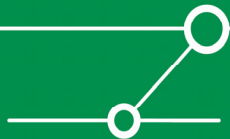


Die BlackBerry Security Diskussion

Dror-John Roecher
droecher@ernw.de
<http://www.ernw.de>



Ziele des Vortrags



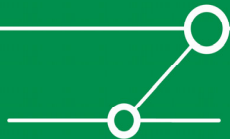
- Aufarbeitung der Security-Diskussion zwecks Klarstellung der aktuellen Sachlage
- Bewertung und Empfehlungen



Agenda

1. Grundlagen zum BlackBerry
2. Übersicht Sicherheitsaspekte
 1. Technische Aspekte
 2. Rechtliche Aspekte
 3. Organisatorische Aspekte
 4. Der User

3. Bewertung & Maßnahmen



Grundlagen zum BlackBerry



Überblick BlackBerry

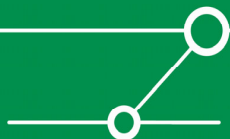
- Ein drahtloses Kommunikationssystem des Herstellers Research In Motion (RIM)
- Einsatzbereiche:
 - E-Maildienst
 - Informations- und Datenaustausch aller Art: Telefon, SMS, Organizer-Anwendung, Browser u. a.
- Besonderer Vorteil: Push-Technologie für E-Mail und andere Daten
- Zugrunde liegende Netzwerktechnologien / Transportmedien
 - GSM / GPRS
 - Internet
 - LAN



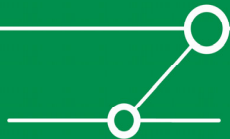
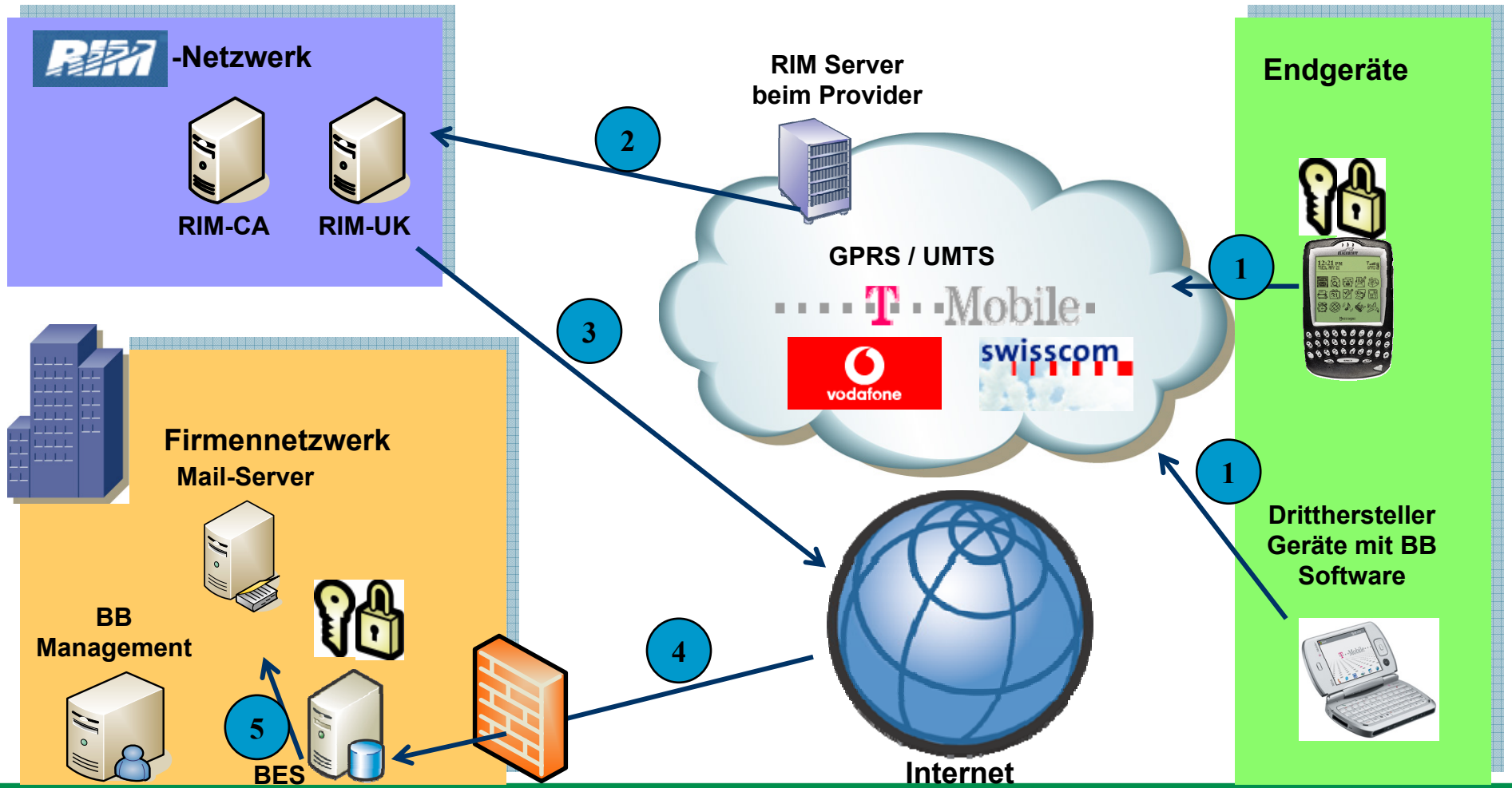
Technische Realisierung

- Client-Server-Architektur
 - Client: BlackBerry Endgerät (RIM-Endgeräte, Geräte von Drittherstellern mit Blackberry-Software)
 - Server: BlackBerry Enterprise Server (BES)

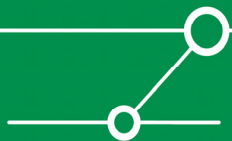
- Ein dem BlackBerry Enterprise Server nachgelagerter Messaging-Server (Microsoft Exchange Server oder ein Lotus Domino Server in Verbindung mit einem Microsoft SQL-Server) dient als Speicherort für Benutzerdaten: E-Mails, kryptographische Schlüssel u. a.



Kommunikation



Sicherheitsaspekte BlackBerry



RIMs Selbstdarstellung

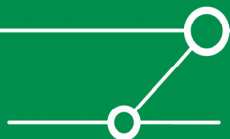


- RIM wirbt mit der Sicherheit der Lösung

Addressing the Enterprise Wireless Data Requirements

- ☑ 1. Established, Reliable, Secure, Push for THEIR enterprise messaging environments
- ☑ 2. Global Solution (NA, Europe, Australia, Asia)
- ☑ 3. Multiple Networks
- ☑ 4. Manageable!!!
- ☑ 5. Secure, Secure, Secure!!!
- ☑ 6. Multiple Device Partnerships
- ☑ 7. Feature Rich (Attachments, GAL, Wireless deletes, etc.)
- ☑ 8. Virtual Machine (VM) Implementation (i.e., J2ME)
- ☑ 9. Platform Extension (MDS with HTTP/XML)

Aus einem Vortrag von „Jim Balsillie“, CEO RIM



RIMs Selbstdarstellung

■ RIM wirbt mit der Sicherheit der Lösung

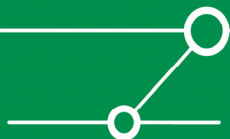
3. FEATURE RICH

BlackBerry Enterprise Server – User Features

- **Secure, Integrated, Advanced Attachment Viewing**
 - Rich text viewer with fonts, formatting and tables
 - Table of contents view and hyperlinks
 - Includes support for Word, Excel, PowerPoint, PDF and more!
- **Cradle-Free Email Synchronization**
 - Full two-way wireless sync of email activity (ie., Deletes, Folder Management)
 - Desktop usage now optional for end users
- **Secure “Over The Air” Java Application Download**
 - An industry first that simplifies application distribution and upgrades
- **Remote Address Lookup (GAL on Exchange, NAB on Domino)**



Aus einem Vortrag von „Jim Balsillie“, CEO RIM



Studien zur Sicherheit von BlackBerry (1)

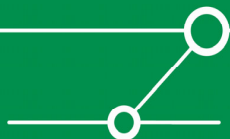


- @stake Studie November 2003:
„...proven platform that provides...secure wireless access...“

NOVEMBER 2003

BlackBerry® by Research In Motion: An @stake Security Assessment

BlackBerry is the leading wireless enterprise solution developed by RIM that keeps mobile professionals connected to people and information while on the go. It is a proven platform that provides users around the world with secure, wireless access to a full suite of business applications, including email, corporate data, phone, SMS, web and organizer features. BlackBerry incorporates the industry's best software, services and hardware, providing the most comprehensive end-to-end wireless solution for corporate environments. It has become the corporate standard for wireless connectivity by properly addressing the needs of both mobile professionals and IT departments. For more information, visit www.blackberry.com.



Studien zur Sicherheit von BlackBerry (2)

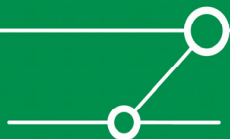


- Austria Secure Information Technology Center (A-SIT) [vergleichbar dem BSI in Deutschland], Oktober 2004
schon ein wenig kritischer im Ton...

Zusammenfassung

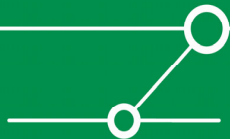
Das BlackBerry Mobile Data Service wurde entwickelt, um Benutzern einen sicheren Zugriff auf ihre im Firmennetzwerk befindlichen Daten zu ermöglichen. Den Kern dieses Service bilden der BlackBerry Enterprise Server und ein Mailserver. Bei der Wahl des Mailservers ist man jedoch auf den Microsoft Exchange Server oder den Lotus Domino Server festgelegt. Bei der Wahl der Endgeräte ist man derzeit auf Handhelds der Firma BlackBerry beschränkt. PDAs und SmartPhones anderer Hersteller werden laut [1] in Zukunft auch RIM Technologie unterstützen und sich in dieses System integrieren lassen.

Die sicherheitstechnischen Eigenschaften des Blackberry können mit denen eines Notebooks verglichen werden. Die Kommunikation mit dem Intranet/Mailserver wird VPN-ähnlich abgesichert, die lokal gespeicherten Daten sind nur durch ein Passwort geschützt und liegen ungesichert im Speicher. Die größte Schwachstelle ist daher der mögliche Verlust oder Diebstahl des Gerätes, der Zugriff auf die gespeicherten Daten möglich macht. Die Schutzmaßnahme der Löschung der Daten, die vom Systemadministrator ausgelöst werden kann, kann leicht umgangen werden.



Übersicht zu beachtende Sicherheitsaspekte

- Technische Aspekte
 - Auf dem RIM Endgerät
 - Während der Übertragung
 - Auf dem Enterprise-Server / im Firmennetz
- Rechtliche Aspekte
 - Patentklagen in den USA – Auswirkungen in der EU?
- Organisatorische Aspekte
 - Datenklassifikation
 - Regelung bei Verlust
 - Regelung bei Ausscheiden des Mitarbeiters
- Handhabung / Risiko „Benutzer“
 - Umgang in der Öffentlichkeit
 - Vermischung privater und geschäftlicher Daten
 - Ablehnung von Regelungen



Technische Sicherheitsaspekte



Der Wegbereiter: FX von phenoelit

- Der wichtigste Vortrag wurde im Dezember 2005 in Berlin von „FX“ gehalten:

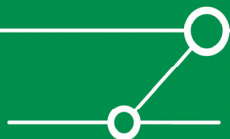
news 02.01.2006 09:36


<< Vorige | Nächste >>

Hacker finden diverse Angriffsflächen bei Blackberry

Die Sicherheitsarchitektur des E-Mail-Push-Dienstes [Blackberry](#) ist laut der Hackergruppe [Phenoelit](#) deutlich anfälliger für Missbrauch, als es nach den Angaben des kanadischen Anbieter Research in Motion (RIM) möglich erschien. In einem Vortrag auf dem 22. Chaos Communication Congress ([22C3](#)) in Berlin lüfteten die Sicherheitsexperten Ende vergangener Woche einige der vom Hersteller bislang gut gehüteten Geheimnisse rund um die Handheld-Lösung. Dabei kamen eine Reihe von Angriffsflächen zu Tage, welche die Kanadier den Testern zufolge trotz ausführlicher Hinweise bis heute noch nicht alle geschlossen haben. Ein Vertreter RIMs saß bei dem Phenoelit-Vortrag im Publikum, wollte sich öffentlich aber nicht zu den Ausführungen in dem Vortrag äußern.

- Eine erweiterte Version wurde im März 2006 auf der Blackhat in Amsterdam gehalten (<http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-fx.pdf>).
- Dieser Vortrag ist wegbereitend und stellt die erste (und bisher einzige) unabhängige technische Security-Analyse dar, in der alle Komponenten der Lösung detailliert untersucht wurden.



Reaktionen auf den FX-Vortrag



■ ■ ■ ■ **T** ■ ■ ■ Mobile ■ BB Solution – BlackBerry 4.0 Security Referenz GRZ IT Gruppe

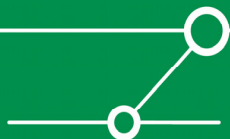
Einführung

Ausgehend von den Punkten, die FX am 30.12.05 während seines Vortrages über BlackBerry auf dem 22. Chaos Communication Congress in Berlin genannt hatte, wurde die BlackBerry Implementierung bei GRZ IT Gruppe überarbeitet und entsprechend angepasst, um mögliche Abstürze einzelner Komponenten aufgrund beschriebener fehlerhafter Anhänge zu vermeiden.

Die Sicherheit der Implementierung an sich ist nicht in Frage gestellt. Dennoch werden durch die Auslagerung einzelner Komponenten in die DMZ mögliche Angriffspunkte minimiert.

Die von FX festgestellten Schwachstellen wurden diskutiert und durch folgende Maßnahmen behoben bzw. eingegrenzt:

http://www.t-mobile.at/_PDF/businessclass/BlackBerry_Security.pdf

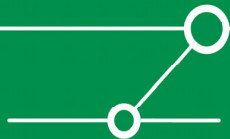


Sicherheitsaspekte – das Endgerät (1)



- Passwortschutz:
 - Sperrung des Gerätes (Bildschirm, Tastatur, USB-Port, Infrarotport) nach einer definierbaren Zeit der Inaktivität, Aufhebung der Sperre nach Passworteingabe

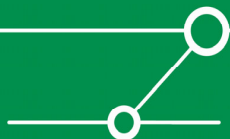
- Passwortsicherheit
 - Erzwungene Passwortqualität
 - Speicherung des Passwortes als SHA1-Hash auf dem Gerät
 - Löschung aller benutzerspezifischen Daten nach einer bestimmbaren Anzahl von falschen Eingaben



Sicherheitsaspekte – das Endgerät (2)

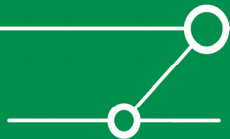
- Datensicherheit
 - Eine aus der Ferne initiiierbare Löschung der Daten bei Bedarf (etwa Diebstahl), Überschreibung der entsprechenden Speicherbereiche mit Nullen und Einsen in mehreren Gängen
 - Ab Version 4.0: lokale Verschlüsselung der Daten

- Zentrale Verwaltung fast aller Funktionen und Merkmale des Endgerätes über Policies, die nach ihrer Erstellung sofort übertragen werden und in Kraft treten.
- Drittapplikationen müssen von RIM signiert werden, sonst funktionieren sie nicht auf RIM Endgeräten (Kostenpunkt: 100 U\$).
- Remote-Kill-Funktion: Kann sehr leicht durch Herausnahme der SIM-Karte umgangen werden [deswegen mE ein überbewertetes Feature], und dafür muss ein funktionierender „Incident-Response“-Prozess etabliert sein
- Viele der genannten Aspekte gelten nur für RIM-Geräte, Geräte von Drittherstellern mit BB-Software beinhalten idR weniger integrierte Sicherheitsmassnahmen.

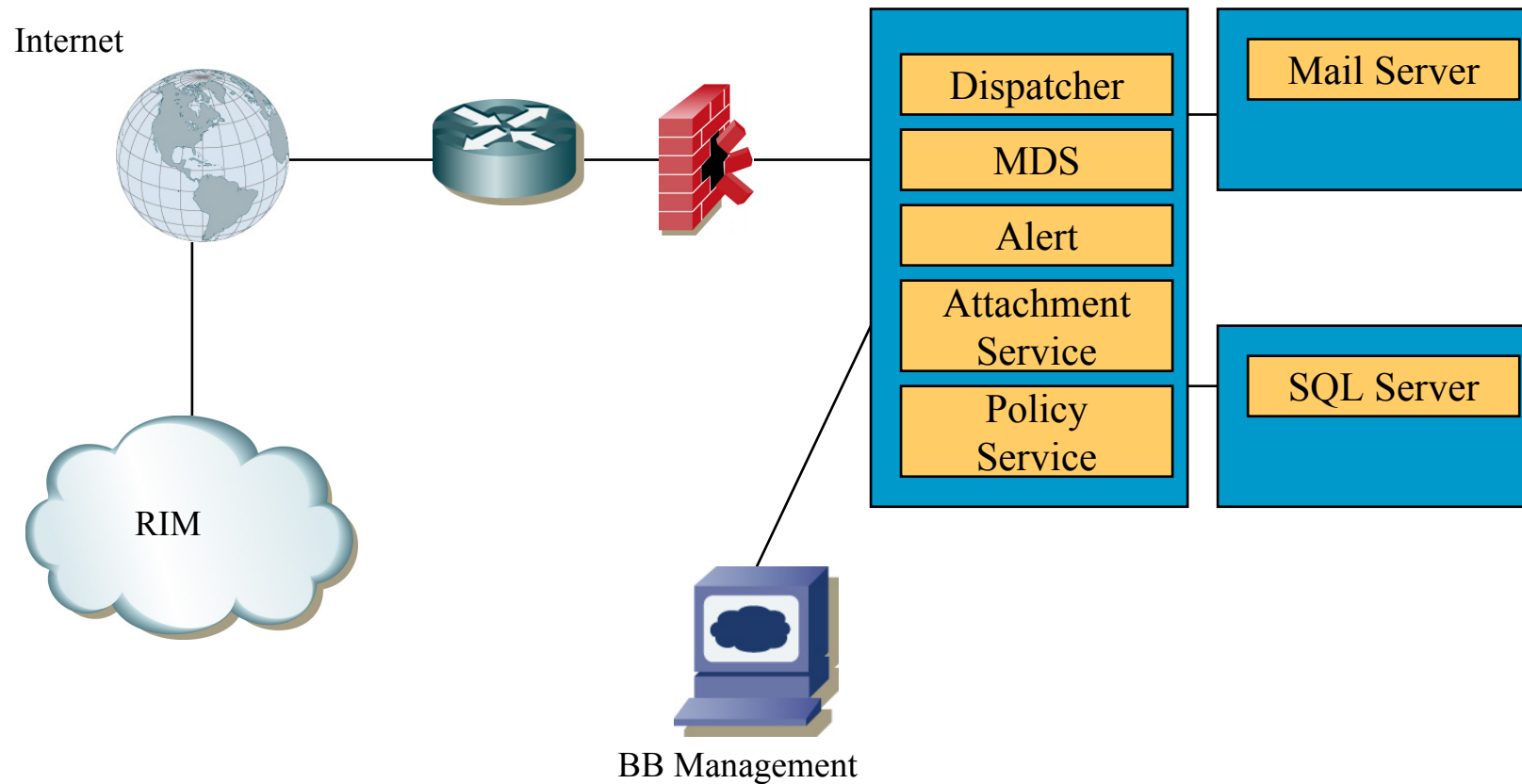


Sicherheitsaspekte – Übertragung
















- Die Protokolle, die zum Einsatz kommen sind nicht offengelegt.
- Phenoelit / FX haben die Protokolle in mühsamer Forschungsarbeit dekodiert und in besagtem Vortrag dokumentiert:
 - PIN Nachrichten werden im Klartext übertragen
 - Session Key wird verschlüsselt mit Device Key, Nachrichten anschliessend mit dem Session Key verschlüsselt. Zugang zum Device Key (dazu später mehr) ermöglicht Entschlüsselung von Nachrichten (dazu gibt es von FX auch ein Programm)
 - SRP Session Setup mit einem fremden Schlüssel und fremder SRP ID möglich:
 - ◆ Rechtmässiger Benutzer wird getrennt
 - ◆ Neue Verbindung vom rechtmässigen Benutzer oder Angreifer führt zur Trennung der zweiten Verbindung
 - ◆ Nach 5 „reconnects“ in weniger als 1 Minute, wird der Key gesperrt. Gerät ist danach unbrauchbar und muss an RIM eingesendet werden
 - PIN Nachrichten können problemlos an alle BlackBerry Benutzer versendet werden (SPAM!)
- Was auch immer im „RIM Secret Network“ geschieht, ist unbekannt. RIM behauptet, dass die Nachrichten nur durchgeleitet und nicht kopiert/entschlüsselt werden/können.

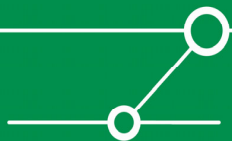


BES Architektur



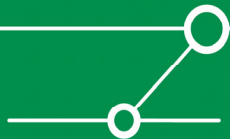
BES Accounts & Privilegien

	Logon Locally	Logon as Service	Local Admin	Exchange RO Admin	Exchange Mail Store Admin
Service Account					
Server Management Account					
User Admin Account					



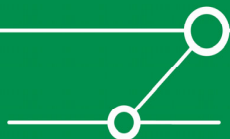
Die SQL-Datenbank im BES

- MS SQL Server mit User-Authentifizierung
 - Keine integrierte Authentifizierung für Domino
 - Tabellen für Nachrichten und Emails
 - Tabelle mit SRP Authentifizierungs-Schlüssel
 - ◆ Das wichtigste „Geheimnis“ zwischen BES und RIM-Endgerät steht dort im KLARTEXT
 - Tabelle mit Geräte-Schlüsseln
 - ◆ Vergangene, aktueller und neuer Schlüssel
 - ◆ Damit kann man den Verkehr entschlüsseln
 - Default-Account der SQL-Datenbank:
user: SA
Passwort: leer

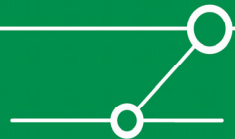
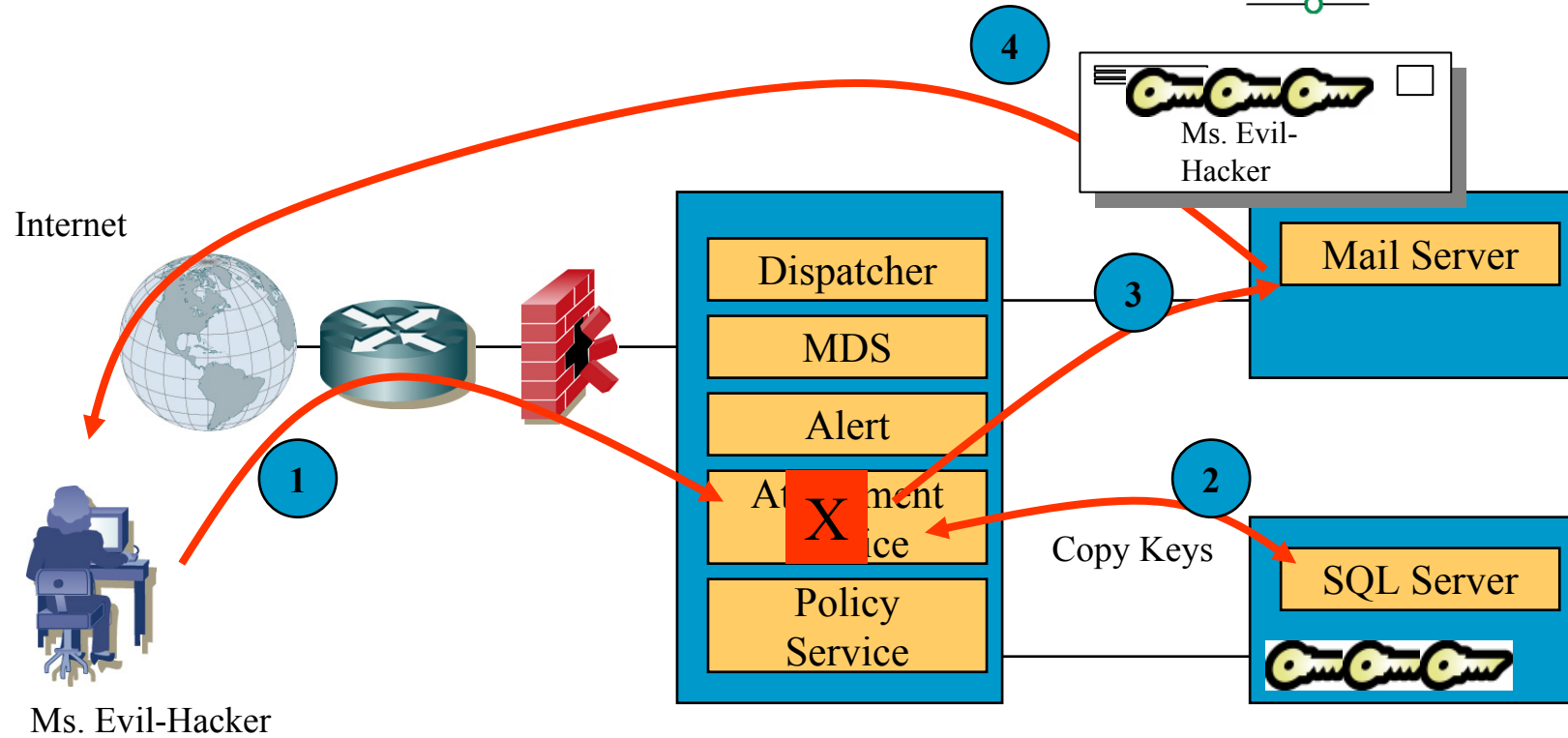


BES Software-Probleme

- BES benutzt Bibliotheken, die teilweise veraltet sind und bekannte, sicherheitsrelevante Bugs enthalten:
 - Zlib : benutzt für die zip-Komprimierung von Anhängen
 - GraphicsMagick: Darstellung verschiedener Bild-Formate
- Dadurch ist es möglich, durch Versenden speziell präparierter Anhänge, Code auf dem BES auszuführen (zum Beispiel: Verbindung zur SQL-Datenbank, die Klartextkeys in eine Email packen und versenden) [siehe nächste Folie]



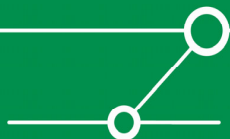
BES Attachment Service Angriff



Das BSI und BlackBerry

- Im Oktober 2005 berichtet die Wirtschaftswoche, dass das BSI vom Gebrauch des BlackBerry abrät:
 - Auf Grund der unsicheren Architektur ist der BlackBerry für den Einsatz in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet,,
[<http://www.heise.de/newsticker/meldung/64610>]

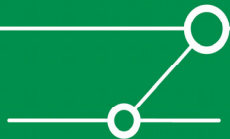
- Das ganze war wohl „nur“ ein Versehen...oder „hohe Politik“ ;-)
 - Die Gerüchte um gravierende Sicherheitslücken im E-Mail-PDA BlackBerry, die Anfang Oktober auf Grund eines Artikels der Wirtschaftswoche auftauchten, sind wohl auf eine Indiskretion beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und Fehlinterpretationen zurückzuführen. In einer nicht für die Veröffentlichung bestimmten, internen Studie habe sich das BSI zwar mit BlackBerry beschäftigt. "Grundsätzlich empfiehlt das BSI aber nur geprüfte Systeme und solche, in die sich eigene Kryptoalgorithmen einbinden lassen", erklärte Michael Dickopf, Sprecher des BSI, gegenüber heise Security.
[<http://www.heise.de/security/news/meldung/64754>]



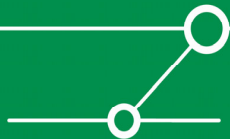
Zusammenfassung Technische Aspekte



- Endgerät:
 - Fehlende Verschlüsselung der Daten auf dem Endgerät (behoben mit aktueller Version 4.0)
 - Ansonsten: Gute Security-Features, falls entsprechend über Policies erzwungene Benutzung (Lockout, Reset, etc).
 - Gute Security qua Design auf den RIM-Endgeräten (dedizierte Funktionalität, keine „Gadget-Features“ wie z.B. MP3-Player)
- Auf der Strecke / Protokolle
 - Grosses Fragezeichen „RIM“-Network. Was passiert dort wirklich? Angeblich nichts...
 - Eingesetzte Protokolle haben teilweise Schwächen
 - ◆ PIN Nachrichten im Klartext
 - ◆ Gefälschtes Session-Setup – mit fatalen Folgen für den Benutzer
 - ◆ PIN SPAM möglich
- BES
 - Grosszügige Privilegien
 - SRP Authentication Keys werden im Klartext in einer MS-SQL-Datenbank abgelegt
 - Device Keys werden im Klartext in einer MS-SQL-Datenbank abgelegt
 - Default-Account „SA“ ohne Passwort
 - Teilweise veraltete Bibliotheken, mit bekannten Bugs im Einsatz, insbesondere im Attachment-Handling



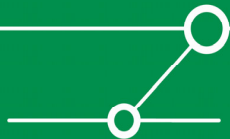
Rechtliche Aspekte - Patentklagen



Die NTP-Patentklage

- NTP gewann 2002 eine Patentklage gegen RIM (NTP besitzt einige Patente im Kontext „drahtlose Emails“).
- 2005 einigten sich NTP und RIM in einem aussergerichtlichen Vergleich auf einen Streitwert von U\$ 450M.
- Dieser Vergleich wurde vom zuständigen Gericht abgelehnt und sprach u.a. ein Verkaufsverbot aus (dessen Durchsetzung bis zur abschließenden Klärung ausgesetzt wurde).
- Anfang 2006 erklärte das US-Patentamt die strittigen NTP-Patente für nichtig.
- RIM und NTP einigten sich im März 2006 auf die Zahlung von U\$ 612,5M – für „unbegrenzte Lizenzen“ aller NTP Patente im BB-Kontext.

- Da das europäische Patentrecht (noch?) vom US-Patentrecht entkoppelt ist, wäre Europa von einer Einstellung des Dienstes in den USA nicht direkt betroffen.



Patentauswirkungen



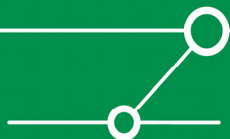
<http://www.heise.de/newsticker/meldung/66130>

news 14.11.2005 15:05

 << Vorige | Nächste >>

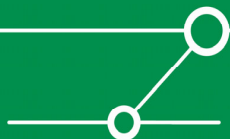
US-Regierung will nicht unter Patentklagen leiden

Die US-Regierung hat Anwälte beauftragt, sich darum zu kümmern, dass die Behörden – ungeachtet möglicher anderer wirtschaftlicher Folgen – von den Auswirkungen der Patentstreitigkeiten über den Mobil-E-Mail-Dienst **Blackberry** verschont bleiben. Auf Grund einer Klage des Patentvermarkters **NTP** gegen den **Blackberry**-Anbieter Research in Motion (**RIM**) läuft dieser Gefahr, sich entweder zu einem horrenden Preis außergerichtlich von der NTP-Forderung freikaufen oder aber den weit verbreiteten E-Mail-Dienst komplett einstellen zu müssen. Zurzeit liegt der Fall in den Händen eines Bezirksgerichts im US-Bundesstaat Virginia.



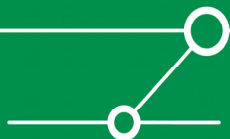
Die Visto-Patentklage

- Visto Corp., ein Anbieter mobiler Email-Lösungen, hält in diesem Kontext einige US-Patente, die u.a. auch gegen Microsoft und Seven Networks durchgesetzt wurden.
- Anfang Mai 2006 reichte Visto eine Patentklage gegen RIM/BlackBerry ein. RIM soll gegen 4 US-Patente der Visto Corp. verstossen haben.
- Da auch diese Klagen sich zunächst nur auf US-Patente beziehen, droht dem BB-Dienst derzeit keine Gefahr von dieser Seite.



Zusammenfassung Patentklagen

- Die NTP-Patentklage ist gescheitert, da die betroffenen Patente vom US-Patentamt für „nichtig“ erklärt wurden.
- Aktuell ist eine Patentklage von Visto anhängig, allerdings auch nur in den USA und der Ausgang ist ungewiss.
- Für BlackBerry-Benutzer in den USA stellen die Patentklagen ein grosses Risiko dar, da erfolgreiche Patentklagen entweder in teuren Vergleichen/Lizenzen enden oder sonst eine Einstellung des Dienstes droht.
- In Europa sind derzeit keine Patentklagen gegen RIM anhängig. Selbst eine erfolgreiche Klage in den USA hätte zunächst keine Auswirkungen in Europa.
- Allerdings gibt es ja auch europäische Unternehmen in den USA – die US-amerikanischen Dependancen sind von diesen Patentklagen betroffen.



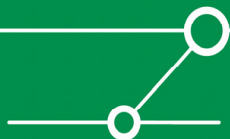
Organisatorische Sicherheitsaspekte



Organisatorisches – der Handheld allgemein



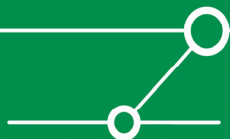
- Welche Daten liegen auf den Endgeräten?
 - Wie sind diese klassifiziert? Welche Konsequenzen hat die Klassifizierung?
- Wozu werden die Endgeräte genutzt?
 - PIM?
 - Applikationszugriff (z.B. SAP)? Über welche Medien? Wie gesichert?
 - Entertainment?
- Wer benutzt die Endgeräte?
 - Admins? Aussendienstler? Manager? Was hat das für Konsequenzen?
- Wo werden die Geräte benutzt?
 - Auf Geschäftsreisen? Im Hotel? Am WLAN-Hotspot im Flughafen? In der Kneipe oder im Fussballstadium [Marke: Schaut mal, ich habe ein neues Gadget]?
- Wem gehört das Endgerät? Wer hat es beschafft?
 - Kann ich eine Sicherheitsrichtlinie auf privaten Geräten erzwingen?



Richtlinien sind notwendig

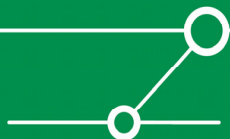
- Die vorangehenden Fragen sollten genutzt werden, um verschiedene Profile zu erstellen:
 - Admin: Fernwartung, PIM, Push-Mail, in der Firma & daheim
 - Manager: PIM, Push-Mail, überall
- Um aus diesen Profilen dann
 - Richtlinien zur Handhabung zu erstellen
 - eine Risikoanalyse zu erstellen

- Oder anders gefragt: Gilt die „Allgemeine Passwort-Richtlinie“ auch für BlackBerrys & PDAs? Ist sie dort technisch umsetzbar? Ist sie auch dem Benutzer gegenüber zumutbar? Oder kann eine „schwächere“ Passwort-Richtlinie nicht vielleicht über andere Massnahmen aufgefangen werden [z.B. 5 Fehlversuche führen zur Zerstörung sämtlicher Daten].



Bei Verlust & Beim Ausscheiden

- Solange der Mitarbeiter, der einen BlackBerry besitzt, im Unternehmen angestellt ist und solange der BlackBerry auch im Besitz des Mitarbeiters ist, ist „alles [mehr oder weniger] ok“.
- Aber...
 - Was passiert bei Verlust des Gerätes [Diebstahl, Verloren]? Gibt es Prozeduren? Sind diese allen Beteiligten [also auch dem Benutzer] bekannt? Sind sie getestet? Funktionieren sie? Sind sie prüfbar [im Sinne der Revision]?
 - Was passiert beim Ausscheiden des Mitarbeiters mit seinem BlackBerry? Darf er ihn behalten? Was passiert mit den Daten? Gibt es Prozeduren? Sind diese allen Beteiligten [also auch dem Benutzer] bekannt? Sind sie getestet? Funktionieren sie? Sind sie prüfbar [im Sinne der Revision]?



Risiko Benutzer



BlackBerry auf ebay



BlackBerry Reveals Bank's Secrets

PRINT MAIL RANTS + RAVES

Page 1 of 3 [next >>](#)

By Kim Zetter [Kim Zetter](#) | Also by this reporter
2003-08-25 12:31:00.0

The eBay ad read "BlackBerry RIM sold AS IS!" So Eugene Sacks (not his real name), a Seattle computer consultant who always wanted one of the pager-size devices to check his e-mail, sent in a bid. For just \$15.50, he bought the wireless device with 4 MB of memory.

The BlackBerry didn't come with a cable, synching station, software or a manual. But it did come with something even more valuable: a trove of corporate data.

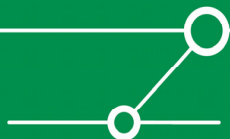
Breaking

Breaking News from AP:

- ◆ Credible lead in Hoffa case, FBI says
- ◆ FBI says it has good lead in Hoffa search
- ◆ Obituaries in the news
- ◆ Elderly woman arrested in insurance scam
- ◆ Search for missing boat captain suspended

See Also

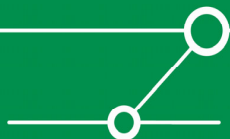
<http://www.wired.com/news/business/0,1367,60052,00.html>



Der Benutzer ist das größte Risiko...



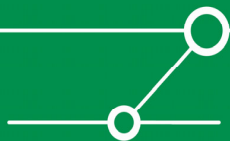
- Der BlackBerry / PDA wird nicht als Gefahrenquelle / Risiko erkannt.
- Instant-On-Erwartung – Ablehnung von Regelungen & Passwörtern.
- Benutzerverhalten: „Backup“ – Aufgrund der Speichergröße ein echtes Problem.
- An „falschen“ Plätzen mit dabei (im Fußballstadion, in der Kneipe, in der Sauna)
- Vermischung von privaten & geschäftlichen Daten (private Termine etc.) – daraus ergeben sich ggf. Haftungsfragen insb. Bei Vertreterregelungen & Ausscheiden des Mitarbeiters.
- Bestehende Sicherheitsmechanismen werden nicht genutzt, wenn Benutzung nicht erzwungen wird.



... und auch die beste Verteidigung



- Sorgfältiger Umgang
- Gute Passwörter
- Verschlüsselung
- Bei entsprechender „Awareness“ ist der Benutzer die wichtigste „Verteidigung“
- „Awareness“ kann nicht ad-hoc implementiert werden, sondern ist Ergebniss eines kontinuierlichen Weiterbildungsprozess (der ein entsprechendes Konzept, Ausdauer und Budget erfordert)



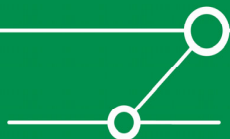
Zusammenfassung & Bewertung



Zusammengefasst...



- Die technischen Risiken existieren und müssen adressiert werden – hier ist wohl erst die Spitze des Eisbergers sichtbar.
- Richtlinien sind für ein gesteigertes Security-Level unverzichtbar. Insbesondere Datenklassifikation [und daraus resultierende Konsequenzen] müssen auf BlackBerrys und anderen mobilen Endgeräten berücksichtigt werden. Die Grundlage bildet eine Risikoanalyse für den geplanten Einsatz.
- Benutzer müssen über Risiken aufgeklärt und im sicheren Umgang mit den Endgeräten geschult werden. Dies ist der wichtigste [und wohl auch schwierigste] Punkt.



Vielen Dank für Ihre Aufmerksamkeit



Fragen?

...

Und Antworten!

