalta uudempien toiminnallisuustasojen käyttöönotto mahdollistaa paremmat suojaukset ja hallinnan mekanismit. Esimerkiksi, Windows Server 2008 R2 lisäsi AD:hen roskakorin, jonka ansiosta poistettuja objekteja voidaan palauttaa. Tämä edellyttää, että kaikki domain-kontrollerit käyttävät vähintään Windows Server 2008 R2 -toiminnallisuustasoa. Korkeammat toiminnallisuustasot mahdollistavat myös paremman salauksen ja autentikointimekanismeja, kuten AES-128 ja AES-256-tuen Kerberos-protokollalle. (Microsoft 2023a.)

Toiminnallisuustasojen päivittäminen edellyttää tarkkaa suunnittelua, sillä kerran nostettua tasoa ei välttämättä voi palauttaa aiempaan tilaan, etenkään vanhemmissa Windows Server -versioissa. Lisäksi korkeampien toiminnallisuustasojen käyttö voi estää vanhempien järjestelmäversioiden domain-kontrollereita liittymästä verkkoon, mikä voi olla merkittävä tekijä päivityspäätöksiä tehtäessä. (Bigelow 2024.)

AD:n autentikointi tukeutuu pääasiassa kahteen standardiin: Kerberokseen ja LDAP:iin (Lightweight Directory Access Protocol). Kerberos tarjoaa yksittäisen kirjautumisen (Single Sign-On, SSO) toiminnallisuuden, mikä mahdollistaa käyttäjille pääsyn yrityksen resursseihin kirjautumalla vain kerran. Tämä parantaa käyttökokemusta ja tehostaa tietoturvaa estämällä käyttäjätietojen välittymisen verkon yli. LDAP toimii puolestaan tietojen hakemiseen ja hallintaan käytettävänä protokollana. (Kinzer 2022.)

4.2 Autentikointiprotokollat ja -käytännöt

4.2.1 Kerberos-protokollan rooli

Kerberosin merkitys on tärkeä AD-ympäristössä tarjoten turvallisen todennusprotokollan, jolla verkon käyttäjien ja valvojien henkilöllisyys todennetaan. Kerberos kehitettiin ratkaisuksi verkon tietoturvaongelmiin ja se mahdollistaa turvalliset kirjautumismekanismit. Näin pystytään varmistamaan, että käyttäjien todennukset tapahtuvat myös suojaamattomissa verkoissa tietoturvaa vaarantamatta. (Messina 2023.)

Kerberos-protokollan keskeinen osa on Ticket Granting Ticket (TGT), joka on todennuksen jälkeen myönnetty lippu. Sitä käytetään pyydettäessä muita palvelukohtaisia lippuja KDC:lta (Key Distribution Center). (Messina 2023.)

Pohjimmiltaan Kerberos käyttää asiakas-palvelin -mallia ja toimii lippuihin perustuen, mikä mahdollistaa turvallisen viestinnän turvattomassa verkossa. Prosessissa on mukana KDC, joka toimii todentamispalvelimena todentaen asiakkaat ja myöntäen heille liput palveluiden käyttöön. KDC käyttää tietokantaa, joka on yleensä AD-toimialueen palveluissa ylläpitämässä suojattua tilitietokantaa. (Messina 2023.)

Kerberos-todennusprosessi on suhteellisen monimutkainen, mutta siinä keskitytään tietojen vaihdon turvaamiseen luvattoman käytön estämiseksi. Aluksi käyttäjä tai asiakas lähettää KDC:lle selväkielisen todennuspyynnön. Jos pyyntö on vahvistettu, KDC

antaa Ticket-Granting Ticketin (TGT) ja istuntoavaimen. Tämän jälkeen asiakas pyytää TGT:n avulla pääsyä tiettyihin palveluihin tai resursseihin ja saa palvelulipun, jos se on hyväksytty. (Loshin 2024.)

Kerberos tarjoaa useita etuja, kuten delegoidun todennuksen, kertakirjautumisominaisuudet ja tehokkaan todennuksen palvelimille ilman, että jokaisen todennusyrityksen yhteydessä tarvitsee ottaa yhteyttä toimialueen ohjaimeen. Kerberos tukee myös keskinäistä todennusta, jolloin varmistetaan, että sekä käyttäjä että palvelu voivat todentaa toistensa henkilöllisyyden. (Loshin 2024.)

4.2.2 Kerberos-todennusprotokollan standardit

Microsoftin Kerberos-toteutus perustuu standardeihin ja on yhteensopiva muiden protokollaa käyttävien järjestelmien kanssa. Kerberos-todennusprotokolla perustuu useisiin avoimiin standardeihin, joista keskeisin on IETF:n (Internet Engineering Task Force) RFC 4120 -standardi. RFC 4120 määrittelee Kerberos Version 5 -protokollan. Se on Kerberos-todennusprotokollan laajimmin käytetty versio. Standardi sisältää yksityiskohtaiset tiedot Kerberos-protokollan toimintamekanismeista, kuten KDC:n (Key Distribution Center) toiminnasta, lippujen (tickets) muodostamisesta ja salausmenetelmistä, joita käytetään tietoturvan varmistamiseen. (Microsoft 2021b.)

Kerberosista on tullut Windows 2000:n jälkeen Windows-ympäristöjen suosituin todennusprotokolla, joka on korvannut NTLM:n (NT LAN Manager) kaltaiset vanhemmat protokollat sen ylivoimaisten tietoturvaominaisuuksien ansiosta. Se muodostaa perustan kertakirjautumiselle, jonka avulla käyttäjät voivat käyttää verkon resursseja tehokkaasti ja turvallisesti todennettuna. (Messina 2023.)

4.3 Muut autentikointimekanismit

AD tukee erilaisia todennusmenetelmiä käyttäjien, päätelaitteiden ja palvelujen todentamiseksi ja valtuuttamiseksi. Näistä ensisijaisia todennusmekanismeja ovat yksinkertainen, SASL (Simple Authentication and Security Layer) ja lisämenetelmä nimeltä "Sicily", joka on tarkoitettu lähinnä yhteensopivaksi vanhojen järjestelmien kanssa. Yksinkertainen todennus on suoraviivainen, eikä siihen tarvita lisäprotokollia. (Microsoft 2024d.)

SASL puolestaan voi käyttää sellaista protokollaa kuin GSS-SPNEGO (Generic Security Service - Simple and Protected GSSAPI Negotiation Mechanism), joka puolestaan voi käyttää Kerberosia tai NTLM:ää ja GSSAPI (Generic Security Services Application Program Interface), joka käyttää aina Kerberosia. Sicily-mekanismi on suunniteltu tukemaan erityisesti NTLM:ää. (Microsoft 2024d.)

Perinteisten Kerberos- ja NTLM-protokollien lisäksi AD on ottanut käyttöön LDAP-protokollan (Lightweight Directory Access Protocol) hakemistopalveluissa. LDAP mahdollistaa virtaviivaisemman lähestymistavan käyttäjien käyttöoikeuksien hallintaan koko organisaatiossa ja tarjoaa menetelmän, jolla voidaan muodostaa yhteys ja olla vuorovaikutuksessa Internet-hakemistojen kanssa. Kerberosin ja LDAP:n käyttö AD:n todennuksessa takaa turvallisen ja tehokkaan järjestelmän yrityksen resurssien hallintaan ja yksinkertaistaa IT-hallintoa tarjoamalla laitteiden ja käyttäjäkokoonpanojen keskitetyn hallinnan. (Kinzer 2022.)

5 Verkkotopologian suunnittelu ja tietoturvan varmistaminen

AD:n verkkotopologian ymmärtäminen ja suunnittelu ovat merkityksellisiä, kun halutaan varmistaa verkon suorituskyky ja käyttäjien pääsy verkon resursseihin. AD-verkkotopologian suunnittelussa keskitytään DC-sijoittelun suunnitteluun sekä verkkojen, aliverkkojen, verkkolinkkien ja verkkolinkkisiltojen suunnitteluun. Tavoitteena on

tehostaa kysely- ja replikointiliikenteen reititystä. Tämä auttaa organisaatiota vähentämään AD-datan replikoinnin kustannuksia, minimoimaan ylläpitovaatimuksia ja optimoimaan asiakastietokoneiden kykyä löytää lähimmät resurssit kuten DC:t ja Distributed File System (DFS, tiedostojen hakemistopalvelin) -palvelimet. Suunnitteluprosessin alussa on ymmärrettävä fyysisen verkon rakenne ja suunnitella AD:n looginen rakenne sisältäen myös hallinnollisen hierarkian, metsäsuunnitelman (forest) ja toimialue (domain)-suunnitelmat kullekin metsälle. (Microsoft 2021a.)

5.1 AD:n verkkorakenteen merkitys tietoturvalle

AD:n turvallisuus on äärimmäisen tärkeää, sillä sitä kautta hallitaan kaikkia järjestelmän käyttöoikeuksia organisaatiossa. Tämä tekee siitä merkittävän kohteen tietoturvahyökkäyksille. AD:n turvallisuuden laiminlyönti voi altistaa organisaation monenlaisille kyber- tai tietoturvahyökkäyksille, jotka voivat johtaa tietojen varkauteen tai järjestelmän korruptoitumiseen. (Vaideeswaran 2023.)

On paljon haasteita, jotka liittyvät palautumiseen AD:n tietoturvaloukkauksen jälkeen. Ne sisältävät lähteen tai hyökkääjän tunnistamisen ja vahingon laajuuden määrittämisen korostaen valppaan seurannan ja katastrofien palautumissuunnitelmien merkitystä (Vaideeswaran 2023.)

5.2 Tietoturvastrategiat verkkotopologian suunnittelussa

Tietoturvastrategiat AD:n verkkotopologian suunnittelussa korostavat AD:n merkitystä yrityksen tietoturvan kannalta hallitsemalla pääsyä järjestelmiin ja resursseihin. Tehokas AD-turvallisuus suojaa käyttäjätunnuksia, sovelluksia ja arkaluonteisia tietoja luvattomalta käytöltä. Strategiat sisältävät oletusasetusten säätämisen organisaation tarpeiden mukaisiksi, varmuuskopiointi- ja palautusprosessien käytön sekä turvallisuuden hallinnan ja raportoinnin keskittämisen. Tapahtumalokien seuraaminen ja

käyttöoikeuksien oikeanlainen hallinta on tärkeää, jotta pystytään havaitsemaan ja estämään mahdolliset tietoturvaloukkaukset ajoissa. (Vaideeswaran 2023.)

6 Ryhmäkäytännöt ja niiden merkitys

Ryhmäkäytännöt (Group Policy) ovat keskeinen osa Microsoftin Active Directoryn (AD) hallintaa ja ne tarjoavat IT-hallinnolle tehokkaan työkalun käyttöoikeuksien, tietoturva-asetusten ja käyttäjäkokemusten hallintaan verkossa. Ryhmäkäytäntöjen avulla voidaan määritellä ja ohjata käyttäjien ja tietokoneiden käyttäytymistä organisaatiossa laajasti ja tehokkaasti, mahdollistaen yhdenmukaisten asetusten käyttöönoton ilman että jokaiseen koneeseen tarvitsee puuttua erikseen. (Buenning 2024.)

Ryhmäkäytäntöobjektit (Group Policy Objects, GPO) ovat AD:n objekteja, jotka sisältävät erilaisia sääntöjä, jotka määrittelevät tiettyjä asetuksia tai rajoituksia organisaation tietokoneille ja käyttäjille. Esimerkiksi, ryhmäkäytännöllä voi määrätä tietoturvapäivitysten automaattisen asentamisen, ohjelmiston asennuskiellot, pääsyn USB-muistitikkuihin tai jopa työpöydän taustakuvan. Jokainen näistä säännöistä voidaan kohdistaa tietylle käyttäjäryhmälle tai tietokoneille tietyssä AD:n organisaatioyksikössä (OU) mahdollistaen tarkan ja kohdennetun hallinnan. (Buenning 2024.)

Ryhmäkäytäntöjen merkitys organisaation tietoturvassa on merkittävä. Ne mahdollistavat keskitetyn hallinnan organisaation tietoturva-asetuksille, kuten salasanakäytännöille, käyttäjätileille ja pääsynhallinnalle, mikä on ensiarvoisen tärkeää organisaation tietojen suojelussa. Tämän lisäksi ryhmäkäytännöt tarjoavat tärkeän mekanismin, jonka avulla voidaan varmistaa, että kaikki työasemat ja palvelimet noudattavat organisaation tietoturvastandardeja, mikä auttaa minimoimaan tietoturvariskit. (Buenning 2024.)

Jatkuvasti muuttuvassa tietoturvaympäristössä ryhmäkäytännöt tarjoavat myös tärkeän välineen nopeaan reagointiin ja mukautumiseen. Kun uusi tietoturvauhka ilmenee, ryhmäkäytäntöjen avulla voidaan nopeasti määrittää tarvittavat muutokset koko organisaatioon ilman, että jokainen laite tai käyttäjäasetus on päivitettävä manuaalisesti. Nopeus ja joustavuus ovat tärkeitä ominaisuuksia, jotka auttavat IT-henkilöstöä ylläpitämään organisaation tietoturvaa tehokkaasti. (Buenning 2024.)

7 Active Directoryn suojauskäytännöt

Microsoftin suositusten mukaisesti AD:n kovennus- ja suojauskäytännöt kattavat useita oleellisia toimenpiteitä. Ne ovat suunniteltu suojaamaan organisaation tietoverkkoa ja vähentämään tietoturvariskejä. Käytännöt keskittyvät minimoimaan haavoittuvuuksia ja hallinnoimaan oikeuksia oikein sekä suojelemaan järjestelmiä ja resursseja. Haavoittuvuuksien minimoimiseksi pyritään varmistamaan, että ohjelmistot ja järjestelmäpäivitykset ovat ajan tasalla. Käyttäjätunnusten suojaamisessa tärkeässä roolissa ovat vahvojen salasanojen käyttäminen ja käyttöoikeuksien tarkka hallinta hyödyntäen pienimpien tarvittavien oikeuksien periaatetta. AD:n kovennuksessa keskitytään pienentämään hyökkäyspinta-ala mahdollisimman pieneksi koventaen järjestelmät tarvittavalla tavalla ja antamalla käyttäjille sekä järjestelmänvalvojille ainoastaan ne oikeudet, jotka ovat välttämättömiä heidän rooliensa mukaisten tehtävien hoitamisen kannalta. Tämä tarkoittaa myös sitä, että esimerkiksi loppukäyttäjän työasemalta estetään kaikkien ylimääräisten ohjelmien, kuten komentokehotteen tai PowerShellin suorittaminen. (Microsoft 2023d.)

Toimialueen ohjainkoneiden (DC) suojaaminen on ensiarvoisen tärkeää niiden ollessa kriittisessä asemassa AD:n hallinnassa. Sekä fyysiset että virtuaaliset DC:t vaativat vahvaa suojaa mahdollisia hyökkäyksiä vastaan. Fyysiset DC:t on hyvä sijoittaa lukittuihin ja valvottuihin tiloihin, joissa turvallisuus on etusijalla. Näiden laitteiden suojauksessa tulisi hyödyntää Trusted Platform Module (TPM) -siruja, jotka tarjoavat laitteistotason turvatoimia, kuten salausavainten, sertifikaattien ja muiden luottamuksellisten tietojen

turvallisen tallennuksen. Lisäksi BitLocker-aseman salausta suositellaan käytettäväksi koko levyn salaukseen. (Microsoft 2023d.)

Virtuaalisille DC:ille on parasta käyttää erillisiä isäntäpalvelimia. Tämä eristys auttaa vähentämään riskiä, että haavoittuvuudet yhdessä virtuaalikoneessa voisivat vaarantaa toisen. Shielded VMs (suojatut virtuaalikoneet) tarjoavat lisäsuojaa virtuaaliympäristöille, estäen luvattoman pääsyn ja käytön. Ne käyttävät salattuja levykuvia ja käynnistyksenaikaista tarkistusta varmistaakseen, että virtuaalikoneet käynnistyvät vain hyväksytyissä ympäristöissä. Tämä suojaa niitä muokkaamiselta tai tarkastelulta luvattomien käyttäjien toimesta. (Microsoft 2023d.)

Päivittämällä DC:t uusimpaan Windows Server -versioon ja noudattamalla turvallisia konfiguraatiokäytäntöjä pystytään lisäämään järjestelmien turvallisuutta. Näihin käytäntöihin kuuluu esimerkiksi etätyöpöytäyhteyksien (RDP) käytön rajoittaminen, muutosten ja konfiguraatioiden hallinta sekä DC:iden internetyhteyksien estäminen. Näin pystytään minimoimaan riskejä ja suojaamaan AD-ympäristöä mahdollisilta tietoturvahyökkäyksiltä. Nämä toimenpiteet yhdessä DC:iden koventamisen Microsoftin ja CIS:n (Center of Internet Security) suositusten mukaan auttavat suojaamaan toimialueen ohjauskoneiden turvallisuutta. (Microsoft 2023d.)

8 Palvelinkovennukset

Palvelinkovennukset ovat keskeisiä toimia organisaation tietoturvan parantamiseksi niiden keskittyessä järjestelmien suojaamiseen luvattomalta pääsyltä ja mahdollisilta hyökkäyksiltä. CIS:n suositukset ja Microsoftin baseline-suositukset tarjoavat kattavia ohjeistuksia ja parhaita käytäntöjä palvelimien kovennukseen. (Microsoft 2023g.)

8.1 CIS Benchmarks

CIS:n suositukset (CIS Benchmarks) ovat yksityiskohtaisia eri järjestelmien, kuten Windows Serverin, turvalliseen konfigurointiin ja koventamiseen. CIS-kovennussuositukset tarjoavat kaksi suositusta turvallisuustason kovennukselle. **Taso 1** keskittyy perustason turvallisuusvaatimuksiin. Se on suunniteltu tarjoamaan perustason turvallisuutta aiheuttamatta merkittäviä keskeytyksiä. Ensimmäisen tason toimenpiteet ovat sellaisia, jotka voidaan ottaa käyttöön suhteellisen helposti, eivätkä ne vaikuta merkittävästi järjestelmän käyttäjien työskentelyyn. (Center for Internet Security 2024.)

Taso 2 suosittelee tiukempia turvallisuuskovennuksia ympäristöissä. Niissä vaaditaan korkeampaa turvallisuutta ja ne voivat aiheuttaa jonkin verran toiminnallisuuden rajoittumista ja työskentelyn keskeytyksiä. (Center for Internet Security 2024.)

CIS tarjoaa myös kovennettuja virtuaalikoneiden kuvia (CIS Hardened Images). Ne ovat esikovennettu vastaamaan joko **Tason 1** tai **Tason 2** kovennussuosituksia. (Center for Internet Security 2024.)

8.2 Microsoftin Baseline-suositukset

Microsoftin suositukset kattavat useita tuotteita ja palveluita, mukaan lukien Azure-pilviympäristö, Microsoft 365 ja Windows Server. Esimerkiksi ”CIS Microsoft Azure Foundations Benchmark” tarjoaa ohjeita Azure-ympäristön turvallisen peruskonfiguraation luomiseksi. Microsoftin sivuilta ladattavat MSFT Security Baselinet puolestaan ovat Microsoftin omia kovennuksia. Microsoft on ollut tärkeä kumppani CIS suositusten kehityksessä ja heidän tuotteilleen luodut ohjeistukset perustuvat asiantuntijoiden konsultointiin ja laajaan palautteeseen. (Microsoft 2023g.)

8.3 Palvelinkovennuksen keskeiset alueet

Palvelinkovennuksessa keskitytään useisiin avainalueisiin, jotka kattavat järjestelmän, verkon ja AD:n perusrakenteen vahvistamisen. Näitä ovat muun muassa:

- **Sovellukset**: Poistetaan oletussalasanat ja hallitaan sovelluskäyttäjien pääsyä.
- **Tietokannat**: Toteutetaan tiukat kontrollit käyttäjille ja suojataan tietokannat salauksella.
- **Käyttöjärjestelmät**: Varmistetaan käyttöjärjestelmien tietoturvapäivitykset.
- **Verkkoturvallisuus**: Varmistetaan palomuurien asianmukainen konfigurointi ja estetään turvattomien ja tarpeettomien porttien ja protokollien käyttö.
- **Palvelimet**: Sovelletaan pienimpien tarvittavien oikeuksien periaatetta ryhmäkäytännöissä ja toteutetaan palvelimien verkkosegmentointi. (Morgenstern. 2023.)

Näiden suositusten noudattaminen auttaa organisaatioita vähentämään hyökkäyspintaa ja poistamaan heikkouksia kuten turvattomia konfiguraatioita ja heikkoja datan salauksia.

Vaikka Microsoftin ja CIS:n turvallisuussuositukset tarjoavat hyvän lähtökohdan järjestelmien kovennukselle, on organisaatioiden arvioitava omat tarpeensa. Asiakkaiden on kovennettava järjestelmänsä arviointiensa mukaisesti. (Microsoft 2023g; Center for Internet Security 2024.)

9 DNS-tietoturva Active Directoryssä

9.1 DNS:n merkitys AD:n toiminnalle

DNS (Domain Name System) on yksi olennaisimmista osista AD:n toimintaa. Se mahdollistaa asiakaskoneiden kyvyn paikantaa DC:t ja niiden välisen keskinäisen kommunikoinnin. AD käyttää DNS:ää niin sanotusti Domain Controllereiden sijaintimekanismina.

Kun AD:n päätoiminnot, kuten autentikointi, päivitykset tai haku suoritetaan, tietokoneet käyttävät DNS:ää DC:iden paikantamiseen. Lisäksi Domain Controllerit käyttävät DNS:ää toistensa löytämiseen. (Microsoft 2022.)

9.2 DNS-tietoturvakäytännöt ja parhaat menetelmät

DNS-tietoturvan parantamiseksi voidaan hyödyntää useita menetelmiä. Näihin kuuluu ulkoisten hakujen suorittaminen käyttämällä turvallista DNS-välityspalvelua tai root hint -palvelimia, jotka ovat autoratiivisia palvelimia. Nämä palvelimet sisältävät tietoja juuritasolla olevista nimipalvelimista. Turvalliset välityspalvelut tarjoavat lisäturvatoimia, kuten huonomaineisten verkkotunnusten luetteloon perustuvan suodatuksen, joka estää pääsyn vaarallisiin sivustoihin ja voi myös parantaa DNS-hakujen nopeutta. Lisäksi DNS-välimuistin suojausmenetelmien käyttö parantaa järjestelmän turvallisuutta ja tehokkuutta estämällä välimuistin manipuloinnin ja optimoimalla DNS-liikennettä. (Allen 2023.)

9.3 DNS-palveluiden haavoittuvuudet ja niiden hallinta

Microsoftin parhaiden käytäntöjen analysoija (Best Practice Analyzer) voi auttaa tunnistamaan ja korjaamaan mahdolliset konfigurointiongelmat, jotka saattavat altistaa DNS-palvelut haavoittuvuuksille. DNS:n turvallisuutta voi parantaa myös suodattamalla DNS-pyynnöt turvallisuuslaitteiden, kuten seuraavan sukupolven palomuurien tai tunkeutumisenestojärjestelmien (IPS) avulla, jotka tarkistavat domain-nimet huonomaineisten verkkotunnusten luettelosta. (Allen 2023.)

10 Advanced Threat Detection ja tietoturvalokitus

10.1 SIEM-järjestelmät ja lokitiedon hyödyntäminen

Microsoft Defender for Identity on pilvipalvelu, joka suojaa organisaatiota identiteettiperusteisia hyökkäyksiä vastaan. Se analysoi paikallisen AD:n tietoja tunnistaakseen kehittyneet uhat, murrettujen käyttäjätunnusten merkit ja haitalliset toimet yrityksen sisällä. Defender for Identity käyttää erityisiä Windowsin tapahtumalokimerkintöjä parantaakseen havaintoja ja tarjoamaan lisätietoja siitä kuka suoritti tietyt toimet, kuten NTLM-kirjautumiset ja turvaryhmien muutokset. Tämän tiedon avulla voidaan vahvistaa organisaation kykyä tunnistaa poikkeavaa toimintaa ja vastata siihen tehokkaasti. (Tran 2020).

SIEM-järjestelmät (Security Information and Event Management) ovat tärkeässä roolissa organisaation tietoturvainfrastruktuurissa. Ne keräävät, analysoivat ja arkistoivat lokitietoja eri lähteistä, kuten Defender for Identitystä, tarjoten kokonaiskuvan turvallisuustilanteesta. SIEM-järjestelmät mahdollistavat reaaliaikaisen seurannan ja hälytysten generoinnin epäilyttävästä toiminnasta, auttaen tunnistamaan uhkia ja reagoimaan niihin nopeasti. Kun Defender for Identity integroidaan osaksi SIEM-ratkaisua, organisaatiot voivat hyödyntää molempien teknologioiden vahvuuksia edistyneiden uhkien torjunnassa ja tietoturvan hallinnassa. (Microsoft 2024a.)

10.2 Hyökkäysten tunnistaminen ja reagointi

Microsoft Advanced Threat Analytics (ATA) on tehokas paikallinen järjestelmä, joka on suunniteltu suojaamaan yritystä pitkälle kehitetyiltä verkkohyökkäyksiltä ja sisäpiirin uhilta. Se käyttää pakettien tarkastustekniikkaa ja integroituu SIEM-järjestelmiin tarjotakseen kattavan suojan. Analysoimalla verkkoliikennettä ja hyödyntämällä käyttäytymisanalytiikkaa ATA voi havaita epäilyttäviä toimintoja ja poikkeamia käyttäjien käyttäytymisessä, mikä mahdollistaa potentiaalisten uhkien nopean tunnistamisen ja niihin reagoimisen. (Microsoft 2023h.)

ATA pystyy havaitsemaan monenlaisia haitallisia hyökkäyksiä ja tietoturvaongelmia, kuten Kerberosiin kohdistuvat hyökkäykset (Pass-the-Ticket), hyökkäyk-set, joissa yritetään varastaa salasanan hash-arvo, eli tiiviste, ja käyttää sitä todentamiseen (Pass-the-Hash), tai DNS-järjestelmää vastaan kohdistuvat hyökkäykset (DNS Reconnaissan-ce). ATA tarjoaa konsolinsa kautta selkeitä ja käyttökelpoisia näkemyksiä. (Metcalf 2015.)

10.3 Tietoturvan auditointi ja seuranta

Käyttöoikeusratkaisun käyttöönotto edellyttää kokonaisvaltaista lähestymistapaa. Siihen kuuluvat suojatut tilit, työasemat, laitteet ja käyttöliittymien suojaus. Työkalut, kuten "Microsoft Defender for Identity" ja sen yhdistäminen Microsoftin pilvipohjaiseen hallintapalveluun (Microsoft Intune) tehostavat tätä tarjoamalla reaaliaikaisen uhkien havaitsemisen ja laajat auditointiominaisuudet. (Microsoft 2024a.)

Windows-päivityksen määrittäminen oikein ja Microsoft Defender for Endpointin integrointi Intuneen ovat tärkeitä vaiheita sen varmistamiseksi, että järjestelmissä on aina uusimmat suojauspäivitykset. Lisäksi sääntöjen asettaminen Microsoft Defenderin palomuurin ”Endpoint Protection Configuration Profile” -profiiliin voi merkittävästi kaventaa hyökkäyspinta-alaa ja valvoa lähteviä ja saapuvia yhteyksiä. (Microsoft 2024a.)

11 Active Directory Disaster Recovery

11.1 Disaster Recoveryn perusteet AD-ympäristössä

AD ympäristön Disaster Recoveryn (katastrofipalautus) ymmärtäminen ja sen vaatimien toimenpiteiden tiedostaminen on erittäin tärkeää organisaation toimintojen turvaamiseksi. Sillä varmistetaan kyky toipua erityyppisistä häiriöistä, kuten tietoturvahyökkäyksistä, luonnonkatastrofeista tai inhimillisistä virheistä. (Microsoft 2023c.)

AD Disaster Recovery tarkoittaa valmistautumista jopa katastrofaalisiin tapahtumiin, jotka voivat aiheuttaa AD-tietojen katoamisen tai vahingoittumisen sekä niistä toipumista. Vankan selviytymissuunnitelman perustana on AD-ympäristön ymmärtäminen, säännölliset varmuuskopiot ja selkeä, harjoiteltu AD:n elvytysprosessi. On tärkeää arvioida, onko täydellinen AD-metsän (AD-forest) palautus tarpeen arvioimalla vahingon laajuus ja harjoitella palautusprosessia säännöllisesti. Näin asiantuntijat oppivat tuntemaan siihen liittyvät vaiheet. Elvytyssuunnitelman mukauttaminen omaan ympäristöön on ratkaisevan tärkeää tehokkaan katastrofinhallinnan kannalta. (Microsoft 2023c.)

11.2 Varmuuskopiointi- ja palautusstrategiat

Toimiva varmuuskopiointi- ja palautusstrategia on oleellista katastrofista toipumisessa. Siihen kuuluu varmuuskopioiden otto säännöllisesti, jotka tallennetaan turvallisesti offline-tilassa, jotta ne eivät altistuisi samoille ongelmille, jotka aiheuttavat toipumistarpeen. Erilaiset varmuuskopiot palvelevat erilaisia palautustarpeita. Varmuuskopiot voivat sisältää järjestelmän koko tilan tai pelkästään tietokoneen tilan ennen käyttöjärjestelmän tai sovelluksen asentamista. Palauttaminen varmuuskopioista ja sen varmistaminen, että varmuuskopiot ovat kattavia ja ajantasaisia, ovat olennaisia vaiheita hyvässä AD-ympäristön katastrofien palautusstrategiassa. (Smilowitz 2024.)

11.3 Toipuminen tietoturvaloukkauksesta ja -poikkeamista

Tietoturvaloukkauksista toipumiseen kuuluu useita kriittisiä ja tärkeitä vaiheita. Vaiheisiin kuuluu muun muassa järjestelmän tunnistaminen ja eristäminen, palautus suojatuista varmuuskopioista ja perusteellinen tutkinta tapahtuman syyn ja vaikutusten ymmärtämiseksi. Salasanojen palauttaminen, vaarantuneiden tilien puhdistaminen ja turvatoimien vahvistaminen ovat vakiomenettelyjä. Jatkuva seuranta tietoturvaloukkauksen merkkien varalta, pienimpien tarvittavien oikeuksien noudattaminen ja

etuoikeutettujen tilien suojaaminen ovat jatkuvia tehtäviä, jotka auttavat minimoimaan tulevien vaaratilanteiden vaikutukset. (Microsoft 2023b.)

12 Johtopäätökset

Tutkimuksesta voi päätellä, että Active Directoryn (AD) tietoturvatoimenpiteiden huolellinen toteutus voi johtaa merkittäviin parannuksiin tietoturvan tasossa. Kun tietoturvaominaisuudet ja hallinnolliset protokollat integroidaan järjestelmällisesti, organisaatioiden kyky vastata tietoturvariskeihin vahvistuu huomattavasti. Tämä on erityisen ilmeistä, kun tarkastellaan, kuinka tietoturvan monikerroksellinen lähestyminen vähentää tietoturvaloukkauksia ja tehostaa käyttäjähallintaa eri tasoilla.

Tutkimuksen myötä käy ilmi, että monikerroksinen tietoturvallisuus, jossa suojausstrategiat ulottuvat kaikille hallinnan tasoille, on keskeinen tekijä uhkien minimoimisessa. AD:n turvallisuuden vahvistaminen tukee myös organisaatioiden kykyä sopeutua jatkuvasti muuttuvaan kyberturvallisuusympäristöön.

Lisäksi teknisten ratkaisujen rinnalla käyttäjien koulutuksen ja tietoturvasta tiedottamisen merkitys korostuu. Kun organisaatiot panostavat tietoturvakoulutukseen ja -tietoisuuden lisäämiseen, ne kykenevät paremmin suojaamaan infrastruktuurinsa ja arkaluontoiset tietonsa. Uskon tämän osoittautuvan tehokkaaksi tavaksi parantaa tietoturvan kokonaisvaltaista hallintaa.

Tutkimuksen tulokset vahvistavat käsitystä siitä, että tietoturvan jatkuva päivittäminen ja säännölliset tarkastukset ovat välttämättömiä korkean turvallisuustason ylläpitämiseksi. Tietoturvan jatkuvasti kehittyvä taso edellyttää säännöllistä uudelleenarviointia ja mukautumista uusiin tietoturvauhkiin, mikä on olennainen osa organisaatioiden pitkäaikaista kestävyyttä ja luotettavuutta tietoturvan näkökulmasta.

13 Pohdinta

Tässä opinnäytetyössä on tullut ilmi, kuinka merkittävä rooli Active Directorylla (AD) on organisaation tietoturvan kannalta. Opinnäytetyö on antanut syvällisen käsityksen AD:n tietoturvallisen toteutuksen monitahoisista näkökulmista, korostaen sen keskeistä asemaa yritysten tietohallinnossa. Työssä esille tulleet AD:n tietoturvallisuuteen liittyvät periaatteet, suunnitteluprosessit ja käytännöt ovat osoittautuneet välttämättömiksi työkaluiksi, joilla voidaan merkittävästi vähentää tietoturvariskejä ja parantaa yritysten kykyä hallita ja suojata arkaluontoisia tietojaan.

Opinnäytetyö on tuonut esiin, kuinka tärkeää on ymmärtää ja hallita AD:n monimutkaisia turvallisuusasetuksia ja protokollia, jotta voidaan varmistaa, että tietoturvatoimet ovat riittävät ja ajantasaiset. Työn aikana kertynyt tietämys ja kokemus AD:n turvallisuusmekanismien toteuttamisesta tarjoaa perustan, joka auttaa rakentamaan vahvemman ja luotettavamman tietoturvarakenteen organisaation AD-ympäristöön. On selvää, että AD:n jatkuva kehitys ja päivitys ovat välttämättömiä, sillä myös tietoturvauhat ja teknologiat kehittyvät jatkuvasti.

Opinnäytetyön tekeminen on valottanut myös sitä, kuinka tärkeää on organisaation sisäisen tietoturvakulttuurin kehittäminen. Tietoturva ei ole vain teknologiaa ja työkaluja, vaan myös ihmisiä ja prosesseja. Tietoturvallisuuden parantaminen vaatii jatkuvaa koulutusta, valistusta ja prosessien kehittämistä, jotta kaikki organisaation jäsenet ymmärtävät tietoturvan merkityksen ja osallistuvat aktiivisesti sen ylläpitämiseen.

Tämän opinnäytetyön kautta on myös korostunut tarve laajemmalle yhteistyölle ja tiedonjaolle tietoturva-asiantuntijoiden, IT-henkilöstön ja organisaation johdon kesken. Tietoturva on koko organisaation laajuinen tehtävä, ja sen menestyksellinen toteutus edellyttää kaikkien osapuolten sitoutumista ja yhteistyötä. Jatkotutkimuksille ja -kehitykselle on selkeästi tilausta, erityisesti kun tarkastellaan AD:n roolia pilvipalveluiden ja hybridiratkaisujen ympäristöissä, jotka ovat nykyään yhä yleisemmin käytettyjä.

Pohdintaosuudessa on tarkasteltu näitä monitahoisia elementtejä, ja se tarjoaa pohjan, jolta organisaatiot voivat lähteä kehittämään ja parantamaan omia tietoturvallisuuden käytäntöjään. Tämä työ on osoittanut, että vaikka AD:n hallintaan liittyvät haasteet ovat suuret, ne ovat myös ratkaistavissa asianmukaisella tietämyksellä, työkaluilla ja asenteella.

Lähteet

Allen, R. 2023. DNS Best Practices: The Definitive Guide. https://activedirectorypro.com/dns-best-practices. 10.3.2024.

Bigelow, S. J. 2024. Active Directory functional levels. https://techtarget.com/searchwindowsserver/definition/Active-Directory-functional-levels. 10.3.2024.

Center for Internet Security. 2024. CIS Benchmarks for Microsoft Windows Server. https://cisecurity.org/benchmark/microsoft_windows_server. 11.03.2024.

Delinea. 2023. What are Privileged Access Workstations (PAWs)? https://delinea.com/what-is/privileged-access-workstations-paws. 2.3.2024.

Heidecker, D. 2024. Protecting Tier 0 the Modern Way. https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/protecting-tier-0-the-modern-way/ba-p/4052851. 10.3.2024.

Kinzer, K. 2022. Active Directory Authentication. https://jumpcloud.com/blog/active-directory-authentication. 10.3.2024.

Löfgren, P. 2024. Active Directory Tiering. https://truesec.com/security/active-directory-tiering. 9.3.2024.

Mar-Elia, D. 2022. Using Tiered Administration for Group Policy Management. https://sdmsoftware.com/security-related/using-tiered-administration-for-group-policy-management/. 9.3.2024.

Makenzie, B. 2024. What is Group Policy in Active Directory? https://www.ninjaone.com/blog/what-is-group-policy-in-active-directory/. 11.4.2024.

Microsoft. 2021a. Designing the Active Directory Site Topology. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/designing-the-site-topology. 9.3.2024.

Microsoft. 2021b. Understanding Active Directory Site Topology. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-active-directory-site-topology. 10.3.2024.

Microsoft. 2021c. Kerberos Authentication Overview. https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview. 10.3.2024

Microsoft. 2022. DNS Overview. https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-top. 9.3.2024.

Microsoft. 2023a. LAPS Overview. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview. 2.3.2024.

Microsoft. 2023b. AD Forest Recovery Planning. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-devise-a-plan. 10.3.2024.

Microsoft. 2023c. AD Forest Recovery Procedures. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-procedures. 11.3.2024.

Microsoft. 2023d. Best Practices for Securing Active Directory. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory. 10.3.2024.

Microsoft. 2023f. Securing Domain Controllers Against Attack. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack. 10.3.2024.

Microsoft. 2023g. Windows Security Baselines. https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines. 11.03.2024.
Microsoft. 2023h. What is Advanced Threat Analytics? https://learn.microsoft.com/en-us/advanced-threat-analytics/what-is-ata. 10.3.2024.
Microsoft. 2024a. Compliance Regulatory Offering: CIS Benchmark. https://learn.microsoft.com/en-us/compliance/regulatory/offering-CIS-Benchmark. 11.03.2024.
Microsoft. 2024b. Privileged Access Access Model. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model. 9.3.2024.
Microsoft. 2024c. Privileged Access Deployment. https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment. 10.3.2024.
Morgenstern, T. 2023. System Hardening and CIS Compliance: the complete guide. https://vulcan.io/blog/system-hardening-and-cis-compliance/. 11.03.2024.
Rossevelt, M. 2023. How Does BitLocker Encrypt Data? https://newsoftwares.net/blog/how-does-bitlocker-encrypt-data/. 2.3.2024.
Smilowitz, C. 2024. Active Directory Disaster Recovery Best Practices. https://lepide.com/blog/active-directory-disaster-recovery-best-practices/. 9.3.2024.
Tran, T. 2020. Microsoft Defender for Identity: Azure ATP Deployment and Management. https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-for-identity-azure-atp-deployment-and/bap/1676122. 9.3.2024.
Vaideeswaran, N. 2023. Active Directory Security Basics. https://crowdstrike.com/cybersecurity-101/active-directory-security/. 10.3.2024.