Factsheet

secure mobility
bring your own device

Impact en risico's van de mobiele trend op techniek, organisatie en processen

De Business Technologists van Atos geven door een bewezen risk-based aanpak invulling aan proces, personeel en technologie rondom mobiliteit. Op deze manier verloopt de transitie naar een Mobile Enterprise op een veilige en gecontroleerde manier.

Mobiele apparatuur en Bring Your Own Device (BYOD) zijn veel besproken onderwerpen in vrijwel alle organisaties. Medewerkers kunnen door middel van mobiliteit tot een meer flexibele indeling komen van werk en privé tijd. Daarmee kunnen hogere productiviteit en medewerkerstevredenheid gerealiseerd worden. Voor organisaties leidt dit meestal tot lagere ICT-kosten.

BYOD is een werkwijze die gevolgen heeft voor techniek, organisatie en medewerkers. Op het gebied van techniek worden vraagtekens gezet bij de veiligheid van data op deze apparatuur. Mobiele malware en het verlies van apparatuur en bedrijfsdata zijn belangrijke aandachtspunten. Voor de organisatie is vaak niet helder welke financiële en juridische consequenties verbonden zijn aan mobiliteit en privé apparatuur. Daarnaast moeten bestaande processen aangepast worden aan de nieuwe manier van werken. Als laatste zijn er aandachtspunten voor medewerkers rondom acceptatie, privacy en de balans tussen werk en privé.

Het is duidelijk dat deze door medewerkers ingezette trend van het gebruik van eigen devices risico's met zich meeneemt en gevolgen heeft voor techniek, organisatie en medewerkers die niet direct duidelijk zijn. Een risico management gedreven integrale aanpak die ingaat op alle aspecten is noodzakelijk om stappen te zetten naar meer productiviteit en medewerkerstevredenheid op een veilige manier.

Secure Mobility

Groei in de markt

Mobiele apparatuur is bezig met een significante opmars. Waar een aantal jaar geleden smartphones nog sporadisch voorkwamen zijn deze nu wijdverbreid. Ditzelfde proces is zich nu aan het herhalen met tablets. Gebruikers gaan over tot de aanschaf en besluiten de apparatuur in te zetten voor zowel persoonlijke als werk gerelateerde doeleinden. Dit proces heet *consumerization*.

Veelvoud aan initiatieven

BYOD en mobiliteit worden op dit moment door het bedrijfsleven en de overheid omarmd. De voordelen die deze ontwikkelingen met zich mee brengen zijn duidelijk en worden gezien als noodzakelijk om competitief te blijven in de markt. Een andere reden is dat de trend niet eenvoudig tegen te houden is door IT afdelingen. Dit geldt in het bijzonder wanneer het management besluit mobiele apparatuur te willen gaan inzetten voor hun werkzaamheden. Om die reden wordt door veel bedrijven een pilot uitgevoerd met mobiele apparatuur. Ook de overheid loopt hierin voorop door de inzet van tablets te faciliteren.

Het nieuwe werken

Mobiliteit is onderdeel van het nieuwe werken: overal en met elk apparaat toegang hebben tot de data benodigd voor het uitvoeren van werkzaamheden. Hiermee kan een strategie gevolgd worden die de organisatie in staat stelt kosten van werkplekken te reduceren. Daarnaast zijn er maatschappelijke voordelen aan mobiliteit zoals het verminderen van de file druk en de daarmee geassocieerde consequenties voor het milieu.

Bring Your Own Device

Bring Your Own Device en mobiele apparatuur worden vaak in één adem genoemd. Het zijn echter losstaande begrippen die weliswaar overlap hebben. Bedrijven kunnen ervoor kiezen om mobiele apparatuur toe te staan, maar alleen indien deze uitgeleverd is door het bedrijf zelf. In dit geval is er geen sprake van BYOD. Wanneer BYOD ter sprake komt zijn er verschillende inzichten in de technische oplossingsrichting. In het algemeen worden de volgende vormen onderscheiden:

- Ontsluiten mail, agenda en contactinformatie met het gebruik van een Exchange beleid wat bepaalde maatregelen op het apparaat afdwingt.
- BYOD met behulp van mobile device management (MDM) software. Deze software wordt geïnstalleerd op het apparaat en kan onder andere een vertrouwde omgeving binnen het apparaat creëren.
- BYOD met behulp van virtual desktop technologie. In dit geval wordt de desktop gevirtualiseerd in een datacenter. Elk willekeurig apparaat kan gebruikt worden om in te loggen op deze 'cloud' oplossing.
- BYOD door integratie in de infrastructuur. Deze aanpak vereist aanpassingen aan de infrastructuur, maar levert een manier van werken op die gebruik maakt van de rekenkracht van privé apparatuur. Hiermee kunnen desktop beheer kosten gereduceerd worden.

Een risico analyse is noodzakelijk om de juiste keuze te maken tussen deze vormen van BYOD. Belangrijke uitgangspunten voor deze risico analyse zijn het type bedrijf en de data die aangeboden gaat worden.

Risico's van mobiliteit

De voordelen van mobiliteit zijn reeds aangehaald. Efficiëntie en het verlagen van kosten zijn belangrijke drijfveren. De risico's geassocieerd met een meer open infrastructuur die een dergelijke vorm van werken ondersteund moeten hierbij onderkend worden om de continuïteit van de bedrijfsvoering niet in gevaar te brengen bij een eventuele overstap. De meest belangrijke onderwerpen daarbij zijn:

- Bedrijfsdata op mobiele apparatuur
- Jailbreaking en root-en
- Mobiele malware
- Grote hoeveelheid aanvalsvectoren

Bedrijfsdata op mobiele apparatuur
Bedrijfsdata op mobiele apparatuur is het meest besproken onderwerp in dit kader. Er wordt een mobiel apparaat geïntroduceerd in het bedrijf (al dan niet een eigen apparaat) waar bedrijfsdata op komt te staan. Technisch is het niet mogelijk om het apparaat op eenzelfde vertrouwd niveau te krijgen zoals dat bijvoorbeeld met een uitgeleverde laptop is. Dat heeft een aantal redenen:

- Er is op dit moment nog geen systeem voorhanden wat vertrouwde images op een dergelijk apparaat kan plaatsen. Het apparaat kan dus niet standaard voorzien worden van degelijke veiligheidsmaatregelen.
- Veiligheid is voor mobiele apparatuur vaak ondergeschikt geweest aan bruikbaarheid bij de ontwikkeling van het apparaat. Dit heeft geleid tot minder ingebouwde beveiliging.
- De besturingssystemen waar de apparatuur op draait zijn relatief nieuw. Daardoor zijn beveiligingsmaatregelen vaak nog niet volledig uitontwikkeld en volwassen.
- Voor Android geldt dat fabrikanten van telefoons oudere toestellen niet voorzien van de laatste versie van het operating systeem. Consumenten met een oudere telefoon lopen een groter risico op dataverlies door met een kwetsbaar besturingssysteem te werken.
- Smartphones en tablets zijn minder krachtiger dan traditionele computers waardoor traditionele beveiligingsmaatregelen als host gebaseerde intrusion prevention en antivirus een grotere impact hebben op de performance van het apparaat. Om die reden worden deze maatregelen vaak achterwege gelaten.

De laatste reden is dat smartphones en tablets relatief gelimiteerde opslagcapaciteit hebben. Om die reden wordt vaak gebruik gemaakt van cloud gebaseerde opslagoplossingen zoals dropbox. Een groot nadeel van dergelijke oplossingen is dat ze data opslaan in de Verenigde Staten waar de Patriot Act de overheid in staat stelt de data op te vragen. Ook geïntegreerde cloud backup oplossingen zoals iTunes en iCloud voor Apple apparatuur kunnen bedrijfsdata opslaan buiten het bereik van de beveiligingsmaatregelen van het bedrijf.

Het is zaak een eenduidig beleid te ontwikkelen voor bedrijfsdata op mobiele apparatuur. Dit geldt voor zowel eigen als door het bedrijf uitgeleverde apparatuur. De controle op de data moet te allen tijde behouden blijven, ongeacht waar deze data zich bevindt. Door dataclassificatie toe te passen in combinatie met Data Leakage Protection (DLP) en Digital Rights Management (DRM) software kan bepaald worden dat gevoelige data niet in aanmerking komt om geplaatst te worden op mobiele apparatuur. Daarnaast kan met MDM software gezorgd worden voor veilige opslag van data.

Bring Your Own Device

Jailbreaken en rooten
Gebruikers van mobiele apparatuur hebben niet de volledige rechten op het apparaat. Dit systeem heeft voordelen, maar zorgt er tevens voor dat gebruiker niet in staat is systeem functies te controleren op validiteit. Administratieve rechten verkrijgen op het apparaat (jailbreaken/rooten) heeft echter ook weer nadelen vanuit het perspectief van beveiliging: er kan niet meer aangenomen worden dat beveiligingsmaatregelen die standaard op het apparaat aanwezig zijn nog actief en correct zijn. Om die reden worden deze apparaten vaak uitgesloten uit de omgeving door de inzet van een technische oplossing. Een belangrijk punt voor de inzet van technische oplossingen is dat deze garanderen dat het apparaat voldoet aan het gestelde beleid. Dat vereist een controle mechanisme op het apparaat zelf.

Malware
Mobiele malware is een snel groeiend probleem. Daarbij moet onderscheid gemaakt worden tussen de verschillende mobiele besturingssystemen omdat deze elk hun eigen methoden voor software distributie hanteren. In het geval van Apple's iOS wordt de code gecontroleerd. Hoe dat proces echter verloopt wordt niet bekend gemaakt, waardoor het onmogelijk is de validiteit daarvan te controleren. Daarnaast zijn er voorbeelden van malware die alsnog in de app store geplaatst worden. Voor Android is de drempel lager: applicaties worden vooraf nauwelijks gecontroleerd maar achteraf verwijderd indien er sprake is van malafide code. De installatie van applicaties, vooral van applicaties van onbekende uitgevers, brengt om die reden altijd een risico met zich mee. Dit risico kan onder andere gemitigeerd worden door een enterprise application store aan te maken en de toegestane applicaties vanuit deze store aan te bieden. Daarnaast is het van belang de scheiding tussen persoonlijke en bedrijfsdata af te dwingen zonder het apparaat ernstige beperkingen op te leggen.

Grote hoeveelheid aanvalsvectoren
Mobiele apparatuur zoals tablets en smartphones hebben een aantal unieke kenmerken. Deze unieke kenmerken leveren echter ook additionele aanvalsvectoren. Daarnaast zijn ook generieke vectoren van toepassing die voor alle apparatuur gelden. De generieke aanvalsvectoren die van toepassing zijn op deze apparatuur zijn de volgende:

- *Wi-Fi.* Alle mobiele apparatuur is in staat contact te maken met een wireless netwerk. Malafide personen op hetzelfde netwerk kunnen deze apparatuur aanvallen. De aard van de wireless netwerken is dusdanig dat het voor aanvallers eenvoudiger is toegang te verkrijgen tot het netwerk dan dit het geval is voor fysieke connecties.

- *Bluetooth.* Deze vector wordt minder vaak gebruikt, omdat het bluetooth protocol voor apparatuur standaard uit staat en bovendien standaard geen signaal uitzendt. Het is echter een functionaliteit die alle mobiele apparatuur heeft en bovendien het apparaat in staat stelt bestanden (en dus malware) te ontvangen. Daarmee vormt het een potentiele dreiging.

- *Infrarood.* Voor deze vector geldt hetzelfde als voor bluetooth. Het protocol heeft echter significante nadelen en is niet aanwezig op alle apparatuur. Bestandsoverdracht via infrarood is echter vele malen sneller dan via bluetooth, dus in het geval van grotere bestanden wordt de techniek regelmatig toegepast.

- *USB.* Het apparaat kan tevens via USB gekoppeld voor bestandsoverdracht, waardoor ook dit protocol een mogelijke aanvalsvector wordt. Malware kan via USB overgedragen worden tussen een laptop en een mobiel apparaat.

- *Web browser.* Net zoals elk apparaat vormt de web browser zelf een aanvalsvector. Hierin verschilt het apparaat niet van andere apparatuur.

- *Email client.* Elk apparaat heeft een ingebouwde email client om van verschillende bronnen email te kunnen ontvangen. Deze email client zelf kan een aanvalsvector zijn omdat het een mogelijk geeft om malware via speciaal geproduceerde email op het apparaat te plaatsen. Sommige MDM oplossingen hebben een eigen implementatie van een email client.

- *Software (malware).* Deze is uitgebreid besproken in de vorige paragraaf.

- *Het besturingssysteem zelf.* Zoals eerder gesteld worden de besturingssystemen vaak niet lang ondersteund door de fabrikanten. Dit levert risico's op indien de apparatuur niet vaak vervangen wordt.

Unieke aanvalsvectoren voor deze apparatuur zijn:

- *GPRS, 3G, UMTS, HSDPA.* Deze vectoren zijn nagenoeg alleen van toepassing op mobiele apparatuur. Er worden andere netwerken gebruikt voor deze protocollen en daarmee vormen deze een aparte aanvalsvector.

- *SMS/MMS. SMS en MMS berichten* vormen een reële aanvalsvector voor mobiele apparatuur. Deze berichten kunnen zelf malafide zijn of links naar malafide sites bevatten. Daarnaast is het mogelijk dat cyber criminelen gebruiken maken van SMS berichten naar betaalde nummers als bron van inkomsten.

- *QR Codes.* Deze vector wordt vaak over het hoofd gezien, maar is een reële vector door de mogelijkheid URL's naar malafide sites in QR codes te coderen. Het probleem van deze codes is dat ze enkel leesbaar zijn voor apparatuur. Er is vaak gebruikers interactie nodig om uiteindelijk de link te openen, maar de praktijk wijst uit dat wanneer men over is gegaan tot het scannen van de code, de gescande link daarna ook geopend wordt. Het scannen van de code is hierin al een eerste blijk van vertrouwen waaraan een logisch gevolg gegeven wordt.

- *Fysieke toegang.* Fysieke toegang is niet uniek voor deze apparatuur. Het gemak waarmee toegang verschaft kan worden echter wel. Waar in het geval van de traditionele desktop het bedrijf zorg draagt voor fysieke beveiligingsmaatregelen, zijn deze niet van toepassing op mobiele apparatuur. Door de vorm en het feit dat dit dure technologie is, heeft de apparatuur en daarmee de data die hier op geplaatst wordt een veel grotere kans gestolen te worden.

Veel van de bovengenoemde vectoren kunnen gedeeltelijk gemitigeerd worden door de inzet van MDM software. Deze oplossing is echter niet alles omvattend. Mobiele apparatuur vraagt om een brede aanpak van informatiebeveiliging die kans op misbruik van de mogelijke aanvalsvectoren mitigeert. Daarbij is een aanpak noodzakelijk die zich zowel richt op het apparaat zelf als op de data en op het beleid rondom het gebruik van mobiele apparatuur.

Techniek, organisatie en medewerker

Het implementeren van BYOD in een organisatie heeft gevolgen voor techniek (ICT), organisatie (o.a. procedures) en medewerker. Tijdens de risicoscan voorafgaande aan de implementatie moeten deze gevolgen voor iedereen helder gemaakt zijn.

1. Techniek

De inzet van mobiele apparatuur heeft verscheidene gevolgen voor de techniek. Belangrijke items daarbij zijn:

- *Wireless netwerk*. Eén van de belangrijkste manieren om met mobiele apparatuur te communiceren is het gebruik maken van een draadloos netwerk binnen organisatie. Dit netwerk is soms nog niet aanwezig en zorgt voor additionele risico's met betrekking tot beveiliging van data. Ook wireless capaciteit kan een probleem zijn wanneer veel meer apparatuur dan gebruikelijk wordt aangesloten.
- *Netwerk segmentatie*. Een apart netwerk segment voor BYOD dient ingeregeld te worden om toegang tot bedrijfsmiddelen op een gecontroleerde manier te faciliteren.
- *Access Management en Single Sign-On (SSO)*. Deze oplossingen moeten zorg dragen voor een beveiligde toegang tot data en een naadloze gebruikerservaring. SSO kan verregaande gevolgen hebben indien applicaties geen centrale authenticatie mechanismen gebruiken.
- *Applicatie provisioning*. Onderdeel van de transitie is het zorgdragen voor het aanbieden van bedrijfsapplicaties. Dat is mogelijk door directe toegang of met de inzet van web applicaties, virtual applicaties en server based computing.

2. Organisatie

Fiscaal en juridisch
Het zakelijk gebruik van privé apparaten heeft ook fiscale en juridische consequenties. Als een organisatie overgaat tot een periodieke vergoeding voor het zakelijk gebruik van een privé apparaat wordt dit onder bepaalde voorwaarden gezien als loon. Hiermee heeft dit ook gevolgen voor de medewerker die maandelijks minder netto salaris ontvangt. Een privé apparaat zakelijk gebruiken heeft ook juridische gevolgen: als een privé apparaat kapot gaat tijdens werktijd valt dit juridisch gezien onder de zakelijke verzekeringen. Dit kan financiële gevolgen hebben voor een organisatie. Valt de vergoeding onder de Werkkostenregeling? Wat is dan het te volgen proces? Krijgt een medewerker een nieuw apparaat of een vergoeding ervoor?

ICT afdeling
Door de komst van mobiele apparatuur en BYOD verandert ook de rol van de ICT afdeling. ICT afdelingen gaan beperktere diensten leveren. Bij een traditionele ICT situatie beheert de afdeling ICT standaard apparatuur van een beperkt aantal merken. De beheersprocessen zijn afgestemd op deze standaardisatie. De invoering van BYOD heeft verregaande gevolgen. Het is onmogelijk voor een helpdeskmedewerker kennis te hebben van elk mobiel apparaat. Het moet voor de helpdesk medewerkers duidelijk zijn wanneer ondersteuning kunnen bieden. Voor medewerkers geldt dat zij niet meer voor alle problemen gerelateerd aan ICT middelen terecht kunnen bij de helpdesk. Ook dit zal aanpassingen vereisen in de manier van werken van organisatie.

Procedures
De invoering van mobiele apparatuur zorgt tevens voor aanpassingen aan procedures binnen organisaties. Het belangrijkste doel van deze aanpassingen is een beveiligde omgeving creëren waarin vertrouwelijke bedrijfsgegevens gebruikt kunnen worden. Met dat uitgangspunten moeten procedures opnieuw onder de loep genomen worden. Het resulterende mobiele beleid dient actief uitgedragen te worden zodat de organisatie bekend is met de regelgeving rondom mobiele apparatuur. Het beleid moet duidelijkheid verschaffen omtrent vragen die spelen rondom mobiliteit en BYOD. Voorbeelden van dergelijk vragen zijn:

- Wie komt er in aanmerking voor mobiele apparatuur of Bring/Choose Your Own Device?
- Wat zijn de procedures omtrent verlies of diefstal?
- Als een medewerker een betaalde app wil installeren voor zakelijke doeleinde, wordt dat toegestaan?
- Hoe wordt er omgegaan met licentiebeheer van zakelijke apps?

3. Medewerker

Medewerkers die een privé apparaat zakelijk gaan inzetten, zullen zich moeten conformeren aan de BYOD policy en zich moeten neerleggen bij eventuele gevolgen en beperkingen die deze met zich meebrengt. Medewerkers moeten hiervan vooraf op de hoogte zijn gebracht door bijvoorbeeld het medewerkersreglement.

Privacy

Een van de aspecten die direct met Mobile Security in verband staat is privacy van de medewerker. Indien het privé apparaat zakelijk ingezet wordt geeft de medewerker een deel van zijn mobiele vrijheid en privacy op. Zo kan voor toegang tot de bedrijfsmiddelen software geïnstalleerd worden om het apparaat te beveiligen en op afstand te beheren. Dergelijke software heeft gevolgen voor de privacy van de medewerker in kwestie. De werkgever kan met dergelijke software mogelijk online activiteiten inzien of inzicht krijgen in persoonlijke gegevens op het apparaat. Deze zaken en de gevolgen ervan moeten duidelijk vooraf bekend worden gemaakt aan medewerkers.

Balans tussen werk en privé

Mobiliteit, BYOD, Het Nieuwe werken zijn ontwikkelingen die allemaal één centraal thema raken: de efficiëntere en productievere medewerker. Thuiswerken brengt echter ook risico's mee. Het kan verleidelijk zijn, bijvoorbeeld wanneer achterstand in het werk is opgelopen, om buiten reguliere werktijden te werken. Het is zaak voor managers om tijdig te constateren dat de werk en privé balans verstoord raakt.

Dit document maakt duidelijk dat een overstap naar een organisatie die mobiliteit faciliteert veel aspecten een rol spelen. De Business Technologists van Atos geven door een bewezen risk-based aanpak invulling aan proces, medewerker en technologie rondom mobiliteit. Op deze manier verloopt de transitie naar een Mobile Enterprise op een veilige en gecontroleerde manier.

Voor meer informatie:
Rob van Os **rob.vanos@atos.net**
Mark Kielman **mark.kielman@atos.net**
Rob van der Staaij **rob.vanderstaaij@atos.net**
of bezoek: nl.atos.net