

BYOD: vloek of zegen?

Meer vrijheid impliceert meer verantwoordelijkheid, en dat geldt zeker bij BYOD.



Wat is BYOD?

BYOD is een term die je steeds vaker tegenkomt, maar wat betekent dit eigenlijk? Bring Your Own Drinks? In Australië schijnt het gemeengoed te zijn om je eigen fles wijn mee te nemen naar een restaurant. Om deze ook daadwerkelijk te mogen opdrieken, betaal je meestal een corkage fee, of in goed Nederlands 'kurkengeld', ter compensatie van gemiste inkomsten voor de horecaondernemer. Maar nee, als we het hier over BYOD hebben, dan hebben we het over een trend die veel IT-managers uit de slaap houdt: Bring Your Own Device...

BYOD is langzaam het bedrijfsleven ingekropen met de opkomst van de mobiele telefoon, een trendgevoelig gadget bij uitstek. Een probleem? Nou nee, totdat de smartphone opkwam en medewerkers met de sim van de baas grote hoeveelheden

mobiele data gingen gebruiken, hun email gingen synchroniseren en zich toegang probeerden te verschaffen tot bedrijfsgevoelige informatie. En vandaag de dag is deze trend de smartphone allang voorbij – zo'n tablet als de iPad is immers ook reuze handig voor het werk, en waarom zou ik eigenlijk die saaie laptop die de IT-afdeling verstrekt, nog gebruiken? Kortom: BYOD is 'here to stay'.

Wat doen we tegen BYOD – of wat moeten we ermee?

Maar wat moet de IT-manager doen, die geconfronteerd wordt met deze zelf meegebrachte hightech gadgets die onmisbaar zijn voor het dagelijks werk? Hard wegrekken? Verstoppen? Alle bedrijfssystemen hermetisch afsluiten voor toegang van buitenaf? Gezien de handigheid van de medewerkers en het feit dat de top van het bedrijf inmiddels al meedoet met deze trend, is dit waarschijnlijk geen houdbare strategie.

Dus, geachte IT-manager, haal diep adem en omhels BYOD. Het is immers beter dan het halve bedrijf te laten verworden tot hackers die met hun nieuwste gadgets toegang proberen te krijgen tot het bedrijfsnetwerk. Maar pas op, ook deze route is niet zonder gevaren: de bedrijfsinformatie

moet nog steeds beschermd worden, de gebruikers verwachten nog steeds support van de IT-afdeling, maar o wee als je aan hun persoonlijke informatie komt, die vanzelfsprekend ook op deze eigen devices staat. Dus: een ander security-paradigma dan de grote muur om het bedrijfsnetwerk, een heldere policy, een nieuw supportmodel, maar ook zeker meer eigen verantwoordelijkheid voor de gebruiker met zijn of haar nieuw verworven vrijheden.

Een nieuw security-paradigma

Door de vloedgolf van zelf meegebrachte devices die niet langer direct door de IT-afdeling beheerd en gecontroleerd worden, ontstaan nieuwe risico's. Naast het verlies van controle over het device kan dit ook makkelijk verloren of gestolen worden. Maar in feite bestaat het security-paradigma van de hoge muur om het bedrijfsnetwerk allang niet meer. Organisaties hebben immers al lang geleden de voordelen van mobiele toepassingen ingezien en hebben daarmee al mechanismen tot veilige toegang van buitenaf geïntroduceerd. Bij BYOD komt daar dan een strengere classificatie bij van welke informatie op welke manier toegankelijk is. En eisen die

in de BYOD-policy gesteld worden aan protocollen die gebruikt worden, welke mogelijkheden er zijn om toegang van buitenaf te blokkeren of het device geheel of gedeeltelijk te wissen, en – last but not least – de verantwoordelijkheden van de gebruiker. In feite security-maatregelen die voor een groot gedeelte parallel lopen met de security-polities voor gebruik van de cloud.

Een heldere BYOD-policy

Naast bedreigingen brengt BYOD ook potentiële (financiële) voordelen voor de organisatie met zich mee. Immers, het volledig van bedrijfswege verschaft device wordt vervangen door een door de medewerker zelf aangeschaft device, al dan niet met een gedeeltelijke vergoeding door de werkgever. Deze vergoeding is dan vaak een belangrijke pijler van de BYOD-policy, evenals een 'fair-use'-policy voor het gebruik van mobiele data. Daarnaast beschrijft de policy de rechten van de medewerker (welke data en welke applicaties zijn toegankelijk), maar ook de plichten (welke maatregelen dient de gebruiker te treffen). Tot slot beschrijft de policy de implicaties van het gedeeld gebruik – bedrijfsmatig en privé – van het device. Het device bevat immers ook persoonlijke data, maar de organisatie verwacht wel dat in geval van verlies het device op afstand gewist kan worden om de bedrijfsinformatie te beschermen.

Een BYOD-supportmodel

Bij BYOD verschuift de support die gebruikers kunnen verwachten, van support van het gebruikte device meer naar de gebruikte applicatie. Industrieanalist Gartner heeft het in dit verband over 'Managed Diversity'. BYOD introduceert immers een grote diversiteit van devices aangezien de gebruiker zelf de keuze maakt. Deze keuze, maar ook de afhankelijkheid met het bedrijfsproces van de gebruikte applicatie, bepaalt de mate waarin de IT-afdeling support kan

leveren voor gebruik van de applicatie op verschillende devices.

Segmentering in gebruikersgroepen is een belangrijke stap in de bepaling van het supportmodel. Immers, gebruikers in een primair proces, zoals verpleegkundigen, pakjesbezorgers of engineers, zullen gezien de afhankelijkheid van dit proces van een mobiele applicatie, meestal niet in aanmerking kunnen komen voor BYOD. Andere gebruikersgroepen, zoals kenniswerkers, sales en management, kunnen een grotere vrijheid bij de keuze van het device krijgen.

In het BYOD-supportmodel betekent dit, dat er minimaal drie niveaus van support beschikbaar dienen te zijn.

- **Platformsupport:** support voor een specifiek platform dat geoptimaliseerd is voor de specifieke gebruikersgroep en businessapplicatie. Gezien de afhankelijkheid met het primaire proces is een 100%-supportmodel vanuit de IT-afdeling hier een vereiste.
- **Applicatiesupport:** support voor een bepaalde applicatie die een aantal eisen stelt aan het gebruikte device. Dit betekent in de praktijk dat een grotere variëteit van devices is toegestaan, maar de beperking bijvoorbeeld zit in het gebruikte operating system. De support ligt binnen dit niveau vaak op een fifty-fifty-basis bij de IT-afdeling en de gebruiker.
- **Ad-hocsupport:** volledige vrijheid van het device, dus volledige ondersteuning van BYOD impliceert dat de IT-afdeling geen ownership kan nemen voor de support op dit device. De gebruiker is voor support dan ook in principe aan zichzelf of 'gelijkgestemden' overgeleverd. Wel kan de IT-afdeling ad-hocsupport leveren voor bijvoorbeeld instellingen voor e-mailsynchronisatie of toegang tot Unified Communications clients.

Een aanbeveling hierbij is om alle support voor mobiele devices in één supportgroep

te organiseren, aangezien hiermee de gefragmenteerde kennis die nodig is om deze diversiteit te beheren en te ondersteunen, op de meest effectieve manier geboden kan worden.

BYOD – de verantwoordelijkheid van de gebruiker

Meer vrijheid impliceert meer verantwoordelijkheid, en dat geldt zeker bij BYOD. Gebruikers zullen zich moeten conformeren aan de BYOD-policy en zich moeten neerleggen bij eventuele gevolgen en beperkingen die deze met zich meebrengt. Voor support zijn gebruikers grotendeels aan zichzelf overgeleverd, maar hier geldt des te meer dat het de facto in organisaties aanwezige principe van peer support – als je een IT-probleem hebt, ga je eerst te rade bij je collega's voordat je de IT-afdeling benadert – geformaliseerd dient te worden: door informele tools, dat wel. Dus hier is gebruik van social media, zoals gebruikersfora en blogs, een geëigende methode om de eigen supportverantwoordelijkheid van de BYOD-gebruikers te faciliteren.

BYOD is dus een ontwikkeling die onontkoombaar is en hierdoor beter omarmd kan worden dan genegeerd. Voor een adequate implementatie van BYOD zijn immers een hoop werk en afstemming noodzakelijk. Maar uiteindelijk is BYOD een win-winsituatie voor werknemer en werkgever – de werknemer drinkt de wijn die hij of zij prefereert, en de werkgever incasseert het kurkengeld in de vorm van lagere kosten voor het device en verhoogde medewerkerstevredenheid.

Voor meer informatie:
Wouter.Bakker@dimensiondata.com

Bezoek ook onze stand op Infosecurity (2-3 november 2011, Jaarbeurs Utrecht), waar het onderwerp Mobile Security aan bod komt!