Veilig gebruik smartphome

Vodafone
Power to you

Gebruik op je werk vooral je eigen smartphone of tablet, maar doe het wel veilig

Gebruik op je werk vooral je eigen smartphone of tablet, maar doe het wel veil
Op weg naar huis de laatste mailtjes beantwoorden, een blik op de financiële bedrijfsresultaten of nog even de laatste aanpassingen voor die belangrijke salespresentatie. Handig, want het kantoor reist gewoon op je eigen smartphone met je mee. Maar wat als die informatie in verkeerde handen komt door een hack of een virus? Bedrijven zien grote voordelen in de 'Bring Your Own Device'-trend, maar worstelen met de beveiliging van bedrijfsgegevens op het toestel van medewerkers. Bescherming van data staat daarom met stip bovenaan de agenda van de CIO.

De urgentie om data op mobiele devices te beveiligen is vanaf 1 januari 2016 nog belangrijker. Organisaties zijn vanaf dan namelijk wettelijk verplicht inbreuken op de beveiliging van privacygevoelige data te melden bij het College Bescherming Persoonsgegevens (CBP) en de betrokkenen. Boetes voor overtreding van de wet kunnen oplopen tot € 810.000 of 10% van de jaaromzet. In dat licht is het begrijpelijk dat IT-afdelingen heel voorzichtig zijn met het toegankelijk maken van bedrijfsinformatie op apparaten die geen eigendom zijn van het bedrijf. Maar de verwachting van werknemers om met eigen devices toegang te krijgen tot email, agenda's en bedrijfsnetwerken neemt snel toe. Zij verlangen naar mobiele toepassingen die hen in staat stellen om op een eenvoudige manier gebruik te maken van de informatiebronnen binnen ondernemingen.

> Bedrijven zoeken naar grip op beveiliging van mobiele apparaten, applicaties en content

Om dit te kunnen faciliteren gaan steeds meer bedrijven over tot het invoeren van een vorm van Enterprise Mobility Management (EMM). Op dit moment gebruikt circa 20% van de Nederlandse organisaties een software hiervoor, zoals Airwatch of MobileIron. Onderzoeksbureau IDC meldde dat nog eens 50% van de Nederlandse organisaties een EMM oplossing overweegt. Deze zijn grofweg in drie niveaus te verdelen: Mobile Device Management, Mobile Application Management en Mobile Content Management.

> Uit het onderzoek van Arxan Technologies blijkt dat 92 van de top 100 betaalde iOS-apps zijn gehackt.

Mobile Device Management (MDM)
MDM is vaak de eerste stap die bedrijven zetten in Enterprise Mobility Management; primair gericht op het beveiligen, beheren en controleren van toegang tot het bedrijfsnetwerk door smartphones en tablets. En alhoewel het een goed beeld geeft welke toestellen toegang krijgen, is niet duidelijk wat de toestellen precies doen. Een voorbeeld zijn de mobiele applicaties die worden geïnstalleerd. Uit **het onderzoek** van Arxan Technologies blijkt dat 92 van de top 100 betaalde iOS-apps zijn gehackt. Op het Android-platform is dit zelfs 100 procent. Ook het merendeel van de populaire gratis apps zijn gehackt. En deze apps hebben de meeste gebruikers op dezelfde smartphone staan waarmee ze ook toegang hebben tot het gevoelige bedrijfsinformatie.

Mobile Application Management (MAM)
Een belangrijke tweede stap in Enterprise Managed Mobility is de beveiliging van het verwerven, distribueren, beveiligen, en het bijhouden van publiek- en privaat gebouwde mobiele applicaties. Hierbij houdt de IT-afdeling centraal overzicht over welke verschillende mobiele applicaties door werknemers worden gebruikt.

MAM richt zich op de hele workflow van het ontwikkelen, testen, distribueren en gebruik van mobiele applicaties. Ook kunnen bedrijven door middel van MAM mobiele applicaties professioneel ondersteunen met versie- en releasemanagement, uitvoeren van compliance audits, rapportages en het nemen van maatregelen wanneer bepaalde applicaties niet voldoen aan de bedrijfsnormen. Dit voorkomt dat er via applicaties malware binnenkomt of hackers toegang krijgen tot bedrijfsinformatie.

Mobile Content Management
Naast devices en applicaties, richten bedrijven zich steeds vaker ook op het delen van content. Soms wordt het ook Mobile File Management genoemd. Met name voor het delen van grote bestanden gebruiken veel werknemers een van de bekende applicaties zoals DropBox, Skydrive, en iCloud. Onbewust dragen ze de het intellectuele eigendom van de documenten over aan de eigenaar van de applicatie. Ze zijn immers bij gebruik akkoord met de voorwaarden. Bedrijven zijn zich hier in toenemende mate van bewust en bouwen met Mobile Content Management beveiligingsmechanismes in om het verlies van gegevens tegen te gaan en de inhoud te beschermen. Voorbeelden zijn het opstand tracken of wissen van de inhoud, gebruikersprofielen aanmaken of bepalen hoe informatie gedeeld mag worden met derden. Dit kan op ieder niveau geregeld worden, zoals printen, email, copy & paste of via apps.

“Naast devices en applicaties, richten bedrijven zich steeds vaker ook op het delen van content.”

Eén aanspreekpunt voor alle telecomdiensten
Mobiele vraagstukken zoals BYOD veranderen in rap tempo compleet de IT-strategie van een bedrijf. Om klanten nog beter te kunnen helpen bij de beveiligingsaspecten hiervan, heeft Vodafone Nederland de **zakelijke ICT-dienstverlener mITE overgenomen**, een van de belangrijkste spelers in Nederland op het gebied van advies, verkoop, implementatie en ondersteuning van Enterprise Mobility Management. Het helpt bij het beantwoorden van vragen die nu vooral spelen in de markt. Waar staan we nu exact qua het ontsluiten van bedrijfsprocessen op mobiele toestellen en wat er moet er nog gebeuren om de mobiele werkplek als een volwaardige werkplek geaccepteerd te krijgen? Begrip krijgen van ‘consumerisation’ en rekening houden met onderwerpen als beveiliging, privacy en compliancy zijn daarbij cruciaal. Zijn organisaties daar klaar voor?

Wilt u meer weten over de zakelijke communicatie oplossingen van Vodafone?
Kijk op onze website of vul het contactformulier in op onze website.