IT-Management

# Automatisch lösen

## [16.03.2016] Eine umfassende IT-Sicherheitsstrategie erfordert, dass alle Geräte einer Behörde gut betreut werden. Auch die besonderen Herausforderungen bei mobilen Geräten sind zu bedenken. Eine passende Client- und Mobile-Device-Management-Lösung kann unterstützen.

Behörden speichern unzählige personenbezogene und sensible Daten und sind in der Pflicht, diese bestmöglich vor fremden Zugriffen zu schützen. Ein wichtiger Baustein einer umfassenden Sicherheitsstrategie ist das sichere Managen aller Geräte wie PCs, Server oder mobiler Geräte. Eine Client- und Mobile-Device-Management-Lösung (MDM) kann hier die notwendige Unterstützung sein. Welche Funktionalitäten sollte eine solche Lösung bieten? Und worauf sollten Behörden bei der Software-Auswahl für Client und Mobile Device Management achten? Software-Lösungen, die in öffentlichen Behörden eingesetzt werden, müssen besondere Anforderungen erfüllen und beispielsweise den strengen Vorgaben des deutschen Datenschutzes genügen. Ganz allgemein stehen zwei Varianten zur Verfügung: Cloud- oder On-Premise-Lösungen. Bei Cloud-Angeboten gilt es genau zu prüfen, wo die Anbieter die Daten hosten, da im Ausland häufig ein wesentlich weniger streng regulierter Datenschutz gilt als in Deutschland. Deutsche Anbieter betreiben nicht zwangsläufig ihre Rechenzentren auch innerhalb der Landesgrenzen. Gerade für öffentliche Behörden sind deshalb On-Premise-Lösungen eine bewährte Methode. Denn dabei wird die Software auf einem behördeneigenen Server implementiert. Somit bleiben alle gespeicherten Daten innerhalb der Organisation und die IT-Abteilung der Behörde behält die volle Kontrolle. IT-Abteilungen sehen sich steigenden Anforderungen bei häufig knappen Budgets und meist wenig Personal gegenüber. Mithilfe einer Client Management Software können Routineaufgaben wie die Betriebssysteminstallation, Software-Verteilung, Inventarisierung von Hardware, Software sowie Lizenzen, die Datensicherung und das Backup automatisiert werden. Das reduziert den Aufwand und senkt die Fehlerquote. Gleichzeitig protokolliert die Lösung alle gesammelten Daten, sodass Administratoren einen schnellen Überblick über alle Systeme gewinnen.

**Schwachstellen erkennen und eliminieren**

Darüber hinaus gibt es Aufgaben, die eine IT-Abteilung auch mit einer hohen Personaldecke nicht von Hand bewältigen kann. So ist es in der Praxis quasi unmöglich für IT-Administratoren, manuell alle Clients und Server laufend auf alle bekannten Sicherheitslücken zu prüfen und die benötigten Updates und Patches einzuspielen. Eine einzige Schwachstelle auf einem Rechner genügt jedoch, um die gesamte IT-Umgebung zu gefährden. Eine gute Client-Management-Lösung deckt diesen Prozess vom Erkennen der Schwachstelle über das Schließen bis hin zur Erfolgskontrolle ab. Alle Clients werden automatisch gescannt und erkannte Sicherheitslücken dem Administrator angezeigt. Während Server und PCs automatisch der Kontrolle der IT unterstehen und fest eingebunden sind, müssen bei der Verwaltung mobiler Geräte andere Gefahren und Herausforderungen bedacht werden. Die meisten heute populären Smartphones und Tablets wurden ursprünglich für Privatanwender entwickelt. Infolgedessen sind die Management-Möglichkeiten mobiler Betriebssysteme oft noch deutlich eingeschränkter als für PCs. Dazu kommt: Administratoren müssen in der Regel mehrere Mobilplattformen unterstützen, die Geräte einrichten und sicher konfigurieren. Vergleicht man die drei gängigsten Mobilplattformen iOS, Android und Windows, zeigt sich schnell, dass dieselben Parameter wie Name, E-Mail-Adresse, Server oder Domäne für die Einrichtung von Exchange-Konten an jeweils unterschiedlichen Stellen eingegeben werden müssen. Für

die Praxis bedeutet das einen enorm hohen Aufwand und setzt voraus, dass der Administrator alle Eingabemasken kennt. Hier hilft eine Verwaltungssoftware, den Aufwand für das Management der mobilen Geräte zu reduzieren und effizienter zu gestalten. Besonders wichtig bei einer Mobile-Device-Management-Lösung ist, dass auch hier die Vorgaben des deutschen Datenschutzes eingehalten und keine dagegen verstoßenden Daten über die Nutzer erhoben werden. So wäre es beispielsweise unzulässig über eine MDM-Lösung Daten zu erheben, an welchem Ort sich ein Nutzer zu einer bestimmten Zeit aufhält. Mit einem deutschen Anbieter, der darauf Rücksicht nimmt, ist die Verwaltung hier auf der sicheren Seite.

**Für mehr Sicherheit aus der Ferne sorgen**

Das mobile Gerät wird einmalig in die Mobile-Device-Management-Lösung aufgenommen. Nach dem Enrollment kann der Administrator Management-Aufgaben, beispielsweise die Exchange-Konfiguration, zentral durchführen. Dazu setzt er die Einstellungen zentral und verteilt diese dann auf alle mobilen Geräte – bei Bedarf auch remote. Das ist vor allem dann interessant, wenn eine zentrale IT-Abteilung für verschiedene Behörden mit mehreren Standorten verantwortlich ist. Die Mitarbeiter müssen nicht extra dem Administrator das Gerät zur Verfügung stellen, damit dieser die Einstellungen manuell vornimmt. Für den Administrator verringert das Arbeiten mit nur noch einer Oberfläche die Komplexität, spart Zeit und reduziert die Fehleranfälligkeit des Prozesses. Mobile Geräte können leichter abhandenkommen als ein PC. Entsprechende Vorkehrungen müssen getroffen werden. In Betracht kommen hier unter anderem das automatische Sperren beim Ausschalten des Bildschirms, die Möglichkeit, das vergebene Profil auch aus der Ferne zu löschen und nicht zuletzt die Vergabe starker Passwörter. Weiterhin muss sichergestellt sein, dass der Administrator die Geräte jederzeit im Blick hat und beispielsweise informiert wird, wenn ein Nutzer das Betriebssystem kompromittiert. Aus diesem Grund sollte eine MDM-Lösung die Möglichkeit bieten, Compliance-Regeln zu definieren, welche dann automatisch und regelmäßig geprüft werden. Bei Verstößen wird der Administrator informiert und hat dann die Gelegenheit, Gegenmaßnahmen zu ergreifen – vom Senden einer E-Mail an den Nutzer bis hin zum Komplett-Löschen aus der Ferne. Um die hohen Anforderungen an die IT-Sicherheit bei Behörden zu erfüllen, ist es unerlässlich, IT-Administratoren die richtigen Werkzeuge an die Hand zu geben. Nur so können sie alle eingesetzten Geräte sicher und effizient managen. Gleichzeitig müssen die eingesetzten Software-Lösungen die strengen Vorgaben des deutschen Datenschutzes erfüllen. Bei der Auswahl einer Lösung muss also der Funktionsumfang ebenso wie die Sicherheit der Lösung selbst genauestens geprüft werden.

()

Dieser Beitrag ist in der März-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, baramundi, MDM, Client-Management