DuD
Datenschutz und Datensicherheit

Amtliche Geschäftsschädigung

Dirk Fox

Die Nachricht der Computerwoche vom 08.06.2005, der Automobilhersteller Audi hege Sicherheitsbedenken gegenüber Blackberry, säte erste Zweifel an der Vertrauenswürdigkeit des vom kanadischen Unternehmen Research In Motion (RIM) betriebenen mobilen E-Mail-Push-Dienstes, über den E-Mails vom Mailserver des Unternehmens an mobile Endgeräte der Mitarbeiter weitergeleitet werden können. Mit weltweit mehr als 3,65 Millionen Nutzern ist RIM der mit Abstand erfolgreichste Anbieter; der Verkauf der liebevoll „Tamagotchi für Manager" genannten Blackbery-SmartPhones wuchs im 3. Quartal 2005 um 56 % (Gartner) – damit erreichen sie im PDA-Markt einen Anteil von über 25 %, deutlich vor Palm (15 %) und HP (6 %).

Die Veröffentlichung der Ergebnisse einer internen Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vom 20.09.2005 durch die Wirtschaftswoche am 05.10.2005 schlug daher ein wie eine Bombe. Darin wird dem Blackberry-Dienst bescheinigt, er sei „auf Grund der (...) unsicheren Architektur für den Einsatz in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet".

Die Befürchtung: Da in Europa alle an ein Blackberry-Endgerät weiter zu leitenden Nachrichten zunächst über das Internet an ein zentrales Mobile Routing Center (MRC) in Egham bei London geschickt würden, könne der britische Geheimdienst auf Verbindungsdaten zugreifen – und vielleicht sogar mehr. RIM-Managerin Eggberry konterte, die BSI-Schlussfolgerungen beruhten „auf einem kompletten Mangel an Kenntnis von RIMs Sicherheitsarchitektur und –infrastruktur" – harter Tobak für ein auf IT-Sicherheit spezialisiertes Bundesamt.

Wirft man einen genauen Blick auf die Ergebnisse der BSI-Analyse, wird jedoch deutlich, dass bei der Durchführung Sorgfalt nicht die oberste Pflicht war. Sein Verdikt leitet das BSI aus den folgenden fünf Kritikpunkten ab:

1. Die Übertragungssicherheit beruhe „vollständig auf proprietären Mechanismen der Firma RIM"; „für die Qualität der Implementierung, der Schlüsselerzeugung und des Schlüsselmanagements liegt jedoch keine unabhängige Evaluierung vor". Tatsache ist: Die Verschlüsselung erfolgt wahlweise mit einem der standardisierten Kryptoalgorithmen AES oder TripleDES, als Mode of Operation wird das ebenfalls standardisierte Cipher Block Chaining (CBC) verwendet – alles fraglos keine proprietären Mechanismen. Für die Implementierung im Blackberry Enterprise Server sowie den Endgeräten liegen zudem mehrere Zertifizierungen nach FIPS 140-2 (Security Requirements for Cryptographic Modules) vor – unabhängiger lässt sich kaum evaluieren.

2. Da das gesamte Nachrichtenaufkommen über ein britisches MRC geleitet wird, „sind dort alle Verbindungsdaten (Absender, Empfänger, Uhrzeit) sowie die (verschlüsselten) Kommunikationsinhalte verfügbar". Stimmt. Aber was gewinnt daraus ein möglicherweise zugreifender britischer Geheimdienst? Mit den Daten lassen sich nicht einmal Kommunikationsbeziehungen aufklären, denn Inhalt, Empfänger- und Absenderangaben der weitergeleiteten E-Mail sind wirksam verschlüsselt.

3. Nach der BSI-Analyse ist es „nicht möglich, eine eigene, von RIM unabhängige Verschlüsselung zum Schutz der Kommunikationsinhalte zu realisieren." Diese Aussage ist unzutreffend: Seit 2003 bietet RIM ein S/MIME Support Package an, mit dem eine Ende-zu-Ende-Verschlüsselung realisiert werden kann – mit Schlüsseln, die der Blackberry-Infrastruktur nicht bekannt sind. Seit kurzem ist zudem ein PGP Support Package erhältlich. Das BSI hingegen behauptet, dass „sich Mail-Anhänge, die vom Nutzer (zum Beispiel mit PGP (...)) verschlüsselt wurden, mit Blackberry nicht übertragen" lassen.

4. Schließlich wird kritisiert, dass der Blackberry Enterprise Server „hoch privilegierten Zugriff auf die Mail/Messaging-Server des Unternehmens [benötigt]. Er kann somit auf den gesamten dort gespeicherten Datenbestand zugreifen." Das ist sachlich zutreffend. Nur: Genau dies ist für die Auswahl und Weiterleitung unvermeidlich – also gerade die Aufgabe des Servers. Unklar bleibt, was daran verwerflich sein soll. Schließlich greift auch der Mailserver des Unternehmens auf den „gesamten dort gespeicherten Datenbestand" zu. Zwar stammt die Mailserver-Software nicht vom kanadischen Hersteller RIM, sondern von Microsoft, IBM oder Novell – warum aber diesen drei amerikanischen Herstellern mehr hinsichtlich einer fehler- und hintertürfreien Softwareimplementierung vertraut werden soll, erschließt sich erst recht nicht. @stake bescheinigte RIM in einer Sicherheitsanalyse sogar eine außergewöhnlich hohe Softwarequalität.

5. Weiter schreibt das BSI, „kritisch ist in diesem Zusammenhang, dass (...) nicht nachvollziehbar ist, welche Nachrichten zwischen Blackberry Enterprise Server und MRC ausgetauscht werden." Der Verdacht, RIM könnte sensible Informationen über Port 3101 nach außen versenden, ist jedoch rein spekulativ – Indizien für die Existenz einer Hintertür bleibt das BSI schuldig. Zudem lässt sich der Vorwurf auch gegen alle anderen IT-Komponenten im Netz erheben.

Der Schaden, den das BSI durch die unsorgfältige Analyse verursacht hat, ist erheblich – sowohl hinsichtlich des Zeitaufwands, der in tausenden Unternehmen zur Aufklärung aufgewendet werden musste, als auch durch die Beschädigung des eigenen Rufs. Mit verdienstvollen Innovationen wie dem IT-Grundschutz hatte sich das BSI aus dem Schatten der Vorgängerbehörde, der BND-Abteilung ZfCh herausgearbeitet – um nun einem „Enigma-Trauma" zu erliegen. Vorauseilend schrieb Lutz Diwell, Staatssekretär im Bundesinnenministerium, vier Tage vor der internen Veröffentlichung der Studie an alle Staatssekretäre und bat „nachdrücklich, keine weiteren Investitionen in Blackberry-Geräte zu tätigen". Statt dessen empfahl er eine Alternativlösung, die von BMI, BMF und BSI „mit Hochdruck" entwickelt werde – mit Steuergeldern, versteht sich.