

Pas op met de eigen laptop

Direct en veilig toegang hebben tot het bedrijfsnetwerk met privé-laptops en -tablets is een speerpunt voor veel organisaties. Hoe kan dat veilig?



Het plannen en realiseren van BYOD (Bring Your Own Device) eindigt niet met een papieren beleidsstuk. Ook als IT-afdeling kun je er vaak al niet omheen, gewoonweg omdat collega's hun eigen tablet, smartphone of zelfs laptop meenemen naar de zaak.

Er kleven gevaren aan BYOD; wat dacht je van de volgende nadelen:

- Als je een privétoestel verbindt met een kantoor-netwerk, bijvoorbeeld Exchange (e-mail), dan kan de beheerder van die technische omgeving ook invloed uitoefenen op je apparaat. Van het instellen van een vereist wachtwoord tot zelfs het uitschakelen van wifi en cameramogelijkheden op het apparaat. Het is natuurlijk meer dan vreemd dat je zelf een apparaat aanschaft en dat een beheerder vervolgens bepaalt wat je wel en niet mag doen. Aan de andere kant is het ook wel logisch

- Minder technisch, maar zeker zo belangrijk is dat mobiele apparaten veel druk leggen op werk-privé-balans van jezelf en je collega's.

Als alternatief hoor je vaak dat organisaties kiezen voor een CYOD (Choose Your Own Device)-beleid, waarbij iedereen een door de werkgever geselecteerd zakelijk apparaat ter beschikking krijgt. Zo kan IT betere ondersteuning bieden en makkelijker invloed uitoefenen op wat wel en niet mag/kan.

Voorkom wel dubbele apparaten. Je kent het wel, mensen die een telefoon van de zaak hebben liggen naast de privételefoon en een eigen tablet mee naar de zaak nemen, maar ook een tablet van de zaak hebben. Maak dus afspraken over privé-gebruik van die apparaten.

Los van alle voor- en nadelen van het meenemen van een tablet is het belangrijk de onderstaande

Het is lastig ervoor te zorgen dat *bring your own device* veilig kan

dat je je aan regels moet houden wanneer je wilt werken met een apparaat dat niet wordt beheerd door diezelfde organisatie.

- Voor IT is het vrijwel onmogelijk om afdoende ondersteuning te bieden aan alle mogelijke soorten apparaten en besturingssystemen, laat staan aan alle apps. Er zijn veel afspraken die je zult moeten maken. Van 'wie configureert het apparaat zodat het zakelijk gebruikt kan worden' tot 'welke systemen geven we toegang; hoe gaan we de beveiliging, mobile device management en appbeheer regelen'.

- Het opzetten van een goed beveiligingsprogramma in een BYOD-omgeving is lastig en kostbaar. Wanneer een organisatie onvoldoende aandacht heeft voor de beveiligingsaspecten en gewoon apparaten configureert, dan is het risico op toekomstige kosten om de problemen op te lossen vele malen groter.

tips in acht te nemen bij het gebruik van je privé-apparaat.

Tip 1: Stel een wachtwoord in

Ook al vind je het oprecht onhandig, stel toch altijd een code in voor je mobiele apparaat, bij voorkeur zelfs een echt wachtwoord in plaats van een viercijferige code.

Tip 2: Doen: e-mailhandtekening

Als je een e-mail stuurt via een tablet of mobiele telefoon, dan staat er automatisch onder de e-mail 'Verzonden vanaf mijn iPad/iPhone'. Dat is handig: je antwoordt via een telefoon veelal iets korter en bondiger. Het is goed dat de ontvanger dat kan duiden, maar het kan veel professioneler. Je kunt je e-mailhandtekening (net als in Outlook) naar eigen wens aanpassen, helaas vooralsnog nog zonder logo's en afbeeldingen.

Over vrijheid, betrokkenheid en verantwoordelijkheid



Inschrijven
met meer
mensen
=
KORTING!

2013 CONGRES Over Het Nieuwe Werken

19 november 2013 / NBC Nieuwegein

Meer informatie en inschrijven: www.ohrw.nl/congres



Opleiding

Leer effectiever werken en papierloos vergaderen met de iPad op 10 oktober in Utrecht.

<http://www.vakmedianetshop.nl/opleidingen/gids/details.asp?pr=17580>



Tip 3: To Cloud or not to Cloud

Informeer bij je werkgever of IT-afdeling welke spelregels er zijn voor het gebruik van mobiele apparatuur. Vraag bijvoorbeeld welke clouddiensten je mag gebruiken, en welke niet. Bij vertrouwelijke en privacygevoelige stukken is het aan te raden om diensten zoals Dropbox niet te gebruiken. Veel ondernemingen kiezen ervoor cloud-diensten als Dropbox te verbieden. Het vraagt vaak veel kennis van eindgebruikers om te begrijpen waar iets wordt opgeslagen en wat wel en wat niet op Dropbox kan. Dat wil niet zeggen dat het niet wordt gebruikt. Collega's experimenteren met tools die wellicht minder veilig zijn. Dropbox-gebruikers moeten wel onthouden: "als iets gratis is, ben je vaak niet de klant, maar het product".

Tip 4: Archiveren op je tablet?

Een tablet kun je het beste zien als een vervanger van een stapel papier onder je arm. Zorg er dus voor dat je een tablet niet gebruikt als een archief-systeem. Je hebt enkele (kopie) documenten nodig om bijvoorbeeld in de trein te lezen. Je tablet is hoogstens een schaduwarchief, en de eigenschap van een schaduwarchief is dat je de inhoud ervan zonder enige twijfel weg kunt gooien. Zorg er dus voor dat je de stukken die wel in je archief / informatiehuishouding van je organisatie thuishoren, overbrengt. Zo kun je bij verlies (zie tip 3) ook zonder enige twijfel je apparaat op afstand wissen. Je bent toch niets kwijt wat je niet kunt reproduceren.

Tip 5: Laat je niet gek maken

We lijken tegenwoordig allemaal wel e-mailverslaafd, zeker met een telefoon en tablet waarmee je e-mail kunt lezen. Vraag je eens af hoe vaak je per dag kijkt of er nog iets nieuws is binnengekomen. En hoe snel heb jij 's ochtends voor je ontbijt al je mail een keer gecheckt? Zeg eens eerlijk! Als je het bij gaat houden schrik je van het aantal keer dat je moet turven. Belangrijk is een goede

balans te vinden tussen werk en privé.

Om deze tip kracht bij te zetten wil ik graag dat je het e-mailicoon zo instelt, dat het niet het aantal ongelezen berichten weergeeft. Als je de iPad op de bank tijdens privétijd gebruikt, ben je eerder geneigd nog even naar je e-mail te kijken als daar een getal staat met het aantal ongelezen berichten. Je kunt deze melding (het zogenoemde 'badge app symbool') uitzetten.

Tip 6: Train tablet gebruikers

Gebruikers hebben vaak veel vragen en als organisatie wil je hen duidelijk maken wat de spelregels zijn. Zorg er dus voor dat gebruikers weten wat de spelregels zijn, hoe ze het apparaat veilig kunnen gebruiken en natuurlijk wat de beste tips en trucs zijn voor het werken met een tablet.

Tip 7: Fiscaal

Fiscaal is er veel te doen over het onderwerp tablet. De fiscus heeft al diverse bedrijven op de vingers getikt dat iPads zijn aangeschaft, zonder dat voldoende aannemelijk was dat de apparaten ook privé (of beter gezegd te veel privé) gebruikt worden. In de huidige regelgeving (juni 2013) wordt een tablet groter dan 17,8 centimeter gezien als een computer. Dat wil zeggen dat een tablet aantoonbaar meer dan 90% zakelijk gebruikt moet worden, om belastingvrij te kunnen verstrekken.

Laat de werknemer een kleine eigen bijdrage betalen

Gelukkig is staatssecretaris Weekers van het ministerie van Financiën sinds maart bezig met het moderniseren van deze wetgeving. De essentie van het voorstel van Weekers is dat wanneer een tablet noodzakelijk is bij het werk, deze kan worden verstrekt (noodzakelijkheids criterium). Als je als organisatie kunt aantonen dat je 'papierloos gaat werken' of bijvoorbeeld zoals ik training geeft in gebruik van de tablet, pakt deze regeling gunstig uit.

Verder kunnen de onderstaande tips helpen:

- Sluit een overeenkomst tussen werkgever en gebruikers voor het gebruik en onderhoud.
- Laat de werknemer een kleine netto eigen bijdrage betalen, hierdoor ligt de bewijslast voor een hoger privégebruik bij de Belastingdienst. ●

Bouke van Kleef, directeur AVK, is trainer, workshopleider en innovatiecoach.