

Sicherheitsanalyse des E-Mail-Push-Dienstes *BlackBerry*

Eine Studie im Auftrag des österreichischen
Bundeskanzleramtes



Kurt Dietrich

{ Kurt.Dietrich@iaik.tugraz.at }

Zentrum für sichere Informationstechnologie - Austria, A-SIT

Inhalt

- Vorstellung
- A-SIT Studie
 - Untersuchungsschwerpunkte
 - Präsentation der Ergebnisse
 - Nicht untersuchte Komponenten
 - Zusammenfassung
- @stake Sicherheitsbewertung
 - Untersuchte Bereiche
 - Präsentation der Ergebnisse
 - Empfehlungen von @stake

A-SIT & Partner



Zentrum für sichere Informationstechnologie - Austria

- gemeinnütziger Verein (seit 1999)
- Unabhängige Beratungsstelle
- Bestätigungsstelle
- Gründer: (OeNB, TU-Graz, BMF)



Partner:

- Institut f. Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK)
- Stiftung Secure Information and Communication Technologies (SIC)



Tätigkeitsschwerpunkte:

- Grundlagenforschung im Bereich Kryptographie und angewandte Informationsverarbeitung
- Lehre / Ausbildung

Weitere Tätigkeitsbereiche

- **eGovernment**
 - Reinhard Posch (CIO des Bundes)
- **Kryptographie**
 - Vincent Rijmen (AES)
- **PKI, Trusted Computing , Side Channel Analysis, Java Security, RFID etc.**
- **IT-Security Expertisen für:**
 - Anwendungen (Communication & Security)
 - Systemsicherheit (VLSI, Netzwerk & Communication Security, E-Government)
 - Netzwerke (VLSI, Krypto, RFID)

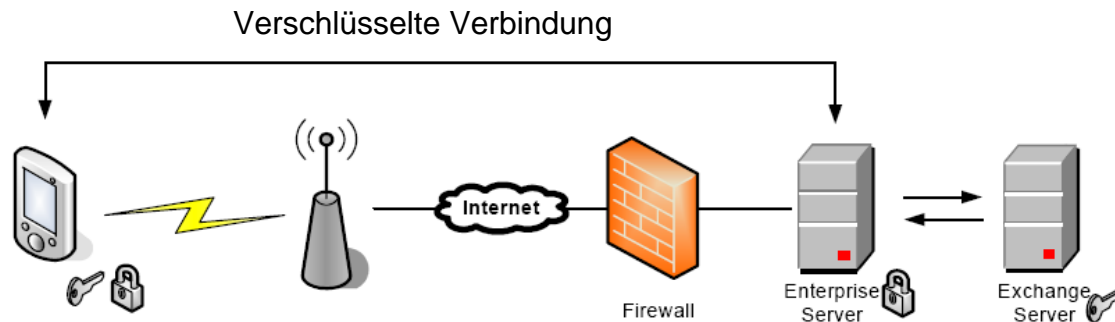
Die A-SIT Studie

- Analyse für Bundeskanzleramt
- Entstanden Oktober 2004
- Ziele:
 - Untersuchung des Konzeptes
 - Aufdecken offensichtlicher Schwächen
- Unterstützung durch Mobilkom Austria & RIM Deutschland

Untersuchungsschwerpunkte

- Übertragungssicherheit
 - Verschlüsselte Übertragung
- Gerätesicherheit
 - Passwörter, Daten
- Applikationssicherheit
 - Einfluss von Fremdsoftware
- Optionale Komponenten
 - S/MIME Package etc.

Übertragungssicherheit 1/2



- AES / TripleDES Verschlüsselung
- FIPS 140-2 Zertifizierung
- Hier: BlackBerry Enterprise Server (BES) hinter Firmenfirewall

Übertragungssicherheit 2/2

- Jedes Gerät hat eigenen Schlüssel
- Schlüsseltausch
 - Desktop, Wireless
 - Periode wichtig
- Schlüsselerzeugung
 - Am Desktop
 - Über speziellen Dienst

Gerätesicherheit 1/2

- Passwörter
 - Regeln über *Policy* steuerbar
 - Mindestlänge, Wiederholungen
 - Eliminierung trivialer Passwörter
- Daten
 - ab Version 4.0 am Gerät verschlüsselbar
 - kein Schutz gegen physischen Einbruch

Gerätesicherheit 2/2

- **Zugriffschutz:**
 - Bildschirmschoner
 - Externe Schnittstellen blockiert (IR, Keyboard, Bluetooth)
 - Löschung der Daten bei Fehlversuch
- **Bei Verlust:**
 - Daten werden weiterhin an das Gerät gesendet!

Applikationssicherheit

- Installation von Fremdsoftware
 - Keine „native“ Applikationen
 - Ab Version 3.6 J2ME Applikationen
- Erweiterte API mit Signatur von RIM
- Entscheidung, ob Applikation vertraut wird liegt beim Anwender
- Installation per Policy verhinderbar

Optionale Komponenten

- S/MIME Support Package
 - End-to-end Security
 - Public Key Infrastruktur (PKI) notwendig
 - Attachments können nicht konvertiert werden

- Desktop Redirector
 - Bei Vorhandensein eines BES nicht möglich

Nicht untersuchte Komponenten

- Server Routing Protokoll (SRP)
- Schlüsselerzeugungsdienst
- Quellcode
 - Serverseitig / Endgerät
- Attachment Konversionsservice
- Handheld Backupservice
- Virenschutz

Zusammenfassung 1/3

Empfehlung:

- Verschlüsselung der Daten am Handheld (ab Version 4)

- Definition einer Policy:
 - Keine Installation von Fremdsoftware
 - Passwortregelung entsprechend den Empfehlungen von RIM
 - Anzahl der Fehlversuche begrenzen
 - Periodischer Schlüsselaustausch

Zusammenfassung 2/3

- Passwortschutz aktivieren
- Periodische Änderung des Passwortes

- Policy kann vom Anwender nicht umgangen werden!

- Periode bis zur Aktivierung des Bildschirmschoners sollte nicht zu groß sein

Zusammenfassung 3/3

- Service um Geräte sperren zu lassen

- Anforderungen an die Benutzer:
 - Benutzer darf das Gerät nicht aus der Hand geben.
 - Benutzer darf niemandem das Passwort verraten.
 - Verlust des Gerätes muss sofort gemeldet werden
 - Vertrauliche Dokumente verschlüsseln oder löschen
 - Bei Verlust des Gerätes muss mit Kompromittierung der Daten am Gerät gerechnet werden
 - Verwendung des S/MIME Paketes

@stake Security Assessment

- Im Auftrag von RIM
- Veröffentlicht im November 2003
- Entstanden im Research Lab Cambridge, Massachusetts zusammen mit lokalem Provider
- Autoren: Chris Eng, Matthew Levine und Ollie Whitehouse

Untersuchte Bereiche

- BlackBerry Wireless Handheld
 - Mikroprozessor, externer Speicher, Hardware Untersuchung
- BlackBerry Enterprise Server
 - Quellcodeanalyse
- BlackBerry Desktop Software
 - Protokollanalyse
- Security Model Matrix
 - Sitzungsübernahme etc.

BlackBerry Handheld

- Untersuchung der Hardware
 - Elektronik, externe Schnittstellen
- Ergebnis
 - Inhalt schwer zugänglich (kompakte Bauweise etc.)
 - Hält einfache Angriffe ab

BlackBerry Enterprise Server

- Abhören der übertragenen Daten mittels *Packet Sniffer*
- Test der Verbindung BES <> Mailserver
- Reverse Engineering der BES Software, Suche nach:
Implementierungsfehlern, Buffer overflows,
Format String Anfälligkeit

BlackBerry Desktop Software

- Untersuchung
 - Kommunikation HandHeld <> Desktop
 - Synchronisation / Backup
 - Angriffe auf das Protokoll

- Ergebnis:
 - Keine Verwundbarkeiten entdeckt

Security Model Matrix

- Basierend auf Fragen von Kunden
 - Vergleich BB zu VPN gleiche Sicherheit
 - Kann RIM die Nachrichten lesen? Nein
 - Sitzungsübernahme nur mit enormem Aufwand
 - Einschleusen von böartigem Code ohne Schlüssel nicht möglich
 - Zugriff auf Firmennetzwerk über PC Verbindung (J2ME Applikation) nur Synchronisation

Konfigurationsempfehlung 1/2

- „*best practices*“ für BlackBerry Kunden
- Keine Credentials (Passwörter, Schlüssel etc.) unverschlüsselt und ungeschützt am BES lassen
- Gefahr eines Angriffes von „Innen“

Konfigurationsempfehlung 2/2

- Errichtung einer sicheren BE-Serverumgebung
 - Test von BES, Mailserver, Desktopsoftware
 - Umsetzen der Microsoft Konfigurationsvorgaben

- Aufstellen von Sicherheitsrichtlinien
 - für Softwareentwicklung (Java Developer Environment - JDE)
 - Sichere *coding practices* für Handheld Applikationen
 - Training der Entwickler

Frage & Antworten

- Quellen

- A-Sit Studie:

- http://www.a-sit.at/technologieb/evaluation/20040112_Studie_Blackberry.pdf

- @stake Security Assessment:

- http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/645094/An_@stake_Security_Assessment.pdf?nodeid=644990&vernum=0