

SEPTEMBER 2016

Fact sheet: Mobile Device Management (MDM)

Definitie:

Mobile device management (MDM) is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.

Source: Wikipedia.org

Ontwikkelingen MDM:

- ☐ Externe en interne klanten vragen om framework voor governance van mobile devices (smartphones / tablets)
- ☐ Bring your own device (BOYD) naar de werkvloer.
- ☐ Het gebruik van mobile devices met corporate data is vrijwel niet te voorkomen.
- ☐ Multi platform ondersteuning required.
- ☐ Een (MDM) governance en control framework staat nog in kinderschoenen.

Top 10 MDM risico's

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

ISACA considerations on controlling and securing mobile devices:

- ☐ **Policy**—A security policy should exist for mobile devices and should include:
 - Rules for appropriate physical and logical handling
 - Controls pertaining to mobile device usage, specifying the type of information, the kind of devices and the type of information services that may be accessible through the devices
- ☐ **Mobile security tools**—Mobile devices should be safeguarded against malicious code by:
 - Scanning apps and other programs/data
 - Regularly updating antivirus software
- ☐ **Encryption**—All data labeled as sensitive should be properly secured while in transit or at rest.
- ☐ **Secure transmission**—The mobile device user should connect to the corporate network via a secure connection, and sensitive information should be adequately protected as per corporate policy.
- ☐ **Device management**—There should be an asset management process in place for tracking mobile devices. It should include procedures for lost and stolen devices and terminated employees,
- ☐ **Access control**—The configuration must include limiting access to sensitive data by disabling data synchronization features that can access shared files or network drives that contain data prohibited for mobile use.
- ☐ **Awareness training**—Ongoing awareness training should be in place to address physical and logical security of mobile devices. This should include identifying types of information being stored on mobile devices.

Top 5 aanbevelingen voor IT auditor:


1. In beeld krijgen van de security risico's & maatregelen vanwege gebruik mobile devices.
2. Bijstellen minimum requirements vanwege gebruik mobile devices.
3. Data classificatie voor MDM toegang en gebruik own devices.
4. Kennis als pijler voor secure governance van mobile devices bij interne of externe klant.
5. MDM governance plaatsen in relatie tot Server en Cloud beveiliging


Key documentation and website links:


References and external links:

- http://en.wikipedia.org/wiki/Mobile_device_management

ISACA:

-  Mobile Devices May Pose Greatest Threat to Confidential Information: New ISACA White Paper:
<http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/Mobile-Devices-May-Pose-Greatest-Threat-to-Confidential-Information-New-ISACA-White-Paper.aspx>

-  Securing Mobile Devices:
<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx>

-  Business Risks and Security Assessment for Mobile Devices:
<http://www.isaca.org/Journal/Past-Issues/2008/Volume-1/Pages/Business-Risks-and-Security-Assessment-for-Mobile-Devices1.aspx>