BRING YOUR OWN DEVICE/CHOOSE YOUR OWN DEVICE

Algemene Inlichtingen- en Veiligheidsdienst

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? De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) heeft een rapport over de stand van zaken uitgebracht waarvan we u de hoofdlijnen niet willen onthouden.

INLEIDING

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.

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. 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 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.

In het BYOD-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.
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 artikel 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 backups 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. Er kan bijvoorbeeld een mobile display oplossing of een beveiligde app ontwikkeld worden 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.

DRIE BYOD UITVOERINGEN

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 Managementbeheeroplossingen (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 displayapplicatie 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, 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 privétablet 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, wordt begonnen 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 commerciele 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.

Dit artikel is een bewerking door de redactie van het rapport 'Bring your own device/ Choose your own device', opgesteld door de AIVD. Het hele rapport is na te lezen op www.vovklict.nl – Intercom 2012.

BRONNEN:

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/