Wat is active directory en waarom is het nuttig voor MKB?

https://aucuba.nl/kennisbank/uncategorized/wat-is-active-directory-en-waarom-is-het-nuttig-voor-mkb/

Active directory is een directoryservice van Microsoft waarmee bedrijven gebruikers, apparaten en toegangsrechten centraal beheren. In plaats van op elk apparaat afzonderlijk accounts en wachtwoorden in te stellen, regelt active directory dit vanuit één centrale omgeving. Voor MKB-bedrijven biedt dat een enorme tijdsbesparing en een stevige basis voor beveiliging. In dit artikel beantwoorden we de meest gestelde vragen over active directory, zodat je weet of en hoe het voor jouw bedrijf werkt.

Hoe werkt active directory in de praktijk?

Active directory werkt als een centrale administratie voor je netwerk. Wanneer een medewerker inlogt op een computer, controleert active directory de inloggegevens en bepaalt het systeem automatisch tot welke bestanden, applicaties en netwerkmappen die persoon toegang heeft. Alles wordt beheerd vanuit één centrale server, de domeincontroller.

In de praktijk betekent dit dat een nieuwe medewerker één account krijgt waarmee hij of zij op alle werkstations en systemen kan inloggen die voor die functie zijn vrijgegeven. Verlaat iemand het bedrijf, dan deactiveer je dat ene account en vervalt de toegang tot alle systemen direct. Beheerders kunnen bovendien groepsbeleid instellen, zogenaamde Group Policy Objects, waarmee ze instellingen zoals schermvergrendeling, software-installaties en beveiligingsregels op afstand uitrollen naar alle apparaten in het netwerk.

Wat zijn de voordelen van active directory voor MKB?

De voordelen van active directory voor MKB zijn centraal gebruikersbeheer, betere beveiliging, tijdsbesparing voor IT-beheer en consistente werkomgevingen voor medewerkers. Zonder active directory beheert elk apparaat zijn eigen gebruikers en instellingen, wat leidt tot inconsistentie, hogere beheerlast en beveiligingsrisico's.

Voor MKB-bedrijven zijn dit de belangrijkste voordelen op een rij:

- **Centraal gebruikersbeheer:** Alle accounts, wachtwoorden en rechten worden op één plek beheerd.
- **Tijdsbesparing:** Nieuwe medewerkers onboarden en vertrokken medewerkers offboarden gaat snel en volledig.
- **Consistente beveiliging:** Beveiligingsbeleid wordt automatisch toegepast op alle apparaten in het netwerk.
- **Schaalbaarheid:** Het systeem groeit mee met je bedrijf, van vijf tot honderd medewerkers.
- **Minder IT-storingen:** Proactief beleid voorkomt dat medewerkers zelf ongewenste software installeren of instellingen wijzigen.

Juist voor bedrijven zonder interne IT-afdeling is dit waardevol. Goed ingericht active directory beheer betekent minder brandjes blussen en meer rust in de dagelijkse bedrijfsvoering.

Wat is het verschil tussen active directory en Azure AD?

Het belangrijkste verschil tussen active directory en Azure AD is de omgeving waarin ze werken. Klassieke active directory draait op een lokale server in je eigen kantoor en beheert apparaten en gebruikers binnen een on-premises netwerk. Azure AD, tegenwoordig ook wel Microsoft Entra ID genoemd, is een cloudgebaseerde variant die is ontworpen voor moderne clouddiensten zoals Microsoft 365.

In de praktijk zien we bij MKB-bedrijven steeds vaker een hybride omgeving: klassieke active directory voor het lokale netwerk, gecombineerd met Azure AD voor cloudtoepassingen. Zo kunnen medewerkers met één account inloggen op zowel hun werkcomputer als op Teams, SharePoint en andere Microsoft 365-diensten. Dit heet hybride identiteitsbeheer en biedt het beste van beide werelden.

Bedrijven die volledig in de cloud werken en geen eigen servers hebben, kunnen ook kiezen voor een pure Azure AD-omgeving zonder lokale domeincontroller. Welke aanpak het beste past, hangt af van je infrastructuur, het aantal medewerkers en de applicaties die je gebruikt.

Wanneer heeft een MKB-bedrijf active directory nodig?

Een MKB-bedrijf heeft active directory nodig zodra er meerdere medewerkers zijn die dezelfde apparaten, bestanden of systemen gebruiken en waarbij toegangsbeheer en beveiliging een rol spelen. Globaal geldt: vanaf vijf medewerkers of meerdere werkstations begint de meerwaarde van active directory duidelijk te worden.

Concrete signalen dat je bedrijf toe is aan active directory:

- Medewerkers delen wachtwoorden of hebben toegang tot systemen die niet voor hen bedoeld zijn.
- Het offboarden van een vertrekkende medewerker kost veel tijd en je weet niet zeker of alle toegang is ingetrokken.
- Nieuwe laptops en werkstations moeten steeds handmatig worden geconfigureerd.
- Er is geen consistente beveiliging op alle apparaten in het netwerk.
- Medewerkers werken op meerdere locaties of apparaten en willen overal hetzelfde account gebruiken.

Bedrijven die groeien of hun IT-infrastructuur willen professionaliseren, profiteren het meest van een goed ingericht active directory. Het legt een stevige basis voor verdere digitalisering en schaalbaarheid.

Hoe richt je active directory in voor een klein bedrijf?

Active directory inrichten voor een klein bedrijf begint met het opzetten van een domeincontroller, het aanmaken van gebruikersaccounts en het definiëren van groepen en toegangsrechten. De technische inrichting vereist kennis van Windows Server en netwerkbeheer, en wordt bij de meeste MKB-bedrijven uitbesteed aan een ICT-partner.

De stappen in het inrichtingsproces zijn doorgaans als volgt:

1. **Infrastructuur bepalen:** Kies je voor een fysieke server, een virtuele server of een cloudoplossing via Azure AD.
2. **Domein aanmaken:** Stel een domeinnaam in voor je organisatie en installeer de domeincontrollerrol op de server.
3. **Gebruikers en groepen aanmaken:** Maak accounts aan voor alle medewerkers en groepeer ze op afdeling of functie.
4. **Rechten toewijzen:** Bepaal per groep welke mappen, printers en applicaties toegankelijk zijn.
5. **Groepsbeleid instellen:** Configureer beveiligingsregels en standaardinstellingen die automatisch worden uitgerold naar alle apparaten.
6. **Apparaten koppelen aan het domein:** Voeg alle werkstations toe aan het domein zodat ze onder het centrale beheer vallen.

Een zorgvuldige inrichting voorkomt problemen later. Fouten in de rechtenstructuur of het groepsbeleid kunnen leiden tot beveiligingslekken of problemen met de toegankelijkheid van systemen. Wij helpen MKB-bedrijven bij het opzetten en beheren van een active directory-omgeving die aansluit op hun specifieke situatie.

Wat kost het beheren van active directory voor MKB?

De kosten voor active directory beheer bij MKB zijn afhankelijk van meerdere factoren: de omvang van de organisatie, de complexiteit van de omgeving, de gekozen infrastructuur en de mate van uitbesteding. Er is geen vaste prijs, maar de kostenstructuur bestaat uit een aantal vaste componenten.

Factoren die de kosten bepalen:

- **Serverinfrastructuur:** Een fysieke server brengt aanschaf- en onderhoudskosten met zich mee. Een cloudoplossing werkt met een maandelijks abonnement.
- **Licenties:** Windows Server-licenties en eventuele Microsoft 365-licenties zijn onderdeel van de totale investering.
- **Beheer en ondersteuning:** Proactief beheer door een ICT-partner voorkomt problemen en verlaagt de kans op dure storingen.
- **Complexiteit van de omgeving:** Meer gebruikers, meer locaties of een hybride omgeving vragen meer beheerinspanning.
- **Initiële inrichting:** De eenmalige kosten voor het opzetten van het domein, het aanmaken van gebruikers en het inrichten van het groepsbeleid.

Voor MKB-bedrijven is uitbesteed beheer vaak kostenefficiënter dan zelf een IT-medewerker in dienst nemen. Je betaalt voor kennis en beschikbaarheid zonder de vaste lasten van een intern team.

Welke beveiligingsrisico's lost active directory op?

Active directory lost een aantal concrete beveiligingsrisico's op die MKB-bedrijven zonder centraal gebruikersbeheer dagelijks lopen. De belangrijkste zijn ongecontroleerde toegang tot gevoelige gegevens, zwakke of gedeelde wachtwoorden, en het niet tijdig intrekken van toegangsrechten bij vertrekkende medewerkers.

Zonder active directory heeft elk apparaat zijn eigen gebruikersaccounts en instellingen. Dit maakt het lastig om overzicht te houden over wie toegang heeft tot wat. Met active directory los je

de volgende risico's structureel op:

- **Ongeautoriseerde toegang:** Rechten worden per functie of afdeling ingesteld, zodat medewerkers alleen zien wat voor hen relevant is.
- **Zwakke wachtwoorden:** Via groepsbeleid dwing je wachtwoordeisen af, zoals minimale lengte en verplichte vernieuwing.
- **Vergeten accounts:** Vertrekkende medewerkers worden centraal uitgeschakeld, zodat er geen actieve accounts achterblijven.
- **Onbeheerde apparaten:** Alle apparaten in het domein volgen hetzelfde beveiligingsbeleid, inclusief schermvergrendeling en software-restricties.
- **Gebrek aan auditsporen:** Active directory legt inlogpogingen en wijzigingen vast, wat essentieel is bij een beveiligingsincident.

Beveiliging begint bij goed gebruikersbeheer. Active directory is daarvoor een van de meest effectieve en bewezen middelen binnen de Microsoft-omgeving. Wil je weten hoe jouw bedrijf er nu voor staat en wat active directory voor jou kan betekenen? Neem gerust contact met ons op voor een vrijblijvend gesprek.