10 Schritte für die Sicherheit in einer BYOD-Umgebung

Leitfaden für bewährte Praktiken

Whitepaper

Highlights

1. **Bildung eines Komitees**
2. **Zusammentragen der Daten**
3. **Identifikation und Priorisierung von Anwendungsfällen auf der Grundlage einer Belegschaftsanalyse**
4. **Erstellung eines Wirtschaftsmodells**
5. **Formulierung von Richtlinien**
6. **Schutz für das Netzwerk**
7. **Schutz für die Daten**
8. **Erstellung eines Projektplans**
9. **Bewertung der Lösungen**
10. **Implementieren der Lösungen**

Eine kürzlich durchgeführte Marktstudie ergab, dass momentan 95 % der Unternehmen in den USA Mitarbeitern erlauben, ihre eigenen Geräte zu benutzen.

ForeScout

Überblick

Mobilgeräte wie Smartphones und Tablets gehören heutzutage zum Arbeitsplatz dazu und sind schnell zu einem unentbehrlichen Werkzeug der Mitarbeiter geworden. Eine kürzlich durchgeführte Marktstudie ergab, dass momentan 95 % der Unternehmen in den USA Mitarbeitern erlauben, ihre eigenen Geräte zu benutzen. Viele gehen sogar noch weiter und verlangen, dass Mitarbeiter ihre eigenen Mobilgeräte kaufen. IT-Abteilungen mussten deshalb auf den durch Manager, andere Geschäftsbereiche und Mitarbeiter ausgeübten Druck reagieren und sogenannte BYOD-Umgebungen (Bring your own device) weitgehend unterstützen.

Während BYOD zweifellos Vorteile bietet – gesteigerte Produktivität, schnellere Entscheidungsfindung, höhere Arbeitszufriedenheit und eine attraktivere und flexiblere Arbeitsumgebung – gibt es mit BYOD assoziierte Sicherheitsrisiken, die von IT-Abteilungen behoben werden müssen. Marktforschungsergebnissen zufolge sind die drei größten Bedenken von IT-Abteilungen bezüglich BYOD Netzwerksicherheit, Datensicherheit und Gerätesicherheit. Obwohl Kosten gespart werden, da Firmen weniger Geräte kaufen müssen, erfordern BYOD-Umgebungen zusätzliche Investitionen für IT-Infrastruktur und Management-Software, sowie die Entwicklung von Richtlinien und Verfahren zur effektiven Verwaltung und Sicherung persönlicher Geräte.

Im Folgenden werden die wichtigsten Schritte beschrieben, die ein Unternehmen durchführen sollte, um ein erfolgreiches BYOD-Programm zu implementieren – eines, das die passenden Richtlinien und Sicherheitsmaßnahmen zum Schutz von Daten und Netzwerk umfasst.

Die 10 Schritte

1. Bildung eines Komitees

Um erfolgreich zu sein, muss ein BYOD-Programm die Anforderungen mehrerer Mitarbeitergruppen erfüllen. Ein Team, das Mitglieder aus verschiedenen IT-Bereichen wie Sicherheit, Netzwerk, Endpunkte und Anwendungen, sowie eine repräsentative Auswahl von Anwendern aus verschiedenen Geschäftsbereichen umfasst, ist empfehlenswert. Es ist wichtig zu entscheiden, wer für den Gesamterfolg des BYOD-Programms verantwortlich ist. Die BYOD-Richtlinien sollten eine Vereinbarung zwischen Mitarbeitern und dem Management der Geschäftseinheit darstellen, mit zusätzlichem Input durch die Personalabteilung. Die Rolle der IT-Abteilung sollte sich auf die Implementierung und Durchsetzung der IT-Kontrollen zur Unterstützung dieser Richtlinien beschränken.

2. Zusammentragen der Daten

Dokumentation des Status Quo. Prüfung der aktuellen Richtlinien und vorherrschenden Einstellungen bezüglich IT-Sicherheit und -Management. Identifikation, welche Abteilungen, Gruppen oder Personen in der Vergangenheit die Entwicklung und Einführung von Richtlinien am stärksten begrüßt und unterstützt haben. Das Zusammentragen der Daten basiert auf den folgenden Bereichen:

- Geräteanzahl nach Plattform, Version des Betriebssystems, Eigentümer (Unternehmen, persönlich, nicht zum Unternehmen gehörendes Personal)
- Bewertung der Daten, die momentan auf und über mobile Geräte übertragen werden
- Auf Mobilgeräten verwendete Anwendungen, Eigentümer der Anwendungen und Anwendungssicherheitsprofile
- Alle von Mobilgeräten benutzten Zugänge, wie Mobilfunk, WLAN, Bridge zu Workstation oder VPN

3. Identifikation und Priorisierung von Anwendungsfällen auf der Grundlage einer Belegschaftsanalyse

Um effektiv zu sein, müssen Richtlinien für Mobilgeräte kontextuell an die verschiedenen Anwendungsfälle der Organisation angepasst werden. Folgendes muss geplant bzw. analysiert werden:

- Wie werden Mobilgeräte genutzt?
- Welche mobilen Anwendungen müssen offline benutzt werden, etwa in Flugzeugen oder Aufzügen?
- Welche Informationen werden über Mobilgeräte zugänglich gemacht?
- Welche Informationen werden auf Mobilgeräten gespeichert?

Network Access Control (NAC) bietet eine der flexibelsten und am meisten automatisierten Methoden zur Sicherung einer BYOD-Umgebung.

4. Erstellung eines Wirtschaftsmodells

Erstellung eines Finanzmodells, das in den folgenden Schritten erweitert und angepasst werden kann. BYOD-Programme werden nicht immer zu direkten Einsparungen führen, aber die Rendite durch gesteigerte Produktivität, größere Arbeitszufriedenheit, eine flexible Arbeitsumgebung und die Fähigkeit, geeignete Bewerber anzuziehen, sollten nicht außer Acht gelassen werden. Folgendes ist dabei zu beachten:

- Gerätekosten (können steigen oder sinken, je nachdem, was das Unternehmen abdeckt)
- Datenverbindungskosten (existieren spezielle Datentarife, die durch Größenvorteil zu Kosteneinsparungen führen?)
- Softwarelizenzkosten (und Überblick über die auf persönlichen Geräten verwendete/installierte Software)
- IT-Infrastrukturkosten (Sicherheit, Management, Bandbreite, Datenschutz)

5. Formulierung von Richtlinien

Für jedes mittelgroße bis große Unternehmen dürfte ein Versuch in „Einheitsgröße" kaum Erfolg haben. Es müssen unterschiedliche Richtlinien für unterschiedliche Gruppen, Abteilungen und Anwendertypen in Betracht gezogen werden. Beispielsweise würde man für den Großteil der Belegschaft einfache Anwendungen wie E-Mails auf den fünf führenden mobilen Plattformen unterstützen. Für den Vertrieb wiederum könnte man eine Sales Force Automation-Lösung auf ein oder zwei mobilen Plattformen unterstützen, während leitende Manager bestmöglichen Support für alle Anwendungen auf der gewünschten Plattform erhalten. Auf Grundlage des gewünschten Risikoprofils des Unternehmens gilt es, ein gutes Gleichgewicht zwischen der Anwendererfahrung und der Sicherheit zu finden. BYOD-Richtlinien sollten umfassend sein und sowohl LANs als auch WLANs schützen. Anwenderfälle sollten sowohl Smartphones und Tablets ansprechen, die drahtlosen Zugriff benötigen, als auch Laptops (Mac und Windows), die Ethernet-Anschluss brauchen.

6. Schutz für das Netzwerk

Sobald man entschieden hat, welche Arten von Geräten zugelassen sind und welche Anwendungen und Daten auf jedem Gerät genehmigt werden, muss festgelegt werden, wie der Zugriff hierauf geregelt und das Netzwerk vor nicht autorisierten, nicht konformen und kontaminierten Geräten geschützt wird. Es mag zwar attraktiv erscheinen, das BYOD-Programm manuell zu verwalten, indem man 802.1X-Konfigurationen und Zertifikate auf eine vorbestimmte Gruppe genehmigter persönlicher Geräte anwendet, aber diese Methode dürfte sich als schwerfällig, statisch und nicht skalierbar erweisen. Network Access Control (NAC) der neuesten Generation bietet eine der flexibelsten und am höchsten automatisierten Methoden zur Sicherung einer BYOD-Umgebung. Next Generation NAC bietet Geräteprofile, Anwenderauthentifizierung, Gäste-Management, Compliance- und Konfigurationsprüfungen, automatische Korrektur und eine detaillierte, richtlinienbasierte Methode, um das passgenau gewählte Modell reibungslos im gesamten Unternehmen zu implementieren und zu verwalten.

7. Schutz für die Daten

Bei jedem BYOD-Projekt muss festgelegt werden, wie man seine Daten schützen möchte. Next Generation NAC schützt die Daten im Netzwerk vor nicht zugelassenen und nicht konformen Geräten, aber es müssen auch die auf dem mobilen Gerät gespeicherten Daten geschützt werden. Ein plattformübergreifendes System zur Verwaltung mobiler Geräte (Mobile Device Management, MDM) bietet die beste Methode zur Verwaltung und Sicherung der Daten auf firmeneigenen und persönlichen Mobilgeräten. MDM-Systeme bieten oft eine Reihe von Mechanismen, die eine Trennung zwischen den firmeneigenen und persönlichen Aspekten eines Geräts durchsetzen. Ein derartiger Mechanismus wäre die Verwendung von Containern für vertrauliche Daten und firmeneigene Anwendungen (wie Firmen-E-Mail) auf einem Mobilgerät, so dass Mitarbeiter außerhalb des Unternehmens-Containers die Kontrolle über das Gerät und die Wahlmöglichkeit von Anwendungen behalten. Container verhindern die Übertragung von Daten von einer Anwendung zur anderen, bieten üblicherweise Verschlüsselung und Schutz vor Datenverlust sowie die Möglichkeit, Firmendaten zu löschen, ohne die persönlichen Daten des Mitarbeiters zu löschen (Teillöschung).

„Egal, welche BYOD-Strategie gewählt wird – es ist nötig zu erkennen, ob nicht verwaltete Geräte für geschäftliche Zwecke eingesetzt werden. Das erfordert NAC."

Gartner, „NAC Strategies for Supporting BYOD Environments" 22. Dezember 2011, Lawrence Orans und John Pescatore

8. Erstellung eines Projektplans

Erstellung eines Plans zur Implementierung von IT-Kontrollen, die die BYOD-Richtlinien unterstützen. Festlegen, ob die Kontrollen in Phasen oder auf einmal implementiert werden. Einige häufig verwendete BYOD-Kontrollen sind:

- Remote-Geräte-Management
- Anwendungskontrollen
- Compliance- und Audit-Berichte
- Daten- und Geräteverschlüsselung
- Verbesserung der Cloud-Storage-Sicherheit
- Datenlöschung von Geräten nach Außerdienststellung
- Widerruf der Zugriffsberechtigung, wenn die Endanwenderrolle sich von Mitarbeiter zu Gast ändert
- Widerruf der Zugriffsberechtigung, wenn Mitarbeiter entlassen werden oder aus dem Unternehmen ausscheiden

9. Bewertung der Lösungen

Laut Gartner stellen NAC und MDM zentrale Komponenten einer umfassenden BYOD-Sicherheitsstrategie dar. Wenn man Lösungen bewertet, sollte man unbedingt die Auswirkung auf das existierende Netzwerk in Betracht ziehen. Außerdem stellt sich die Frage, wie gut die Lösung in bestehende IT-Systeme wie Verzeichnisse, Patch-Management, Ticketsystem, Endpunktschutz, Schwachstellenanalyse und SIEM-Systeme integriert werden kann.

10. Implementieren der Lösungen

Die Entwicklung und Optimierung der betrieblichen Prozesse ist für die Skalierung eines BYOD-Projekts entscheidend. Beginnen sollte man mit einem Pilotprojekt (Auswahl der Anwender aus jeder Abteilung oder nur IT-Personal), um die BYOD-Richtlinien zu testen und zu verbessern. Erweiterung des Programms auf eine Zielgruppe von 500 bis 1000 Mitarbeitern in bestimmten Abteilungen, um die betrieblichen Prozesse zu skalieren und zu verbessern. Öffnung des Programms für alle Mitarbeiter, vielleicht nacheinander in verschiedenen Geschäftsbereichen, je nach betrieblichen Kriterien.

Über ForeScout

ForeScout ist der führende Anbieter für intelligente Zugangskontrolle und Security Management und bietet Unternehmen umfassende Sichtbarkeit, Transparenz und richtlinienbasierte Kontrolle über Nutzer, Geräte und Anwendungen im Netzwerk. Dies erlaubt es Unternehmen, ihr Netz kontinuierlich zu monitoren und Sicherheitsvorfälle sowie Cyberattacken automatisch zu beheben. ForeScouts CounterACT ist leicht zu implementieren, offen und skalierbar und wird bereits von über 1500 Unternehmen und Regierungsorganisationen eingesetzt. ForeScout hat seinen Hauptsitz in Campbell, Kalifornien, und vertreibt seine Lösungen über ein Netzwerk von autorisierten Partnern weltweit. **Weitere Informationen finden Sie unter www.forescout.com.**

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
USA

T 1-866-377-8771 (USA)
T 1-408-213-3191 (Intl.)
F 1-408-371-2284 (Intl.)
www.forescout.com

Doc: 2013.0008