Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bring your own device

Choose your own device

Voorwoord

Smartphones en tablets winnen in hoog tempo terrein bij het bedrijfsleven en de overheid. Mensen maken in toenemende mate privé gebruik van mobiele apparaten en willen die ook op de werkplek gebruiken. Het toelaten van het eigen apparaat van de medewerker voor zakelijk gebruik noemen we Bring Your Own Device. De technologie komt uit de consumentenmarkt en heeft niet zonder meer het beveiligingsniveau dat nodig is voor gebruik binnen de rijksoverheid. Hoe kunnen organisaties, en vooral die bij de rijksoverheid, dan toch op verantwoorde wijze smartphones en tablets invoeren?

Het Nationaal Bureau Verbindingsbeveiliging van de AIVD doet onderzoek naar veilige verwerking van overheidsinformatie op smartphones en tablets. De AIVD concludeert dat de huidige generatie apparaten acceptabel beveiligd kan worden, zodat hierop gevoelige informatie kan worden verwerkt. Op dit moment zorgt dat nog voor minder gebruikersvriendelijkheid.

Wij zien echter ontwikkelingen op het gebied van besturingssystemen en beveiligingsproducten voor smartphones en tablets waarmee op termijn een betere beveiliging haalbaar is, zonder in te leveren op gebruiksgemak en functionaliteit.

Overheidsorganisaties die gebruik willen maken van smartphones en tablets moeten een degelijke analyse maken van te beschermen belangen, dreigingen, maatregelen en risico's. Hierbij moet de hele infrastructuur worden meegenomen. Op basis van die risicoanalyse kunnen vervolgens beveiligingsmaatregelen voor tablets en smartphones worden genomen.

Deze beveiligingsmaatregelen verschillen per product. Het is daarom aan te bevelen de gebruiker slechts te laten kiezen uit enkele apparaten: Choose Your Own Device in plaats van Bring Your Own Device. De AIVD is graag bereid hierbij te adviseren.

Rob Bertholee
Hoofd Algemene Inlichtingen- en Veiligheidsdienst

Inhoud

Samenvatting

Technologische innovatie en goedkope mobiele datacommunicatie ontketenen een nieuwe revolutie, namelijk die van de mobiele apparatuur. De grenzen tussen privé en werk vervagen en werknemers willen de technologieën die hun privéleven al verrijken ook in de werksfeer gebruiken. Er ontstaat zo voor organisaties binnen de rijksoverheid een zekere druk om eigen apparatuur van medewerkers, zoals *smartphones* en *tablets*, toe te staan voor zakelijk gebruik. Dit duiden we aan als *Bring Your Own Device* (BYOD).

BYOD biedt voordelen, zoals flexibiliteit in de werkuitvoering. Maar BYOD brengt ook beveiligingsrisico's met zich mee, die de beschikbaarheid, integriteit en exclusiviteit van bedrijfsgegevens kunnen bedreigen. Dit rapport biedt een overzicht van deze informatiebeveiligingsrisico's en mogelijke maatregelen daartegen. Het gaat hierbij om algemene kantoortoepassingen, zoals e-mail, agenda en intranettoegang. De documenten of andere gegevens die ingezien, bewerkt of gedownload worden, zijn ten hoogste gerubriceerd als Departementaal Vertrouwelijk.

De risico's in BYOD hebben voor een groot deel te maken met de verwerking en opslag van bedrijfsgegevens op het device, buiten de bescherming van de organisatie. Door verlies of diefstal van het device kunnen gegevens verloren gaan of in handen vallen van onbevoegden. Door back-ups van het device kunnen vertrouwelijke gegevens bovendien elders terecht komen, bijvoorbeeld op de thuiscomputer of bij de leverancier van het device.

Ook kunnen het device en de bijbehorende applicaties beveiligingslekken bevatten. Andere risico's schuilen in de gegevensuitwisseling en communicatie tussen het device en de computers van de organisatie. Te denken valt aan afluisterpraktijken of aan aanvallen op de backofficesystemen.

De rijksoverheid kan de risico's rond BYOD verminderen door maatregelen te treffen in de techniek, in beleid en processen rond de aanschaf en in het gebruik van mobiele apparatuur. Overheidsorganisaties die gebruik willen maken van smartphones en tablets, moeten dus eerst een degelijke analyse van te beschermen belangen, dreigingen, maatregelen en risico's maken. De maatregelen die ze vervolgens treffen, zijn sterk afhankelijk van de BYOD-uitvoering die toegestaan wordt. Als er weinig mogelijkheden zijn om de devices te beschermen, is het verstandig alleen BYOD-varianten toe te staan waarin zo min mogelijk gegevens op het device terecht komen. U kunt bijvoorbeeld een *mobile-display*-oplossing of een beveiligde *app* ontwikkelen in plaats van de standaard e-mail- en agenda-applicaties van een device. Hoe vrijer de gebruiker is om zelf een uitvoering te kiezen, des te groter kunnen de risico's voor de organisatie zijn. Daarom raadt de AIVD aan om *Choose Your Own Device* te hanteren, waarbij de gebruiker slechts uit enkele apparaten kan kiezen.

In de praktijk zijn drie BYOD-uitvoeringen te onderscheiden: het 'open device', het device als 'mobile display' en het device met een 'beveiligde app'.

Het ‘open device’ is het mobiele apparaat zoals dat in de winkel ligt. Daarop zijn applicaties meegeleverd, zoals e-mail- en agenda-apps. Soms kunnen deze zonder al te veel risico’s gebruikt worden, bijvoorbeeld als het alleen relatief weinig gevoelige en ongerubriceerde informatie betreft. Het grootste risico vormt in dit geval het verlies van het device, inclusief de daarop aanwezige gegevens. Om de risico’s te verminderen kan bijvoorbeeld wachtwoordauthenticatie op het device worden ingesteld. Ook kan de gegevensopslag worden versleuteld en kan ingesteld worden dat deze wordt gewist na meerdere mislukte inlogpogingen. Dit kan ook op afstand gebeuren. Er zijn commerciële Mobile Device Management-beheeroplossingen (MDM) verkrijgbaar waarmee dit geregeld kan worden, mits de gebruiker dit voor zijn device toestaat. Ook is het zaak om goede afspraken te maken over het gebruik en de buitenbedrijfstelling van het device en dit vast te leggen in een gebruikersovereenkomst. Het is belangrijk voldoende aandacht te schenken aan het beveiligingsbewustzijn van de medewerkers. Zonder het gebruik van aanvullende technische maatregelen op het device, de communicatie en de backoffice, is het gebruik van deze variant voor het verwerken van Departementaal Vertrouwelijke informatie echter te risicovol.

Het ‘mobile display’ is een applicatie waarmee de gebruikersinterface van een kantoorapplicatie of een virtuele werkplek op het device wordt weergegeven. De werkplek of kantoorapplicatie draait op een server in de backoffice van de gebruikersorganisatie. Deze variant beperkt de hoeveelheid gegevens die op het device terecht komt.

Om de integriteit van de mobile display-applicatie te beschermen, is het nodig onbevoegde toegang tot het device en de installatie van onbetrouwbare software daarop te voorkomen. Dit kan overeengekomen worden via een gebruikersovereenkomst en afgedwongen worden via een MDM-beheeroplossing. Zonder het gebruik van aanvullende technische maatregelen op het device en beveiliging van de communicatie en de backofficesystemen, is het gebruik van deze variant nog te risicovol voor het verwerken van Departementaal Vertrouwelijke informatie. Bovendien heeft deze oplossing altijd een breedbandverbinding nodig met de backoffice, wat deze oplossing minder gebruikersvriendelijk maakt.

De ‘beveiligde app’ is een applicatie die ervoor zorgt dat gegevens verwerkt en opgeslagen worden binnen een beveiligde omgeving op het device. De applicatie verzorgt zelf de benodigde bescherming, zoals de versleuteling van gegevens en de beveiliging van de datacommunicatie, onafhankelijk van de beveiligingsopties van het device. Hiermee kunnen de potentiële risico’s tot op zekere hoogte worden beperkt. De geschetste risico’s kunnen verder worden verkleind door aanvullende technische maatregelen op het device, zoals bijvoorbeeld het opslaan van sleutelmateriaal en gegevens op een speciaal ontwikkelde SD-kaart en beveiliging van de backofficesystemen. Daarom heeft deze variant de meeste kans om op niveau Departementaal Vertrouwelijk te komen. Deze oplossing is bovendien gebruikersvriendelijker omdat geen permanente verbinding met de backoffice nodig is.

Kort samengevat biedt een 'beveiligde app' op dit moment de beste bescherming van informatie. De voorkeur van de AIVD gaat daarom uit naar een beveiligde app in combinatie met vertrouwde cryptografische hardware en aanvullende technische beveiligingsmaatregelen. Helaas biedt de commerciële markt nog weinig van dergelijke oplossingen en geen van deze oplossingen kan beveiliging van gerubriceerde gegevens combineren met de vrijheid die een gebruiker van zijn privé-tablet of -smartphone gewend is. Er zijn echter wel positieve trends zichtbaar. Daarom verwacht de AIVD dat op termijn de gewenste combinatie van veiligheid en gebruikersvriendelijkheid beschikbaar komt, bijvoorbeeld door de vraag naar betrouwbare mobiele betalingsmogelijkheden. Waarschijnlijk zullen dergelijke oplossingen platformgebonden zijn en dus meer geschikt voor Choose Your Own Device dan voor Bring Your Own Device.

Om te bepalen welke vorm van BYOD kan worden toegestaan, begint u met een passende risicoanalyse voor het gebruiksscenario. Het belang van een risicoanalyse is extra groot omdat de huidige beveiligingsoplossingen nog steeds in ontwikkeling zijn en de leveranciers veel moeite moeten doen om de jonge technologie onder controle te krijgen. Het is daarom nog niet mogelijk om 'blind' op de commerciële beveiligingsoplossingen te vertrouwen, zeker niet voor gerubriceerde informatie. In een risicoanalyse komen onder andere de specifieke aspecten van de organisatie, de gebruikte apparatuur en de gevoeligheid van de gegevens aan bod. Hierin dient interactie met de gebruikers te zijn, om de wensen voor BYOD mee te nemen in de analyse. Hiermee leert een organisatie goed welke vorm van BYOD en welke risico's aanvaardbaar zijn en welke informatiebeveiligingsmaatregelen hij moet treffen.

Naast de technische beveiligingsmaatregelen moet aandacht besteed worden aan goed gebruik van het apparaat door de medewerker. Het is zaak om richtlijnen op te stellen voor toegestaan en acceptabel gebruik. Daarnaast zijn ook heldere procedures voor de ingebruikname of buitengebruikstelling van het apparaat nodig en toezicht op de naleving daarvan. De veiligheidsbewustwording van de werknemer van de risico's en de eigen verantwoordelijkheid is van groot belang.

Het borgen van de maatregelen dient tijdens de gehele levenscyclus van de BYOD goed in balans te zijn. Deze levenscyclus begint bij de keuze van een apparaat en eindigt bij het buiten gebruik stellen van deze apparatuur. Tijdens deze levenscyclus kunnen nieuwe dreigingen en/of kwetsbaarheden ontstaan en moet u toetsen of de getroffen maatregelen nog afdoende zijn of dat additionele maatregelen benodigd zijn. Een goed ingeregelde beheerorganisatie is hierbij noodzakelijk.

BYOD op een verantwoorde wijze invoeren binnen de rijksoverheid vergt een goede voorbereiding en goed beheer over de gehele periode van gebruik en buitendienststelling. Dit is voor een groot deel afhankelijk van de soort informatie waarmee de organisatie werkt. Met dit rapport helpt het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD organisaties op weg.

1 Het fenomeen Bring Your Own Device

Technologische innovatie en de beschikbaarheid van goedkope mobiele datacommunicatie hebben een nieuwe revolutie ontketend, namelijk die van de mobiele apparatuur (*devices*). Consumenten – en dan met name de jongere generaties – maken zich steeds sneller deze nieuwe technologieën eigen, veelal gestimuleerd door innovatieve en sociale applicaties.

1.1 BYOD en het Nieuwe Werken

Veel organisaties nemen maatregelen om de vrijheid van werknemers te verhogen met betrekking tot plaats- en tijdsongebonden werken, ook wel aangeduid als Het Nieuwe Werken (HNW). Nu de grens tussen de privé- en de werkomgeving vervaagt, zijn werknemers steeds vaker geneigd om de technologieën die hun privéleven al vereenvoudigen ook in de werksfeer te gebruiken. Consumenten hebben veelal eerst thuis de beschikking over nieuwe apparatuur en willen deze vervolgens overal kunnen gebruiken: een verschijnsel dat *consumerisation* wordt genoemd. Er ontstaat zo voor organisaties een zekere druk om deze nieuwe apparatuur, zoals smartphones en tablets, te introduceren op de werkvloer.

Het toelaten van eigen apparatuur van de medewerker voor zakelijk gebruik wordt aangeduid als *Bring Your Own Device* (BYOD). In dit concept bepaalt de gebruiker welk apparaat het beste geschikt is voor gebruik in de persoonlijke en de zakelijke omgeving.

De vraag is niet meer of de ontwikkeling van BYOD doorzet, maar hoe een organisatie het beste met deze ontwikkeling omgaat. De ervaring leert immers dat medewerkers de apparatuur gewoon meenemen naar het werk en gebruiken voor het lezen van bijvoorbeeld e-mails, documenten en websites.

1.2 BYOD en de strategische ontwikkelingen binnen de rijksoverheid

Het BYOD-concept is een logische stap binnen de strategische ontwikkelingen van de rijksoverheid, zoals verwoord in de I-Strategie Rijk.

Om de overheid als werkgever aantrekkelijker te maken in een vergrijzende arbeidsmarkt stimuleert de rijksoverheid Het Nieuwe Werken (HNW). Hiertoe werd al de Digitale Werkomgeving Rijksdienst geïntroduceerd. Voor HNW is het behoud van de eigen werkomgeving – onafhankelijk van tijd en plaats – een uitgangspunt. Bijvoorbeeld door de eigen pc-werkomgeving (virtueel) mee te nemen. BYOD kan positief bijdragen aan HNW.

BYOD kan bovendien een rol spelen in de kostenreductie binnen de rijksoverheid. Recent onderzoek van PwC toont aan dat HNW leidt tot een sterke kostenverlaging voor woon-werkverkeer en tot een forse stijging van de productiviteit (1% van het BBP).

Doordat medewerkers zelf een passende vorm van automatisering kunnen kiezen en gemakkelijk toegang hebben tot bedrijfsinformatie, onafhankelijk van tijd en plaats, stijgt de arbeidsproductiviteit. Het toelaten van eigen apparatuur kan daarnaast leiden tot minder beheerlast en minder uitgaven aan de IT-ondersteuning.

Slim gebruik van BYOD en andere nieuwe ICT-middelen, zoals socialemediatoepassingen of teleconferencing, kan bovendien de verkokering binnen de overheid tegengaan. Medewerkers uit publieke organisaties werken steeds vaker samen in grensoverstijgende verbanden. Of het nu projecten zijn, taskforces of ketens, deze samenwerkingsverbanden, co-creaties vereisen dat de IT-middelen daarop zijn ingesteld. Dit maakt het uitwisselbaar maken van applicaties en systemen belangrijk.

1.3 Verantwoorde introductie van BYOD in uw organisatie

Voor overheidsorganisaties is het zaak voorbereid te zijn op de vraag van medewerkers naar BYOD. Het toepassen van BYOD biedt niet alleen mogelijkheden, maar introduceert ook kwetsbaarheden. Gebruik van eigen apparatuur kan de beveiliging van gegevens aanzienlijk bemoeilijken. Het verlangen naar flexibiliteit enerzijds en de noodzaak tot gedegen gegevensbeveiliging anderzijds levert een spanningsveld op. Organisaties zullen daarom tijdig regelingen moeten treffen om de voordelen van BYOD maximaal te benutten en de daaraan verbonden risico's te beheersen. Hiervoor is het nodig om tijdig te overwegen hoe BYOD veilig toe te staan is.

Hoe kunnen organisaties, vooral binnen de rijksoverheid, BYOD op verantwoorde wijze invoeren? Welke impact heeft een specifieke BYOD-uitvoering op de organisatie? Dit rapport geeft richting aan dit vraagstuk door de kenmerken van het BYOD-concept in een generieke vorm te introduceren en de problematiek van informatiebeveiliging en de mogelijke oplossingen te schetsen. Kortom, een overzicht van de uitdagingen, risico's, mogelijke maatregelen en keuzes.

1.4 Reikwijdte van dit rapport

Dit rapport gaat over mobiele apparaten die continu verbonden (kunnen) zijn aan een mobiel telecommunicatienetwerk. Het gaat om apparaten die het eigendom van de gebruiker zijn en beperkt zich tot gebruik daarvan voor algemene kantoortoepassingen, zoals e-mail, agenda, intranettoegang en het inzien, bewerken of downloaden van documenten. Het gaat niet over het gebruik van gespecialiseerde toepassingen.

Verder beperkt dit document zich tot gebruik van gegevens die ten hoogste gerubriceerd zijn als Departementaal Vertrouwelijk volgens het Voorschrift Informatiebeveiliging Rijksdiensten – Bijzondere Informatie (VIR-BI). Dit niveau is het laagste niveau van gegevensrubricering van bijzondere informatie.

Dit document is geschreven voor Chief Information Officers (CIO's) en IT-managers bij overheidsinstellingen, maar kan ook gebruikt worden door beveiligingsfunctionarissen die adviseren over het gebruik van mobiele apparatuur.

2 Welke uitvoering van BYOD past bij uw organisatie?

De ontwikkelingen rond telecommunicatie en mobiele apparatuur gaan zo snel dat op de markt een groot aantal technische platformen (combinaties van hardware en besturingssystemen) verkrijgbaar is. Binnen deze platformen bestaan zoveel uitvoeringen dat het niet mogelijk is om alle varianten te beschrijven. Dit onderzoek beperkt zich daarom tot hoofdlijnen en algemeen aanvaarde uitgangspunten. Op basis daarvan worden de meest voor de hand liggende informatiebeveiligingsrisico's en beveiligingsmaatregelen beschreven.

2.1 Verschillende BYOD-vormen

De overheid en het bedrijfsleven passen BYOD in de praktijk al op verschillende plekken toe. Een vaak toegepaste vorm is het gebruik van zakelijke e-mail en een agenda op smartphones. Medewerkers gebruiken hiervoor hun eigen telefoon, die de gegevens ophaalt van de mailserver van de organisatie. Voor het telefoongebruik wordt vaak een standaardvergoeding of declaratiemodel toegepast. De beveiligingsmaatregelen blijven veelal beperkt tot een beleid waaraan de gebruiker zich dient te houden. Ook telewerken op de thuiscomputer komt al langer voor. Doorgaans kiezen organisaties voor een oplossing in de vorm van een virtuele werkplek om dit veilig mogelijk te maken. Inmiddels staan enkele departementen en andere overheidsorganisaties soms ook mobiele apparaten zoals tablets toe voor bedrijfstoepassingen.

Er bestaat mobiele apparatuur die zich goed leent voor bedrijfsmatig gebruik en die toegevoegde waarde heeft in de kantooromgeving. Te denken valt aan laptops en *notebooks*, *netbooks* en *ultrabooks*, telefoons en smartphones, *PDA's* en tablets.

Afhankelijk van de leverancier maakt de mobiele apparatuur gebruik van een specifiek besturingssysteem, zoals iOS van Apple, Android van Google, Windows Mobile van Microsoft of BlackBerry OS van Research in Motion. Deze platformen hebben elk hun specifieke eigenschappen, standaarden, ondersteunende programmeertalen en beveiligingsmogelijkheden.

2.2 Ontwikkelingen op het gebied van BYOD gaan snel

Het BYOD-concept wordt snel populairder en veel organisaties tonen interesse voor de toepassingen. Beleidsmakers verwachten in 2013 bijna een halvering van het aantal organisaties dat BYOD verbiedt (van 69% naar 37%), zo blijkt uit onderzoek. Het aandeel organisaties dat BYOD gaat aanmoedigen zal haast verdubbelen (van 24% naar 46%)[1]. De verwachting is zelfs dat Nederland leidend wordt op het gebied van eigen apparatuur binnen organisaties: in 2013 zal naar verwachting 37%[2] van de organisaties een vorm van BYOD toepassen. Beveiliging is hierbij de grootste zorg.

[1] Bron: *Bring Your Own Technology survey, CIO magazine augustus 2011*

[2] Bron: *Citrix Global BYO index, 2011*

De snelle opmars van tablets toont aan hoe door middel van innovatie de toepassing en gebruikswijze van ICT veranderen. Het is goed denkbaar dat in de toekomst nieuwe technologieën een vergelijkbare invloed krijgen.

Doordat de rekenkracht en opslagcapaciteit van mobiele apparaten toeneemt, doen zij steeds minder onder voor de thuiscomputer. Ook vervagen de scheidslijnen tussen smartphones, tablets, *slates*, netbooks en laptops. Steeds meer hybride vormen komen op de markt, zoals tablets met los toetsenbord of smartphones met een tablet als docking station.

De levenscyclus van consumentenelektronica wordt steeds korter. Nieuwe apparaten krijgen al binnen enkele maanden een opvolger. Om niet continu mee te hoeven veranderen, bevat een BYOD-concept daarom bij voorkeur een stabiele component, die de belasting voor de beheerorganisatie beperkt, zoals een applicatie die onafhankelijk is van de hardware.

Met de toename van de mogelijkheden en het gebruik van mobiele apparatuur nemen de beveiligingszorgen toe. Dit speelt zeker voor BYOD, waar de scheiding tussen en zakelijk en privé-gebruik van het apparaat verdwijnt. De vraag naar beveiligingsoplossingen voor mobiele apparatuur neemt hierom toe. Verschillende leveranciers ontwikkelen momenteel oplossingen om een scheiding tussen zakelijk en privégebruik beveiligingstechnisch mogelijk te maken. Het gaat daarbij bijvoorbeeld om hardwarematige scheidingen of een logische scheiding door middel van virtualisatietechnieken.

Ook komen er steeds meer toepassingen voor het beheer van apparatuur in een zakelijke omgeving op de markt. Deze toepassingen maken het bijvoorbeeld mogelijk de beveiligingsinstellingen van het device en het aanbrengen van softwareupdates op afstand te verzorgen. Dergelijke oplossingen worden *Mobile Device Management (MDM)*-oplossingen genoemd. Zij zijn vaak beperkt tot het platform van één leverancier, maar een aantal leveranciers ontwikkelt momenteel beheertoepassingen voor meerdere platformen.

2.3 Vrijheid versus beheersing in BYOD-varianten

Er zijn verschillende varianten van BYOD mogelijk. Deze verschillen in de mate van vrijheid voor de gebruiker en de controle die kan worden uitgeoefend door de organisatie. De bepalende factoren zijn:

- de mate van vrijheid die de gebruiker krijgt om zijn eigen device en leverancier te kiezen;
- de organisatie van de ondersteuning en het beheer van het device;
- de vrijheid die de gebruiker krijgt om toepassingen op het device te gebruiken.

2.3.1 Vrijheid in de keuze van het device en de leverancier

Er zijn twee varianten te onderscheiden:

- *Bring Your Own Device*: de gebruiker schaft zelf een device aan en gebruikt dit ook zakelijk;
- *Choose Your Own Device*: de gebruiker selecteert zijn eigen device binnen de kaders die de organisatie bepaalt, schaft het aan en gebruikt het vervolgens zowel zakelijk als privé.

In het eerste geval heeft de gebruiker maximale vrijheid in de keuze van het soort, merk en type device. Daardoor wordt een scala aan verschillende devices en platformen in de organisatie geïntroduceerd. In het tweede geval wordt de keuze beperkt, waardoor alleen specifieke soorten en platformen worden geïntroduceerd.

In de huidige fiscale vergoedingsregelingen kan het bekostigen van een device (in eigendom van de medewerker) door de werkgever onaantrekkelijk zijn, omdat een eindheffing wordt geheven als een bepaalde vergoedingsdrempel wordt overschreden. Echter, het is niet ondenkbaar dat medewerkers zelf de kosten willen en zullen dragen. Onderzoek[3] toont aan dat medewerkers momenteel het gebruik van eigen technologie veelal volledig zelf betalen. Dit is uiteraard enigszins afhankelijk van de belastingregelingen in een land. Binnenkort wijzigt de situatie echter door de komst van de werkkostenregeling. Uitgangspunt van deze regeling is dat voor een onbelaste vergoeding middelen voor 90% zakelijk moeten worden gebruikt.

2.3.2 *Vrijheid in keuze voor ondersteuning en beheer van het device*

Er zijn verschillende beheervormen mogelijk. De gebruikersondersteuning en het beheer kunnen uit de volgende aspecten bestaan:

- de beantwoording van vragen over de functionaliteit en het gebruik van het device;
- onderhoud van de software op het device;
- reparatie of vervanging bij defecten, verlies of diefstal;
- bewaking van de beveiliging van het device;
- installatie van applicaties;
- configuratie van het device, zoals instellingen om het device te verbinden met de systemen van de organisatie.

Het spectrum voor ondersteuning en beheer varieert van enerzijds 'volledige ondersteuning en beheer door de eigen organisatie' tot anderzijds 'service tot aan het stopcontact'. Het eerste uiterste geeft maximale controle aan de organisatie, maar vergt de grootste beheerinspanning. Het andere uiterste biedt alleen ondersteuning en beheer met betrekking tot de data en de verbinding met de organisatie, waardoor de beheerinspanning beperkt blijft.

De beveiligingsoverwegingen rond de verschillende beheervormen komen in hoofdstuk 4 aan bod.

2.3.3 *Vrijheid in keuze van de toepassing(en) op het device*

De grootste informatiebeveiligingsrisico's liggen daar waar de gegevens worden verwerkt en opgeslagen. Dit is op het device zelf en in de backofficeomgeving van de organisatie.

De controle over de dataverwerking en gegevensopslag op het device is sterk afhankelijk van de toepassingen (de applicaties of apps) die op het device worden gebruikt. Hoe meer vrijheid de gebruiker heeft om te bepalen welke applicaties hij gebruikt, des te minder controle de organisatie heeft over de verwerking of opslag van de gegevens.

[3] *Bring Your Own Technology survey, CIO magazine augustus 2011*

Om een passende applicatie te selecteren, is het belangrijk te weten welke informatie wordt verwerkt en welke eisen worden gesteld aan de beveiliging hiervan. Een centrale vraag hierbij is in hoeverre de gebruiker informatie op het device mag opslaan en in hoeverre sporen daarvan mogen achterblijven.

We onderscheiden een aantal fundamentele varianten:

Variant	Kenmerk	(Beveiligings)voor- en nadelen
'Open device'	De controle over de beveiliging wordt overgelaten aan de gebruiker van het device. Voor bedrijfsmatig gebruik worden de standaardapplicaties van het device gebruikt of applicaties die door de gebruiker zelf gekozen zijn. Voorbeeld: gebruik van de e-mail- en agendafunctionaliteit via de standaardapplicaties op een smartphone of tablet.	+ Voor gebruikers is dit de meest flexibele vorm. - De afhankelijkheid van de leverancier van het device en de daarop meegeleverde applicatie(s) leidt tot onduidelijkheid over de veiligheid. - Er kunnen gemakkelijk veel gegevens op het device achterblijven.
Device als 'mobile display'	Bij deze variant bevinden zich weinig of geen gegevens op het device, maar wordt een toepassing gebruikt om de schermuitvoer van een applicatie in de backoffice op het device weer te geven. Voorbeeld: virtuele desktopapplicatie.	+ Deze oplossing minimaliseert de hoeveelheid gegevens op het device. + Er zijn diverse commerciële oplossingen beschikbaar waarbij werkomgevingen gevirtualiseerd worden op een backofficeserver en als virtuele kantoorapplicatie of werkplek op het device worden weergegeven. Deze oplossing wordt al veel gebruikt voor mobiel- en thuiswerken. + Deze variant geeft de organisatie ruime controle over het gebruik. - Voor gebruikers is dit een tussenvorm in de vrijheid van gebruik; privé de eigen apps, zakelijk de mobile-display- app. - Een breedbandige en betrouwbare internetverbinding is nodig om te kunnen werken. - Het device is niet bruikbaar op locaties waar geen verbinding beschikbaar is zoals vliegtuig of (vele) locaties binnen gebouwen.
Device met 'beveiligde app'	In deze vorm worden gegevens alleen op het device verwerkt en opgeslagen binnen een beveiligde applicatie met vertrouwde cryptografische hardware en aanvullende technische beveiligingsmaatregelen. Het device kan hiermee wel gegevens bevatten, maar deze zijn beschermd in een door de applicatie gecreëerde beveiligde omgeving.	+ De data op het device worden beschermd op het niveau dat de organisatie zelf nodig vindt. + De organisatie heeft volledige controle over de gebruikte beveiligingsmaatregelen en kan daarom gevoelige informatie uitwisselen tussen het device en de backoffice. + Ook zonder internetverbinding kan gewerkt worden, als met enige regelmaat de gegevens met de centrale omgeving gesynchroniseerd worden. - Deze oplossing vergt de ontwikkeling van specialistische software. Voor hogere beveiligingsniveaus kunnen ook extra hardware en aanpassingen in het besturingssysteem en het communicatienetwerk nodig zijn. Dit verhoogt de kosten van deze oplossing.

3 Welke risico's brengt BYOD met zich mee?

Het gebruik van het BYOD-concept is net als elk ander gebruik van IT-middelen niet zonder beveiligingsrisico's. Vooral de bescherming van bedrijfsgegevens is cruciaal. Het is belangrijk om de risico's op juiste wijze in kaart te brengen. Daarna moet de organisatie bepalen welke maatregelen ter bescherming moeten worden getroffen en welke variant van BYOD toelaatbaar is. Dit vraagt doorgaans om een afweging tussen functionele wensen en de benodigde informatiebeveiliging.

3.1 Vertrouwelijke informatie vereist bescherming

Elke overheidsorganisatie heeft gegevens nodig voor de uitvoering van zijn taken. De vertrouwelijkheid en het vereiste beschermingsniveau van deze gegevens kunnen sterk verschillen.

Gegevens binnen de rijksoverheid worden beschermd volgens het Voorschrift Informatiebeveiliging Rijksoverheid (VIR). Voor Bijzondere Informatie[4] is een aparte regeling opgesteld, het Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie (VIR-BI). Het VIR-BI beschrijft de rubriceringniveaus voor bijzondere informatie, zoals staatsgeheim (Stg. Confidentieel, Stg. Geheim en Stg. Zeer Geheim) en departementaal vertrouwelijk (Dep. Vertrouwelijk) en de daarbij behorende beveiligingseisen.

Deze eisen zijn ook geldig als de gerubriceerde informatie op eigen apparatuur van een medewerker wordt verwerkt. Omdat het gebruik van mobiele apparatuur buiten de directe controle van de werkgever gebeurt, levert dat extra risico's op. Het is belangrijk om deze risico's te beoordelen en voldoende maatregelen ertegen te treffen.

Ook ongerubriceerde informatie moet passend beschermd worden. Ten eerste kan daarop ook wet- of regelgeving van toepassing zijn. Persoonsgegevens moeten bijvoorbeeld beschermd worden conform de Wet bescherming persoonsgegevens. Daarnaast kan openbaarmaking van vertrouwelijke interne informatie, zoals financiële informatie of politieke besluitvorming, imagoschade veroorzaken voor de betreffende overheidsinstantie. Ten slotte kan de vertrouwensrelatie tussen overheid en burger of bedrijfsleven worden aangetast als informatie via een veiligheidslek bij de overheid op straat komt te liggen.

3.2 Verschillende beveiligingsrisico's

Om te bepalen welke beschermingsmaatregelen nodig zijn voor de gegevens op devices, is het belangrijk om na te gaan welke risico's zich waar voordoen. Informatiebeveiligingsrisico's worden gewoonlijk naar drie aspecten onderverdeeld.

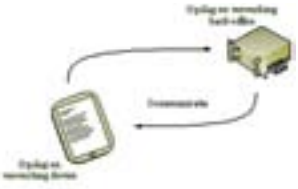
[4] Bijzondere informatie betreft die informatie waarvan kennisname door niet-gerechtigden tot nadeel kan leiden voor één of meer ministeries, de Staat der Nederlanden of haar bondgenoten.

Ten eerste zijn er risico's met betrekking tot de **beschikbaarheid** van gegevens; is de bedrijfsinformatie tijdig beschikbaar als deze nodig is? Ten tweede zijn er risico's met betrekking tot de **integriteit** van de gegevens; is de informatie wel betrouwbaar en niet per ongeluk (of opzettelijk) aangepast? Ten slotte zijn er risico's met betrekking tot de **vertrouwelijkheid** (of **exclusiviteit**) van gegevens; is het zeker dat de gegevens alleen in te zien zijn door een bevoegde persoon en niet door anderen?

3.3 Niet alleen het device zelf is kwetsbaar

We beschouwen drie onderdelen waar risico's en kwetsbaarheden kunnen liggen.

1. Het device: de verwerking en opslag van gegevens op het device zelf.
2. De datacommunicatie: de gegevensuitwisseling tussen het device en de backofficesystemen van de organisatie, bijvoorbeeld wifi of een mobiel datacommunicatienetwerk.
3. De backoffice: de computersystemen van de organisatie waar de gegevens centraal worden opgeslagen en beheerd, zoals de mailserver of de bestandsopslag.



Figuur 1. Devices, communicatie en backoffice

Het zwaartepunt van de informatiebeveiligingsrisico's kan op verschillende punten liggen, afhankelijk van de specifieke BYOD-variant. De risico's en maatregelen zijn hieronder verder beschreven.

3.3.1 Risico's en maatregelen voor het device

Gegevensopslag en -verwerking op een device vormt een risico als dit zonder beveiligingsmaatregelen buiten de beveiligde omgeving van de organisatie plaatsvindt. Al snel blijft vertrouwelijke informatie op het device achter, die bij verlies of diefstal in verkeerde handen kan vallen. Ook kunnen onbevoegden, zoals familie of vrienden, gegevens inzien, bijvoorbeeld als ze, bedoeld of onbedoeld, op het scherm meekijken.

Ook hebben devices (draadloze) verbindingsmogelijkheden voor synchronisatie of back-up van gegevens. Voorbeelden zijn Bluetooth en wifi. Deze communicatiekanalen kunnen kwetsbaarheden bevatten die aanvallers kunnen gebruiken om toegang tot het device en de gegevens daarop te verkrijgen. Hetzelfde geldt voor de aansluiting die op het device aanwezig is, zoals USB of een aansluiting voor een docking-station.

Een belangrijk risico vormt de toegang van de leverancier van het device tot de gegevens op het device. Veel devices hebben de mogelijkheid automatische back-ups van gegevens te maken. Waar deze terechtkomen en hoe zij zijn beschermd is niet altijd duidelijk. Als een device defect is, wordt dit gewoonlijk ingeleverd bij de leverancier of winkelier. Als de gegevens niet eerst zijn verwijderd of ontoegankelijk zijn gemaakt, kunnen zij in verkeerde handen vallen.

De applicaties die de medewerker gebruikt kunnen ook beveiligingslekken bevatten. Zo zijn er diverse applicaties die de contactpersonen of agenda uitlezen, maar dit is ook mogelijk voor andere gegevensgebieden op het device.

Tevens kunnen de applicaties data 'lekken' naar het device, dat wil zeggen dat gegevens die in applicaties gebruikt worden, achterblijven op het device. Dat levert risico's op.

Maatregelen ter waarborging van vertrouwelijkheid van gegevens
Maatregelen om de vertrouwelijkheid van gegevens te beschermen zijn vooral gericht op het verminderen van gegevensopslag en achterblijven van gegevens op het device (lekken). Te denken valt aan oplossingen als 'mobile display' of het gebruik van specifiek ontwikkelde applicaties.

Maatregelen tegen onbevoegd gebruik, verlies of diefstal zijn bijvoorbeeld authenticatie en de versleuteling van de dataopslag op het device. Ook bestaat de mogelijkheid om lokaal of op afstand de gegevens (of het sleutelmateriaal voor de opslag) te wissen na een aantal mislukte inlogpogingen of na melding van verlies of diefstal.

Het risico op datalekkage door applicaties kan worden beperkt door een oplossing te gebruiken als 'mobile display', waarin alleen de schermweergave op het device plaatsvindt. Aangezien devices vaak de mogelijkheid hebben om schermafbeeldingen op te slaan, is dit echter niet 100% waterdicht. Een alternatief is het aanbieden van een eigen vertrouwde beveiligde applicatie die alle data zelf versleutelt, rekening houdt met deze dreigingen en geen data 'lekt'.

Om enige controle over de gegevens op het device te houden, moet worden voorkomen dat data naar fabrikanten of andere dienstverleners lekt. Daarom moet back-up en synchronisatie met *cloud*-opslagdiensten worden beheerst of geblokkeerd. Ook is het zaak dat er geen data blijvend op een device worden opgeslagen (bijvoorbeeld met een 'virtuele-desktop'-achtige constructie) of gecontroleerde versleuteling te gebruiken, bijvoorbeeld in een zelfontwikkelde app. Dit is extra belangrijk bij reparatie van defecte devices, omdat data niet altijd te verwijderen zijn voordat een device voor reparatie wordt aangeboden.

Er zijn MDM-oplossingen beschikbaar die deze beveiligingsfunctionaliteit (geheel of gedeeltelijk) bevatten.

Voor Departementaal Vertrouwelijke gegevens zijn aanvullende maatregelen nodig. Technische maatregelen zijn bijvoorbeeld het blokkeren van alle onnodige functionaliteit, het extra veilig samenstellen en configureren van het besturingssysteem (*hardening*) en het gebruik van aanvullende vertrouwde cryptohardware (SD-kaart met cryptochip en versleutelde opslag). Procedurele maatregelen zijn bijvoorbeeld de verplichting dat de gebruiker het device altijd bij zich draagt of veilig opbergt.

Een ander beveiligingsrisico betreft de integriteit van gegevens op het device. Het bezit van verkeerde informatie kan net zo schadelijk zijn als het uitlekken van informatie. Het is mogelijk dat gegevens verloren gaan doordat gebruikers niet altijd even zorgvuldig omgaan met hun device. Of dat gebruikers de integriteit van het device bewust aantasten, bijvoorbeeld door *jailbreaken* of *rooten*. Dit opent het device voor installatie en gebruik van applicaties, waar *backdoors*, *keyloggers* en andere kwaadaardige functies in kunnen zitten.

Fouten in applicaties kunnen leiden tot aantasting van de integriteit van gegevens. Synchronisatieproblemen van gegevens kunnen leiden tot verouderde gegevens met het risico op verkeerde beslissingen. Het is belangrijk om ook hiermee rekening te houden.

Maatregelen ter waarborging integriteit van het device en de gegevens

Om de integriteitrisico's van het device te beperken, zijn MDM-oplossingen beschikbaar. Het is bijvoorbeeld mogelijk bepaalde beveiligingsinstellingen te activeren, zodat de gebruiker geen onbekende applicaties kan installeren. Met deze oplossingen kan ook gecontroleerd worden of het device alle kritieke beveiligingsupdates bevat. Voor een device in eigendom van de gebruiker zal dit alleen mogelijk zijn met zijn toestemming.

Om de kans op *hack*-aanvallen op het device te verminderen is het verstandig dat al het verkeer van- en naar het device via een vertrouwd netwerk loopt, bijvoorbeeld een met cryptografie beveiligd netwerk (Virtual Private Network, VPN) en/of een door de telecommunicatieprovider verzorgde koppeling naar een vertrouwd bedrijfsnetwerk ('private Access Point Name').

Voor Departementaal Vertrouwelijk geldt dat de integriteit van gegevens maar ook van sleutelmateriaal, configuratie-instellingen en software gecontroleerd moet worden door middel van *checksums* (controlegetallen).

De praktijk
Gangbare devices bieden enige bescherming tegen de genoemde risico's. Voor devices in eigen beheer kunnen beveiligingsinstellingen (*policies*) worden ingesteld die voor een minimaal beveiligingsniveau zorgen. Het activeren van bijvoorbeeld wachtwoordbeveiliging en encryptie van de gegevens is meestal standaard mogelijk.

Hoe sterk deze maatregelen op een bepaald device zijn, is niet altijd duidelijk, omdat meestal weinig details beschikbaar zijn over de implementatie van de beveiligingsmaatregelen. De ervaring van de AIVD leert dat u niet altijd kunt vertrouwen op de gedocumenteerde beveiligingsmaatregelen. Als zij niet juist geïmplementeerd zijn of eenvoudig te 'kraken' zijn, kan de wachtwoordbeveiliging worden omzeild zonder dat de data op het device verloren gaan. Ook zijn gevallen bekend waarbij fabrikanten de beveiligingsmaatregelen en versleuteling van apparatuur ongedaan konden maken. Het op afstand wissen van gegevens op devices bij verlies of diefstal is niet mogelijk als de datacommunicatie verbroken is.

Ten slotte is het belangrijk om na te gaan welke functionele en technische eigenschappen van een besturingssysteem een risico kunnen vormen. Worden er bijvoorbeeld continu screenshots gemaakt die gevoelige informatie kunnen bevatten? Wordt op veilige wijze omgegaan met de invoer van het toetsenbord? De antwoorden op deze vragen bepalen welke risico's bestaan en welke maatregelen nodig zijn.

3.3.2 Risico's in de datacommunicatie
Mobiele devices communiceren met het kantoornetwerk via een draadloze datacommunicatieverbinding. Voor deze verbinding spelen risico's op de gebieden van exclusiviteit en beschikbaarheid.

De communicatie kan onderschept worden als deze niet goed is beveiligd. Als zonder aanvullende maatregelen gebruik wordt gemaakt van communicatiekanalen met bekende zwakheden (zoals gsm en Bluetooth) levert dat een risico op. Daarnaast kan er niet altijd op vertrouwd worden dat de afzender van de informatie juist wordt weergegeven. Het afzendernummer van een sms of een telefoonnummer is immers te manipuleren, dit wordt ook wel 'spoofen' genoemd.

Het is belangrijk om te beseffen dat de beschikbaarheid van gegevens afhankelijk is van een derde partij, de telecommunicatieprovider. Als een mobiel netwerk uit de lucht is, kan de medewerker niet meer bij de gegevens. De gevolgen hiervan kunnen uiteenlopen van verwaarloosbaar ongemak tot groot verlies aan productiviteit of reactievermogen.

Maatregelen ter waarborging van exclusiviteit van de gegevens
Om de vertrouwelijkheid van de gegevens tijdens communicatie te beschermen kan een extra beveiligingslaag worden toegepast, zoals het versleutelen van de datacommunicatie. Dit kan bijvoorbeeld door het netwerkverkeer tussen het device en de backoffice te versleutelen en te beschermen door een VPN-verbinding. Alternatief kan de communicatie tussen een applicatie en de backofficesystemen versleuteld worden, bijvoorbeeld door middel van het beveiligde SSL- of TLS-communicatieprotocol. Dat maakt tevens sterke vormen van authenticatie op de backoffice mogelijk met beveiligingscertificaten.

De praktijk
Veel devices hebben verschillende communicatieverbindingen, zoals wifi, gsm en Bluetooth. Hierdoor is het lastig alle verbindingen op hetzelfde niveau te beveiligen, de communicatie-infrastructuur is zo zwak als de zwakste schakel. De communicatieverbinding waarover gegevensuitwisseling met de backoffice plaatsvindt kan veelal via een VPN-verbinding worden beveiligd. Hiervoor zijn protocollen als IPsec op devices te configureren. Door dit in te richten kan de beveiliging van de datacommunicatie met de backoffice voor de verschillende soorten devices op een gelijk niveau gebracht worden.
Daarnaast ondersteunen devices vaak het SSL- of TLS-protocol in applicaties, waarmee de verbindingen met servers en applicaties in de backoffice versleuteld kunnen worden.

3.3.3 Risico's in de backoffice

Door devices toegang te geven tot de kantooromgeving, kunnen risico's ontstaan voor de backofficesystemen.

Het toelaten van devices op een vertrouwde computerinfrastructuur kan bijvoorbeeld leiden tot introductie van virussen en andere kwaadaardige toepassingen. Het begrip 'Trojaans paard' wordt heel tastbaar met het toelaten van relatief ongecontroleerde devices die niet van de organisatie zelf zijn. Door het openstellen van backofficesystemen kunnen ook externe dreigingen ontstaan, zoals hackpogingen vanaf internet en pogingen de dienst 'uit de lucht' te halen (zogenaamde *Denial of Service*-aanvallen).

Als het backofficesysteem voor gegevenstoegang vertrouwt op de identiteit van de gebruiker zoals die door het device is gecontroleerd en vastgesteld, kunnen risico's ontstaan als het device gejailbreakt of gehackt is. In dat geval kan de identiteit gemanipuleerd zijn. Het is beter de identiteit van de gebruiker aan de backofficekant te controleren door middel van authenticatie op de server of een applicatie aldaar.

Bij gebruik van BYOD wordt de organisatie in toenemende mate afhankelijk van de backofficesystemen. Waar deze eerst alleen voor intern gebruik tijdens kantooruren waren bedoeld, kunnen zij nu 24 uur per dag, 7 dagen per week gebruikt worden. Als de intern gehanteerde servicelevels hierop niet zijn afgestemd en de beheerorganisatie niet is ingericht om een zo hoge beschikbaarheid te garanderen, dan worden gebruikers mogelijk teleurgesteld door de beschikbaarheid van het backofficesysteem.

De praktijk

De organisatie moet de inrichting van de infrastructuur herbeschouwen. Het koppelen van computersystemen aan mobiele devices over een netwerk levert altijd risico's op, zeker als over de devices zelf maar beperkte controle bestaat.

De authenticatie van devices en gebruikers moet sterk genoeg zijn en de verbindingen zelf moeten beveiligd worden, bijvoorbeeld door een VPN te gebruiken. Bovendien moet in de infrastructuur voldoende scheiding aangebracht worden tussen vertrouwde en onvertrouwde netwerken. Zo kunnen de potentiële gevolgen van kwetsbaarheden of aanvallen worden beperkt.

Algemene netwerkbeveiligingsoplossingen zoals firewalls, monitoring tools en Intrusion Detection Systemen (IDS) kunnen worden ingezet. Daarnaast zijn ook specifieke beveiligingsoplossingen beschikbaar voor afzonderlijke diensten zoals e-mail en documentenbeheer.

3.4 Overige risico's en maatregelen

In de vorige paragrafen zijn verschillende risico's rond de technische componenten van BYOD getoond. Daarbij zijn voorbeelden van maatregelen aangedragen om de risico's te beperken. Ook buiten de techniek kunnen maatregelen genomen worden. Bijvoorbeeld in beleid, de organisatie, beheer- en bedrijfsprocessen en in de aansturing van de medewerkers die BYOD (gaan) gebruiken.

Aanpassing van het bestaande beveiligingsbeleid ligt voor de hand. Als hierin bepaalde beperkingen voor het gebruik van mobiele devices gelden, is het goed om na te gaan of het BYOD-concept wel bij de organisatie past.

Het is mogelijk dat het BYOD-concept niet voor alle medewerkers wordt toegestaan, maar alleen aan personen met een bepaalde functie. In dat geval is het belangrijk om de toegevoegde waarde van de functionaliteit voor de betreffende functie te bepalen.

Gedrag is een belangrijk onderdeel van de informatiebeveiliging. Hoe goed beveiligd een device of toepassing ook is, onkundig, onbewust of doelbewust verkeerd gebruik geeft risico's. Het is daarom verstandig afspraken te maken over welk gebruik van BYOD toegestaan is, eventueel in combinatie met een sanctiebeleid. Dit kan bijvoorbeeld door het beleid te communiceren en een gebruikersovereenkomst op te stellen waarin de medewerker akkoord gaat met zijn verantwoordelijkheden voor de gegevensbescherming op zijn device. Dit kan worden gekoppeld aan het in juridische zin afbakenen van verantwoordelijkheden.

De medewerker dient bijvoorbeeld in te stemmen met logging en monitoring van communicatie en moet accepteren dat er gevolgen zijn als hij gemaakte afspraken niet nakomt.

Het is verstandig in het oog te houden hoe het beveiligingsvoordeel van een maatregel opweegt tegen de belemmeringen die de medewerker daarvan ondervindt. Maatregelen werken beter als werknemers ze begrijpen en niet als onnodig hinderlijk ervaren. Wanneer een medewerker het nut van de maatregel onvoldoende inziet, zal hij eerder geneigd zijn deze te omzeilen als dat mogelijk is. Het is aan te raden om maatregelen te kiezen die 'natuurlijk' zijn en niet als een belemmering worden ervaren. Als maatregelen met aansprekende voorbeelden worden gemotiveerd en als de aanwezige risico's duidelijk zijn, zullen medewerkers hiervoor sneller begrip tonen. Het blijft daarbij belangrijk om medewerkers regelmatig op gewenst gedrag en kwetsbaarheden attent te maken.

Tot slot bestaat bij zakelijk gebruik van privé-devices het risico dat de licenties van de op het device aanwezige software worden overtreden als deze alleen privégebruik toestaan (zogeheten *Home-use*-licenties).

4 Hoe gaat u om met risico's in de levenscyclus van het device

4.1 De levenscyclus van een device in vijf fasen

Om de risico's, overwegingen en maatregelen met betrekking tot BYOD goed in kaart te krijgen, worden vijf fasen in de 'BYOD-levenscyclus' van een device onderscheiden.

1. **De selectie:** de keuze van het specifieke device. Deze stap bepaalt in hoeverre verderop in de cyclus controle mogelijk is over het gebruik. Wordt de gebruiker helemaal vrij gelaten in zijn keuze of moet het device aan bepaalde (minimum)eisen voldoen?
2. **De ingebruikname:** om gebruik te kunnen maken van de bedrijfsinformatie, zal het device moeten worden geconfigureerd om het met de backofficesystemen te verbinden. Deze stap vergt afspraken over de gegevenscommunicatie en de maatregelen die op het device worden geactiveerd.
3. **Het gebruik en beheer:** de belangrijkste fase in het gebruik van de apparatuur. Binnen deze fase vindt de daadwerkelijke toegang tot en gebruik van gegevens plaats. Hier spelen dan ook de meeste risico's.
4. **De ondersteuning:** onderhoud is nodig, in het bijzonder van de software, zowel van het besturingssysteem als van de applicaties. De omgang met reparatie en ondersteuning is belangrijk voor de beveiliging van gegevens.
5. **De buitengebruikstelling:** aan het eind van de (zakelijke) levensduur zal het device veilig buiten gebruik gesteld moeten worden.

Figuur 2. levenscyclus van een device

De vijf fasen zijn hierna uitgewerkt, inclusief de risico's en praktische maatregelen.

4.1.1 De selectie

De selectie van een device vormt het startpunt van de levenscyclus en is een belangrijk moment in BYOD. Een device kan op verschillende criteria worden geselecteerd.

Het is belangrijk om in deze fase duidelijk te hebben waarom u BYOD wilt toepassen en welke voordelen dit de organisatie biedt. Is dit onvoldoende duidelijk, dan is het wellicht verstandig om BYOD niet toe te staan. Het is in elk geval aan te raden om de doelstellingen van BYOD en de voorwaarden voor het gebruik van devices vast te leggen. Het is belangrijk om in deze fase duidelijkheid te hebben over welke devices of platformen worden toegestaan, tot welke informatie deze toegang mogen krijgen en onder welke voorwaarden deze toegang wordt verleend.

In de selectiefase worden het device en de functionaliteit die nodig is voor het zakelijk gebruik bepaald. De gebruiker zal dit gewoonlijk zo veel mogelijk zelf willen doen. Vanuit de organisatie is echter van belang dat het device op een veilige manier ingezet kan worden voor de benodigde functionaliteiten. Dit geldt met name voor de gegevensverwerking en opslag op het device en de communicatie met de kantooromgeving. Het device moet voldoen aan de eisen van de organisatie.

Overwegingen

Het device: de verschillende gebruiksvormen bepalen de eisen voor de selectie van een device. Daarbij is de vrijheid in de keuze van het device zeer bepalend. Als de gebruiker de vrije keuze krijgt, is het zaak een lijst met benodigde functionaliteiten op te stellen, zoals versleutelde opslag en communicatie, wachtwoordbeveiliging, en de mogelijkheid tot het op afstand wissen van het device.

Als een organisatie de toegestane devices wil beperken kan deze daarvoor een lijst met ondersteunde merken en typenummers hanteren. Een goede tussenvorm kan een lijst met ondersteunde platformen zijn, zoals BlackBerry OS, iOS of Android, eventueel met ondersteunde versies.

In het geval van vrije keuze koopt de werknemer als consument in een winkel een device naar keuze. Een alternatief is de medewerker een keuze te laten maken uit een 'bedrijfswinkel', waarbij de werkgever bepaalt welke devices in het assortiment verkrijgbaar zijn.

4.1.2 De ingebruikname

Na de selectie en aanschaf krijgt de organisatie doorgaans voor het eerst met het device te maken. De eerste activiteit in de fase van ingebruikname is het al dan niet toestaan van het device. Voldoet het aan alle gestelde eisen?

Het risico bestaat dat deze vraag onvoldoende aandacht krijgt en de organisatie devices toelaat die technisch ongeschikt, verouderd, onveilig of onbetrouwbaar zijn. Het is niet altijd eenvoudig deze toets uit te voeren. Hoe wordt bijvoorbeeld beoordeeld of de beveiliging van het device niet doorbroken is, bijvoorbeeld door jailbreaking. En bevat het device wel alle beveiligingsupdates?

Als het device de toets heeft doorstaan, kan het worden geconfigureerd voor gebruik in de zakelijke omgeving. Hiertoe worden de vooraf bepaalde beveiligingsmaatregelen op het device aangebracht, zoals beveiligingsinstellingen en beveiligingsapplicaties, bijvoorbeeld via een MDM–toepassing. Ook worden het gebruikersaccount en de verbinding met de backofficesystemen ingesteld. Dit laatste kan de ICT-beheerorganisatie zelf doen of het aan de gebruiker overlaten door hem de benodigde instructies te verstrekken.

Overwegingen
Het device: de informatiebeveiliging begint bij het device zelf. Door de configuratie van de beveiligingsinstellingen van het device kunnen de toegang tot het device en de gegevens daarop worden beveiligd. Gebruik van sterke versleuteling van de gegevensopslag en datacommunicatie is aan te raden. Dit kan door gebruik te maken van de standaardfunctionaliteit of door middel van afzonderlijke applicaties.

De inrichting van sterke versleuteling (encryptie) is geen triviale bezigheid en vraagt naast de juiste algoritmen en parameters ook goed procedurele maatregelen, zoals veilig sleutelbeheer en adequate respons op eventuele incidenten met versleuteling.

De communicatie: ook de communicatie dient voldoende beveiligd en versleuteld te zijn. Tot en met het niveau Departementaal Vertrouwelijk kunnen organisaties gebruikmaken van het door de AIVD goedgekeurde OpenVPN-NL.

De backoffice: het is belangrijk om ook de backofficesystemen te beveiligen. Bijvoorbeeld door verschillende beveiligingslagen aan te brengen, niet alleen op netwerk- of deviceniveau, maar ook op persoonsniveau. Waar mogelijk kunnen beveiligingsopties worden afgedwongen. Mogelijk moeten extra licenties worden aangeschaft voor het nieuw aangesloten device.

4.1.3 Het gebruik en beheer
Tijdens de periode van gebruik zal het device beheerd moeten worden. Niet alle BYOD-gebruiksvormen vergen evenveel beheer. 'Mobile display' vraag vooral beheer aan de backofficekant, omdat er in die variant weinig of geen gegevens op het device worden opgeslagen.

Als wel informatie op het device wordt opgeslagen, moeten maatregelen genomen worden om te zorgen dat de gegevens niet onbedoeld openbaar worden. Een deel van de maatregelen is preventief van aard en is al bij de ingebruikname getroffen, zoals versleuteling of authenticatie. Een ander deel is detectief van aard, zoals het monitoren van de datacommunicatie om verdachte patronen te herkennen, of correctief zoals het op afstand wissen van gegevens bij verlies of diefstal.

Het grootste risico vormt het gebruik van het device. Voor het gebruik moet de medewerker in ieder geval voldoende kennis hebben van de risico's, informatiebeveiligingsrichtlijnen en procedures, zoals de (tijdige) meldingsplicht bij verlies of diefstal. Het is nodig regelmatig aandacht te geven aan deze richtlijnen.

In deze fase moet ook het beheer van het device geregeld worden. Dit kan (deels) door de leverancier worden uitgevoerd en/of (deels) door de organisatie.

Overwegingen
Het device: op verschillende punten kan het beheer zich uitstrekken naar het mobiele device. Na diefstal of verlies bijvoorbeeld is het raadzaam om een mogelijkheid te hebben om de informatie op het device op afstand te kunnen wissen.

Let bij gebruik ook op de standaardfunctionaliteit van het device. Bij verschillende devices is een automatische back-upfunctie ingericht. Deze functionaliteit is niet altijd even geschikt om vertrouwelijke informatie op te slaan. Het is bijvoorbeeld mogelijk dat deze informatie in het buitenland wordt opgeslagen, wat nadelige juridische en privacygevolgen kan hebben.

De communicatie: het afluisteren van datacommunicatie is het belangrijkste communicatierisico. De versleuteling moet intact blijven; dit vraagt om goed sleutelbeheer. Zodra sleutels gecompromitteerd raken, moeten deze worden ingetrokken en vervangen.

De backoffice: met behulp van logging en monitoring kunnen organisaties onregelmatigheden in het verkeer detecteren en eventueel correctieve actie ondernemen (zoals het beperken of weigeren van de toegang tot informatie).

4.1.4 De ondersteuning

Er zijn verschillende niveaus en soorten van ondersteuning voor het device te onderscheiden. Het is in ieder geval zaak om van tevoren goed af te spreken tot waar de ondersteuning van de organisatie reikt.

Omdat het device eigendom van de werknemer is, is deze meestal ook verantwoordelijk voor het (laten) oplossen van technische storingen van dit device. Het is echter onwenselijk dat devices met gevoelige informatie zonder aanvullende maatregelen terechtkomen bij fabrikanten en dienstverleners. Het is namelijk niet te waarborgen dat deze externe partijen zorgvuldig met de informatie omgaan. Bovendien komt lang niet altijd hetzelfde device (inclusief gevoelige informatie) na reparatie weer bij de gebruiker terug. Het wordt soms vervangen door een ander exemplaar van hetzelfde type.

Overwegingen
Het device: het probleem van informatielekken via reparatie speelt niet alleen bij BYOD maar bij alle apparatuur van de organisatie. Afspraken met leveranciers bevatten niet altijd maatregelen op het gebied van informatiebeveiliging. Niet alle organisaties hebben eigen procedures opgesteld om de informatie op devices te wissen. Daarnaast is het soms (met name bij defecten) onmogelijk om gegevensdragers (volledig) te wissen.
Dit probleem kan worden beperkt door adequate versleuteling te gebruiken. Dit is aan te raden als het device gevoelige gegevens kan opslaan. Daarnaast is het verstandig om met gebruikers af te spreken defecten direct te melden, om de toegang vanaf het device (eventueel tijdelijk) uit te kunnen schakelen. Eventueel kunnen op afstand de gegevens worden gewist. Het is uiteraard het veiligst om een variant te gebruiken waarin geen gevoelige gegevens op het device terecht komen.

4.1.5 De buitengebruikstelling

Buitengebruikstelling kan verschillende redenen hebben. De medewerker kan zelf een nieuw device wensen. De medewerker kan uit dienst treden of van functie wisselen. Het device kan ook onherstelbaar defect geraakt zijn. Mogelijk leidt een gewijzigd risicoprofiel van de organisatie ertoe dat aanvullende beveiligingsmaatregelen nodig zijn die het device niet ondersteunt.

Bij het buiten gebruik stellen hoeft de technische levensduur van het device nog niet voorbij te zijn: het device kan wellicht nog steeds privé worden gebruikt. In dat geval moet de bedrijfsinformatie zorgvuldig van het device verwijderd worden en de toegang van het device tot de infrastructuur beëindigd worden.

Overwegingen

Het device: bij het uit gebruik nemen van een device dienen de gegevens op het device zelf zorgvuldig te worden verwijderd. Daarnaast is het zaak stapsgewijs elke vorm van toegang tot de gegevens te elimineren. De procedures hiertoe kunnen per device verschillen. Als het device niet langer zakelijk wordt gebruikt, moet vooraf duidelijk zijn welke gegevens zich waar bevinden.

4.2 Risicoanalyse nodig voor BYOD

Zoals gezegd is de keuze voor een BYOD-concept niet eenvoudig. Het toestaan ervan – in welke vorm dan ook – vereist een zorgvuldige risicoanalyse. Dit is een stap die elke organisatie samen met zijn medewerkers moet maken.

In de risicoanalyse worden de risico's afgewogen tegen de voordelen van de extra functionaliteit, potentiële kostenbesparingen en personeelsdoelstellingen. Het is van essentieel belang te bepalen hoe gevoelig de gegevens zijn en welke risico's aanvaardbaar zijn. Dit bepaalt de keuze voor een specifieke BYOD-vorm, waarna de bijbehorende beveiligingsmaatregelen uitgewerkt en ingevoerd kunnen worden. Vanwege de grote verscheidenheid aan organisaties, devices, specifieke risico's en maatregelen is dit maatwerk.

Om u op weg te helpen, volgen hieronder de essentiële stappen in het proces.

1. Breng de behoefte van gebruikers van eigen devices in kaart. Maak daarbij onderscheid tussen de toepassing (e-mail, agenda, documenten en dergelijke) en de vertrouwelijkheid van de gegevens die worden gebruikt (zoals gerubriceerd, openbaar, vertrouwelijk, persoonsgegevens).
2. Breng op basis van de gebruikersbehoefte in kaart welke typen device qua functionaliteit in aanmerking komen. Bijvoorbeeld tablets of smartphones.
3. Houd bij het verwerken van gerubriceerde informatie rekening met het VIR-BI. Bij Departementaal Vertrouwelijke gegevens zijn extra maatregelen nodig.
4. Voer op basis van de mate van vertrouwelijkheid van de gegevens een risicoanalyse uit om de belangrijkste risico's te bepalen.
5. Selecteer de maatregelen die de risico's tot een acceptabel niveau kunnen reduceren. Hiervoor kunt u de in hoofdstuk 3 en 4 genoemde maatregelen gebruiken.

4.3 Borging van de maatregelen

In het vorige hoofdstuk kwamen de beveiligingsrisico's en bijbehorende maatregelen die spelen bij de invoering van BYOD aan bod. Deze maatregelen moeten goed geborgd worden in de organisatie en zijn processen.

Om te zorgen dat de noodzakelijk geachte maatregelen daadwerkelijk worden toegepast is het aan te raden om processen en procedures op te stellen voor de verschillende stadia in de levenscyclus van het device.

Selectie:
bij de selectie van een device is het mogelijk om alleen devices met een acceptabel beveiligingsniveau toe te staan. Deze selectie kan plaatsvinden op basis van zowel globale eisen (gebruik van een bepaald platform of ondersteuning van een app) als op basis van een strakkere beperking van devices (bijvoorbeeld door het hanteren van een 'whitelist').

Ingebruikname:
bij ingebruikname van de apparatuur zullen bepaalde handelingen plaats moeten vinden, vaak 'provisioning' genoemd. De gebruiker kan deze verrichten, maar wellicht is het noodzakelijk dat een supportmedewerker deze taak op zich neemt. Het is ook aan te raden om de eigenschappen van het device centraal vast te leggen, om bijvoorbeeld te kunnen beoordelen of een device nog voldoet aan de gestelde toegangseisen. Het is bovendien raadzaam na te gaan of er garantie op het device aanwezig is.

Gebruik en beheer:
de mate van inzet van de eigen beheerorganisatie is sterk afhankelijk van het door de gebruiker gekozen model. Vaak zullen nieuwe applicaties met de bijbehorende processen ondersteund moeten worden om medewerkers veilig toegang te kunnen verlenen. Het is verder aan te bevelen om extra aandacht te besteden aan logging en monitoring van de communicatie en de gegevensverwerking. In deze fase kunt u via training en voorlichting de gebruiker informeren over de vormen van gebruik die toegestaan zijn.

Ondersteuning:
het niveau van gebruikersondersteuning kan sterk verschillen. Uitgebreide ondersteuning door de eigen organisatie zal veel aandacht en tijd van de beheerorganisatie vragen, maar het gebruikersgemak verhogen. Lichtere ondersteuning en uitbesteding beperken de beheerlast. In dit geval is het belangrijk om procedures te volgen bij het afnemen van support bij andere organisaties; zo kan het op afstand wissen van gegevens wenselijk zijn. Hiervoor is het wel nodig dat gebruikers supportaanvragen – ook als die buiten de organisatie worden afgehandeld – melden en registreren.

Buitengebruikstelling:
bij het buiten gebruik stellen van devices zal aanwezige informatie verwijderd moeten worden en zal het device een 'decommissioning'-procedure moeten doorlopen die de toegang tot gegevens via het device onmogelijk maakt.

De processen, verspreid over de hele levenscyclus, zorgen voor een adequate beheersing van de devices en de gegevens. Het is cruciaal dat de procesuitvoering wordt gemonitord en dat adequaat op incidenten en kwetsbaarheden wordt gereageerd. Het is daarnaast zeer belangrijk zich bewust te zijn van de risico's in de verschillende fasen van de levenscyclus, zoals genoemd in dit hoofdstuk.

5 Meer informatie

Voor vragen kunt u contact opnemen met:

Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD
Postbus 20010
2500 EA Den Haag

Telefoon: 079-3205050
Telefax: 079-3200733
E-mail: nbv@minbzk.nl
www.aivd.nl/organisatie/eenheden/nationaal-bureau/

Voor nadere informatie over de AIVD:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Telefoon: 079-3205050
Telefax: 079-3200733
www.aivd.nl

Colofon
Deze uitgave is tot stand gekomen door de AIVD,
Nationaal Bureau Verbindingsbeveiliging in samenwerking met PwC.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
AIVD/NBV
Postbus 20010
2500 EA Den Haag

Juli 2012