Beveiliging en beheer mobiele apparaten

Mobility staat bij menig IT-manager en CIO op de agenda.

Hoewel het onderwerp al langer op de agenda staat, worstelen veel organisaties nog altijd met hoe ze dit moeten aanpakken. Mobility is meer dan werken op een tablet of smartphone. Bij mobility spreken we over robuuste beveiligingsoplossingen voor apparaten die aan het corporate netwerk worden gekoppeld.

Drie aandachtspunten

'Gaan we mobiel werken?' Is al door de meeste organisaties positief beantwoord. Nu is men op zoek naar: 'Hoe gaan we dat doen?' en 'Waar moeten we op letten?'
Voordat u overgaat tot implementatie van een dergelijke oplossing zult u eerst drie vragen moeten beantwoorden.

Wat wil ik bereiken?

De eerste vraag is wat wilt u met mobiel werken bereiken? Vaak ligt het antwoord op terreinen als beter gemotiveerde medewerkers, flexibiliteit en kostenbesparingen. Dat betekent dat u zo min mogelijk drempels moet opwerpen en dat u de gebruikerservaring moet laten aansluiten bij wat een specifieke medewerker nodig heeft om zijn of haar werk goed te doen.

Wie, wat, welke?

De tweede vraag is: Wie mag welke informatie vanaf welke plek bekijken en met welk apparaat (device)? Ook moet worden beslist welke apparaten welke rechten krijgen. Zo kunt u instellen dat bepaalde data of bepaalde applicaties niet benaderd mogen worden met een privéapparaat.

Rechten?

En tot slot is het belangrijk vast te leggen wie welke rechten heeft. Welke medewerkers mogen welke informatie inzien en/of wijzigen? Daarbij is het ook belangrijk of die medewerkers met een eigen apparaat werken, of dat ze een toestel gebruiken dat door de werkgever is verstrekt en wordt beheerd.

Beveiliging en beheer mobiele apparaten

Enterprise Mobility platform

Bedenk welke techniek nodig is om de gekozen strategische aanpak te realiseren. U kunt daarbij kiezen voor best-of-breed-oplossingen, zo lang die maar goed op elkaar aansluiten en het beheer overzichtelijk blijft. Een betere keuze is een geïntegreerd Enterprise Mobility platform dat alle aandachtspunten in zich verenigt.

De vijf belangrijke onderdelen van zo'n platform:

- MDM (Mobile Device Management), om devices op afstand te beheren en eventueel te wissen in geval van verlies of diefstal;
- MAM (Mobile Application Management), alle zakelijke applicaties op afstand via een pushmechanisme toe te voegen, te verwijderen of te updaten;
- Een oplossing om bestanden op een veilige manier te delen, zodat men niet in de verleiding komt om Dropbox te gebruiken;
- Follow me, waarbij data je volgt naar een andere locatie/device zonder dat men alle applicaties weer opnieuw moet opstarten;
- Een virtuele werkplek zodat medewerkers op ieder apparaat – of het nu een iPad of een Windows PC is – dezelfde gebruikerservaring hebben.

Kortom, een strategische keus om mobiel werken te ondersteunen behelst veel meer dan beslissen voor Bring of Choose Your Own Device.

Benieuwd naar de mogelijkheden voor uw organisatie?
Neem dan contact met ons op.

auxzenze
IT MAKES SENSE

'Hof van Zutphen'
Industrieweg 85
7202 CA Zutphen
T +31(0)88 55 85 250
F +31(0)88 55 85 260
E info@auxzenze.nl
W www.auxzenze.nl