BYOD: Overkomt het je of heb je een beleid?

Smartphones en tablets vervangen meer en meer vaste telefoons, laptops en de PC. Soms zijn dit privétoestellen van werknemers en dan spreken we over Bring Your Own Device (BYOD). Voor een succesvolle en veilige invoering van BYOD is het raadzaam een beleid op te stellen, zodat iedereen goed op de hoogte is van rechten en plichten. Op die manier is bedrijfsinformatie veilig en is de privacy van gebruikers gegarandeerd. In dit artikel leggen wij graag uit waar je aan moet denken bij het opstellen van een beleid, hoe het 7C-stappenplan kan helpen en hoe je controle houdt over de devices.

“Voor een veilige invoering van BYOD is het raadzaam een beleid op te stellen.”

1. Bring your Own ... drama?

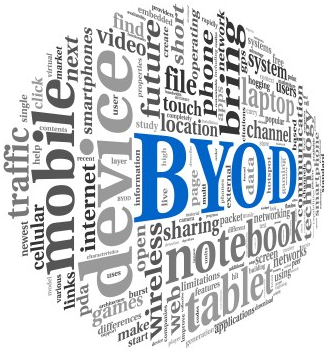
Uit vele onderzoeken blijkt dat Bring Your Own Device bijdraagt aan productiviteit en werkplezier. Bring Your Own is bovendien het toekomstmodel waarmee een nieuwe generatie opgroeit. Generatie Y verwacht dat ze de vaardigheden én spullen die ze in hun vrije tijd gebruiken ook in hun carrière kunnen inzetten.

Bij veel organisaties zie je overigens het fenomeen Choose Your Own, waarbij werknemers kunnen kiezen uit een beperkt aantal toestellen, die worden aangeboden vanuit de werkgever. Hier wordt ook handig ingespeeld op de verschillen tussen werknemers en ook wel generaties: een telefoon die kan ‘bellen en sms’en’ of het nieuwste type smartphone met data-abonnement.

Beveiliging op orde

Alle voordelen ten spijt, beveiliging is natuurlijk het grootste issue. We kennen allemaal de verhalen: medewerkers die gênant beeldmateriaal op hun zakelijke iPad bekijken, computers met geheime documenten bij het grofvuil, onbeveiligde laptops met bedrijfsinformatie die in de trein blijven liggen, of werknemers die alles in een cloud gooien waar de Amerikaanse overheid zomaar in mag kijken. Zoiets zouden jouw collega’s nooit doen, toch? Die kans is toch aanwezig, want in 60% van de organisaties waar met privétoestellen gewerkt wordt, is er nog geen beleid opgesteld.

Foute boel, want Bring Your Own kan simpelweg niet zonder eenduidig en goed gecommuniceerd beleid. Dit maakt privacy, beveiliging en financiën duidelijk en legt rechten en plichten vast. Zaak is ook om goed uit te leggen *waarom* deze regels er zijn, en dit ook te verbinden aan het belang van de werknemers. Bijvoorbeeld: "Wij willen het bedrijfsnetwerk graag vrij van virussen houden, zodat jij altijd overal bij kan en geen tijd verliest."



"Bring your Own is het toekomstmodel waarmee een nieuwe generatie opgroeit."

2. One device, three perspectives

Voordat we ingaan op het opstellen van het beleid en software om BYOD mee te handhaven, belichten we het fenomeen eerst vanuit de verschillende oogpunten: die van de gebruiker, de leidinggevende en de IT-er.

Gebruikers

Veel mensen vinden beveiliging van bedrijfsdata geen interessant onderwerp en vinden al die veiligheidsregels te complex, onduidelijk of belemmerend. Of ze hebben er intern niets over gehoord "dus het zal wel goed zijn".

Samsung of Apple? Werknemers willen het toestel van hun keuze gebruiken want die kennen ze en vinden ze prettig werken. Het is een verlengstuk van hun persoonlijkheid en voor sommigen een statussymbool. De voorkeur is vaak behoorlijk uitgesproken. Ook willen ze door hun werkgever tegemoet gekomen worden in de kosten die ze maken. Ze willen vrijheid, ook in de keuze van de apps waarmee ze werken en garantie op hun privacy voor het privégebruik. Ze willen duidelijkheid over wat wel en niet mag en waar ze met problemen naar toe kunnen. Maar bovenal willen ze gemakkelijke toegang tot alle documenten, natuurlijk wel de laatste versie, en vinden ze het handig om vanaf de smartphone een printopdracht te kunnen geven.

Werkgevers en leidinggevenden

De meesten vinden BYOD een prima ontwikkeling die ook goed bij het gedachtengoed van Het Nieuwe Werken past: werken kan anywhere, anytime and on any device. Ze willen graag wel dat door het gebruik van mobiele devices en de juiste applicaties, de werkprestaties ook daadwerkelijk verbeteren. Daarom is het goed om ook op strategisch niveau hierover na te denken: wat wil je bereiken met een hogere mobiliteit?

“BYOD past goed bij HNW: werken kan anywhere, anytime and on any device.”

Kostenpost of besparing?

Ook hebben werkgevers te maken met het kostenplaatje. Levert BYOD nou geld op omdat je geen toestellen meer hoeft te verstrekken, of kost het juist geld door het extra beheerwerk? Het antwoord is simpel: BYOD levert waarschijnlijk geen direct geld op maar betaalt zich wél terug in meer tevreden en productieve werknemers en dat is onbetaalbaar. Zorg er wel voor dat werknemers BYOD niet gaan ervaren als een verkapte bezuiniging. Dit kan bijvoorbeeld door zakelijke kosten ruim te vergoeden of door een periodieke vaste vergoeding te geven.

Duurzaam is beter

Daarnaast kan BYOD bijdragen aan de duurzaamheidsdoelstellingen, aangezien mobieltjes worden gemaakt van allerlei schaarse grondstoffen en de batterijen vervuilende stoffen bevatten. Ook met het oog op stroomverbruik is één mobieltje beter dan twee.

Privacy en regels

Leidinggevenden hebben de verantwoordelijkheid om gebruikers op de hoogte te brengen van gevaren die op de loer liggen. Privacygevoelige informatie bijvoorbeeld, die op straat komt te liggen bij diefstal of verlies, of virussen die op een toestel staan en die het bedrijfsnetwerk vervuilen. En wat bij een zakelijk conflict of gedwongen ontslag? Wat gebeurt er dan met het abonnement en het device? Je wilt dan natuurlijk alle zakelijke data kunnen verwijderen van het device en een eventueel afgegeven SIM-kaart weer terugkrijgen. In geval van ontslag en een persoonlijke SIM is het dan ook aan te raden om alle zakelijke data en apps te laten verwijderen.

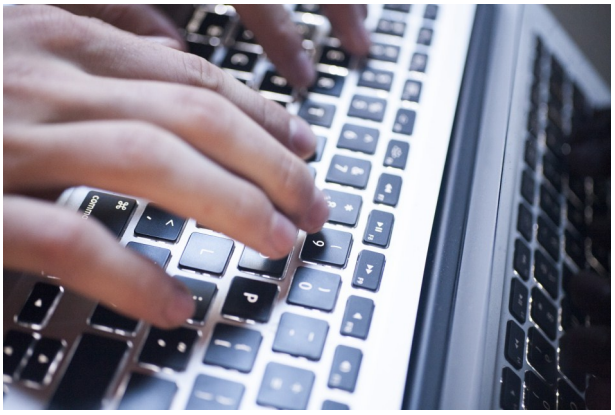
Afdeling IT

De afdeling IT heeft veel energie en tijd gestoken in het inrichten van een schoon en stabiel netwerk en zit eigenlijk niet te wachten op vervuilde apparaten die allemaal ondersteund moeten worden en veel extra beheerwerk opleveren. Ze staan ook voor grote uitdagingen: er zijn momenteel meer dan 110 verschillende toestellen die op Android draaien. Men moet misschien nog bijkomen van de omslag tussen het tijdperk waarin IT bepaalde waarmee gewerkt werd, naar de situatie nu, waarin gebruikers zelf bepalen waarmee ze werken. Maar BYOD kan ook werk uit handen nemen. In veel organisaties zie je namelijk dat mensen die een vraag hebben over hun toestel deze stellen aan een collega met hetzelfde toestel en niet meer aan de IT-helpdesk. Het is in ieder geval van belang om IT te faciliteren met goede Mobile Management Software.

“Het formuleren van BYOD-beleid is een organisatiebreed vraagstuk.”

Business IT alignment

In het grotere plaatje is het sowieso interessant om de rol van IT in de organisatie onder de loep te nemen. Je wilt toewerken naar een situatie waarin IT niet meer vraaggestuurd werkt en denkt, maar zodanig vervlochten is met de processen, dat zij zelf met voorstellen komen. Van een passief faciliterende houding (“hier heb je waar je om vroeg”) naar actief meedenkende IT’ers. Een eerste stap kan zijn om zaken die vroeger primair bij IT lagen, nu organisatiebreed op te pakken, zodat er wederzijds begrip en inzicht ontstaat. Bijvoorbeeld het opstellen van BYOD-beleid: dit is bij uitstek niet een zaak van de IT-afdeling alleen. Management, HR, facilitaire zaken, interne communicatie en de werkvloer zelf: stel samen een BYOD-beleid op dat past in de mobiele strategie, de interne processen en werkwijze en waar de gebruikers zich goed bij voelen.



3. One Device? One Policy!

Waarom een beleid? Naast eerdergenoemde redenen als veiligheid en privacy nodigt het gezamenlijk opstellen van een BYOD-beleid uit na te denken over vragen als:

- Op welke manieren draagt mobiliteit bij aan productiviteit?
- Welke applicaties en informatie dient altijd beschikbaar te zijn?
- Wat zijn de mogelijke nadelen van BYOD?
- Worden alle type toestellen ondersteund?
- Is alle benodigde kennis van Mobile Management al in huis of is er opleiding nodig?

“De belangrijkste C is die van Communicate.”

Eindgebruiker aan het woord

Bij het maken van een BYOD-beleid is het van belang om te luisteren naar wat de (eind)gebruiker graag wil of wat voor ideeën hij heeft met betrekking tot het beleid. Dit is namelijk degene die elke dag te maken gaat krijgen met de gemaakte afspraken. Een manier om dit te bereiken is om verschillende afdelingen en groepen gebruikers te betrekken in het maken van het beleid of om gebruikers te vragen wat zij belangrijke aandachtspunten vinden met betrekking tot BYOD. Maar hoe ga je nou zo’n beleid opstellen? Het 7C stappenplan kan u een eind op weg helpen.

7C stappenplan

Door het 7C stappenplan te gebruiken doorloop je alle benodigde stappen om te komen tot een eenduidig en breed gedragen beleid. De belangrijkste C is die van Communicate. Blijf gedurende het hele proces communiceren over de ontwikkelingen. Mensen weten nu eenmaal graag waar ze aan toe zijn en zo kan er ook gereageerd worden en eventueel worden bijgesteld. Hieronder vind je een korte samenvatting van de stappen die we doorlopen bij het opstellen van een BYOD-beleid.

1. **Check:** check in welke mate werknemers al hun eigen toestellen gebruiken en zo niet, of ze dit zouden willen.
2. **Combine:** stel een team samen met vertegenwoordigers van alle afdelingen en betrek zo de gehele organisatie erbij.
3. **Concept:** begin met een conceptversie.

4. **Communicate:** communiceer deze conceptversie, peil de reacties en verwerk deze feedback.
5. **Create:** werk het concept uit en regel wat nodig is, zoals Mobile Management Software.
6. **Confirm:** ga het beleid consequent uitvoeren.
7. **Compliance:** evalueer het beleid en stel eventueel bij.

Bij het opstellen van het beleid moet over meerdere zaken goed worden nagedacht, zoals privacy en imago van het bedrijf, financiën, beheer en natuurlijk beveiliging. Deze vraagstukken bespreken we nu stap voor stap.

"Met Mobile Management Software zie je hoe het device zakelijk en privé gebruikt wordt."

Privacy en imago

Mag de werkgever in de documenten van de werknemer kijken? Omdat het device zowel zakelijk als privé wordt gebruikt, zullen er afspraken gemaakt moeten worden om de privacy van de gebruiker te waarborgen. Mobile Management Software biedt de mogelijkheid om te kijken hoe het device zakelijk en privé gebruikt wordt door middel van Applicatie Analytics. Gebruikers vinden het soms overdreven of voelen zich oncomfortabel dat hun organisatie zoveel inzicht heeft in hun privégegevens en smartphonegebruik. Goede afspraken geven duidelijkheid en voorkomen problemen.

Maar ook de gebruiker heeft een verantwoordelijkheid: zo mogen er geen foto's, filmpjes en andere bestanden op het device staan die schadelijk kunnen zijn voor het imago van het bedrijf of in strijd zijn met de wet. Geef daarom duidelijk aan wat onwenselijke content is.

Financiën

Een vaste vergoeding per maand voor zakelijke belletjes of betaal je het hele abonnement? Wat doe je met buitenlandverkeer? Een beperkte of onbeperkte databundel? Gaat zakelijk bellen intern over het WIFI-netwerk? Ook hier moet in overleg een aantal beslissingen genomen worden. Je kan ook denken aan twee SIM-kaarten in één toestel: DualSIM. Bij de meeste smartphones is dit met een kleine extensie mogelijk. Ook handig bij ontslag, want dan levert de werknemer de zakelijke SIM-kaart gewoon in. Stel een budget op met daarin hoeveel u uit wilt geven aan BYOD. Aan de hand hiervan wordt het ook makkelijker om keuzes te maken over abonnementskosten, Mobile Management toepassingen en Cloud services.

Beheer

Zakelijke applicaties nemen meer en meer de functie van de PC over en bevorderen productiviteit. Maar wat voor applicaties zijn dit en wie krijgt welke op zijn device? Het is natuurlijk ook belangrijk om gebruikers aan te laten geven welke applicaties ze graag zouden gebruiken, of welke juist helemaal niet.

Ga je applicaties aanbieden of zelfs pushen naar de toestellen? Met Mobile Management Software is het mogelijk om gebruikers bepaalde applicaties aan te bieden zonder dat zij zelf langs de 'appshop' hoeven. Het biedt ook de mogelijkheid om applicaties aan te raden zodat de gebruiker weet welke applicaties worden ondersteund of zijn goedgekeurd door de beheerder. Voordeel hiervan is uniformiteit in werkwijze in de organisatie. Met de software kan je ook applicaties blokkeren of toegang beperken. Vergeet niet dit duidelijk te communiceren. Het is handig om een blacklist te maken met daarin applicaties die op de werkvloer worden geweigerd. In het beleid wordt verder ook opgenomen of alle besturingsprogramma's worden toegelaten op het bedrijfsnetwerk en hoe je onderhoud pleegt.

"Privacy, financiën, beveiliging en beheer zijn zaken voor in het beleid."

Beveiliging

Smartphones die op Android en Windows draaien hebben het probleem dat ze soms 'foute' applicaties kunnen downloaden. Deze kunnen vervolgens alle informatie die op de smartphone staat lezen of zelfs verwijderen wat natuurlijk zeer onwenselijk is als er gevoelige of belangrijke informatie op de smartphone staat. Het is mogelijk om op afstand toegang te krijgen tot de devices zodat je deze kunt beheren. Bij verlies of diefstal kan je daarmee een *full* of *partial wipe* uitvoeren. Bij een *partial wipe* verwijder je alleen de zakelijke gegevens, bij een *full wipe* alle gegevens.

Deze zaken rondom privacy, financiën, beveiliging en beheer komen allemaal in het beleid te staan. Als dit ook nog eens duidelijk gecommuniceerd wordt naar de gebruikers, is de organisatie goed op weg naar meer mobiliteit en werkplezier!

Conclusie

Bring of Choose Your Own Device is op de meeste werkplekken al realiteit en vraagt om een reactie. Het opstellen van een strategie en een beleid zorgt ervoor dat iedereen weet waar hij aan toe is en BYOD daadwerkelijk de productiviteit en werkplezier verhoogt, zonder dat er beveiligingsrisico's genomen worden. Bij het opstellen van het beleid is de gehele organisatie betrokken, zodat het realistisch en breed gedragen is. Het 7C stappenplan is hierbij een goede leidraad.

"Het opstellen van een BYOD-beleid zorgt ervoor dat iedereen weet waar hij of zij aan toe is."

Waarom WCS TeleAdvies

WCS TeleAdvies geeft samenwerking vorm. Dit doen wij door samen met onze klant een communicatie-omgeving in te richten die perfect is afgestemd op de strategie, kernactiviteiten en werkprocessen binnen de organisatie. Ook bieden wij praktische gereedschappen om de visie over klantcontact en bereikbaarheid te vertalen naar de juiste houding en kennis van medewerkers. Heldere communicatie, duidelijke werkafspraken en goede bereikbaarheid zijn essentieel voor het succes van elke organisatie. Neem gerust contact op voor meer informatie of een vrijblijvende kennismaking. Wij zijn u graag van dienst!

Wilco Smit, Business Consultant
WCS TeleAdvies B.V. | Stemerdingweg 5 | Soesterberg
0346 - 350808 | www.wcsteleadvies.nl | info@wcsteleadvies.nl