baramundi

Whitepaper

Schnell und sicher durch Automatisierung

Eine Managementsoftware für alle Endgeräte

Empower your IT

INHALT

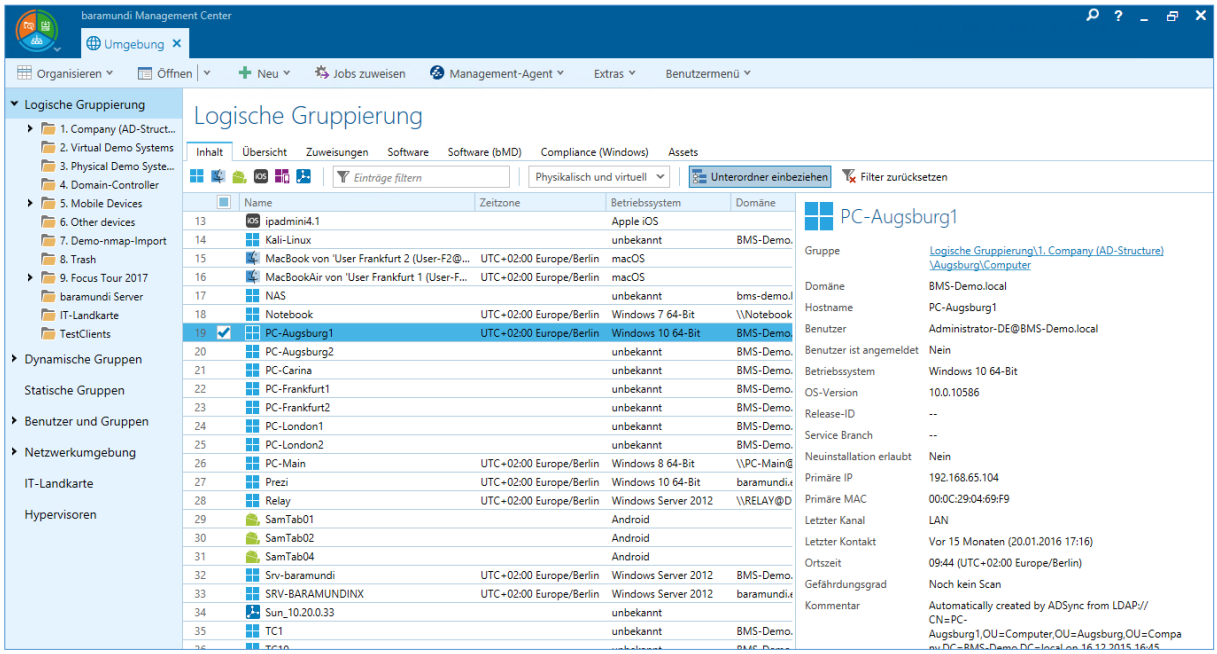
1 Steigende Anforderungen an IT-Abteilungen

Die Entwicklung der IT schreitet immer rascher voran. Vergingen zwischen Zuses Z1 und den ersten PCs noch Jahrzehnte, sorgt die Industrie inzwischen für technische Revolutionen fast im Monatstakt. Mit der Leistungsfähigkeit und Vielfalt der Geräte wachsen auch die Anforderungen an die Administration.

So arbeiten viele Anwender inzwischen nicht mehr allein an PCs und Notebooks, sondern setzen parallel oder sequentiell auch Smartphones und Tablets ein. E-Mails werden unterwegs beantwortet, eine Recherche am PC begonnen und auf dem Smartphone fortgesetzt, eine Präsentation per Tablet gesteuert. Mobile Geräte nutzen andere Betriebssysteme und Anwendungen als PCs, benötigen aber ebenfalls Zugriff auf Firmendaten und E-Mails und müssen daher ebenso zuverlässig abgesichert werden.

Es bietet sich daher an, die Verwaltung aller Endgeräte in einer Lösung zu bündeln. Damit lassen sich einheitliche Standards durchsetzen und ein umfassender Überblick über den Zustand des Netzwerks und aller Endgeräte gewinnen. Gleichzeitig lassen sich künftige, neue Gerätetypen in eine solche ganzheitliche Lösung einfach integrieren.

Mit einer Unified Endpoint Management Lösung können zudem Routineaufgaben automatisiert und somit effizienter, schneller und einfacher erledigt werden. Das sorgt für die nötige Übersicht und erhöht gleichzeitig die Sicherheit des Unternehmensnetzwerks. Dieses Dokument gibt einen Überblick über Administrationsaufgaben, die auf jeden Fall automatisiert werden sollten.



Einheitliche Übersicht über alle Gerätetypen/Plattformen

2 Routinearbeiten automatisieren

2.1 Betriebssysteme und Anwendungen verteilen

Ein neuer Mitarbeiter wird eingestellt. Für die IT-Abteilung heißt das: Ein PC-Arbeitsplatz und/oder ein Notebook müssen bereitgestellt werden. Die Neuinstallation eines Rechners mit Betriebssystem und allen benötigten Anwendungen nimmt – inklusive aller nötigen Neustarts, der Auswahl der passenden Treiber etc. – schnell mehrere Stunden in Anspruch. Mit einer Managementlösung schrumpft dieser Aufwand auf wenige Mausklicks zusammen:

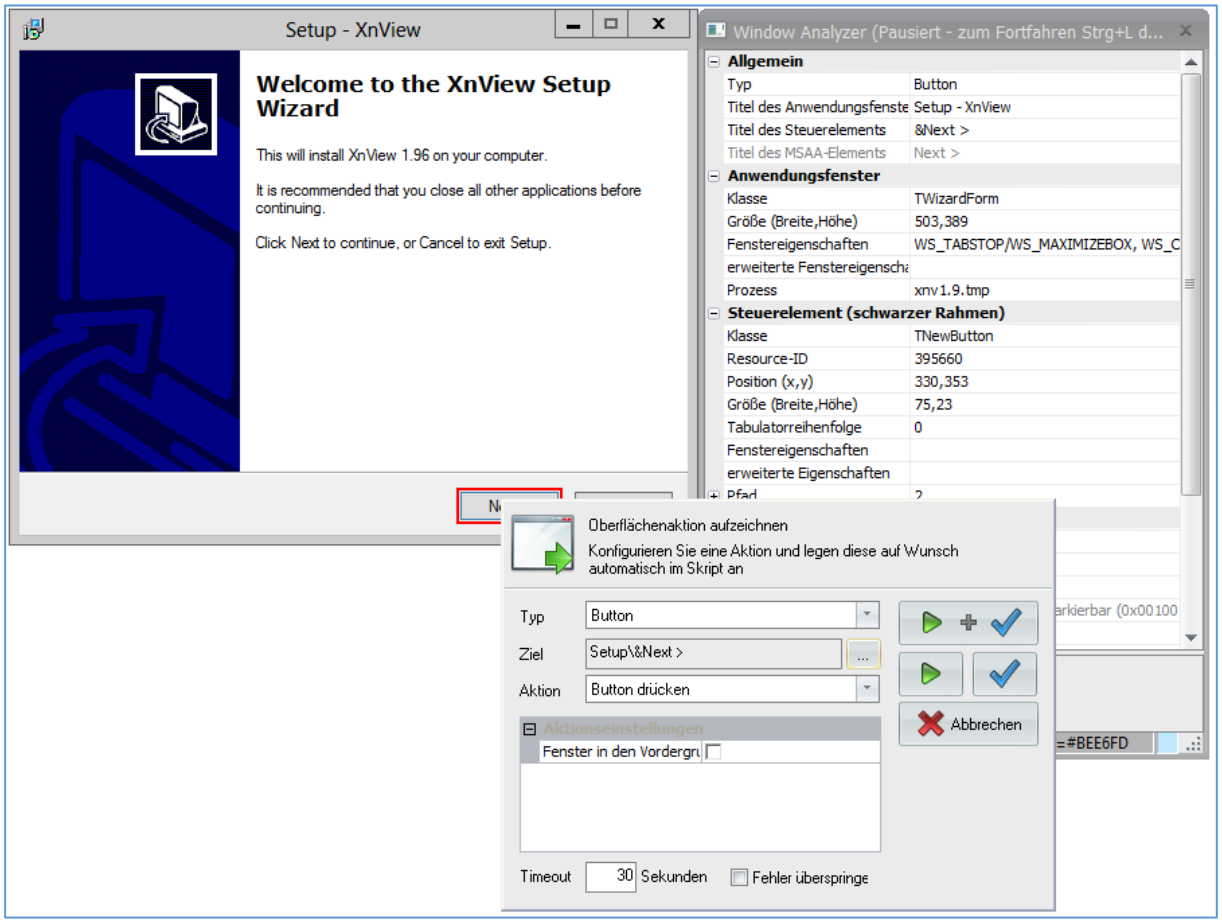
Anstatt von Hand oder per Skript ein Setup ablaufen zu lassen, wird das neue Gerät automatisch im Netzwerk erkannt. In einem Durchgang wird die Festplatte vorbereitet und es werden die nötigen Treiber zugeordnet. Intelligente Lösungen nutzen die native Installationsmethode des OS-Herstellers und erhalten so den vollen Gewährleistungsanspruch. Per Wake-on-LAN können Rechner sogar über Nacht neu installiert werden.

Auch Software lässt sich automatisiert verteilen. Meist wird eine Standardausstattung für ein Einsatzprofil definiert. Bei Bedarf rollt der IT-Administrator dieses Softwarepaket dann per Mausklick auf das Zielsystem aus – auch auf mehreren Geräten parallel, inklusive der nötigen Neustarts und in höchster Installationsqualität unter Nutzung von Original-Setup-Methoden. Dabei gibt die Automatisierungslösung jederzeit eine Rückmeldung zum Installationsstatus und gegebenenfalls zu aufgetretenen Fehlern. Einmal definierte Aufgaben können jederzeit wiederverwendet werden, wenn einige Monate später ein weiterer neuer Kollege beginnt oder ein Gerät ausgetauscht werden muss. Gleichzeitig sorgt die automatisierte Installation für standardisierte Rechnerkonfigurationen und eine geringe Fehlerzahl.

Häufig muss Software installiert werden, für die der Hersteller keine standardisierten Installationspakete zur Verfügung stellt. Die dann benötigten Skripte zur Oberflächenautomatisierung lassen sich mit Hilfe von Tools, die in gängige Management-software integriert sind, einfach und intuitiv erstellen. Selbst problematische Setups werden so zentral

und automatisiert mit dem vom Softwarehersteller vorgesehenen Setup-Verfahren installiert, die Herstellergarantie bleibt erhalten.

Über eine Managementsoftware lassen sich Anwendungen aber nicht nur verteilen, sondern auch vom Client entfernen. Bei der Auswahl einer Lösung sollte darauf geachtet werden, dass dies auch für Programme möglich ist, die nicht über die Managementsoftware installiert wurden. Auf diese Weise lassen sich beispielsweise Applikationen, die Anwender unerlaubt auf ihren Rechner aufgebracht haben, effizient entfernen.



Oberflächenautomatisierung per Wizard mit dem baramundi Automation Studio

Die zentrale, automatisierte Installation von Anwendungen und Betriebssystemen hat zudem einen positiven Nebeneffekt für IT-Administratoren und Endanwender: Im Fall von Performance-Problemen und hartnäckigen Fehlern kann einfach der Arbeitsplatz über Nacht neu installiert werden, anstatt aufwendig nach der Ursache zu suchen. Auf diese Weise steht bei minimalem Zeitaufwand schnellstmöglich wieder ein voll funktionsfähiges Gerät zur Verfügung. Auch die Migration einer großen Zahl von Arbeitsplätzen, zum Beispiel auf ein neues Betriebssystem wie Windows 10 oder eine neue Office-Version, lässt sich so automatisiert abwickeln.

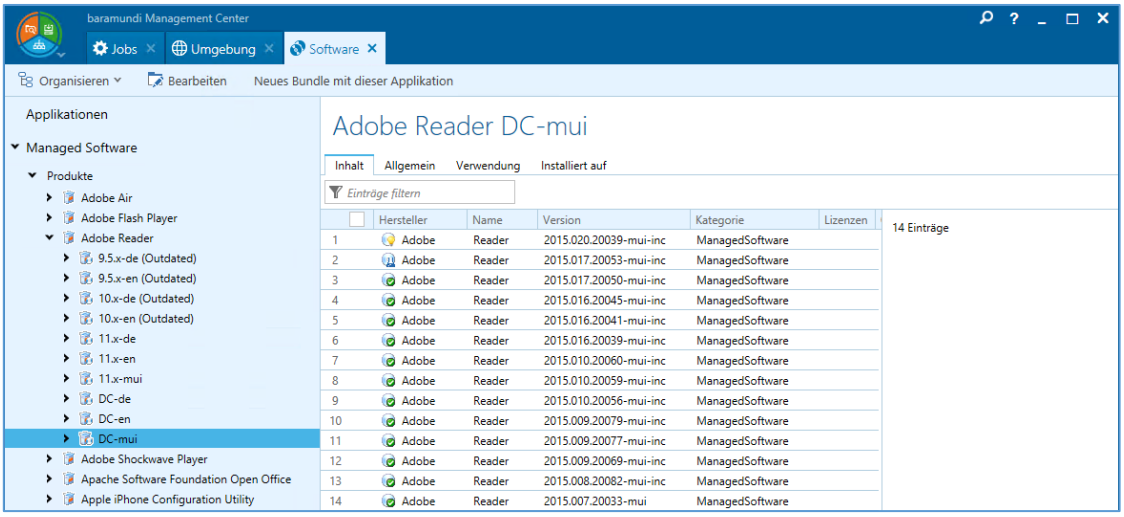
2.2 Schwachstellen erkennen und Updates automatisieren

Einmal installiert und fertig? Leider nein. Laufend erscheinen Updates für Anwendungen und Betriebssysteme. Diese müssen schnellstmöglich auf allen Rechnern eingespielt werden. Dabei geht es nicht nur um neue Features, sondern vor allem um die Sicherheit: Neue Versionen und Patches schließen Sicherheitslücken, über die potenzielle Angreifer ins Unternehmensnetzwerk eindringen und großen Schaden anrichten könnten. Die Konsequenzen reichen vom Imageschaden über die Offenlegung von Firmeninterna bis zu juristischen Folgen, wenn Kundendaten gestohlen werden und Verstöße gegen Datenschutzgesetze vorliegen.

Firewall und Virenscanner sind zwar unabdingbare Bestandteile eines wirksamen Sicherheitskonzepts, aber gegen Angriffe über nicht gepatchte Schwachstellen weitgehend wirkungslos. Wenn bei einem sogenannten „Reverse Connection"-Angriff der Rechner eines Mitarbeiters unter Ausnutzung einer Schwachstelle dazu gebracht wird, eine Verbindung mit dem Kontrollserver des Angreifers aufzubauen, greift die Firewall in der Regel nicht ein, da der Kontakt verschlüsselt auf Standardkanälen aus dem Unternehmen heraus aufgebaut wird. Es ist daher unabdingbar, Schwachstellen auf jedem einzelnen Endgerät im Blick zu behalten und je nach Gefährdungsgrad schnellstmöglich zu schließen.

Doch jede Woche werden rund 100 neue Schwachstellen erkannt und dokumentiert, wie die Statistiken der National Vulnerability Database des US-CERT belegen. Hier kann die Managementsoftware den IT-Administrator durch einen automatisierten, regelmäßigen Scan aller Clients und Server unterstützen. Als Ergebnis erhält der Administrator übersichtliche Listen, zum Beispiel der gefährlichsten Schwachstellen im Unternehmensnetzwerk oder der Clients mit den meisten Sicherheitslücken. So kann er priorisieren und gezielt die Lücken schließen.

Verfügt die Lösung neben dem Schwachstellenscanner auch über ein Patch Management, lassen sich erkannte Lücken auch gleich zentral und automatisiert schließen. Neben Microsoft-Patches sollte die Managementlösung grundsätzlich auch Updates für häufig genutzte Anwendungen wie Adobe Reader, Java oder Firefox zentral und automatisiert verteilen, die aufgrund ihrer großen Verbreitung bei Angreifern besonders populär sind. Aktuelle Softwarepakete für zahlreiche Anwendungen sind dabei auch als Managed Software vom UEM-Hersteller verfügbar. Diese können auch nach eigenen Richtlinien für produktive Nutzung oder zum Test freigegeben werden.



Verteilfertige Softwarepakete mit unterschiedlichen Freigabe Leveln

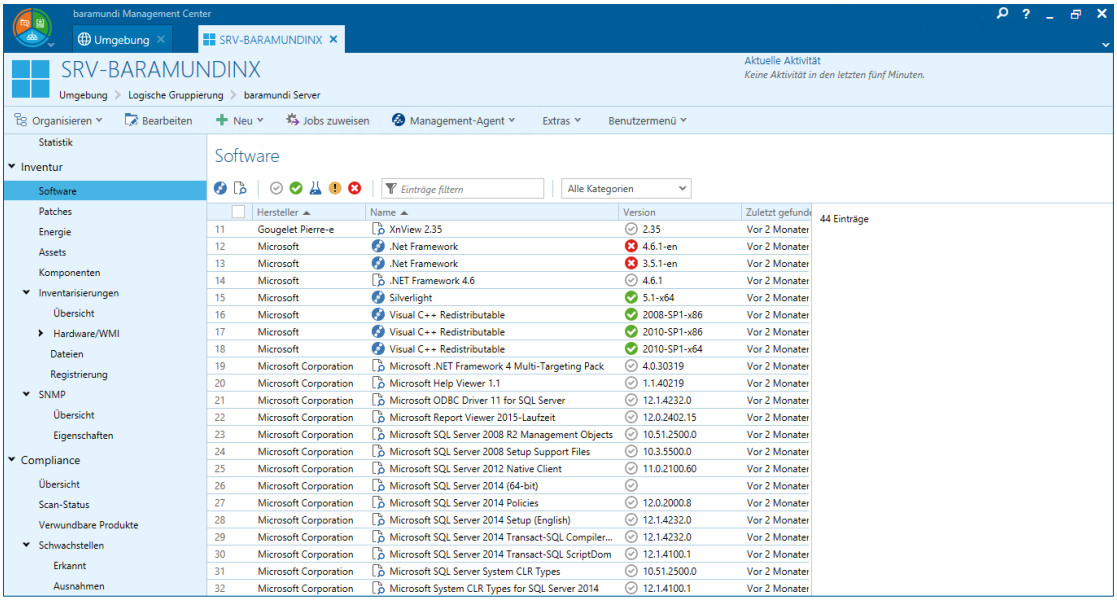
Für ein wirksames Schwachstellenmanagement genügt es aber nicht, von einer Lücke zu wissen und die Installation eines Patches anzustoßen. Essentiell ist auch das Wissen darüber, ob das sicherheitsrelevante Update tatsächlich auf allen Clients angekommen ist. Installationen können fehlschlagen, vom Benutzer blockiert werden oder ein Notebook kann im Außeneinsatz nicht erreichbar sein. Die eingesetzte Lösung muss daher eine Rückmeldung zum Installationsstatus sowie zu etwaigen aufgetretenen Fehlern geben, um sicherzustellen, dass tatsächlich alle Lücken geschlossen werden.

2.3 Hardware und Software inventarisieren, Lizenzen managen

Ein umfassender Überblick ist nicht nur wichtig, um Schwachstellen zu erkennen und Sicherheit zu garantieren. IT-Verantwortliche müssen auch den Einsatz von Hard- und Software berichten oder im Fall eines Lizenzaudits durch einen Softwarehersteller die korrekte Lizenzierung nachweisen können. Unter Kostengesichtspunkten ist es wichtig, ungenutzte Software zu erkennen, die auf Clients schlummert und teure Lizenzen bindet.

Eine automatisierte Inventur mit einer Management Lösung klärt exakt und rasch, welche Hard- und Software im Unternehmensnetzwerk überhaupt im Einsatz ist. Damit ist jederzeit eine aktuelle Datenbasis für eine managementfähige Auswertung verfügbar. Gerade im Zusammenhang mit Volumen- und Upgrade-Lizenzen ist es nicht einfach, den Überblick zu behalten. Hier sorgt ein integriertes Lizenzmanagement für Übersicht und Compliance.

Zusätzlich kann auch die tatsächliche Nutzung eines Programms erfasst werden, um unnötige Kosten zu vermeiden. Dazu wird der Start einer Anwendung auf den einzelnen Endgeräten protokolliert. Dies zeigt, auf welchen Rechnern ein Programm in einem vorgegebenen Zeitraum ungenutzt bleibt – und welche Lizenzen daher eingespart werden können. Wichtig: Die eingesetzte Lösung muss dabei die europäischen Datenschutzvorgaben einhalten und darf keine Überwachung des individuellen Mitarbeiterverhaltens zulassen.



Auflistung der installierten Software

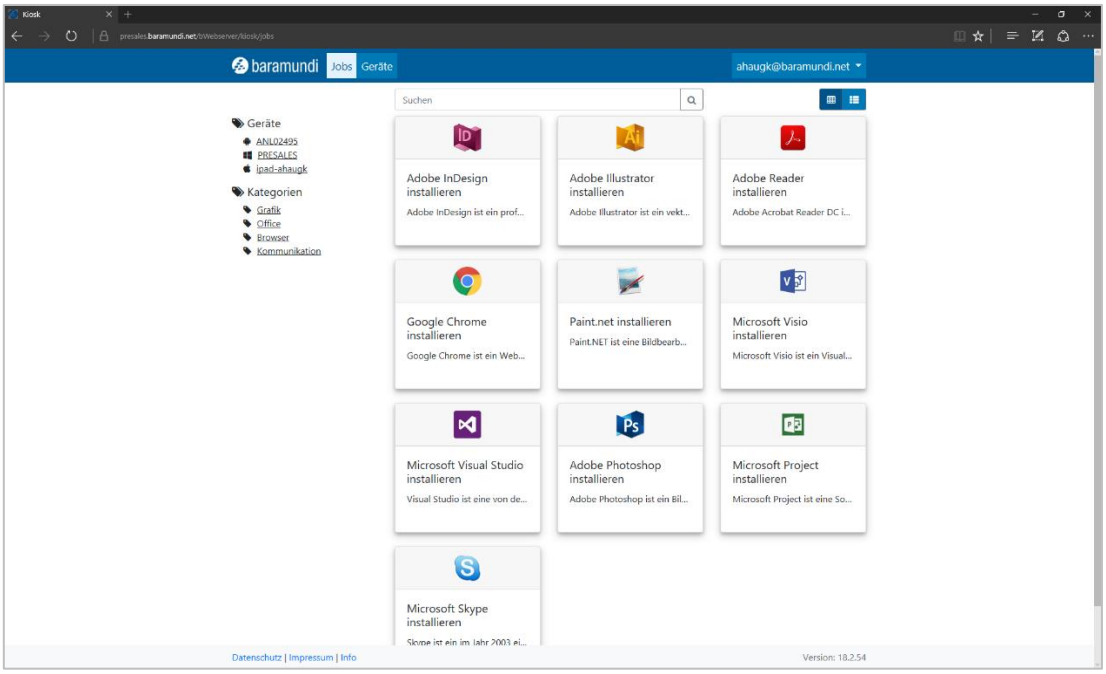
Auch der IT-Support profitiert von der automatisierten Inventur: Integrierte Helpdesk-Lösungen erlauben es den Supportmitarbeitern bei Anfragen schnell die Hard- und Softwareausstattung des betreffenden Arbeitsplatzes zu erfassen. Korrekte Daten des betreffenden Endgeräts sind essentiell, um das Anliegen des Nutzers schnell und kompetent bearbeiten zu können.

2.4 Intelligent automatisieren: Zeitsteuerung und Self-Service

In vielen Unternehmen gibt es Wartungszeitfenster, die festlegen, dass Administrationsaufgaben auf bestimmten Rechnern nur zu vorgegebenen Zeiten erfolgen dürfen. Leistungsfähige Managementsoftware stellt daher zeitgesteuerte Aufgaben zur Verfügung. So wird es möglich, eine Patch Installation gezielt innerhalb eines bestimmten Zeitfensters auf einem Endgerät ablaufen zu lassen.

Eventgesteuerte Aufgaben entlasten den IT-Administrator dagegen bei der Reaktion auf Ereignisse. Zum Beispiel: Wenn auf einem Client bei der Inventarisierung das Spiel XY entdeckt wird, dann soll dieses automatisiert entfernt werden. Anstatt bei jedem Fund des Spiels selbst eingreifen zu müssen, erhält der Administrator nur noch einen Report über eine ausgeführte Deinstallation.

Komfortabel für IT-Administrator und Anwender ist die Möglichkeit, vorbereitete Installationsabläufe in einem Self-Service-Kiosk zur Verfügung zu stellen. Dies ermöglicht eine schnelle, unkomplizierte Bearbeitung von Standardanfragen, zum Beispiel die Installation von Browsern – und zwar exakt dann, wenn der Nutzer es wünscht und für ein reibungsloses Arbeiten benötigt. Gleichzeitig wird das Supportaufkommen verringert, da diese Aufgabe bei Abruf vollautomatisch abläuft. Auch über solche Self-Service-Installationen sollte der Administrator jederzeit den Überblick behalten.



Self-Service-Kiosk für die Anwender

Leistungsfähige Managementsoftware bietet darüber hinaus die Möglichkeit, Anwender in Installationsabläufe mit einzubeziehen, ohne als Administrator die Kontrolle aus der Hand zu geben. Zum Beispiel kann dem Nutzer das Recht eingeräumt werden, eine Patch Installation, die einen Neustart erfordert, innerhalb eines vorgegebenen Zeitfensters zu verschieben. So werden die Kollegen nicht in ihrem Arbeitsfluss gestört und die Installation läuft während einer Kaffeepause ab. Gleichzeitig ist sichergestellt, dass die Verteilung eines kritischen Patches nicht zu weit hinausgeschoben werden kann.

2.5 Integration in die bestehende Infrastruktur

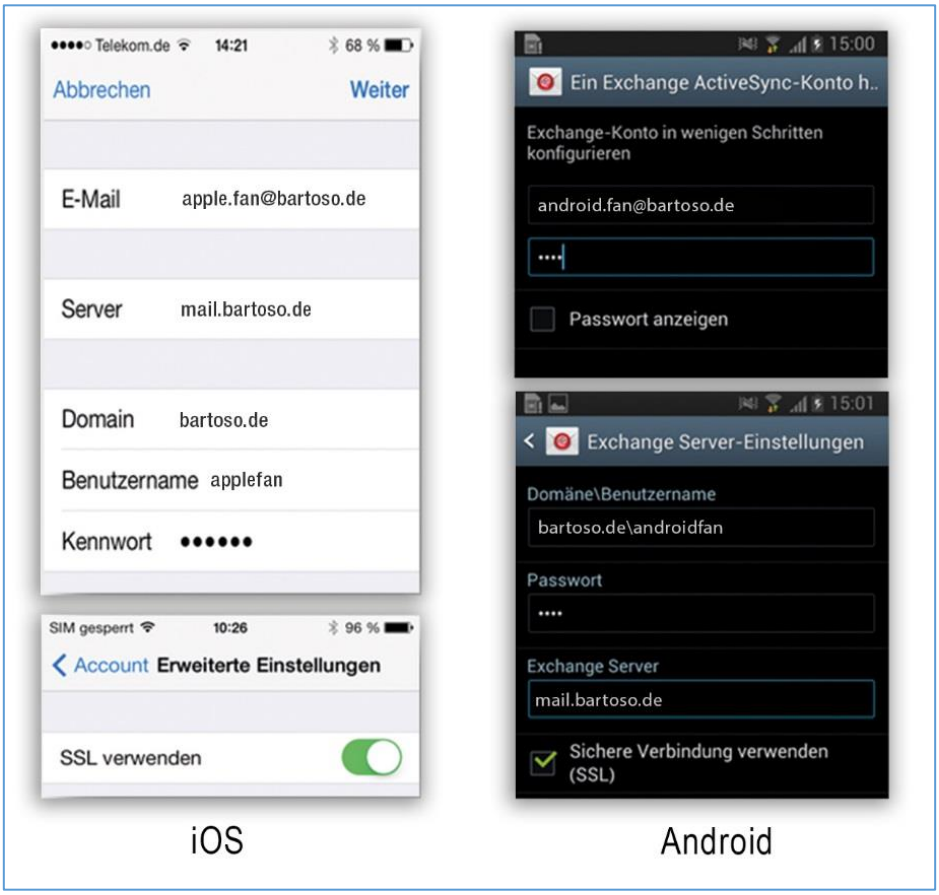
Die Managementsoftware sollte auch nicht als neue Insel in der bestehenden Infrastruktur gesehen werden. Um hier eine nahtlose Integration zu ermöglichen, muss die Managementsoftware über moderne Schnittstellen verfügen. Nur so lassen sich auch weitere organisatorische Prozesse automatisieren. So ist es zum Beispiel möglich, dass nach Erfassung des neuen PCs im ERP-System automatisch ein Endgerät mit allen wichtigen Daten wie Inventarnummer, Kostenstelle, etc. in der Managementlösung angelegt und sofort mit Software und Konfigurationen versorgt wird.

Ebenso ist eine Integration in ein bestehendes Ticketsystem möglich. So erhält der Supportmitarbeiter stets aktuelle Informationen über die verwendete Soft- und Hardware am Endgerät und kann im Bedarfsfall auch Neuinstallationen auslösen.

3 Mobilgeräte managen

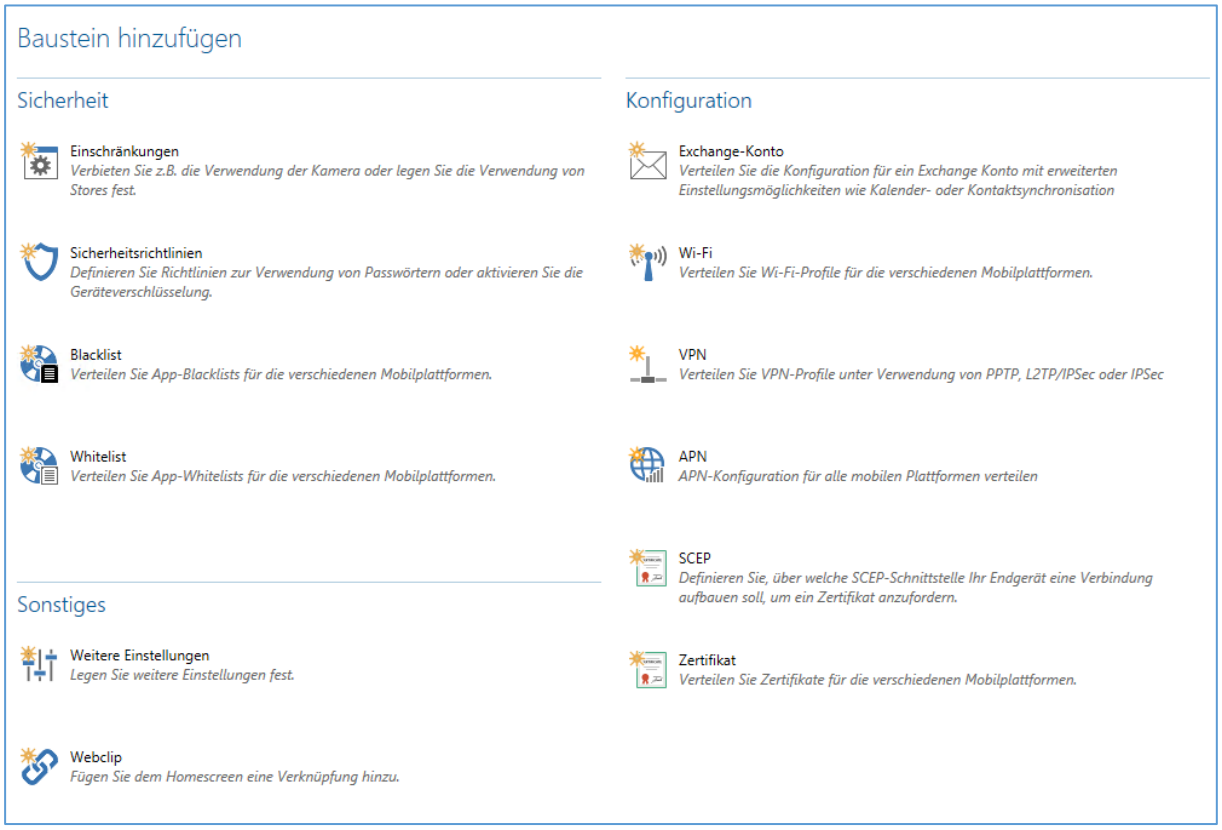
Der Gebrauch von mobilen Geräten ist in vielen Unternehmen zum Standard geworden und viele Mitarbeiter wollen von ihren eigenen mobilen Geräten aus auf Unternehmensdaten zugreifen. Für Firmen kann das einige Vorteile bringen, allerdings sollten sich die IT-Verantwortlichen der Risiken bewusst sein. Damit sich Notebooks, Tablets und Smartphones sicher in den Berufsalltag integrieren lassen, ist ein effektiver Schutz samt einer Inventarisierung Grundvoraussetzung. Idealerweise ist das Management der mobilen Geräte in die UEM-Lösung integriert, denn viele Aufgaben bei der Verwaltung von Mobilgeräten lassen sich ebenfalls automatisieren.

Vergleicht man beispielsweise die zwei gängigsten Mobilplattformen iOS und Android, zeigt sich schnell, dass dieselben Parameter wie Name, E-Mail-Adresse, Server, Domäne und Verschlüsselung 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. Dieser Workflow lässt sich durch die Verwendung plattformübergreifender Profilbausteine und eine zentrale Verwaltung der Geräte stark vereinfachen.



Exchange-Konfiguration auf verschiedenen Mobilplattformen

Das Smartphone oder Tablet muss dazu einmalig in die Verwaltungslösung aufgenommen werden („Enrollment“), zum Beispiel durch Verwendung des Apple Device Enrollment Programs (DEP) oder durch Scannen eines QR-Codes. Anschließend können Managementaufgaben – im Beispiel die Exchange-Konfiguration – über die Lösung zentral durchgeführt werden. Auf einer einheitlichen, plattformübergreifenden Oberfläche werden die entsprechenden Einstellungen gesetzt und können anschließend auf die verwalteten Geräte übertragen werden.



Plattformübergreifende Profilbausteine zur Konfiguration mobiler Endgeräte

Die Vorteile liegen auf der Hand: Der Administrator muss nicht mehr wissen, wo auf welchem Mobilgerät welche Einstellung vorgenommen wird – er nutzt stets die bekannte Oberfläche seiner zentralen Managementkonsole. Das verringert die Komplexität, spart Zeit und reduziert die Fehleranfälligkeit des Prozesses. Unterm Strich ergibt sich damit auch ein Mehr an Sicherheit.

Ein weiterer Vorteil: Aufgaben lassen sich über eine Managementsoftware auch „Over-the-Air“ durchführen, ohne dass ein Administrator das Gerät in die Hand nehmen muss. Nimmt ein Nutzer beispielsweise an einem Außenstandort ein neues iOS-Gerät in Betrieb, wird dieses per Apple DEP automatisch im Management registriert. Anschließend kann der Administrator die weitere Konfiguration vornehmen. Die dabei verwendeten Abläufe und Aufgaben lassen sich

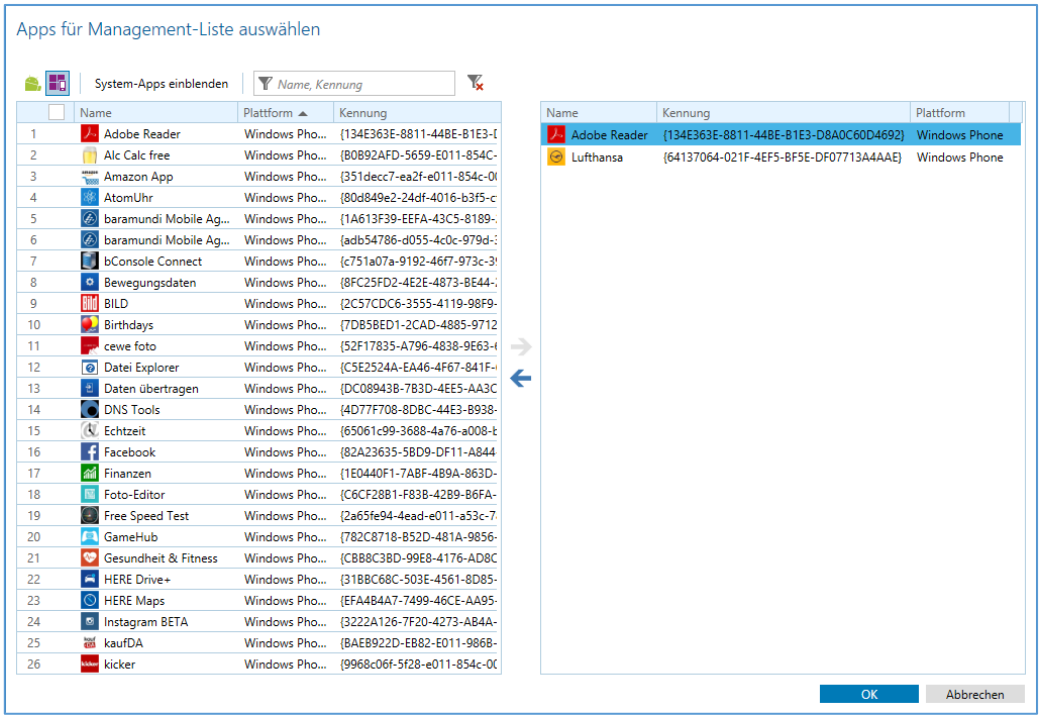
vorbereiten und immer wieder verwenden – auch für eine größere Anzahl von Geräten gleichzeitig.

Mobile Geräte können leichter verloren gehen als ein PC. Dagegen müssen entsprechende Vorkehrungen getroffen werden. In Betracht kommen hier u.a. automatisches 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 durch einen Jail Break kompromittiert.

Aus diesem Grund sollte eine Managementlösung die Möglichkeit bieten, Compliance-Regeln zu definieren, welche automatisch und regelmäßig geprüft werden. Bei Verstößen wird der Administrator informiert und hat so die Möglichkeit, Gegenmaßnahmen – wie eine E-Mail an den Nutzer bis hin zur Löschung des Geräts aus der Ferne – zu ergreifen. Ebenso wichtig wie das Unterbinden von Manipulationen ist das zeitnahe Aktualisieren der Firmware, sobald der Hersteller eine neue Version anbietet. Diese bringt in der Regel nicht nur neue Funktionen, sondern beseitigt auch Schwachstellen. Derartige Upgrades können auf modernen Plattformen bereits ferngesteuert werden.

Um die Ausführung gefährlicher Apps zu verhindern oder eine Auswahl als vom Unternehmen vertrauenswürdig eingestufter Apps anzubieten, sollte die Lösung Block- bzw. Allow Listen unterstützen. Dann kann der Administrator auf kompatiblen Mobilgeräten die Installation bzw. Ausführung ungewünschter Apps unterbinden. Umgekehrt ermöglicht der Allow Listing Ansatz, explizit erlaubte Apps zu definieren, so dass alle nicht gelisteten Apps an der Installation bzw. Ausführung gehindert werden.



App-Auswahl für Block- und Allow Listing

Je nach Präferenz des Administrators kann entweder Allow oder Block Listing für ein jeweiliges Endgerät genutzt werden. Nach der Entscheidung für den Listentyp, werden die entsprechenden Apps der Liste hinzugefügt und dann als Profil auf das Mobilgerät übertragen.

Als aktives Mitglied der AppConfig Community – eine Initiative führender EMM-Hersteller – hat sich baramundi dem Ziel verschrieben, die Verteilung und Konfiguration von Apps unter Nutzung von nativen Mitteln der Betriebssystemhersteller zu vereinfachen. Die Suite bietet vielfältige Funktionalitäten zu Mobile Device Management (MDM) und Mobile Application Management (MAM) und wird durch geeignete Apps von Drittanbietern aus dem Dokumentenmanagementsysteme (DMS)-/Personal Information Management (PIM)-Umfeld um Mobile-Content-Management (MCM)-Funktionalitäten ergänzt. Die Verbindung dieser Bereiche gelingt durch Konfigurationsstandards auf Ebene von iOS und AppConfig, so dass die Managementlösung auch für die komfortable Verteilung und Einrichtung der MCM-Funktionen sorgt, deren inhaltliche Funktionen wie Datensynchronisation und Datenbearbeitung jedoch den Drittanbieter-Apps vorbehalten bleibt.

Die Integration des Enterprise Mobility Management in eine Software Suite für Endpoint Management spart nicht nur Aufwand bei Einrichtung, Wartung und Bedienung. Es ermöglicht darüber hinaus, Mobilgeräte und PCs in gemeinsamen Gruppen und Organisationseinheiten zu verwalten und einheitliche Standards durchzusetzen. Dieser Ansatz gilt zudem als zukunftssicherer, da sich neue Geräteklassen leichter in eine einheitliche Lösung einbinden lassen.

4 Datensicherheit und Datenschutz

IT-Administration bedeutet auch die Verantwortung für Datensicherung und Datensicherheit. Unerlässlich ist daher ein automatisiertes Backup. So lassen sich im Fall des Falles Daten und Benutzereinstellungen einfach und unkompliziert wiederherstellen – bis hin zum Word Dictionary und den Desktop Icons. Auch diese Abläufe lassen sich über eine Managementsoftware zuverlässig automatisieren.

Ebenso wichtig ist zudem die Einhaltung der geltenden Rechtsvorschriften zum Datenschutz. Da aus den zahlreichen Nutzerdaten, die ein Managementsystem potentiell erfasst, auf ein individuelles Nutzerverhalten geschlossen werden könnte, muss deren Einhaltung sichergestellt werden – etwa durch ein differenziertes Rechtemanagement oder eine zusammenfassende Darstellung und Speicherung von Daten. Wichtig ist daher, dass der Hersteller der Managementlösung die hierzulande geltenden Datenschutzvorgaben bereits beim Design der Lösung berücksichtigt und sie entsprechend implementiert hat.

Über die baramundi software GmbH

baramundi software entwickelt Unified Endpoint Management zur zentralen Verwaltung von PCs, Mobilgeräten und Servern. Sie automatisiert Softwareverteilung, vereinfacht Patchmanagement und schafft Transparenz im Netzwerk. baramundi trägt so maßgeblich zur IT-Sicherheit bei und setzt Ressourcen frei.

www.baramundi.com

Sie möchten sich die baramundi Management Suite ansehen? Melden Sie sich zum Live Webinar an!

Erleben Sie im kostenfreien Webinar, wie Sie mit der baramundi Management Suite Ihre PC-Clients, Server und Mobilgeräte automatisiert verwalten und absichern.

www.baramundi.com/de-de/it-training/webinare/

baramundi

Wir freuen uns, Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

+44 2071 93 28 77
request@baramundi.com
www.baramundi.com

+48 735 91 44 54
request@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

+43 1 71 72 85 45
request@baramundi.com
www.baramundi.com

+39 340 8861886
request@baramundi.com
www.baramundi.com

+41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

+1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com