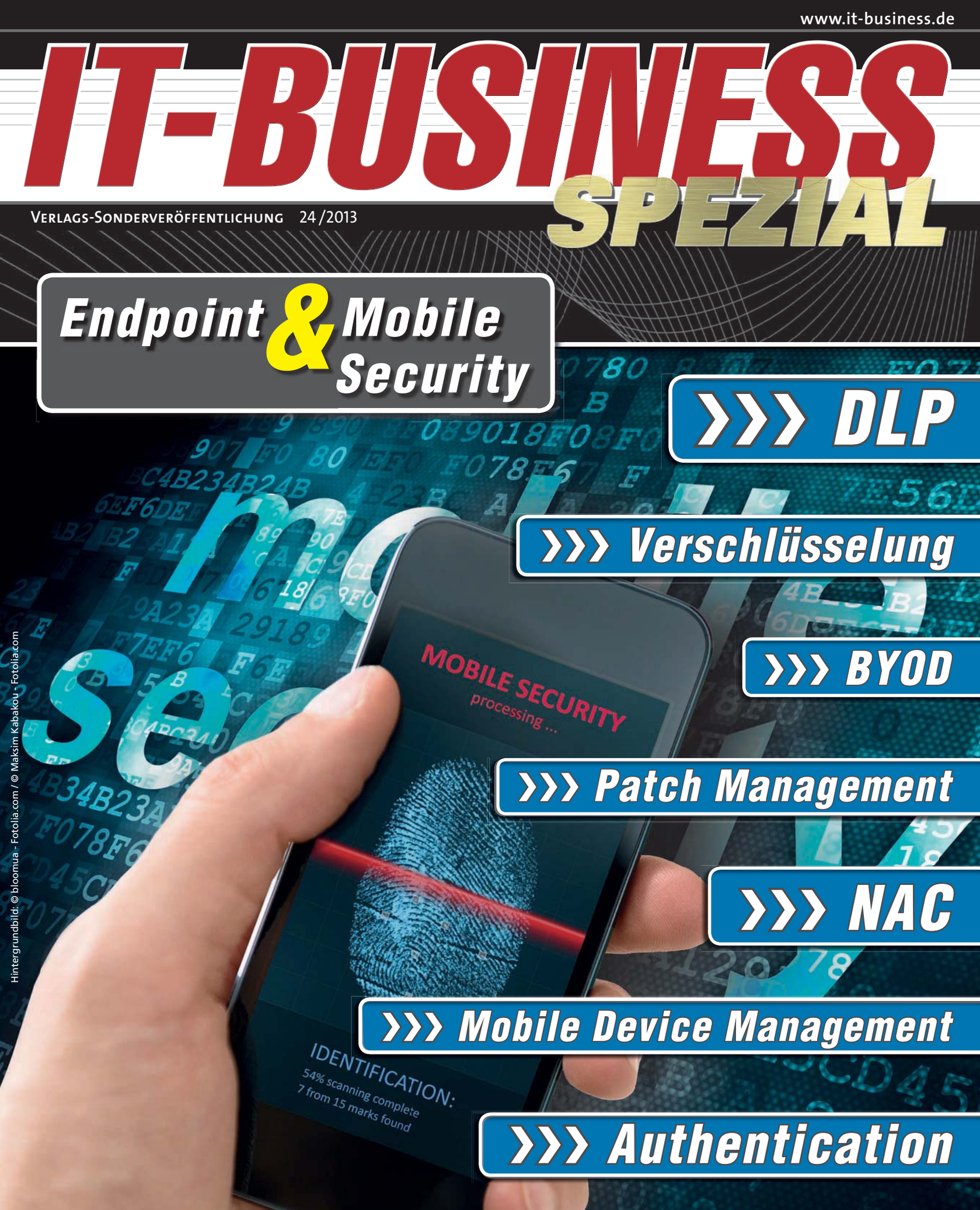
www.it-business.de

IT-BUSINESS SPEZIAL

Verlags-Sonderveröffentlichung 24 /2013

Endpoint & Mobile Security



- DLP
- Verschlüsselung
- BYOD
- Patch Management
- NAC
- Mobile Device Management
- Authentication

Vogel Business Media

Technologie, Anbieter, Partner-Business

INTERVIEW

ESP für Smartphone und Tablet

In Autos gehören sie zum Standard: Systeme, die übermüdete Fahrer warnen oder ein Schleudern verhindern. IT-Administratoren müssen auch beim Management von Mobilgeräten nicht auf Sicherheitsassistenten verzichten. Armin Leinfelder, Produktmanager beim Client-Management-Hersteller baramundi software AG, beschreibt, wie das praktisch funktioniert.

Armin Leinfelder, Produktmanager bei baramundi software AG

„Auf mobilen Geräten lassen sich Sicherheitsrichtlinien auf herkömmliche Weise nur bedingt durchsetzen..“

Armin Leinfelder
Produktmanager bei baramundi

ITB: Herr Leinfelder, Mobile-Device-Management, kurz MDM, ist aktuell ein vieldiskutiertes Thema in der IT. Warum sollten sich Unternehmen damit beschäftigen?

Leinfelder: Über die Bedeutung von Smartphones und Tablets müssen wir ja nicht mehr sprechen. Nicht nur für das Management oder für Mitarbeiter im Außendienst sind die mobilen Geräte inzwischen unverzichtbar geworden und müssen zuverlässig funktionieren, um ein produktives Arbeiten zu unterstützen. Für Unternehmen und deren Daten bringen sie aber auch ein neues Risiko und neue Herausforderungen mit sich.

ITB: Inwiefern?

Leinfelder: Die Geräte sind klein und mobil, gehen also viel leichter verloren. Ferner sind sie mit klassischen PC-Management-Lösungen nicht zu verwalten. Und: Die aktuell verfügbaren Modelle sind vorrangig für den Consumer-Markt entwickelt worden. Es sind keine Administratorenrollen vorgesehen, wie wir das unter Windows kennen. Jeder Benutzer kann auf seinem Gerät praktisch machen, was er will. Damit lassen sich Sicherheitsrichtlinien auf herkömmliche Art und Weise nur bedingt durchsetzen.

ITB: Welche Strategie schlagen Sie IT-Verantwortlichen vor?

Leinfelder: Gewisse Eigenschaften, wie ein ausreichend komplexes Passwort zum Schutz von Gerät und Daten, kann man mit MDM zentral über einfache Policies erzwingen. Aber da der Administrator typischerweise nicht ohne Weiteres die Installation einzelner Apps unterbinden kann, ist es wichtig, die Anwender als Geräte-Admins zu sensibilisieren und mit ins Boot zu holen. Weil das allein aber blauäugig wäre, ist zusätzlich eine kontinuierliche Kontrolle nötig, ob die Anwender sich an die Spielregeln des Unternehmens halten und die Geräte tatsächlich compliant sind.

ITB: Wie sieht das praktisch aus?

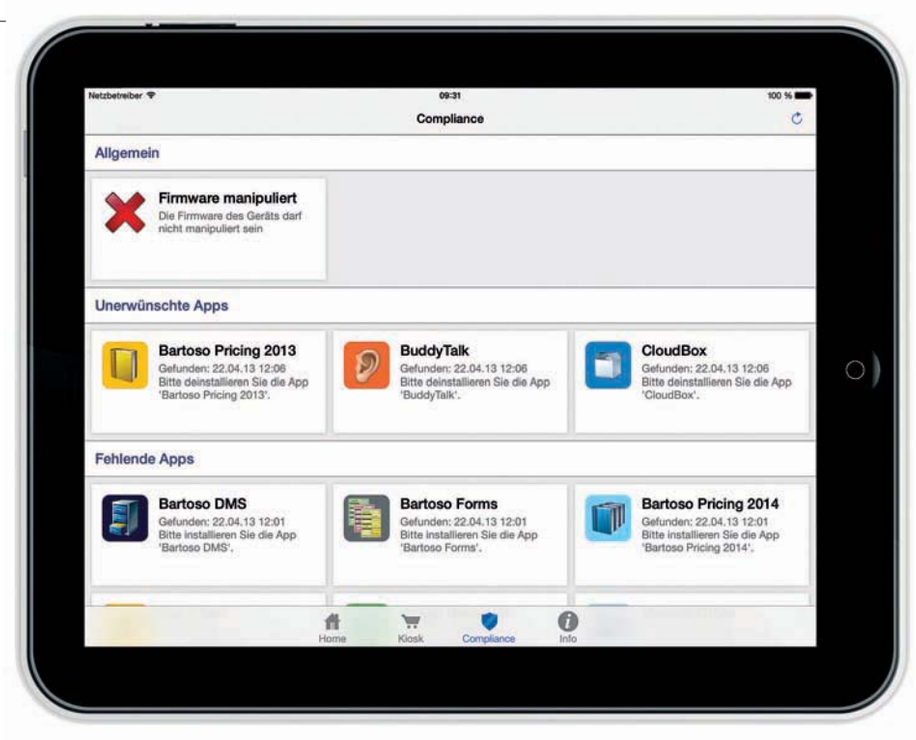
Leinfelder: In unserer MDM-Lösung gibt es die Möglichkeit, die Installation von Apps sowie Konfigurationseinstellungen per baramundi-Kiosk bereitzustellen. Der Endbenutzer kann diese Aktionen jederzeit abrufen. Damit geben Administratoren den Anwendern eine klare Empfehlung: Installiert bitte gerne alle geprüften Apps aus dem Kiosk auf das Firmengerät – aber nichts anderes.

ITB: Und wenn sich jemand nicht daran hält?

Leinfelder: Administratoren können die verwalteten Geräte automatisch und regelmäßig inventarisieren lassen. Und sie können Regeln festlegen, die mit dem Er-

Das Unternehmen

Die baramundi software AG entwickelt und vertreibt Client- und Server-Management-Softwarelösungen zur zentralen und zur automatisierten Verwaltung von auf Microsoft basierenden IT-Umgebungen. Im Mittelpunkt des Portfolios steht die baramundi Management Suite, eine modular aufgebaute Verwaltungslösung für PCs, Server und Mobilgeräte. Mehr als 1.200 Kunden aller Branchen und Unternehmensgrößen profitieren seit über 13 Jahren von der profunden Erfahrung und den innovativen Produktentwicklungen. In unabhängigen Kundenumfragen wurde baramundi mehrfach mit Bestnoten für Produktqualität, Service und Support ausgezeichnet. Als Produkte eines deutschen Herstellers halten die baramundi-Lösungen die deutschen Datenschutznormen ein.



Die MDM-Lösung von baramundi gibt den Mitarbeitern eine Übersicht über den Compliance-Status und ermöglicht die Installation von Apps.

gebnis der Inventur abgeglichen werden. Zum Beispiel: Die „datenhungrige" Taschenlampen-App X ist verboten. Oder sie definieren eine Business-App Y als erforderlich. Oder natürlich: Kein Jailbreak. Das Ergebnis dieses Abgleichs zeigt ihnen das Compliance-Dashboard an – nach Geräten, nach Schweregrad des Verstoßes, wie Sie wollen.

ITB: Und dann kann der Admin einschreiten...

Leinfelder: Richtig. Der Administrator entscheidet, was passieren soll. Bei einem minderschweren Verstoß spricht er den Kollegen vielleicht nur an. Er kann aber beispielsweise auch festlegen, dass automatisch das Exchange-Profil des Gerätes deinstalliert wird und so die Unternehmensdaten schützen. Im Extremfall kann er das Gerät sogar „remote wipen": Er löscht aus der Ferne alle Daten. Übrigens: Auch der Nutzer kann jederzeit den Compliance-Status seines Gerätes abrufen. Viele Compliance-Verstöße passieren ja nicht aus Böswilligkeit, sondern aus Versehen oder Unwissenheit. Mit der Warnung geben wir dem Nutzer die Möglichkeit, schnell selbst wieder für Compliance seines Gerätes zu sorgen. Und der Administrator wird so von zusätzlicher Arbeit entlastet.

baramundi Mobile Devices

Die baramundi-Lösung für das automatisierte Management mobiler Geräte unterstützt die Betriebssysteme Android, iOS und Windows Phone. Abgedeckt wird der gesamte Lifecycle eines mobilen Gerätes von der Aufnahme in die Management-Lösung bis zum sicheren Löschen der Daten bei Verlust oder Außerbetriebnahme. Auch ein Bring-Your-Own-Device-Szenario lässt sich mit baramundi Mobile Devices unkompliziert bewältigen. Die Lösung ist in die bewährte, anwenderfreundliche Oberfläche der baramundi Management Suite eingebunden.

ITB: baramundi legt einen Schwerpunkt auf das Thema Datenschutz. Warum spielt das beim MDM eine besondere Rolle?

Leinfelder: Mobilgeräte sammeln eine Vielzahl von schutzwürdigen Daten, zum Beispiel Standort, gewählte Rufnummer und so weiter. Wir sind als deutscher Hersteller den deutschen und europäischen Datenschutznormen verpflichtet und achten darauf, dass mit unserer Lösung keine unzulässige Überwachung des individuellen Mitarbeiterverhaltens möglich ist. Und: Wir sind als deutsches Unternehmen nicht gezwungen, eine Schnittstelle für – überspitzt gesagt – die NSA einzubauen. Das gilt für unsere gesamte baramundi Management Suite, in die unsere MDM-Lösung integriert ist. Diese Integration betrachten wir übrigens als wesentlichen Vorteil unserer Lösung.

ITB: Worin liegt dieser Vorteil?

Leinfelder: Unsere MDM-Lösung ist kein zugekauftes Modul, sondern eine komplette Eigenentwicklung, die nahtlos in die baramundi Management Suite eingepasst ist. Das bedeutet: Nur eine Benutzeroberfläche, nur eine gemeinsame Datenbank und nur ein Support-Ansprechpartner. Anwender müssen nicht zwei Systeme lernen, pflegen und bedienen. Und wir sehen diesen Ansatz ganz einfach als zukunftssicherer an.

ITB: Weshalb ist eine integrierte Lösung eine gute Investition in die Zukunft?

Leinfelder: Es ist offensichtlich, dass Mobilgeräte zunehmend klassische PCs und Notebooks ergänzen. Und es ist zu beobachten, dass die Geräteklassen zunehmend verschwimmen. Schon jetzt gibt es Apps nicht nur auf dem Smartphone, sondern auch auf dem Desktop-PC oder Windows-Rechner mit Android-Komponente. Dafür sehen wir unsere Kunden gut gerüstet, weil sie zukünftige Geräte und Geräteklassen einfacher abdecken können als Unternehmen, die zwei getrennte Systeme für MDM und Client-Management einsetzen. Nehmen Sie zum Beispiel ein „Surface Pro"-Gerät von Microsoft – ist das eher ein Tablet oder mehr ein Notebook? Mit einer integrierten Management-Lösung ist das egal, da Sie PCs und mobile Geräte gleichermaßen damit verwalten können. □