ZEBRA

KONZIPIERUNG EINER ROBUSTEN MOBILEN SICHERHEITSRICHTLINIE: die Hauptrisiken und wie Unternehmen sie vermeiden können.

Die IT-Sicherheit für Mobilgeräte wird oft mit einer Versicherung verglichen. Etwas, das man einplanen muss für den Fall der Fälle. Doch diese begrenzte Sichtweise geht am eigentlichen Punkt vorbei. Sicherheit bietet mehr als nur eine Maßnahme beim Eintreten eines bestimmten Ereignisses. Sie kann auch als Versprechen angesehen werden – sie erlaubt Ihrem Unternehmen, ohne Gefahr von Sicherheitsverletzungen seinen Geschäften nachzugehen und innovativ zu sein.

In diesem White Paper werden die wichtigsten Faktoren bei der Entwicklung einer robusten Richtlinie zur mobilen Sicherheit beleuchtet. Es werden die Hauptrisiken gezeigt und was Sie dagegen tun können, damit Sie die neuen Gelegenheiten nutzen können, um die Produktivität, Effizienz und Genauigkeit unternehmensweit zu verbessern.

Kein Universalansatz

Es gibt unterschiedliche Meinungen zum Nutzen von Sicherheit. Worüber sich jedoch alle einig sind, ist, dass es sich hierbei um ein komplexes Thema handelt, das viele Bereiche des Unternehmens betrifft. Wenn man sich die Vielfalt der Mobilitätsnutzungsfälle, Anwendungsmethodiken und Implementierungsoptionen individueller Unternehmen betrachtet, wird der Gesamtnutzen von Sicherheit sowie deren Komplexität offensichtlicher.

In einem Einzelhandelsgeschäft können mit Tablet-PCs ausgerüstete Mitarbeiter Kunden schnell bedienen. Aber diese Kunden wollen eine Zusicherung, dass die privaten Informationen, die sie preisgeben, auf diesen Geräten auch geschützt sind. Bei der Fertigung ist ein Wachstum bei Wearable-Technologien zu verzeichnen. Dieser Wandel erfordert, dass der Datenfluss von einer großen Anzahl von Endpunkten geschützt werden muss.

Anwendungsmethodiken hängen ebenfalls vom jeweiligen Nutzungsfall und Gerätetyp ab. Von Web-basierten Apps bis hin zu nativen mobilen Apps oder sogar Mischformen – sie alle stellen einzigartige Sicherheitsanforderungen an das Unternehmen dar.

Die verfügbaren Mobil-Implementierungsoptionen können für noch mehr Komplexität sorgen. Falls im Unternehmen ein BYOD-Programm (Bring Your Own Device) oder Endverbrauchertechnologie genutzt wird, muss das IT-Team unter Umständen zusätzliche Mitarbeiter einsetzen. Diese müssen interne Sicherheitslösungen entwickeln, wenn Endverbraucher-Betriebssysteme für Mobilgeräte nicht den erforderlichen Grad an Sicherheit bieten. Es müssen auch weitere Überlegungen angestellt werden, wenn es um den Schutz von Netzwerkaktivitäten und die Sicherheit von WAN- oder WLAN-Verbindungen geht.

Mobilitätsplattformen müssen alle dieser Sicherheitsaspekte berücksichtigen und gleichzeitig den Anspruch des Unternehmens an die mobile IT erfüllen. Das Ziel eines jeden Unternehmens sollte darin bestehen, die Datensicherheit zu wahren, ohne dabei die täglichen betrieblichen Abläufe zu beeinträchtigen. Was sind die Hauptbedrohungen und welche Faktoren sollte eine robuste Richtlinie zur mobilen Sicherheit abdecken?

ES IST EIN WACHSTUM BEI WEARABLE-TECHNOLOGIEN ZU VERZEICHNEN.

Dieser Wandel erfordert, dass der Datenfluss von einer großen Anzahl von Endpunkten geschützt werden muss.

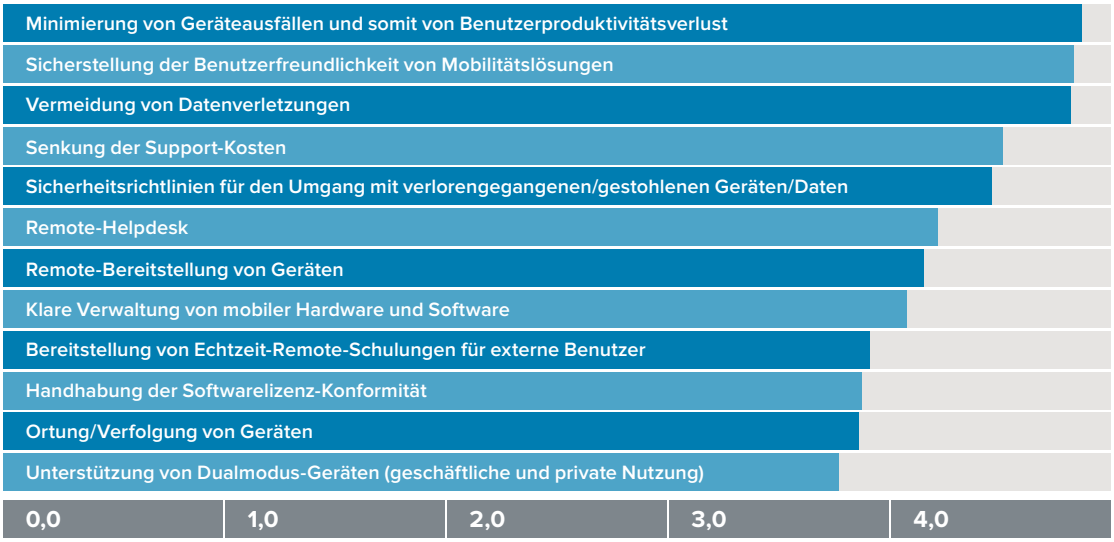
Erkennung der Risiken

Aufgrund ihrer grundlegenden Merkmale sind Mobilgeräte für wesentlich mehr Sicherheitsbedrohungen anfällig als Desktop-Systeme. Wegen ihrer geringen Größe und Portabilität können sie leicht gestohlen werden. Mehrzweck-Betriebssysteme und -Anwendungen können Cyber-Kriminellen mehrere Angriffsflächen bieten, wenn sie nicht berücksichtigt werden. Zudem reduziert die Kommunikation über offene und ungeschützte WLANs oder Mobilfunknetze zusätzlich den Schutz von Unternehmens- oder Kundendaten, was weitere Überlegungen hinsichtlich der Kontrolle des Zugangs auf ungeschützte Netzwerke erfordert.

Laut der Branchenanalysten von VDC ist die Verhinderung von Verletzungen der Datensicherheit eine der drei wichtigsten Investitionsvorhaben von Unternehmen, wenn es um Mobilität geht. Über Sicherheitsrichtlinien zu verfügen, wenn es zu einem verlorengegangenen oder gestohlenen Gerät gekommen ist, gehört zu den wichtigsten fünf Vorhaben – hinter der Minimierung von Ausfallzeiten, der Gewährleistung von Benutzerfreundlichkeit und der Reduzierung von Support-Kosten. [1]

Bewerten Sie die folgenden Mobilitätsprobleme gemäß ihrer Bedeutung für Ihr Unternehmen

(1 = extrem unwichtig; 6 = extrem wichtig)



[1] *„Total Cost of Ownership Models - Enterprise and Government Mobility Applications“, VDC Research, Josh Martin, David Krebs*

Und dies sind auch keine allzu simplen Risiken. Wenn man die übergreifenden Sicherheitsbedenken näher betrachtet, findet man sowohl interne als auch externe Bedrohungen. Die Studie von VDC Research wird von einer Umfrage von TechTarget SearchSecurity zu den fünf wichtigsten mobilen Sicherheitsproblemen in Unternehmen bekräftigt.[1] Jedes der großen Probleme, die von den 487 Teilnehmern genannt wurden, hatte mit Firmendaten zu tun.

1. Geräteverlust – z. B. das Vergessen eines Firmen-Tablet-PCs oder -Smartphones in einem Taxi oder Restaurant
2. Anwendungssicherheit – z. B. Daten, die für Entwickler von freien mobilen Apps zugänglich gemacht werden
3. Gerätedatenlücke – z. B. das Risiko, dass Cyber-Kriminelle Zugriff auf Firmenanwendungen erhalten, die auf privaten Geräten ausgeführt werden
4. Malware-Angriffe – z. B. Trojaner, Überwachungstools oder schadhafte Anwendungen
5. Gerätediebstahl – z. B. verbreitete Daten nach dem Diebstahl eines Premiumgeräts

Es stehen der Ruf und der Umsatz des Unternehmens auf dem Spiel. In einem Artikel auf CIO.com heißt es:[2] *„Je intensiver Mitarbeiter und Vertragspartner Mobilgeräte verwenden, um auf Anwendungen und Daten zuzugreifen, umso wichtiger ist es, diesen Zugang zu schützen. Außerdem muss verhindert werden, dass die Mobilgeräte, die eigentlich die Produktivität und den geschäftlichen Erfolg steigern sollen, unautorisiert auf Informationen und andere Ressourcen zugreifen, da dies gefährlich ist und den Umsatz reduzieren könnte.“*

Es bleibt die Frage: Welche Maßnahme kann Ihr Unternehmen ergreifen, um mit der fortwährenden Bedrohung der mobilen Unternehmenssicherheit umzugehen?

[1] *Top 5 enterprise mobile security issues, TechTarget, 2012*

[2] *http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html*

Bekämpfung der Bedrohung

Bei der zunehmenden Abhängigkeit von mobilen Technologien müssen Unternehmen nach einer flüssigeren Reaktion auf Sicherheitsprobleme suchen. Analysen von Gartner, Forrester und Information Week zeigen einige der wichtigen Maßnahmen, die IT-Abteilungen als Reaktion auf interne und externe Risiken ergreifen können.

Forrester empfiehlt auch die folgenden sieben Maßnahmen für das Mobilgerätemanagement (MDM) und die mobile Sicherheit:

- PIN-Pflicht (starke Kennwörter)
- Selektive Rücksetzmöglichkeit (unabdingbar für ein BYOD-Programm)
- Jailbreak/Root-Erkennung
- Datenverschlüsselung
- Virtuelle private Netzwerke (VPNs)
- Schutz vor Datenlecks (um zu verhindern, dass unautorisierte Benutzer aus Unbedachtheit oder absichtlich Daten freigeben)
- ActiveSync-Gerätebeschränkung

Diese Maßnahmen sind lediglich „Wunschlisten“ der IT-Abteilung, wenn das Unternehmen nicht willens ist, die mobile Sicherheit ernst zu nehmen. Führungskräfte spielen eine wichtige Rolle, wenn es darum geht, die Sicherheit zu einem Thema auf der Vorstandsebene zu machen und Ressourcen zur Bekämpfung der zunehmend raffinierteren Bedrohungen einzusetzen.

Um effektiv vorzugehen, zahlt es sich aus, die meist verbreiteten Vorschriften und internationalen Best Practices hinsichtlich Sicherheit zu kennen. Ein kurzer Überblick über diese Standards zeigt die Maßnahmen, die jedes Unternehmen in seiner Richtlinie zur mobilen Sicherheit aufnehmen sollte:

- Schutz bei verlorengegangenen oder gestohlenen Geräten
- Schutz von Daten, die übertragen werden
- Schutz von gespeicherten Daten
- Mobiles Anwendungsmanagement
- Sicherstellung der Einhaltung von Vorschriften
- Gerätekontrolle, -verwaltung und -überwachung
- Hoher Datenschutz
- Minimierung der Administrationskosten zur Pflege sicherer Plattformen
- Bereitstellung von starken Authentifizierungs-/Zugangskontrollen
- Maximierung der Verwendung bestehender IT-Infrastruktur

Das Unternehmen muss darauf aufbauend eine Mobilitätsrichtlinie entwickeln, die diese Sicherheitsmaßnahmen beinhaltet. Neben Nutzungsfallszenarios sollte die Sicherheit bei der Geräte- und Betriebssystemwahl eine ebenso große Rolle spielen.

SICHERHEITSMANAGEMENT-FUNKTIONEN[3]
Automatisches Enrollment und Gerätebereitstellung
Kennwortpflicht
Geräterücksetzung, Remote-Sperrung
Anwendungs- und Benutzerkonten-Audit-Fähigkeiten
Jailbreak-Erkennung
Datenschutzfunktionen
Anwendungskontrollen
Mobile NAC
AV, Anti-Spam, Endpunkt-FW und Endpunkt-IDS
Gerätebasierte Zertifikate
Aktive Überwachung der oben genannten Schutzmaßnahmen
Firmen-VPN
Schlüssel- und Zertifikatverwaltung

[3]Quellen: Bericht von Information Week, November 2011; Bericht von Forrester, Antworten auf die wichtigsten Fragen zur mobilen Sicherheit, 2011; Bericht von Gartner, MCM_MQ April 2011.

Die Kosten bei falschen Entscheidungen hinsichtlich Mobilität

„277 Millionen Mobilgeräte, die bis zum Jahr 2016 über eine Schutzmaßnahme verfügen.“

Unternehmen, die von niedrigen Einstiegspreisen angelockt werden, sollten aufgrund der starken Verbreitung von Sicherheitsrisiken die Nutzung von Endverbrauchergeräten von der Stange überdenken. Die meisten Endverbraucher-Betriebssysteme auf diesen Geräten verfügen nicht über alle Sicherheitsfunktionen, die Unternehmen benötigen. Studien zeigen, dass die Gesamtbetriebskosten (TCO) bei der Verwendung von Endverbrauchergeräten für Unternehmensanwendungen zwischen 40 % und 78 % höher liegen können als bei speziellen Unternehmensgeräten.[3] Das Thema Sicherheit ist hierbei ein entscheidender Faktor.

Endverbrauchergeräte, die für Unternehmensanwendungen verwendet werden, sind eine Einladung für Angriffe. In einer BYOD-Studie von Decisive Analytics[4] berichtete fast die Hälfte (46,5 %) der untersuchten Unternehmen von einer Daten- oder Sicherheitsverletzung aufgrund eines Mitarbeitergeräts, das das Firmennetzwerk nutzte. Es werden signifikante Investitionen getätigt, um dieser Bedrohung entgegenzutreten. Doch es gibt keinerlei Garantie dafür, dass diese Sicherheitsnotbehelfe auch bei zukünftigen Bedrohungen wirksam sein werden.

Spezielle robuste Unternehmensgeräte hingegen werden dafür konzipiert und erweitert, um die Einhaltung wichtiger Sicherheitsvorschriften zu erfüllen und zu vereinfachen. Der Umfang der Sicherheits-Compliance kann äußerst breit (z. B. Benutzerschulungen) und sehr detailliert (z. B. die Validierung der Integrität kryptografischer Algorithmen) sein.

Kein Gerät und keine mobile OS-Plattform kann unabhängig Compliance gewährleisten. Doch der Kauf von Geräten und Softwareplattformen von einem Hersteller, der sich auf Sicherheitsmerkmale konzentriert, steigert die Wahrscheinlichkeit einer Compliance und reduziert den administrativen Validierungsaufwand. Dies wiederum verringert Audit-Kosten, kann Strafgebühren verhindern und macht möglicherweise Datenverletzungen hinfällig. All das wirkt sich positiv auf den Unternehmenserfolg aus.

3 „Total Cost of Ownership Models - Enterprise and Government Mobility Applications“, Josh Martin & David Krebs, VDC Research; „A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices“, Jack Gold, Gold Associates

[4] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Betriebssystem- und App-Sicherheit im Fokus: Android

Unternehmen, die Endverbrauchergeräte in Betracht ziehen, stehen mehrere große Namen zur Auswahl: Google, Apple und Microsoft. Die Android-Plattform von Google hat den größten Marktanteil (81 % des globalen Marktes 2015)[5]. Aufgrund ihrer Sicherheitsmerkmale ist sie zudem attraktiv für Unternehmen, die die Nutzung von Endverbrauchergeräten in Betracht ziehen. Das gilt insbesondere im Vergleich zu alternativen Endverbraucher-Betriebssystemen. Anwendungs-Sandboxing, Berechtigungen für Ressourcenzugriff und Datenverschlüsselung sind nur einige der Beispiele der starken Sicherheitsmerkmale von Android.

Die meisten Bedenken hinsichtlich der Sicherheit von Android haben mit potenzieller Malware in Google Play – dem App-Store der Plattform – zu tun. Apple überwacht seine App Store-Apps gründlich, da es eine strenge Kontrolle über den Signierungsprozess hat. Trotzdem betrifft das Sicherheitsrisiko bei Google Play auch alle anderen öffentlichen App-Stores. Jeder ist anfällig für Malware und Sicherheitsverletzungen (sogar der App Store von Apple).

Die beste Vorgehensweise zur Nutzung von Geräten, die für Unternehmen sicher sind, ist die Bereitstellung einer Anwendungssperre und/oder die Verwendung eines vertrauenswürdigen Unternehmens-App-Store. Mobility Extensions (Mx) von Zebra bietet einen besseren Schutz. Durch die Vereinfachung der Einhaltung von Mobilitätsanforderungen und Vorschriften können Unternehmen auf Endverbrauchergeräten einen Sicherheitsgrad der Unternehmensklasse erhalten.

Im Verbindung mit einem Unternehmens-App-Store gewährleisten Erweiterungen, die Whitelisting, AD/LDAP-Authentifizierung, Schlüsselverwaltung und andere wichtige Sicherheitsfunktionen für Unternehmen umfassen, dass IT-Abteilungen unbesorgt Endverbrauchergeräte ausgeben können.

[5] http://www.idc.com/getdoc.jsp?containerId=prUS40664915

Es liegt auf der Hand, dass es bei der Gewährleistung der mobilen Sicherheit um mehr geht als nur um die Integrität des Unternehmens für den Fall, dass es bei Daten und Geräten zu einem Sicherheitsvorfall kommt. Es geht auch um die Unterstützung individueller betrieblicher Anforderungen in Bezug auf die mobile Strategie und die Reduzierung der Gesamtbetriebskosten bei Mobilitäts-Rollouts im ganzen Unternehmen. Mobile Sicherheit wird vor allen Dingen weiterhin evolutionär sein und hohe Achtsamkeit, ständige Prüfungen und Aktualisierungen erfordern.

Während sich die Unternehmensmobilität in wenigen Jahren stark weiterentwickelt hat, ist die Sicherheitslandschaft nicht mehr wiederzuerkennen (und verändert sich weiter). Die Herausforderungen sind komplex und die Lösungen weitreichend. Sie sollten einzeln und in Verbindung mit den Prioritäten des Unternehmens untersucht werden. Es ist nicht sinnvoll, über eine strenge Sicherheitsrichtlinie zu verfügen, wenn diese den Betrieb einschränkt und Sie wettbewerbsunfähig und Ihre Mitarbeiter unproduktiv macht. Auf der anderen Seite ist man anfällig für Angriffe, wenn man sich überhaupt nicht um Sicherheit kümmert. Die robustesten Richtlinien zur mobilen Sicherheit mindern Ihre Risiken und lähmen dabei nicht den Betrieb und Innovationen.

Es ist wichtig, eine Balance unter den Prioritäten Ihrer Richtlinie zur mobilen Sicherheit zu erreichen – damit Sie mit individuellen Teilrichtlinien für unterschiedliche Nutzungsfälle Ihre wichtigen geschäftlichen Anforderungen und die Bedürfnisse der Endbenutzer unter einen Hut bringen.

Eine nützliche Checkliste

Angesichts der Komplexität und Anzahl wichtiger Faktoren, die berücksichtigt werden müssen, kann die Entwicklung einer Mitarbeiterrichtlinie zur mobilen Sicherheit ein schwieriges Unterfangen sein. Diese Checkliste soll Ihnen dabei helfen sicherzustellen, dass die Wahl, die Sie treffen, unternehmensweit erfolgreich sein wird – insbesondere hinsichtlich der Balance der Anforderungen von Benutzern, dem Unternehmen und der Sicherheit.

1 **Informieren Sie alle:**
Sorgen Sie dafür, dass jeder über Sicherheitsbedrohungen Bescheid weiß, und erstellen Sie eindeutige Nutzungsrichtlinien, die erklären, was erwartet wird.

2 **Ändern Sie Kennwörter regelmäßig:**
Kennwörter sollten mindestens alle 30 Tage aktualisiert werden, und Sie sollten die Implementierung obligatorischer Kennwortänderungen (inklusive Kriterien zur Kennwortstärke) in Ihren Anwendungen in Erwägung ziehen.

3 **Schaffen Sie komplette Transparenz bei allen Geräten:**
Verwenden Sie Mobilgerätemanagement-Tools, um verlorengegangene oder gestohlene Geräte umgehend zu orten und im Bedarfsfall das Gerät unbrauchbar zu machen oder zurückzusetzen. Setzen Sie Nutzungsüberwachung und Warnhinweise ein, um zu wissen, wo sich jedes Gerät befindet und wie es gerade genutzt wird.

4 **Erstellen Sie eine Whitelist:**
Stellen Sie sicher, dass Personen nur Zugriff auf eine Whitelist mit Websites haben – diejenigen, die Sie für die Nutzung auf Ihren Geräten genehmigen.

5 **Sorgen Sie für Schutz gegen Malware:**
Indem Sie interne Apps und Anwendungsquellen auf Ihren Geräten auf eine Whitelist setzen, können Sie sich vor einer Infizierung schützen. Und indem Sie zusätzlich kontrollieren, dass das Gerät Anwendungen nicht auf eine andere Art erhält (z. B. über eine externe Verbindung oder eine Speicherkarte), können Sie sich noch besser gegen Malware und schadhafte Anwendungen schützen.

6 **Aktualisieren Sie Ihre Geräte:**
Stellen Sie mithilfe kontrollierter und/oder automatisierter Updates sicher, dass Ihre Geräte stets die neueste Software nutzen.

7 **Bringen Sie Daten in unterschiedlichen Bereichen unter:**
Konfigurieren Sie Ihre Geräte so, dass die Daten in separaten verschlüsselten Bereichen untergebracht sind, damit es Angreifern praktisch unmöglich gemacht wird, darauf zuzugreifen.

8 **Implementieren Sie eine vollständige Verschlüsselung:**
Wo Personen mit hochsensiblen Daten arbeiten, können Sie die Daten, die sich auf Geräten befinden, und diejenigen, die über kabellose Netzwerke gesendet werden, verschlüsseln.

9 **Verwenden Sie einen Unternehmens-App-Store:**
Zugriff auf öffentliche App-Stores sollte vermieden werden. Stattdessen sollen Anwendungen von einem vertrauenswürdigen Unternehmens-App-Store heruntergeladen werden.

10 **Beurteilen Sie den Sicherheitsgrad stets neu:**
Für Mobilitätssicherheit zu sorgen, ist keine einmalige Angelegenheit – es ist von größter Bedeutung, die eigenen Strategien und Best Practices stets zu erneuern, um mit den sich weiterentwickelnden Bedrohungen zurecht zu kommen.

ERFAHREN SIE, WARUM DIE SICHERHEIT NUR DER ANFANG IST, WENN SIE EIN NEUES MOBILES OS WÄHLEN.

ENTDECKEN SIE DIE ANDEREN WICHTIGEN FAKTOREN AUF
WWW.ZEBRA.COM/MOBILITYREVOLUTION

Zentrale Nordamerika und Unternehmenszentrale
+1 800 423 0442
inquiry4@zebra.com

Zentrale Asien-Pazifik
+65 6858 0722
contact.apac@zebra.com

Zentrale EMEA
zebra.com/locations
mseurope@zebra.com

Zentrale Lateinamerika
+1 847 955 2283
la.contactme@zebra.com