Zakelijk gebruikte privétoestellen uitdaging voor elke IT-beheerder

20 oktober 2017

Dat geldt zeker voor bedrijfsomgevingen waarin vaste en mobiele telefonie zijn geïntegreerd. Werknemers gebruiken privétoestellen, of dat nu mag of niet. Vooral de jongste generatie medewerkers is erg gehecht aan zijn eigen smartphone en weet bovendien precies hoe je met het apparaat je werk kunt vergemakkelijken.

Daarvoor is dan vaak wel de instemming van de IT-beheerder nodig. Al was het maar om privétoestellen toegang te geven tot de Exchange server, zodat de werknemer bij zijn zakelijke e-mails en agenda kan. Ook voor de koppeling tussen privé smartphone en andere bedrijfsapplicaties, zoals de systemen voor klantbeheer en personeelszaken, moet de beheerder een veilige oplossing bieden.

CYOD Welk beleid moeten organisaties opstellen voor het gebruik van privé mobieltjes op de werkvloer? Steeds vaker kiezen ze voor Choose Your Own Device (CYOD), waarbij de werknemer kan kiezen uit een beperkt aantal modellen die de organisatie ondersteunt. Dat houdt het voor de IT-beheerder iets overzichtelijker dan bij Bring Your Own Device (BYOD), waarbij personeel helemaal zelf bepaalt met welk toestel ze werken. Overzichtelijker, doordat je bijvoorbeeld de keuze kunt beperken tot toestellen waarop hetzelfde besturingssysteem staat, zoals Android, iOS of Windows Phone. Vervolgens is het de vraag hoe je zakelijke apps, bestanden en verbindingen optimaal beveiligt op een privétoestel.

Gelukkig bestaan daarvoor tegenwoordig goede oplossingen. De meeste zijn gebaseerd op containerisatie, waarbij je de zakelijke elementen volledig gescheiden houdt van privé toepassingen en inhoud. Om toegang te krijgen tot de ‘zakelijke container’ moet de werknemer separaat inloggen. Secure Device Management Voor organisaties die hun mobiele en vaste telefonie hebben geïntegreerd of dat van plan zijn, is er Secure Device Management (SDM). Vodafone biedt dat als onderdeel van zijn One Business-portfolio, een groep van producten en diensten voor de integratie van vast en mobiel. SDM is een vorm van mobile device

management (MDM).

Vodafone Secure Device Management is een betaalbaar beheerplatform in de cloud. De IT-beheerder krijgt online toegang tot een beheermodule, waar hij instellingen kan wijzigen en nieuwe mobiele aansluitingen en toestellen kan toevoegen. De module stelt de beheerder ook in staat om actie te ondernemen als zich een beveiligingsprobleem met de smartphone van een werknemer voordoet. Zo kan hij ingrijpen bij diefstal of vermissing van het toestel, bijvoorbeeld door de inhoud op de telefoon te blokkeren of zelfs te vernietigen.

Managed mobility services binnen Vodafone One Business kunnen organisaties meer doen om hun CYOD-beleid handen en voeten te geven. Zo kunnen ze voor hun werknemers een interne webshop inrichten. In de shop staan de smartphones die de IT-beheerders ondersteunen. Aan de medewerker de keuze welk toestel en welk abonnement hij of zij neemt. Er zijn zelfs mogelijkheden om de dienstverlening uit te breiden met managed mobility services. Hierbij bieden de experts van Vodafone ondersteuning bij het installeren van Secure Device Management, het overzetten van contactlijsten en het correct installeren van zakelijke apps op de smartphones.