AUSZUG AUS... MOBILE BUSINESS AUSGABE 4-5|2016

KRASSE SICHERHEITSLÜCKEN

DIE GEFAHR DROHT IM WLAN

IM INTERVIEW ERLÄUTERT CHRISTIAN KEHL, *Technical Business Developer beim IT-Dienstleister Appsphere AG, warum sich die meisten Nutzer mobiler Endgeräte in den Unternehmen zwischen absoluter Einschränkung bis hin zu grenzenloser Freiheit bewegen. Zudem legt er dar, inwieweit an dieser Stelle sogenannte „Mobile Device Policies" greifen könnten.*

Herr Kehl, wie steht es aktuell um die Einbindung mobiler Endgeräte in die Prozesse deutscher Unternehmen?

CHRISTIAN KEHL: Eine Studie hat kürzlich ergeben, dass bei rund 50 Prozent aller befragten Unternehmen jeder Mitarbeiter mit drei oder mehr mobilen Geräten arbeitet. Damit werden Firmendaten wie E-Mails, Kontaktinformationen, Dateien oder Kennwörter auf zahlreichen verschiedenen, oftmals auch privaten Geräten genutzt. Leider mangelt es häufig an einer zentralen Administration der Devices.

Welche Sicherheitsgefahren drohen dadurch?

KEHL: Die jederzeitige Verfügbarkeit von Unternehmensinformationen, die ja eigentlich ein Vorteil für Firmen und Angestellte sein sollte, wird schnell zum Nachteil. Denn ohne ein Regelwerk und die zentrale Verwaltung kann schlicht nicht kontrolliert werden, wohin bestimmte Daten verteilt oder ob diese eventuell sogar ausspioniert werden. Die größte Gefahr liegt aber sicherlich in Download und Nutzung kompromittierter Anwendungen. Ein ebenso großes Risiko geht von der Verbindung mit öffentlichen WLANs einher. Dies betrifft nicht nur Firmen-Smartphones, sondern auch die privaten Geräte.

Wie wahrscheinlich ist es eigentlich, dass jemand das eigene Smartphone hackt und spioniert?

KEHL: Das Risiko wird häufig unterschätzt, weil man sich nicht vorstellen kann, wer Interesse an den eigenen Daten haben sollte. Wenn man jedoch bedenkt, dass man sogar schon sein Banking per Smartphone erledigt, schärft das vielleicht die Sinne. Im Unternehmensumfeld ist das natürlich erst recht wichtig. Neben Apps gilt unabhängig von Betriebssystem und Smartphone besonderes Augenmerk der Nutzung öffentlicher WLANs. Außerdem sucht jedes Mobilgerät bei aktiviertem WLAN ständig nach gespeicherten Verbindungen. Diese Scans und Verbindungsversuche können sehr einfach von Dritten mitgelesen werden. Da ungesicherte WLAN-Verbindungen außerdem absolut einfach simuliert werden können, erhalten Dritte einfach Zugang zu SMS-Speicher, persönlichen Kontaktlisten, Geo-Daten und eben auch zum Dateisystem. Sogar der komplette Datenverkehr und persönliche Informationen werden auf diesem Weg mitgelesen, ohne dass es Betroffene merken.

Welche Schlussfolgerungen müssen die Verantwortlichen daraus ziehen?

KEHL: Wichtig ist eine ständige und nachhaltige Sensibilisierung der Mitarbeiter beispielsweise mit dem Hinweis, dass ungenutzte WLAN-Profile regelmäßig gelöscht und das WLAN bei Nichtbenutzung am besten deaktiviert werden sollte. Mitunter haben Unternehmen bereits Mobile-Device-Management-Lösungen (MDM) im Einsatz. Diese werden allerdings häufig noch nicht voll ausgeschöpft, weil nur die unterschiedlichen Plattformen und Geräte verwaltet oder Zugangsinformation zum Mail-System bereitgestellt werden. In puncto

„Immer mehr Mitarbeiter arbeiten mit drei oder mehr mobilen Geräten.“

Christian Kehl, Appsphere AG

Sicherheit besteht da auf jeden Fall noch Nachholbedarf.

Gerade „Bring your own Device (BYOD)“ steht zumeist in der Kritik. Wie vermeiden Unternehmen, dass über die Privatgeräte der Mitarbeiter Gefahren entstehen?

KEHL: An der Stelle kommt wieder MDM ins Spiel, das entsprechend erweitert werden müsste. Dadurch können E-Mail-Services und/oder die IT-Infrastruktur nur für registrierte und richtlinienkonforme Geräte freigegeben und auch der Zugriff auf Unternehmens- und persönliche Arbeitsdokumente kann voneinander separiert und so besser kontrolliert werden. Hinzukommen sollte eine Data Leak Prevention (DLP), welche die unautorisierte Weitergabe von Dateien verhindert. Hier muss granular definiert und geregelt werden, welcher Benutzer, welches Gerät auf welche Anwendungen oder Services und sogar welcher Dokumenteninhalt gelesen, bearbeitet und getauscht werden darf.

Helfen „Mobile Device Policies“?

KEHL: Papier ist leider geduldig. Daher ist eine technische Unterstützung unabdingbar. Aus meiner Sicht arbeiten Smartphone-Hersteller mit MDM-Lösungsanbietern dabei noch nicht ideal zusammen. Microsoft ist aber beispielsweise ein Anbieter, der beides unter einem Dach vereint. Mit Windows 10 Mobile hat man den richtigen Ansatz gewählt: Von Anfang an stehen die granulare Verwaltung, Sicherheit und Kontrolle im Unternehmenseinsatz im Vordergrund – bei gleichzeitigem Freiraum der Benutzer. Durch „Schieberegler“ ist das zwischen absoluter Einschränkung bis hin zu grenzenloser Freiheit frei konfigurierbar.

Wie handhaben Unternehmen den Umgang mit Apps?

KEHL: Am besten sollten Apps im eigenen Enterprise Store mit Self-Service-Funktionen für Firmenanwendungen und rechtskonformes Lizenzmanagement mit integriertem Asset-Management zentral bereitgestellt werden. Alternativ sind die Stores der Hersteller wie Apple, Microsoft oder Blackberry gute Anlaufstellen. Letztere stellen in der Regel sicher, dass keine schädliche Software verbreitet wird, auch wenn es keine hundertprozentige Garantie dafür gibt.

Was bringt die Zukunft an neuen Geräten für mobile Benutzer – und somit auch an Herausforderungen für die Unternehmens-IT?

KEHL: Microsoft versucht aktuell, im Zusammenspiel von Windows 10 Mobile und Continuum aus dem Smartphone einen PC zu formen. So sind mobile Anwendungen mit Maus, Tastatur und Monitor direkt am Smartphone nutzbar. Es wird spannend sein zu beobachten, ob hier Anbieter wie Apple nachziehen. Abgesehen von der neuen Hardware, die dafür notwendig sein wird, wird das Thema Sicherheit somit nochmal bedeutender.

KONSTANZE KULUS