IT-Sicherheit und Datenschutz bei mobilen Mitarbeitern

Die Zeiten, als ein Notebook unterm Arm ein Zeichen für eine besonders wichtige Position im Unternehmen war, sind längst vorbei. Smartphone und Tablet sind ebenso wie ein Laptop heute selbstverständliche Arbeitswerkzeuge zahlreicher Mitarbeiter in vielen Branchen. Allerdings wird dabei oft übersehen, dass sich auf ihnen zahllose vertrauliche Informationen und schützenswerte Daten befinden, diese Geräte im mobilen Einsatz aber auch besonders verwundbar sind.

IT-Sicherheit wird oft mit einer Kette verglichen, bei der unter Belastung das schwächste Glied bricht. Tatsächlich ist es aber so, dass es bei IT-Sicherheit meist nicht ein schwaches Glied gibt, sondern dass durch eine Unachtsamkeit oder eine nicht optimale Vorbereitung jeder Baustein zum Einfallstor für Schadsoftware und Angreifer werden kann. Treffender ist daher der Vergleich mit einer Fußballmannschaft, die auf Abseits spielt: Passt nur einer kurz nicht auf – sei er auch sonst ein noch so guter Spieler – kann es schon passiert sein.

Wie ein Fußballtrainer mit seinem Team regelmäßig Standardsituationen übt, müssen auch IT-Verantwortliche in Firmen ihre Mitarbeiter immer wieder schulen, auf neue Angriffsmethoden hinweisen und für Gefahren sensibilisieren. Denn es ist schon viel gewonnen, wenn sich Mitarbeiter bei einer E-Mail überlegen, ob sie wirklich auf den Anhang klicken sollen, ob es eine gute Idee ist, bei einem Dokument aus unbekannter Quelle Makros zuzulassen und ob der Chef eine ungewohnt hohe Überweisung ins Ausland tatsächlich aus dem Urlaub per E-Mail anordnen würde. „Ein Sicherheitskonzept ist nur so gut wie die Personen die es nutzen“, weiß Karsten Schwarz, Spezialist IT-Security, bei Nösse Datentechnik. „Ständige Weiterbildung der Mitarbeiter ist daher noch vor der Technik der wichtigste Punkt in jedem Konzept.“

In der Abwehr müssen alle mitarbeiten

Im Gegensatz zum Trainer stehen IT-Verantwortlichen in Unternehmen zusätzlich zu ihrer Mannschaft auch zahlreiche technische Möglichkeiten zur Auswahl. Firewall und Virenschutz sollten zur Grundausstattung gehören und tun es in den meisten Firmen glücklicherweise auch. Moderne Sicherheitskonzepte müssen allerdings darüber hinausgehen. „Der Irrglaube, die Unternehmensgröße entscheidet darüber, ob man für Kriminelle interessant ist, muss dringend aus den Köpfen verschwinden“, so Security-Spezialist Schwarz.

Lediglich Lösungen auszuwählen, die in Tests am besten abgeschnitten haben oder deren Anbieter den besten Preis macht, ist keine erfolgversprechende Strategie. Moderne Schadsoftware findet selbst zwischen ausgezeichneten Einzelprodukten Schlupflöcher. Deshalb ist es heute wichtig, Security-Produkte einzusetzen, die miteinander kommunizieren.

Das wären, um im Bild der Fußballmannschaft zu bleiben, die Innenverteidiger. Sind sie gut, weiß jeder von ihnen immer, was der andere tut. Falls es doch einmal Zweifel oder unerwartete Situationen gibt, sprechen sie sich durch kurze, klare Kommunikation ab. Bleiben noch die Außenverteidiger. In der Firmen-IT lassen die sich mit mobilen Mitarbeitern gleichsetzen: Mal sind sie im Büro, mal arbeiten sie von zu Hause, mal sind sie bei Kunden unterwegs. Als Flügelflitzer sind sie für Dynamik und Effizienz bekannt – aber wie lassen sie sich in ein Security-Konzept einbeziehen?

In klassischen Security-Szenarien ist das ein Albtraum. Denn es ist nie klar, welches Gerät sie verwenden, wie dessen Schutzniveau ist und ob es sicher kommunizieren kann. Mobile Device Management (MDM) hilft Unternehmen, diese Fragen zu beantworten und sicherzustellen, dass Mitarbeiter auch auf Mobilgeräten sicher arbeiten können. Dazu ermöglichen MDM-Lösungen Mitarbeitern einfach Zugriff auf E-Mails, Dokumente oder unternehmensinterne Software und sorgen zugleich für den Schutz des Unternehmensnetzwerks.

Was Mobile Device Management leisten kann

Im Mittelpunkt jedes Mobile Device Managements steht die Aufgabe, das mobile Endgerät und dessen Betriebssystem so abzusichern, dass es beim Zugriff auf die Unternehmensressourcen keine Gefahr darstellt. Dazu wird etwa überprüft, ob Nutzer ungewünschte Veränderungen vorgenommen haben (Jailbreak oder Rooting) und ob sie sich an Sicherheitsrichtlinien halten, zum Beispiel in Bezug auf die Stärke des Passworts. Daneben hilft MDM auch, die wachsende Zahl mobiler Geräte im Griff zu behalten, indem es weitgehend automatisiert Bestandslisten führt, also die Geräte bestimmten Mitarbeitern zuordnet und deren Rechte und Benutzerkonten verwaltet, die Inbetriebnahme erleichtert und die Versorgung mit Apps gewährleistet.

Ein gutes MDM gibt IT-Sicherheitsverantwortlichen auch Möglichkeiten, bei Diebstahl oder Verlust eines der Geräte einzugreifen, es zu sperren oder Inhalte sicher zu löschen (Fachbegriff dafür ist „Remote Wipe“). Wichtig ist zudem nicht erst seit dem Inkrafttreten der DSGVO, dass beim Zugriff auf die Geräte alle Datenschutzbestimmungen eingehalten werden.

Falls die private Nutzung des Firmen-Smartphones erlaubt ist, gilt es auch sauber zwischen beruflichen und privaten Daten zu trennen. Da Mobilbetriebssysteme und Apps aber danach streben, auf möglichst alle Nutzerdaten zuzugreifen, ist das keine einfache Aufgabe. Zum Beispiel sollten Mobiltelefonnummern von Geschäftspartnern nicht vom privat genutzten Messenger übernommen und zu den Kontakten hinzugefügt werden. Andersherum sollten private E-Mails auch privat bleiben und nicht auf den Firmenservern archiviert werden.

Gleichzeitig sind Smartphones, Tablets oder Firmen-Notebooks auch deshalb besonders gefährdet, weil sie sich oft mit einem unbekannten WLAN verbinden und ohne den Schutz der Firewall des Firmennetzwerks im Internet bewegen. Zudem stellt ihre Mobilität grundsätzlich ein Risiko dar: Im Zug, am Flughafen, im Restaurant oder auf einer Konferenz fällt es Unbefugten wesentlich leichter, physisch auf ein Gerät zuzugreifen als in einer Büroumgebung. Deshalb bietet ein gutes MDM auch Verschlüsselungsmechanismen, sorgt für die Absicherung des Gerätezugangs per PIN, Kennwort oder Biometrie (Fingerabdruck oder Gesichtserkennung).

Keine moderne IT ohne Mobile-IT

Trotz der beschriebenen Risiken kann es sich kaum jemand leisten, auf Mobilität und mobiles Arbeiten zu verzichten. Schließlich erhöht die Nutzung der Unternehmensressourcen unterwegs die Produktivität, verkürzt Abläufe erheblich und macht ganz neue Geschäftsprozesse oft überhaupt erst möglich. Deshalb gilt es, die Balance zwischen einer größtmöglichen Freiheit der Anwender bei der Benutzung und den Anforderungen der IT-Sicherheit und des Datenschutzes zu finden.

Mobile Device Management ermöglicht Unternehmen bei freier Wahl der Endgeräte die Vorteile mobiler IT ohne Compliance-Probleme zu nutzen. Allerdings lässt sich nicht pauschal sagen, welche MDM-Lösung für ein Unternehmen die richtige ist. Dazu müssen zuerst die individuellen Anforderungen analysiert werden. Dabei hilft ein guter, geschulter IT-Security-Consultant. Den erkennt man an seinen Zertifizierungen sowie am Partnerstatus seines Unternehmens bei den Herstellern.

Pressekontakt
punktgenau PR
Christiane Schlayer
Fon +49 (0)911 9644332
Mobil +49 (0)179 5053522
christiane.schlayer@punktgenau-pr.de
www.punktgenau-pr.de

Nösse Datentechnik GmbH & Co. KG
Patrick Bormacher
Maybachstr. 11
51381 Leverkusen
Telefon: +49 (0)2171 7003-553
p.bormacher@noesse.de
www.noesse.de