Link: https://www.computerwoche.de/a/vielfalt-ohne-ende,2501649

Mobile Security

Vielfalt ohne Ende

Datum: 09.01.2012

Software Software für Gerätemanagement hilft, die zunehmende Vielfalt mobiler Geräte in den Unternehmen in den Griff zu bekommen. Doch Tools und Technologien können.

Bereits im nächsten Jahr sollen einer aktuellen Morgan-Stanley-Studie zufolge mehr Internetnutzer mobil im World Wide Web surfen als über den PC am Schreibtisch. Das hat weitreichende Folgen für die Arbeitswelt, prognostiziert eine IDCStudie zum gleichen Thema: Waren es bei der Umfrage 2010 noch weltweit 30 Prozent der Arbeitnehmer, die ihre privaten Endgeräte für geschäftliche Anwendungen einsetzten, sind es in diesem Jahr bereits 40 Prozent. Auf diese Weise spült der Trend "Bring-Your-Own-Device" (BYOD) eine ganze Armada privater Endgeräte in die Unternehmensnetzwerke - ein kaum beherrschbares Sicherheitsrisiko für Unternehmen.

Kontrolle über Client-Landschaft geht verloren

Die Unternehmen können der Entwicklung zunächst durchaus Positives abgewinnen. Viele springen auf den fahrenden Zug auf, weil sie eine erhöhte Mitarbeiterzufriedenheit, größere Mobilität der Angestellten, flexiblere Arbeitsmodelle oder eine Senkung der IT-Kosten erwarten, wie der britische Marktforscher Vanson Bourne jüngst in einer Umfrage ermittelte. Doch vier von fünf IT-Verantwortlichen in den Firmen befürchten einer COMPUTERWOCHE- Studie zufolge auch, aufgrund von BYOD die Kontrolle über ihre Client-Landschaft zu verlieren, und bangen um die Sicherheit der Unternehmensdaten. "Unternehmen glichen früher sicherheitstechnisch einer Burg mit festen Ein- und Ausgängen", sagt Lynn-Kristin Thorenz, Director Research and Consulting bei IDC. "Diese Zeiten sind mit dem Aufkommen des Cloud Computings und der Nutzung von Mobilgeräten endgültig vorbei." Smartphones und Tablets gelten nicht umsonst als Einfalltore für Malware, Trojaner und Wi-Fi-Hacker. Der US-amerikanische Netzwerkspezialist Juniper verzeichnet für die Zeitspanne zwischen Mitte 2009 und 2011 einen Anstieg entsprechender Attacken auf Android-Geräte um 400 Prozent. Doch damit nicht genug der Gefahrenherde. Die Palette der Mobilgeräte umfasst neben dem Typus Privat-Handy noch weit mehr Gerätearten wie robuste Industrie-Handhelds, Fahrzeugortungsgeräte oder RFID-Chips, die gleichfalls Unternehmensdaten mobil übertragen. Bereits in 75 Prozent der Unternehmen kommt mehr als nur ein mobiles Betriebssystem zum Einsatz, errechnete Marktforscher Forrester.

Geräte-Management gegen das Chaos

"Verstärkt durch den Trend BYOD wird die Gerätevielfalt in den Unternehmen insgesamt künftig noch zunehmen", erläutert IDC-Analystin Thorenz. Die CIOs stünden nun vor dem Problem, die Vielfalt an Geräten in die Sicherheitsstruktur zu integrieren, so Thorenz weiter. "Dafür bedarf es eines aktiven Gerätemanagements auf einer einheitlichen Plattform, um mit dem Chaos umgehen und die Sicherheit der Unternehmensdaten gewährleisten zu können." Vor einer kaum noch kontrollierbaren Situation stand auch Claus Horstmann aus dem Team MDE Servicedesk beim Versorgungsdienstleister ista. ista Deutschland erfasst für Hausverwalter und -eigentümer, aber auch für Energieversorgungsunternehmen in vielen tausend deutschen Privathaushalten Daten für den Energie- und Wasserverbrauch. Die Erfassung der Daten erfolgt über mobile Ablesegeräte. Die Verbrauchsdaten gelangen über eine Infrarot- oder Bluetooth- Schnittstelle vom Mess- auf das Ablesegerät.

ista: Übersicht über die Gerätewelt

Doch die IT-Betreuung der mobilen Ablesegeräte wurde immer schwieriger. Ausgestattet mit einem herstellereigenen Betriebssystem, ließen sich Einstellungen wie Netzwerkverbindungen oder technische Probleme nur zentral in den ista-Niederlassungen vor Ort bearbeiten. "Die Ableser mussten regelmäßig zu uns kommen, um Software-Updates aufspielen oder Einstellungen vornehmen zu lassen. Das bedeutete einen enormen Zeitaufwand für die IT wie für die Außendienstmitarbeiter", sagt Horstmann. "Die Situation war irgendwann nicht mehr tragbar. Es war kaum möglich, den Überblick zu behalten, welches Gerät von wem, wie und mit welchen Einstellungen genutzt wird." ista entschied sich daher, seine Ableselösung auf Basis neuer Hard- und Software komplett umzugestalten. "Wir haben eine Lösung gesucht, die ein sicheres wie effektives Gerätemanagement erlaubt", erläutert Horstmann. ista entschied sich schließlich für Afaria aus dem Hause der SAP-Tochter Sybase, unter anderem aufgrund der Plattformunabhängigkeit.

Mithilfe dieser Software können die ista-IT-Mitarbeiter Gerätekonfigurationen heute zentral ändern. So lassen sich Sicherheitsvorgaben auf den Geräten regelmäßig aktualisieren und Sicherheitsrichtlinien zuverlässig durchsetzen. "Wir haben jetzt für jedes Gerät den kompletten Lebenszyklus im Blick", so Horstmann. "Einstellungen lassen sich aus der Ferne und regelmäßig automatisch auf den Geräten vornehmen. Das ist nicht nur komfortabel und zeitsparend für beide Seiten, sondern gibt dem Unternehmen auch ein hohes Maß an Sicherheit in Bezug auf genutzte Assets. Geräte- Wildwuchs hat bei uns keine Chance."

Sicherheit nicht rein technikgetrieben betrachten

Doch so wertvoll das Gerätemanagement als Kontrollinstrument für die Datensicherheit im Unternehmen auch ist - das Thema Sicherheit dürfe nicht rein technikgetrieben sein, meint IDC-Analystin Thorenz: "Tools und Technologien erfüllen ihren Zweck nur dann, wenn sie in ein ganzheitliches Sicherheitskonzept eingebunden sind." Daraus müsse nicht nur hervorgehen, welche Richtlinien für den Umgang mit mobilen Geräten gelten, sondern auch, wie diese Richtlinien im Unternehmen gelebt und umgesetzt werden sollen. Das sieht auch die Mehrheit der Unternehmen so: Laut Vanson Bourne befürworten 94 Prozent der befragten Unternehmen klare Richtlinien im Umgang mit privaten Mobilgeräten, erst 44 Prozent der Firmen verfügen jedoch über eine solche BYOD-Policy. Hier gibt es offensichtlich noch erheblichen Gesprächsbedarf.

Links im Artikel:

[1] **http://itunes.apple.com/de/app/sap-agenda/id454699216?mt=8**
[2] **https://www.computerwoche.de/subnet/sap/agenda201104/**
