“Gebruiksvriendelijkheid en veiligheid gaan prima samen.”

In de sterk gedigitaliseerde wereld wordt het goed bewaken van gevoelige gegevens steeds belangrijker. Niet alleen consumenten, maar ook bedrijven zien de noodzaak om waardevolle data veilig te kunnen gebruiken, opslaan en verplaatsen. Kiezen voor een IT-leverancier die de bescherming van gegevens hoog in het vaandel heeft staan, ontzorgt, waardoor ondernemers vooral weer met hun eigen werk bezig kunnen zijn. “Gebruiksvriendelijkheid van een oplossing gaat boven alles”, aldus Gerrit Bloot, Senior Business Unit Manager Apple, bij Apple-distributeur Tech Data.

Waarom is juist deze gebruiksvriendelijkheid zo belangrijk, dit heeft toch niets met veiligheid te maken?

“In eerste instantie zou je denken van niet, maar je hebt misschien zelf weleens gemerkt dat iets wat ingewikkeld is om te gebruiken, hierdoor juist vaak verkeerd gebruikt wordt.

Wanneer je bijvoorbeeld een telefoon van de zaak hebt die volledig is dichtgezet met allerlei codes en andere beperkingen, ga je vaker met je eigen apparaat even snel dat berichtje sturen, of even die notulen doormailen. Je kiest ervoor om de ingewikkelde route te omzeilen door zelf te werken met een apparaat dat wel ‘gewoon doet’ wat je wilt.

Mensen realiseren zich vaak niet dat ze door hun eigen apparaten te gebruiken gevoelige bedrijfsinformatie mogelijk onveilig versturen. Er is dan direct een risico op een lek. Tegelijkertijd heeft het bedrijf zelf geen idee dat de door hen vaak zo zorgvuldig opgezette beveiliging door medewerkers wordt genegeerd, omdat deze te ingewikkeld is.”

Hoe kun je dan voorkomen dat mensen met hun eigen apparatuur gaan werken? Je kunt als bedrijf toch niet de privé-telefoons van al je medewerkers controleren?

"Nee, dat is zeker niet de bedoeling. Het is alleen ook niet nodig om gebruik van persoonlijke apparatuur voor bedrijfsdoeleinden te ontmoedigen, sterker nog, het is vrij eenvoudig om hetzelfde mobiele apparaat zowel voor zakelijk als privégebruik in te richten, zonder dat je hiermee de privacy van de gebruiker aantast, noch de veiligheid van de bedrijfsinformatie. Als medewerker wil je natuurlijk niet dat de baas kan inzien wat jij in je vrije tijd doet of met wie jij allemaal privé contact hebt.

Op bepaalde toestellen kun je dit eenvoudig laten inrichten, zowel op hardware- als op softwareniveau kun je zakelijk van privé gescheiden houden binnen één device. Als gebruiker merk je eigenlijk niets van de aanpassing die dan wordt gemaakt, dat is weer de gebruiksvriendelijkheid die zo belangrijk is, terwijl je er als ondernemer of bedrijf wel zeker van bent dat bijvoorbeeld het verzenden van e-mails vanaf dat toestel aan strenge veiligheidseisen voldoet."

Maar als zowel privégegevens als zakelijke gegevens op hetzelfde toestel staan, hoe werkt het dan als het toestel bijvoorbeeld kwijtraakt of de betreffende persoon uit dienst gaat?

"Een toestel kan op afstand geblokkeerd of gewist worden, bovendien kunnen via het MDM-systeem (Mobile Device Management) van het bedrijf, alle zakelijke gegevens en apps van het toestel verwijderd worden, terwijl de privégegevens en -instellingen bewaard blijven. Los van hoe een toestel aan de voorkant door de gebruiker wordt beveiligd, heeft een werkgever nooit toegang tot gegevens op een toestel.

Dit is onmogelijk gemaakt, zodat de privacy van de gebruiker niet op het spel komt te staan. Werkgevers kunnen het toestel dus wel (op afstand) wissen, maar hebben geen toegang tot die gegevens. Ook overheidsinstellingen hebben die toegang niet. Bel- en berichtdata van toestellen kunnen dus niet worden uitgelezen en ook de vingerafdruk van de 'touch-ID'-herkenning wordt in een write-only memory opgeslagen en is nooit uit te lezen.

Bovendien, als je als bedrijf gegevens wél zou opslaan, zodat je deze op verzoek van bepaalde (overheids-)instanties kunt vrijgeven, creëer je openingen voor hackers. Als er dan een keer iets misgaat, heb je een probleem, vooral als gebruiker, maar zeker ook als bedrijf, dan kun je de deuren wel sluiten. Data van eindgebruikers zijn privé en moeten privé blijven. Zo wist Apple bijvoorbeeld altijd je digitale voetstappen; dit is voor zowel het bedrijf als de gebruiker een veiligheidswaarborging."

Welke mogelijkheden zijn er voor bedrijven en organisaties?

"Er is een speciaal programma, het zogenaamde 'Device Enrollment Programma' (DEP) ontwikkeld wat een gemakkelijke, snelle en veilige manier is om Apple-producten te gebruiken en uit te rollen in de organisatie. Voorheen moesten ICT-afdelingen fysiek instellingen configureren op elk apparaat.

Nu kunnen ze op grote schaal draadloos apparaten uitrollen. Alle bedrijfsgegevens worden automatisch en op een veilige manier op het toestel geladen, terwijl eindgebruikers het toestel ook voor privédoeleinden kunnen gebruiken zonder dat vertrouwelijke (bedrijfs-)informatie in gevaar komt.

Daarmee ben je als organisatie mobieler en sneller. Met DEP definieert de ICT-afdeling in een dashboard de configuratie voor werknemers en functiegroepen. De medewerker ontvangt vervolgens een nieuw apparaat direct vanuit de leverancier. Na openen wordt het apparaat automatisch aan het bedrijf gekoppeld waarna de loginnaam en het wachtwoord van de medewerker worden gevraagd.

Daarna worden alle apps en gegevens automatisch geïnstalleerd en heeft de medewerker de mogelijkheid om ook de persoonlijke zaken te installeren zonder dat dit in conflict komt met de bedrijfspolicy. De ICT-afdeling heeft het apparaat nooit aangeraakt, de medewerker doet het allemaal zelf. Met die gedachte is DEP ontwikkeld. Het scheelt kosten en tijd. Ook voor de zakelijke gebruiker stelt Apple gebruikersgemak dus op één. De deployment-programma's van Apple zijn een standaard onderdeel van het besturingssysteem van elk Apple-product.

Er wordt echter wel vanuit gegaan dat bedrijven die DEP willen inzetten, beschikken over een directory service zoals Active Directory en een MDM-systeem waarin de gebruikers en bedrijfspolicies zijn opgenomen. Wat je veel ziet na implementatie van DEP, is dat werknemers minder vaak een beroep doen op de helpdesk van een bedrijf. Door gebruik te maken van de oplossing kunnen bedrijven besparen op software voor device management en op die helpdesk.

Voordeel voor ondernemingen is dat DEP altijd verbinding heeft met de bedrijfsserver, dus als een medewerker een harde reset uitvoert en alles wist, staan alle gegevens en instellingen er weer opnieuw op als het device weer wordt opgestart. Daarbij wordt de gebruikerservaring niet beperkt. Het DEP-portal is voor ICT-afdelingen gemakkelijk te beheren en met de aangesloten software kunnen bedrijven zelf voorkeuren instellen en beveiligen."

Hoe veel wordt DEP inmiddels gebruikt?

"DEP is anderhalf jaar op de markt en een substantieel deel van de voor zakelijk gebruik uitgerolde iOS-producten loopt nu via DEP. Eindklanten kennen de voordelen van DEP inmiddels ook en eisen bij grote projecten vaak dat de uitrol via DEP loopt. De wet datalekken kan daarmee te maken hebben, omdat bedrijven zich steeds meer bewust zijn van de gevaren die ICT met zich mee kan brengen. Het is goed dat dit bewustzijn groeit, nu ook nog de kennis dat een passende oplossing niet ingewikkeld hoeft te zijn."

Gebruik maken van DEP is kosteloos, vraag naar de mogelijkheden bij uw reseller.

Apple Inc.