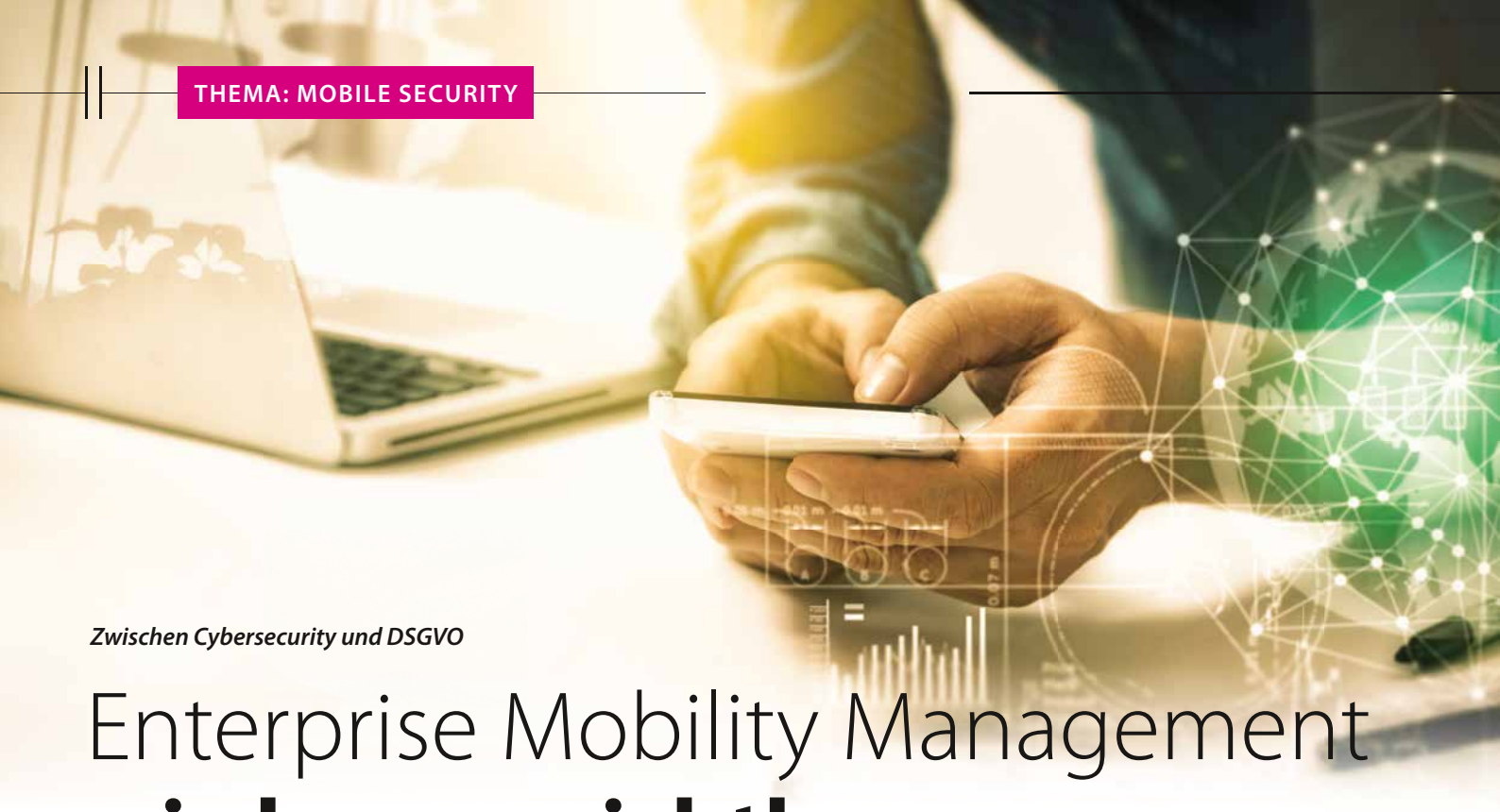

Zwischen Cybersecurity und DSGVO

Enterprise Mobility Management **wird unverzichtbar**

Eine gute IT- und Datensicherheit wissen viele erst dann zu schätzen, wenn es bereits zu spät ist. Im Hinblick auf die bevorstehende EU-Datenschutzgrundverordnung (DSGVO) ist dies kein gutes Omen. Und vor allem im Bereich „Mobile" drückt der Schuh gewaltig.

Laut der diesjährigen IDC Studie zur Mobile Security in Deutschland gehen 52% der IT-Verantwortlichen davon aus, dass Mitarbeiter die Gefahren im Umgang mit mobilen Endgeräten unterschätzen und damit selbst zu einer noch größeren Bedrohung für die IT als Cyber-Kriminelle werden.

Von Geräten über Anwendungen zu Inhalten

Je smarter mobile Technologien werden, umso weniger geht es Nutzern um das Gerät selbst, sondern darum, was damit möglich ist – sprich Anwendungen. Wo früher nur reines Mobile Device Management (MDM) – also die Verwaltung der reinen mobilen Geräte innerhalb des Unternehmensnetzwerkes – erhältlich war, braucht es deshalb jetzt auch ein Mobile Application Management (MAM). Mittels MAM legen Administratoren fest, auf welche Anwendungen Nutzer zugreifen können. Mobile Content Management (MCM) definiert als dritter Zweig die Regeln für mobil transportierte Inhalte. Um all diese Aufgaben gemeinsam und übersichtlich in einer Oberfläche erledigen zu können, bietet baramundi mit der baramundi Management Suite eine integrierte Enterprise-Mobility-Management-Lösung (EMM) an.

Sicheres EMM beginnt bei den Standardkonfigurationen

Klassische MDM-Funktionalitäten, wie die erstmalige Einbindung von Geräten in die Managementlösung und die Konfiguration der Geräte, dürfen bei einer umfassenden EMM-Lösung nicht fehlen. Je mehr diese Standardprozesse automatisiert werden, umso besser für den Administrator. Neben der Arbeitserleichterung im Vergleich zur manuellen Konfiguration bedeutet es nicht zuletzt eine deutlich geringere Fehlerquote. Leicht verständliche Standardprozesse, auch für Nutzer mit Basis-IT-Kenntnissen, sind auch im baramundi Modul Mobile Devices enthalten: beispielsweise das Geräte-Enrollment über einen QR-Code. Über E-Mail erhalten Nutzer dabei von der IT-Administration einen Code zugeschickt, scannen diesen mit ihrem neu zu registrierenden Gerät ein bestätigen die Verwaltung durch die EMM-Suite und das Gerät kann fortan verwaltet werden. Apple bietet mit seinem Device Enrollment Program (DEP) an, dass iOS-Geräte bereits vor der Aushändigung an die Mitarbeiter direkt für die jeweilige Managementlösung registriert werden.

Der Administrator definiert vielfältige Einstellungen und managt Geräte mit verschiedenen Betriebssystemen über eine einheitliche Oberfläche: Parameter wie Name, Domäne und Server werden über eine einheitliche Maske eingegeben; Zugangsdaten für VPN, Wi-Fi und E-Mail werden verteilt und Regeln zur Passwortkomplexität oder automatischen Sperrung bei vordefinierter Inaktivität festgelegt. Ein gutes EMM unterstützt außerdem bei Updates von Apps und Firmware. Im Falle eines Jailbreak (iOS) oder Root (Android), also einer Modifikation des Betriebssystems, werden Schutzfunktionen durch den Fremdeingriff ausgehebelt. Das Risiko,

sich dann Schadsoftware einzufangen, steigt damit stark an. Automatische Compliance-Prüfungen und eine sofortige Alert-Funktion bei etwaigen Verstößen müssen deshalb unbedingt in der EMM-Lösung enthalten sein.

Spezielle Vorkehrungen für Enterprise Mobility

Die unkontrollierte Installation von Anwendungen auf mobilen Geräten sind eine der größten Sorgen jedes IT-Verantwortlichen. Es liegt im Interesse der Unternehmen, die Auswahl der installierbaren Applikationen zu kontrollieren. Dies funktioniert über sogenanntes App-Black- bzw. Whitelisting. Der Administrator kann hierbei bestimmte Apps explizit erlauben oder verbieten. Diese Listen werden sodann je nach Nutzerprofil und entsprechenden Compliance-Richtlinien auf das Mobilgerät übertragen und bieten damit sowohl Schutz vor potenziell gefährlichen Apps aus unbekannter Quelle als auch Anwendungen, die allzu umfassenden Datenzugriff verlangen.

Zum weiteren Schutz der Unternehmensdaten können Nutzer auch auf spezielle Container-Apps für sogenanntes Personal Information Management (PIM) und Dokumentenmanagementsysteme (DMS) zugreifen. Zu PIM zählen persönliche Daten wie Kontakte, Termine, Notizen und E-Mails, die streng von den anderen Daten zu isolieren sind. Stecken alle kritischen Unternehmensdaten in einer Container-App, sind diese vor der Interaktion mit „privaten" Applikationen oder durch private Dateien eingeschleuste Malware geschützt. Zur weiteren Sicherheit werden die Daten in der Container-App verschlüsselt. Sollte ein Gerät verloren gehen, haben Administratoren auch aus der Ferne Zugriff auf Daten und können diese innerhalb der Container-App gegebenenfalls löschen – Stichwort Enterprise Wipe oder Selective Wipe. Ausgewählte Unternehmensdaten werden vernichtet und private Daten bleiben unangetastet. So wird auch der Einsatz von Bring-your-own-Device (BYOD), also der Einbindung von privaten Mobilgeräten in das Unternehmensnetzwerk für IT-Administratoren sicherer und leichter zu managen.

Das richtige Maß finden

Vielen Unternehmen, vor allem im Mittelstand, fehlen die nötigen personellen und finanziellen Ressourcen für eine allumfassende mobile Sicherheitsstrategie. Außerdem wollen Nutzer von Sicherheitsvorkehrungen oft wenig hören, da diese Funktionalitäten einschränken und für viele Nutzer die persönliche Produktivität im Vordergrund steht. Die IT-Administration befindet sich stetig in einem Balanceakt, um das richtige Maß zwischen Kontrolle und einfachem und schnellem Workflow für die Nutzer zu bieten. Verbote alleine schützen sicher nicht – die Nutzer selbst müssen geschult und sensibilisiert werden, welche Gefahren beim Einsatz mobiler Geräte möglich sind und wie man diese abwehrt. Zusätzlich kann Nutzern ein Self-Service-Bereich innerhalb der EMM-Lösung zur Verfügung gestellt werden. Dieser entlastet die Support-Mitarbeiter und schafft für die IT-Administration freie Zeit, sich anderen Aufgaben zu widmen.

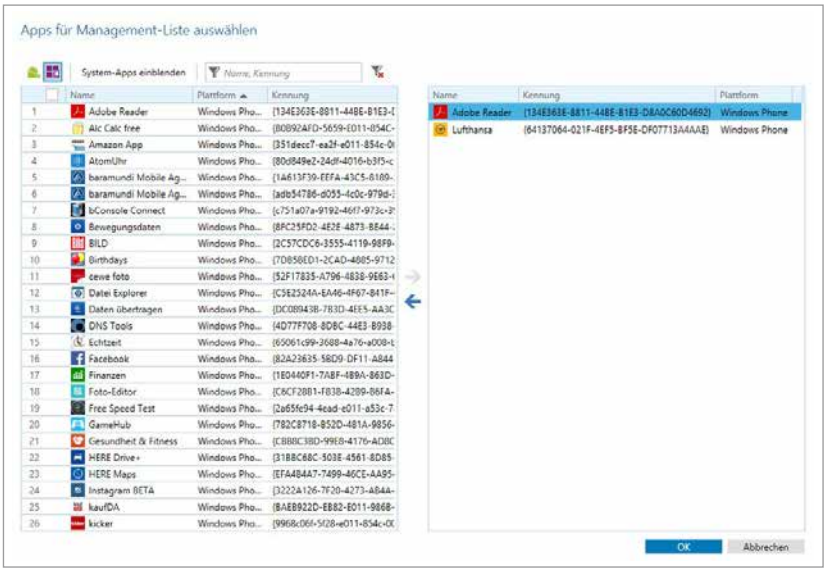

Bild: App-Auswahl für Black- oder Whitelisting

Die DSGVO-Uhr tickt

Es bleibt nur noch weniger als ein Jahr bis zur EU-Datenschutzgrundverordnung (DSGVO), die bis spätestens Mai 2018 in Unternehmen umzusetzen ist. Ab dann müssen Unternehmen belegen können, dass ihre Daten sicher sind und jegliche Verletzung sofort melden. Bei Verstoß sehen die Regeln zur Speicherung, Verarbeitung und Weitergabe von Daten von EU-Bürgern harte Strafen vor: Bußgelder von bis zu vier Prozent des Jahresumsatzes oder bis zu 20 Millionen Euro. Und noch nicht alle Unternehmen sind ausreichend darauf vorbereitet. Schließlich bedeutet die DSGVO nicht nur eine umfassendere Sicherheitsstrategie für die Gesamt-IT, sondern auch eine Optimierung des Managements und eine Schulung aller Mitarbeiter. Fakt ist: „Mobile" muss aufgrund der Nähe zum Nutzer und der Gefahr unerkannter Schatten-IT durch BYOD und den damit verbundenen Sicherheitsrisiken eine besondere Stellung einnehmen. Unternehmen sollten hier besser schon gestern als heute aktiv geworden sein.

Unternehmen sollten allen drei Bereichen – MDM, MAM und MCM – die gleiche Aufmerksamkeit schenken. Besonders in Zeiten knapper IT-Budgets bei gleichzeitigem Wachstum der Aufgaben und komplexer werdenden Bedrohungen sollten effiziente Tools zur Unterstützung der IT-Abteilungen eingesetzt werden. Die Zusammenfassung aller Aufgaben des Enterprise Mobility Managements in eine übersichtliche und automatisierte Lösung ist für Administratoren, vor allem in Hinblick auf die aktuellen Herausforderungen der Cybersecurity und DSGVO, unverzichtbar.

Armin Leinfelder

WEB-TIPP:
www.baramundi.de