MDM / MAM

Grip op je bedrijfsdata met behoud van privacy

Maak kennis met Mobile Device Management en Mobile Application Management

Dat de smartphone het krantje op de Wc heeft vervangen, geeft aan dat het mobiele tijdperk onomkeerbaar is. En geef de Wc-bezoeker eens ongelijk. Hoe ontspannend ook, voor jou als IT manager brengt deze exponentiële groei van apparaten die verbonden zijn met internet een uitdaging met zich mee op het gebied van beheer en security. Komt het niet al vanuit eigen beweging om hier stappen in te nemen, dan is het wel de AVG wetgeving die je verplicht hier actie op te ondernemen. Gelukkig biedt Mobile Device Management (MDM) of Mobile Application Management (MAM) uitkomst voor het centraal beheren van al je mobiele devices. Lees hieronder hoe MDM of MAM jou kan helpen.

MDM uitgelegd

Met Mobile Device Management (MDM) beheer je mobiele devices zoals smartphones, tablets en laptops vanuit een centrale beheerportal. Dit doen wij met Intune. Via de beheerportal kan je policies afdwingen op de devices die in de MDM omgeving zijn opgenomen. Een hele mond vol, maar wat kan je allemaal beheren? Als we het kort samenvatten kan je:

- devices op afstand vergrendelen en/of wissen. Bijv. bij verlies of diefstal;
- beperkingen instellen voor o.a. roaming, apps en back-ups naar prive clouds;
- diverse zaken configureren zoals WiFi en e-mailaccounts;
- programma-updates centraal uitrollen naar meerdere toestellen tegelijk.

Wordt jij hier al enthousiast van? Lees dan hieronder verder.

Beveilig je zakelijke device
Je device beveiligen doe je door ‘Policies’ in te stellen in de portal. Hiermee regel je bijvoorbeeld beveiligingsinstellingen (pincode, encryptie) en toegang tot het bedrijfsnetwerk (WiFi, VPN). Ook configureer je applicaties zoals mail, agenda en contactgegevens.

Beveilig je mobiele e-mail
Er gaat nogal wat mail op een dag via je smartphone of tablet. Je wilt natuurlijk dat dit veilig gebeurt. Met MDM en MAM heb je de mogelijkheid bedrijfsmail te verwijderen van de smartphones of tablets. Dit bijvoorbeeld als iemand uit dienst treedt of er een geschil is met een medewerker.

Beveilig je Apps
Met alle toepassingen van hierboven zijn je mobiele apparaten voorzien van security policies en startklaar voor zakelijk gebruik. Maar hoe staat het met je Apps? Met MDM en MAM kan je bedrijfsapps beschikbaar stellen aan gebruikers en beveiligen volgens de wijze waarop jij dit eist. Wel zo makkelijk en veilig.

Continue beveiliging
Met Defender voor Endpoint wordt automatisch gedetecteerd of zich er bedreigingen voor doen. Denk hierbij aan verdacht netwerkverkeer op het toestel. Als een bedreiging wordt gedetecteerd en een acceptabel bedreigingsniveau overschrijdt, kan jouw organisatie het volgende doen:

- **Toegang blokkeren**: je kunt geen apps gebruiken terwijl je bent aangemeld bij jouw werkaccount.

- **Gegevens wissen**: verwijder jouw werkgegevens uit een of meer werk-apps.

Verschil tussen MAM en MDM

We zien regelmatig dat medewerkers hun eigen mobiele toestel willen gebruiken voor zakelijk gebruik of hun zakelijke toestel inzetten voor prive gebruik. In beide gevallen is MAM erg geschikt, omdat je dan niet het apparaat volledig beheerd, maar puur de zakelijke applicaties. Daarnaast is het een goede oplossing die de privacy van je medewerkers respecteert, zonder concessies te doen aan de beveiliging van de bedrijfsgegevens. Zo is er nooit discussie over privacy of de angst dat je de privécollectie aan kattenfoto's gelijk wist.

Tegelijkertijd biedt het je wel de mogelijkheid om ervoor te zorgen dat je grip hebt op de zakelijke applicaties en toegang hiertoe. Zo kan je ervoor zorgen dat data vanuit die apps nooit naar het privé device gekopieerd kan worden en bijv. pincodes afdwingen.

Een combinatie van MDM en MAM is ook mogelijk. Kortom, mogelijkheden zat. Het gaat er wat bij jouw organisatie past. Wij geven je graag het juiste advies.

Wil je weten wat voor jouw organisatie de beste vorm is?

Onze consultant Marco vertelt het je graag.

Neem contact op met Marco via de onderstaande contactgegevens.

marco.vermoen@vtmgroep.nl
0174 255 891

Technical IT-consultant