Konzept: Mobile Security im deutschen Mittelstand

Zum Schutz eines Unternehmens ist bei einem Einsatz vom Mobile Devices darauf zu achten, dass ein geeignetes Sicherheitskonzept besteht. Dieser Herausforderung hat sich die mVISE angenommen und ein ganzheitliches Mobile Security Konzept entwickelt.

1 Worum geht es?

Seit der Nutzung von Mobile Devices (hier: Smartphones und Tablets) hat das Themenfeld Mobile Security immer mehr an Bedeutung gewonnen. Viele Unternehmen stellen sich die Frage, wie sie sich der Herausforderung stellen können, wenn sie Mobile Devices als selbstverständliche Instrumente des modernen Arbeitens ansehen. Durch die Verwendung von Mobile Devices im geschäftlichen Umfeld lassen sich verschiedenste Aufgaben orts- und zeitunabhängig erledigen. Dennoch sind gerade Mobile Devices anderen Gefahren ausgesetzt als herkömmliche Computer. Trotz einer Vielzahl an Sicherheitsmechanismen in den Devices und Diensten, die sie verwenden, existieren unzählige Schwachstellen und Bedrohungen, denen Beachtung geschenkt werden muss. Mobile Devices besitzen unter anderem sensible Daten, wie Kontakt- und Zahlungsinformationen, GPS Koordinaten sowie private und geschäftliche E-Mail Accounts. Wird dem Bereich Mobile Security keine oder nur wenig Beachtung geschenkt, so kann es zu erheblichen Schäden bei den Unternehmen kommen.

2 Was sind die Herausforderungen?

Unternehmen investieren viel in den Schutz ihrer IT-Systeme, lassen allerdings ihre Mobile Devices außer Acht. Eine mögliche Ursache hierfür liefert ein mangelndes Verständnis sicherheitsrelevanter Fragestellungen, die besonders Angreifern vielfältige Angriffsvektoren liefern[1]. Die Sicherheitsexperten der mVISE haben sich der Fragestellung angenommen, welche Maßnahmen benötigt werden, um einen umfassenden Schutz der Mobile Devices aus Unternehmenssicht zu gewährleisten. Letztendlich sollte als Ergebnis ein Konzept herauskommen, welches das Thema Mobile Security in verschiedenen Bereichen aufnimmt und somit einen umfassenden Schutz bietet. Da es dafür allerdings keinen allgemeingültigen Lösungsweg gibt, musste überlegt werden, welche Bereiche für ein ganzheitliches Mobile Security Konzept in Betracht kommen könnten.

3 Welchen Bereichen sollte Beachtung geschenkt werden?

Im Folgenden werden die verschiedenen Bereiche Vorgestellt, denen aufgrund des Mobile Security Konzeptes Beachtung geschenkt werden sollte.

3.1 Technische Sichtweise

Für die technische Überwachung der Mobile Devices und zum Schutz des Unternehmens bedarf es verschiedenster technischer Komponenten. Zu diesen zählen zum einen EMM-Systeme (Enterprise Mobility Management), welche die Administration der Devices und einen sicheren Umgang mit diesen ermöglichen soll und zum anderen MTD-Systeme (Mobile Threat Defense) welche zu einem

[1] Vgl. BSI (2012), S. 11.

mVISE AG | Wanheimer Straße 66 | 40472 Düsseldorf | security@mvise.de | +49 211 781 780 0 | www.mvise.de

proaktiven Schutz der Devices und somit des Unternehmens beitragen.

Die Kernkomponenten des EMM-Systems bestehen dabei aus den drei folgenden Systemen:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Mobile Information Management (MIM)

Mit diesen lassen sich unter anderen die Anwendungen auf den Devices verwalten sowie die Informationen, die diese Geräte tagtäglich verarbeiten. Ein Schutz der Unternehmensdaten kann durch diese Systeme allerdings nur bedingt gewährleistet werden, da diese Systeme primär für die Verwaltung von Mobile Devices ausgelegt sind.

> Tipp:
>
> MTD-Systeme lassen sich problemlos in EMM-Systeme verschiedenster Hersteller integrieren.

Einen anderen Ansatz strebt ein MTD-System (Mobile Threat Defense) an. Es verflogt eine proaktive Vorgehensweise zum Schutz des Device und den Unternehmensdaten. Gartner definiert MTD in seinem Market Guide for Mobile Threat Defense Solutions als technische Lösung, die einen oder mehrere Teile der nachfolgenden Gliederungspunkte beinhaltet[2]:

- Device Behavioral Anomalies
- Vulnerability Assessments
- Network Security
- App Scans

Durch die Verwendung von Crowdsourced Threat Intelligence, einem cloudbasierten Dienst, kann auf Bedrohungen reagiert werden, bevor diese zu einer Gefahr für das Unternehmen werden. Neben den von Gartner genannten Kernkomponenten finden sich weitere, die ein solches System unbedingt beinhalten sollte[3]:

- Mobile Threat Prediction
- Mobile Threat Detection
- Mobile Threat Prevention

3.2 Organisatorische Sichtweise

Richtlinien und Maßnahmen bilden ein Regelwerk zur Schaffung von Informationssicherheit. Anerkannte Standards wie ISO27001 oder BSI IT-Grundschutz setzen diese voraus. Grundsätzlich muss bei einer Richtlinie allerdings beachtet werden, dass es keine allgemeingültige Richtlinie für ein Unternehmen gibt, die es in der Zukunft nicht weiterzuentwickeln gilt. Vielmehr bedarf es einem Prozess der stetigen Verbesserung, um eine Richtlinie und somit das Unternehmen vor bestehenden und neuen Gefahren zu schützen.

> Tipp:
>
> KVP-Mechanismen für eine ständige und nachhaltige Verbesserung der Mobile Security Richtlinie.

Aus diversen, frei zugänglichen Richtlinien vom BSI oder dem SANS-Institut gehen verschiedene Schutzbereiche hervor, die in einer Mobile Security Richtlinie Anwendung finden sollten. Zu diesen gehören unter andrem:

- Netzwerksicherheit
- Gerätesicherheit
- Datensicherheit

3.3 Schulung und Sensibilisierung

Zur Schaffung und Aufrechterhaltung eines Sicherheitsbewusstseins für die IT ist es zwingend notwendig, die Mitarbeiter in regelmäßigen Abständen zum Thema IT-Sicherheit zu sensibilisieren

[2] Vgl. Girad/Zumerle (2016).

[3] Vgl. Check Point (2017).

und zu schulen. Dabei bedarf es einen Verantwortlichen für die Konzeption und Umsetzung eines Schulungs- und Sensibilisierungsprogramms innerhalb des Unternehmens. Allgemein wird der Prozess einer Konzeption eines solchen Programms durch die Unternehmensführung, dem IT-Sicherheitsbeauftragten oder dem Personalleiter angestoßen. Auslöser sind meist neue Vorgaben. Aufgrund dessen, dass der Mitarbeiter als Schlüsselfaktor eines jeden Unternehmens anzusehen ist und sprichwörtlich eine Kette nur so stark wie das schwächste Glied ist, wird grundsätzlich empfohlen Schulungs- und Sensibilisierungsprogrammen regelmäßig durchzuführen. Generell tragen Mitarbeiter zum Unternehmenserfolg und dessen Schutz bei, indem sie Richtlinien und Vorgaben einhalten sowie die IT-Sicherheit von Systemen sicherstellen. Durch Unkenntnis oder auch Vorsatz können durch Mitarbeiter sicherheitsrelevante Fehler verursacht werden. Aus diesem Grund sollte sich jedes Unternehmen das Ziel setzen, IT-Sicherheit an alle Mitarbeiter zu vermitteln. Dies hat eine besondere Bedeutung für den Fortbestand des Unternehmens. Gleichzeitig sollte IT-Sicherheit bei allen Mitarbeitern ein fester Bestandteil im Arbeitsalltag werden. Dazu müssen diese Regelungen und Maßnahmen einhalten. Dies kann allerdings nur dadurch erreicht werden, indem die Mitarbeiter kontinuierlich geschult und sensibilisiert werden. Möglich ist dies bspw. durch Schulungseinheiten oder Kampagnen[4]. Zu empfehlen ist, den Schulungs- und Sensibilisierungsprozess fest im Unternehmen zu etablieren. Gleichzeitig ist darauf zu achten, dass IT-Sicherheit von der obersten Organisationsebene akzeptiert wird, da diese nicht immer auf Akzeptanz unter den Mitarbeitern stößt. Das Management sollte IT-Sicherheit unterstützen und fördern sowie die dafür notwendigen Ressourcen zur Planung, Umsetzung und Weiterentwicklung bereitstellen. Wird all diesen Aspekten Beachtung geschenkt, kann ein Schulungs- und Sensibilisierungsprogramm nach bestimmten Kriterien entwickelt werden.

Hinweis:

EMM und MTD bilden die technische Basis für ein funktionierendes Mobile Security Konzept.

4 Zusammenspiel von EMM und MTD

EMM-Lösungen konzentrieren sich auf die unternehmensinterne Verwaltung von Mobile Devices und schaffen zum Teil eine gewisse Basissicherheit. Diese Sicherheit bezieht sich darauf, dass die Geräte vor unautorisierten Zugriffen geschützt werden, dass Unternehmensdaten aufgrund von einem physischen Verlust des Gerätes nicht in die falschen Hände geraten, dass vermeintlich unsichere Apps nicht auf den Geräten installiert werden und dass der Datenverkehr bzw. der Informationsaustausch mit Geschäftsdaten geregelt werden kann[5]. All diese Funktionen bieten aber keinen umfassenden Schutz im Hinblick auf Risikominimierung und Bedrohungsabwehr vor Angreifern. Aus diesem Grund und dem Funktionsumfang diverser MTD-Systeme lässt sich annehmen, dass EMM im Zusammenspiel mit einer MTD-Lösung einen umfassenden technischen Lösungsansatz für Mobile Security bietet. Dies bestätigt unter anderem der Security Spezialist Check Point in seinem Blog.

[4] Vgl. BSI (2014).

[5] Vgl. Kohne u. a. (2015), S. 72 ff.

5 Was bietet die mVISE AG an?

Neue mobile Prozesse sowie neuartige Bedrohungen für Mobile Devices zeigen, dass ein statisches Regelwerk, wie es ein EMM bietet, nicht ausreicht, um sich umfassend vor Bedrohungen zu schützen. Es bedarf vielmehr einem ganzheitlichen Lösungsansatz bestehend aus technischen und organisatorischen Komponenten sowie eine strikte Weiterbildung der Mitarbeiter in Themen der IT-Sicherheit.

Die mVISE AG berät, unterstützt und setzt um! Bei den Herausforderungen des Schutzes Ihres Unternehmens unterstützen wir Sie im vollen Umfang. Unsere IT Security Experten haben in den letzten Jahren im Bereich Mobile Security umfassende Erfahrungen und Erkenntnisse aus vielen verschiedenen IT Umfeldern sammeln können.

6 Ausblick

Sicherheitsvorfälle ausgelöst durch Mobile Devices führen zu immer höheren finanziellen Schäden in kleinen und mittelständischen Unternehmen. Dies zeigt, dass es besonders wichtig ist, bestehende Sicherheitskonzepte zu überarbeiten und besonders im Bereich der Mobile Security neue Konzepte einzuführen. Gerade kleine und mittelständische Unternehmen sind laut einer IDC Studie davon überzeugt, dass die Sicherheitsvorkehrungen in Mobile Devices ausreichend sind. Die Anzahl an steigenden Sicherheitsvorfällen beweist allerdings das Gegenteil.

Für die Zukunft empfehlen wir, Konzepte speziell für die Sicherheit von Mobile Devices zu entwickeln und umzusetzen. Nur dadurch kann ein ganzheitlicher Schutz des Unternehmens gewährleistet werden.

Über den Autor

Sebastian Werner arbeitet als Consultant bei der mVISE AG. Zu seinen Kernkompetenzen zählt unter anderen die Entwicklung moderner Sicherheitskonzepte.

7 Referenzen

BSI (2012): Leitfaden Informationssicherheit: IT-Grundschutz kompakt, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

BSI (2014): M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02312.html

Check Point (2017): Check Point Blog, https://blog.checkpoint.com/

Girard, J./Zumerle, D. (2016): Market Guide for Mobile Threat Defense Solutions, http://techorchard.com/wp-content/uploads/2016/11/market_guide_for_mobile_threat-prevention.pdf

Kohne, A./Ringleb, S./Yücel, C. (2015): Bring Your Own Device: Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten, 1. Aufl., Wiesbaden 2015.

Sebastian Werner

Consultant bei der mVISE AG
Mail: sebastian.werner@mvise.de
Mobil: +49 152 03495297