FOREST - IT

INFORMATION SECURITY

Mobile Device Management, een Forest-IT gestructureerde aanpak

Mobiele apparaten zoals smartphones en tablets zijn nu al niet meer weg te denken uit onze samenleving zowel privé als zakelijk. De vraag naar zakelijke toepassing van deze devices neemt onomstotelijk toe. Dit roept de volgende vraag op: hoe gaan we als onderneming hier mee om?

Wordt het inzetten van Mobile Devices een onderdeel van de bedrijfsvoering of verbieden we dit. Is er al een visie omtrent dit onderwerp en indien men het gebruik gaat toepassen, hoe dan?

Vooropgesteld dat de wens er is om Mobile Devices in te gaan zetten zal er een keus moeten worden gemaakt; staan we het gebruik van eigen apparaten toe op de bedrijfsinfrastructuur of worden er bedrijfsapparaten uitgeven.

Immers zou het niet handig zijn als we onze vertrouwde privé gebruikte smartphone of tablet ook op het werk zouden kunnen gebruiken voor mail, social media zoals twitter,en het creëren/ lezen van documenten etc.

Consumerization

Onderzoek heeft aangetoond dat medewerkers productiever zijn als ze bij het gebruik van devices hun eigen favoriete type (consumerization) mogen gebruiken. De een geeft de voorkeur aan een iPhone en/of iPad de ander voor een op android zoals Samsung, of een op windows gebaseerde smartphone en tablet.

Mede door de 24-uurs economie; verconsumentering, virtualisatie, cloud computing en een steeds vager onderscheid tussen werken en privé wordt het eenvoudiger en praktisch voor werknemers om aangesloten te blijven op de bedrijfsomgeving volgens het zgn. "Martini concept": anytime, anyplace, anywhere.

Bijkomend aspect van consumerization is dat dit kostenverlagend kan werken . Uit onderzoek blijkt dat als werknemers mede verantwoordelijk zijn voor het beheer van hun eigen devices, de beheerskosten dalen.

Security

Echter, Mobile Devices zijn geen volwaardige computers en hebben hun beperkingen wanneer het aankomt op beveiliging en toepassingen.

Naast de boven genoemde voordelen kleven er ook een aantal risico's aan het verlenen van de vrije keus en het gebruik daarvan. Risico's zoals data leakage, mixen van privé en zakelijk gebruik en het operationeel managen van dit geheel (voor sommige branches is er zelfs wet en regelgeving omtrent omgang met data).

Risico Management

Idealiter gezien wordt er vanuit de wens een visie gecreeerd waarna een Risico Assessment nodig is om de strategie en beleid te bepalen; Mobile Device Management dus. Wanneer de strategie, het beleid en de aanpak gedefinieerd zijn kan de implementatie uitgevoerd worden.

Onderdeel van het Risico Assessment is het bepalen wie de devices gaan gebruiken, iedereen of alleen medewerkers met een specifieke rol.

Bijvoorbeeld: sommige gebruikers hebben toegang tot gevoelige data. Geef je hen volledig of beperkte toegang tot deze gevoelige data bij het gebruik van een Mobile Device?

Het is belangrijk om de data te classificeren om te kunnen bepalen of welke data toegankelijk gemaakt kan worden vanaf een mobile device, en wat de impact en kosten zijn om de beveiliging te waarborgen. Na deze stap kan er een begin gemaakt worden met het bepalen van het beleid,de strategie en implementatie

Forest-IT heeft veel expertise mbt dit onderwerp neem contact met ons op voor meer informatie.

MDM Risico Assessment template:

The key issue to mobile security is that no single security solution will work, given the nature of the mobile environment. And just extending the existing security infrastructure for mobile smartdevices simply isn't practical. Enterprises must treat mobile security as an independent task, and as an independent task, mobile-usage-specific security policies must be created and implemented. A comprehensive risk analysis of the potential security hazards associated with the use of mobile smartdevices should be the first step along the path of mobile smartdevice security policy creation.

Business Objectives

- Trendsetting
- Functionality
- Dynamic or Static

Mobile Device Management Risk Assessment

User Scenario

- Consumers (C)
- Employees (E)
- High Officials (H)

Classification

The impact of a threat can be determined by the value of the assets affected by the threat. Throughout this report we use the following list of possible affected assets:

- Personal Data
- Corporate intellectual property
- Classified Information
- Financial Assets
- Smartdevice and service availability and functionality
- Personal and political reputation

Components

- iPad
- iPhone
- Android Tablet
- Android Phone
- Windows Tablet
- Windows Phone
- Blackberry phone
- Blackberry Tablet

General Risks

1. Data Leakage
2. Unintentional data disclosure
3. Improper decommissioning
4. Phishing
5. Spyware
6. Network spoofing attacks
7. Surveillance
8. Dialerware
9. Financial malware
- Network congestion
- *Distributed malware attack*
- *Collection of environmental data*

Opportunities

- Sandboxing and capabilities
- Controlled software distribution
- Remote application removal
- Backup and recovery
- Extra authentication and non-repudiation options
- Extra encryption options
- Diversity

Specific Risks

- iPad
- iPhone
- Android Tablet
- Android Phone
- Windows Tablet
- Windows Phone
- Blackberry phone
- Blackberry Tablet

General Controls

1. Data Leakage
2. Unintentional data disclosure
3. Improper decommissioning
4. Phishing
5. Spyware
6. Network spoofing attacks
7. Surveillance
8. Dialerware
9. Financial malware
- Network congestion
- *Distributed malware attack*
- *Collection of environmental data*

Specific Controls

- iPad
- iPhone
- Android Tablet
- Android Phone
- Windows Tablet
- Windows Phone
- Blackberry phone
- Blackberry Tablet