

So sichern Sie BlackBerrys optimal!

Angefangen hatte alles damit, dass die deutsche Wirtschaftswoche im Herbst 2005 einen internen Bericht des Bundesamts für Sicherheit in der Informationstechnik BSI zitierte. „Aufgrund der unsicheren Architektur ist der BlackBerry für den Einsatz in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet“, meinte der Bericht. Die darauf folgende Welle von Pressemeldungen war enorm.



Christian Burger

Nomasis AG

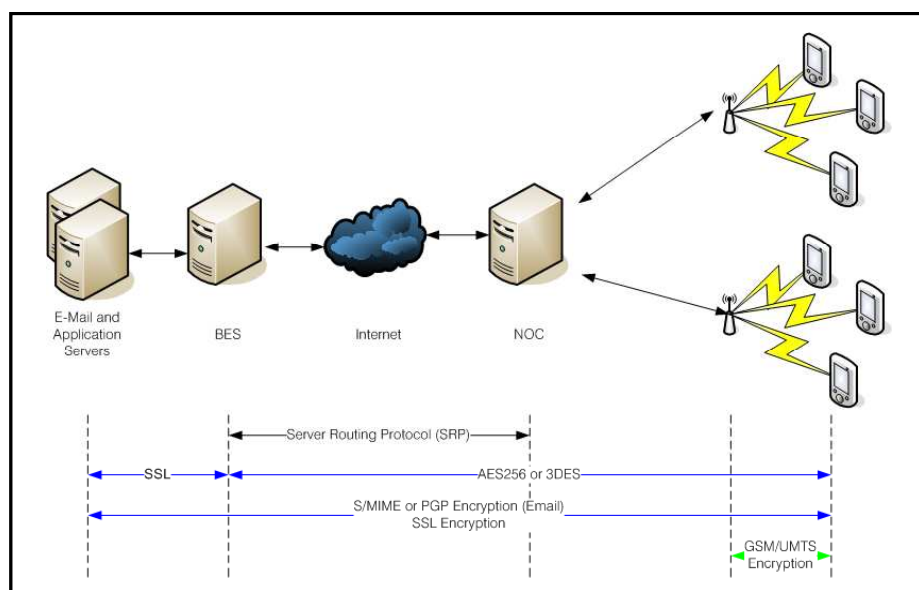


Abbildung - Die Architektur des BlackBerry-Services

Kaum ein Blatt im deutschsprachigen Raum, das die Nachricht nicht druckte. Das BSI relativierte den ursprünglich nicht für die Öffentlichkeit gedachten Bericht anschliessend und betonte, dass es nicht im Besitz des Quellcodes der Software sei und der Bericht deshalb nicht auf einer konkreten Schwachstelle oder Backdoor basiere. Der Schaden für den Hersteller RIM war trotzdem enorm: In der Folge entschieden sich unter anderem der französische Staat, die deutsche Bundeswehr und einige namhafte Unternehmen gegen die Push-E-Mail-Lösung aus Kanada. RIM versuchte seinen Ruf durch verschiedene unabhängige Gutachten wiederherzustellen.

So händigte RIM verschiedenen Regierungen seinen Quellcode zum Review aus, zertifizierte das Produkt nach Common Criteria und liess die renommierte @stake aus Kalifornien eine Analyse zur Sicherheit des Produktes durchführen. Zudem führten wahrscheinlich Hunderte von Unternehmen eigene interne Sicherheitsanalysen zum Produkt BlackBerry durch. Die letzte umfassende und von unabhängiger Stelle durchgeführte Analyse ist wohl die vom Fraunhofer Institut SIT in Deutschland. Aufgrund der technischen Architektur des Services (s. Abb.) untersuchten die meisten Analysen folgende drei Aspekte:

- Das Endgerät

- Die Integration ins Unternehmensnetzwerk und die E-Mail-Infrastruktur
- Den Transportweg zwischen Unternehmensnetzwerk und Endgerät

Dabei sind alle namhaften Analysen zu folgendem Resultat gekommen:

- Der Handheld erfüllt höchste Sicherheitsanforderungen, sofern man einige von RIM empfohlene Einstellungen vornimmt, unter anderem die Verschlüsselung des Hauptspeichers, die Kontrolle der verschiedenen Schnittstellen (Bluetooth etc.) und die Umsetzung entsprechender Passwort-Policies. Übrigens werden die Policies beim BlackBerry zentral auf dem BlackBerry Enterprise

PLATTFORM FÜR INFORMATIONSSICHERHEIT

Server BES administriert und können nicht durch den Benutzer deaktiviert werden.

- Die Integration in das Firmennetzwerk erfolgt nach gängigen Standards. Der BES baut über einen Proxy die Verbindung ins Internet auf. Jedoch benötigt der BES weitgehende Administratorrechte auf dem E-Mail-System (vor allem bei MS-Exchange). Dies könnte es RIM theoretisch erlauben über eine Backdoor sämtliche Informationen des E-Mail-Systems abzu ziehen und an das Network Operation Center NOC zu übertragen. Allerdings besteht dieses Risiko bei jeder Software (z.B. auch bei Microsoft) und ist nicht BlackBerry-spezifisch.

- Der Übertragungsweg zwischen BES und Endgerät wird mit aktuell als sicher geltenden Algorithmen (3DES oder AES256) verschlüsselt und kann somit ebenfalls als sicher bezeichnet werden. Auch der Schlüsselaustausch zwischen BES und BlackBerry erfolgt entweder direkt über die Desktop-Software oder aber über einen Shared Secret, der sowohl am BES als auch am Endgerät eingegeben werden muss und RIM nicht bekannt ist. Einzig das NOC, das von RIM betrieben wird, stellt eine potenzielle Schwachstelle dar. Bis jetzt hat niemand die Systeme im NOC auf Backdoors oder Schwachstellen überprüfen können da RIM dies bis dato nicht zugelassen hatte. Ob wirklich die von unabhängiger Stelle überprüften Versionen (z.B. beim Review des Fraunhofer Institutes SIT) im NOC im Einsatz sind, wurde bis jetzt noch von keiner unabhängigen Stelle bestätigt.

Gegenmassnahmen

Auch wenn das Restrisiko sehr klein ist, dass RIM die E-Mail-Daten seiner Kunden abhören

könnte, so ist es doch vorhanden. Wer einen Angriff auf die Vertraulichkeit von Daten plant, muss zuerst einmal in den Besitz der Daten kommen, um diese zu entschlüsseln. Diese Bedingung ist hier klar erfüllt, denn die Daten werden ja über das von RIM kontrollierte NOC geroutet. Wer sich gegen dieses Restrisiko absichern will, kommt nicht darum herum, weitere Massnahmen umzusetzen.

Für die Absicherung der E-Mails gibt es auf dem Markt bereits einige Produkte. So können z.B. PGP oder S/MIME als Methode für die Verschlüsselung und Authentisierung von E-Mails implementiert werden. Die Absicherung von Applikationen erfolgt am besten über SSL zwischen dem Handheld und dem Applikationsserver.

Eine weitere Lösung hat Anfang 2009 der deutsche Hersteller CORISECIO GmbH präsentiert. Das Produkt Mobile PKI für BlackBerry integriert eine komplette PKI-Lösung in die BlackBerry-Umgebung und bindet die Software-Zertifikate an die Geräte-ID und an die SIM-Karte. Das erwähnenswerte dabei ist vor allem, dass nicht nur Emails sondern sämtliche Kommunikation zwischen BES und BlackBerry verschlüsselt werden. Wichtig war bei der Integration, dass die Benutzerfreundlichkeit und die Interoperabilität mit dem System nicht beeinträchtigt werden. Der Benutzer merkt nichts von der zusätzlichen Sicherheit und kann sein System wie gewohnt benutzen.

Generell wäre Wünschenswert, wenn der Kunde das NOC selbst betreiben könnte oder aber es durch eine unabhängige Stelle (z.B. beim Provider) betrieben würde. Das ist aber bislang nicht möglich und scheint auch in nächster Zukunft nicht geplant.

Email-Sicherheit von A-Z

1/3 Top-Themen am

security zone **podium**
PLATTFORM FÜR INFORMATIONSSICHERHEIT

am 7. Mai 2009

Villa Belvoirpark, Zürich

Details unter:

www.security-podium.ch

Fazit

Verglichen mit anderen Push-E-Mail-Lösungen setzt der BlackBerry nicht nur was die Usability anbelangt hohe Standards. Auch in Sachen Sicherheit gibt es kaum ein Produkt auf dem Markt, das den Kanadiern das Wasser reichen könnte. Sowohl auf dem Handheld als auch bei der Integration in das Unternehmensnetzwerk war Sicherheit stets ein Designkriterium, das konsequent umgesetzt wurde. Bei der Übertragung zwischen BES und Handheld verlassen die Daten per Definition die geschützte Firmenumgebung und müssen deshalb besonders geschützt werden. BlackBerry trägt dieser Tatsache mit aktuellen Methoden und Algorithmen Rechnung, verpasst es aber leider, die Funktion des NOC in unabhängige Hände zu legen. Dies wiederum nährt bei allzu misstrauischen Zeitgenossen Zweifel an der Sicherheit des Produktes. Wer sich zu diesen zählt, wird nicht darum herumkommen, die Kommunikation zwischen den Endgeräten und dem BES mit Drittprodukten abzusichern.