# ERNW Newsletter 11 / Juli 2006

Liebe Partner, liebe Kollegen,

willkommen zur elften Ausgabe des ERNW-Newsletters mit dem Thema:

# BlackBerry Security
# &
# Mobile Security

Version 1.2 vom 31. August 2006

von:

Dror-John Röcher (droecher@ernw.de)

Dieser Newsletter beinhaltet eine Zusammenfassung der aktuellen Security Diskussion rund um BlackBerry Geräte und RIM-Email-Push-Dienste. Neben den technischen Aspekten werden auch organisatorische Aspekte und der Benutzer berücksichtigt.

## INHALTSVERZEICHNIS

# 1 EINLEITUNG

Mobile Endgeräte sind aus dem Geschäftsleben seit Jahren nicht mehr wegzudenken – neben den klassischen Laptops und PDAs haben sich in den letzen drei Jahren vor allen anderen die BlackBerry-Endgeräte im Unternehmensumfeld durchgesetzt; zunächst ausschließlich als Geräte des Herstellers „Research in Motion“ (RIM), seit 2004 wird die BlackBerry Software allerdings auch für mobile Geräte anderer Hersteller und Betriebssysteme (PocketPC 2002, Windows Mobile 5.0, Symbian, PalmOS) vertrieben.

Das Erfolgskonzept von RIM, dem Hersteller der BlackBerrys, beruht auf der Email-Push-Technologie, die das mühsame „pullen“ von Emails überflüssig macht, indem ankommende Email-Nachrichten umgehend auf den Blackberry „geschoben“ werden. Dadurch ist ein Blackberry-Benutzer jederzeit und an jedem Ort per Email erreichbar (sofern eine Verbindung zum Mobilfunknetz aufgebaut werden kann); der Dienst beschränkt sich nicht auf das reine Empfangen von Emails, sondern ermöglicht auch das Versenden eben jener von unterwegs auch ohne Laptop.

Der Einsatz dieser Geräte birgt aber auch Risiken und diese werden in diesem Newsletter beleuchtet. Dabei werden nicht nur die technischen Risiken erläutert, sondern in verstärktem Masse werden auch organisatorische Risiken betrachtet. Dieser organisatorische Teil ist in seiner Anwendung nicht auf BlackBerrys beschränkt, sondern lässt sich auf die meisten Formen des „Mobile Computing“ anwenden.

Im ersten Teil (Kapitel 2) wird ein kurzer Überblick über die Komponenten einer BlackBerry Enterprise Server Lösung und über die Kommunikationsabläufe gegeben.

Der zweite Teil (Kapitel 3) diskutiert die vorhandenen technischen Sicherheitsmerkmale.

Im dritten Teil (Kapitel 4) werden die „weichen“ Faktoren berücksichtigt – Policies, Prozesse und Benutzer.

Das Team von ERNW (Deutschland) und ERNW.PT (Portugal) wünscht Ihnen viel Spaß beim Lesen und stehen Ihnen jederzeit für Fragen oder Diskussionen zur Verfügung.



## 2 GRUNDLAGEN DER BLACKBERRY KOMMUNIKATION UND DER RIM-DIENSTE

Das Kommunikationsschema des BlackBerry-Dienstes entspricht weitgehend einer klassischen Client-Server Architektur; als Clients kommen entweder Endgeräte des Herstellers „Research in Motion" RIM oder Endgeräte von Drittherstellern, auf denen die BlackBerry-Software installiert ist, zum Einsatz. Die Serverkomponente stellt der „BlackBerry Enterprise Server" (BES) dar, der im Firmennetzwerk installiert wird und eine Verbindung zum firmeneigenen Mailserver unterhält. Derzeit funktioniert der BES ausschließlich in Kombination mit Microsofts Exchange-Server, IBMs Notes-Server oder Novells Groupwise Server; die klassischen Mail-Protokolle SMTP und POP3 bzw. IMAP4 werden vom BES nicht unterstützt[1].

Der Dienst ist ein so genannter „Push"-Dienst; dies bedeutet, dass der Client den Server nicht in beliebigen Intervallen nach neuen Nachrichten fragt, sondern dass der Server, sobald neue Nachrichten für einen Benutzer ankommen, diese aktiv auf das Endgerät „schiebt" (siehe Abbildung 1) Die Verbindung vom BES wird dabei nicht direkt zum Endgerät aufgebaut, sondern zunächst in eins von mehreren Verteilzentren, die RIM weltweit unterhält und von dort wird die Nachricht letztlich über das GSM-Netz des Mobilfunkproviders auf das Endgerät übertragen. Um die Nachricht vor unbefugtem Zugriff zu schützen, verschlüsselt der BES diese vor der Übermittlung und das Endgerät entschlüsselt die ankommenden Nachrichten. Umgekehrt, d.h. mit Nachrichten die vom Endgerät aus versandt werden, funktioniert der Dienst

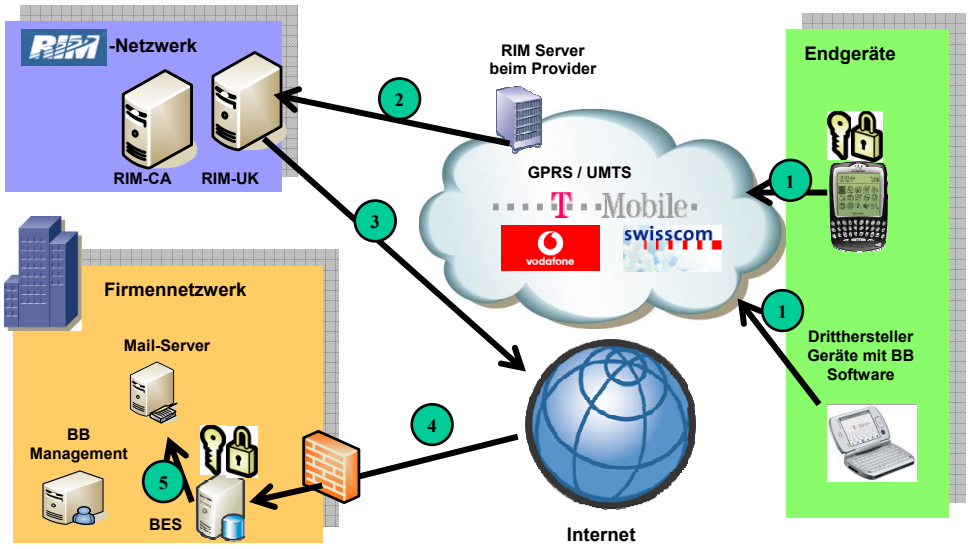



**Abbildung 1 Kommunikationsschema**

ähnlich wie mit ankommenden Nachrichten, nur dass der Weg in umgekehrter Reihenfolge durchlaufen wird: Das Endgerät verschlüsselt die Nachricht und übermittelt diese über das RIM-Verteilzentrum an den BES, welcher sie entschlüsselt und an den Firmen-Mailserver zur Auslieferung weiterleitet.

---

[1] *Die klassischen Mail-Protokolle werden von einigen Mobilfunkprovider in einer Variante „BlackBerry für Privatanwender" ohne BES-Infrastruktur unterstützt. Diese Art des BlackBerry-Betriebs wird in diesem Newsletter aber nicht weiter betrachtet.*

# 3 TECHNISCHE ASPEKTE

Die Betrachtung der technischen Sicherheit einer BlackBerry-Lösung kann sich nicht allein auf eine Betrachtung der Kryptokomponenten beschränken (obwohl gerade diese Komponenten im Fokus der Kritik des BSI[2] waren, die dazu führte, dass die Deutsche Bundeswehr eine geplante Ausstattung der politischen Führungsebene mit BlackBerry Endgeräten im Dezember 2005 strich), sondern muss sich auf das Gesamtpaket, bestehend aus „Endgerät", „BlackBerry Enterprise Server", „Übertragungsweg" und „Kryptoeinsatz", erstrecken. Grundsätzlich können die Endgeräte in zwei verschiedene Kategorien unterteilt werden: Endgeräte des BlackBerry Herstellers RIM, nachfolgend „RIM-Endgeräte" genannt und Endgeräte von anderen Herstellern, auf denen die BlackBerry-Software installiert ist, nachfolgend „Dritthersteller-Endgeräte" genannt.

Eine Nutzung des Blackberry-Dienstes ohne „BlackBerry Enterprise Server" ist zwar möglich, für den Unternehmenseinsatz aber nicht sinnvoll, weil dadurch viele zentrale Sicherheitsmechanismen nicht verfügbar sind und die Endgeräte dann unter der vollen Kontrolle der Endanwender stehen.

## 3.1 Das Endgerät

Die ersten Generationen von RIM-Endgeräten waren qua Design als „sicher" zu bewerten, da außer der Datenverbindung zum Mobilfunknetz und einer Schnittstelle zur Synchronisation mit einem PC keine weiteren Schnittstellen zur Verfügung standen und die Funktionalität auf das Notwendigste beschränkt war. MP3-Player, Kamera und Webbrowser, Bluetooth und WLAN waren nicht verfügbar, womit diese Endgeräte als „Gadget" untauglich waren und als reine „Business-Geräte" einzustufen waren. Viele neuere RIM-Endgeräte bieten dieses „secure qua Design" nicht mehr, da neben den rein notwendigen Funktionalitäten zusätzliche integriert sind; dies reicht soweit, dass z.B. das RIM-7270 mit „Voice over IP over WLAN" (VoWLAN) zwei Funktionalitäten kombiniert, die jede für sich als sicherheitstechnisch „problematisch" zu bewerten sind, für die Kombination gilt dies umso mehr.

RIM-Endgeräte können vom „Blackberry Enterprise Server" (BES) aus mit so genannten „Policies" zentral konfiguriert werden[3]. Diese Konfigurationsmöglichkeiten sind sehr weit reichend und bieten speziell in den Bereichen Zugangsschutz und Verschlüsselung viele sinnvolle Einstellungen um die Daten auf dem Endgerät, insbesondere bei Verlust der Hardware, gegen unbefugten Zugriff zu schützen. Mit Hilfe der Policy lässt sich auch der Passwortschutz zentral konfigurieren – dies beinhaltet neben der Passwortkomplexität auch die Passwortlebensdauer und das automatische Sperren des Geräts nach einer definierbaren Zeit. Im gesperrten Zustand sind alle Schnittstellen deaktiviert und abhängig von der Konfiguration wird auch der Inhalt des nicht-flüchtigen Speichers bei der Sperrung verschlüsselt.

Die vorgenannten positiven Merkmale und Eigenschaften („secure qua design" und „zentrale BES-Policies") gelten ausschließlich für RIM-Endgeräte (und insbesondere für Geräte mit der Software-Version 4.0 oder höher); Dritthersteller-Endgeräte basieren in der Regel entweder auf Windows Mobile oder Symbian und kombinieren die BlackBerry-Funktionalität mit vielen weitern „Features", moderner Smartphones: Photo- und Videokamera, Bluetooth, USB, Infrarot, WLAN, GPRS/UMTS/Edge, MMC/SD-Speicherkarten, Internet-Browser, Office-Applikationen (Textverarbeitung, Tabellenkalkulation, Adobe Reader, etc) und der Möglichkeit beliebige Software (durch den Endbenutzer) nachzuinstallieren. Hinzu kommt, dass auf diesen Geräten

---

[2] *Im Oktober 2005 drang eine interne BSI Beurteilung zur BlackBerry-Sicherheit an die Öffentlichkeit. Im Kern zielt die Kritik auf 2 Punkte. Zum Einen dass die Kommunikation immer über Knoten im Ausland (die RIM-Netzwerke) läuft und zum Anderen, dass sich die eingesetzten Kryptoalgorithmen nicht durch eigene ersetzen lassen. Deswegen rät das BSI vom Gebrauch für „hoch sensible" Daten ab. http://www.heise.de/security/news/meldung/64610 und http://www.heise.de/security/news/meldung/67089*

[3] *Eine durchdachte Policy von t-mobile.at für Blackberry-Enterprise Kunden ist unter: http://www.t-mobile.at/_PDF/businessclass/BlackBerry_Security.pdf veröffentlicht und kann als (Diskussions)-Grundlage zur Erstellung einer eigenen BES-Policy dienen.*

die auf dem BES eingerichteten zentralen Policies nicht greifen können, da diese Policies auf Betriebssystemebene arbeiten und nur mit dem RIM-eigenen Betriebssystem kompatibel sind (und eben nicht mit Windows Mobile, Symbian oder Palm OS). Durch diese zusätzlichen Features und durch die Benutzung von all-round, single-user Betriebssystemen wächst die Angriffsfläche erheblich, insbesondere auch für Schadsoftware. Auch wenn aktuell Malware für Windows Mobile noch Mangelware ist - das Potential für Viren und Würmer sich über mobile Endgeräte zu verbreiten oder diese zu befallen und ihr Schadwerk auf diesen zu verrichten, ist enorm und es wird allgemein erwartet, dass diese Endgeräte verstärkt in den Fokus der Virenprogrammierer geraten werden; ein erster plattformübergreifender Virus ist seit März 2006 bekannt[4] und stellt einen Meilenstein in der Entwicklung von Viren für Windows Mobile dar.

Auf RIM-Endgeräten können nur Java Applikationen (J2ME MIDlets) installiert werden. Diese unterliegen den Einschränkungen der J2ME-Spezifikationen von SUN[5]; MIDlets können nur auf den für die Java Virtual Machine vorgesehen Speicher zugreifen, ein Zugriff auf andere Daten des Geräts ist für die MIDlets nicht möglich. Allerdings bietet das Betriebssystem erweiterte APIs an, die den Zugriff auf Netzwerkressourcen, Telefonbuch, etc. ermöglicht. Diese erweiterten APIs stehen nur von RIM signierten MIDlets zur Verfügung. Allerdings werden MIDlets vor der Signierung nicht von RIM untersucht – es wird lediglich registriert, wer die API (welche Firma, welches Programm) benutzt. Somit obliegt es letztendlich doch wieder dem Anwender zu entscheiden, ob er einem Programm (bzw. dem Programmursprung) vertraut oder nicht. Es wird empfohlen die Ausführung und Installationen von MIDlets durch die BES-Policy zu unterbinden.

## 3.2 Die Kryptokomponenten

Die in Abbildung 1 dargestellte durchgängige Verschlüsselung von Nachrichten zwischen dem BlackBerry-Endgerät und dem BES stellt eines der Hauptmerkmale der BlackBerry-Security dar und wird insbesondere von RIM als „vorbildliche Lösung“ vermarktet[6]. Je nach Konfiguration werden bis zu vier Schlüssel generiert, die jeweils spezifische Aufgaben in Bezug auf die Sicherheitsanforderung (Authentizität, Integrität und Vertraulichkeit von Nachrichten und von Daten auf dem Endgerät) haben. Per default-Einstellung werden nur der „Master Encryption Key“ und der „Message Key“ erstellt, die für die Verschlüsselung sämtlichen Datenverkehrs zwischen Endgerät und BES benutzt werden. Zusätzlich kann ein „Content Protection Key“ erstellt werden, welcher die Daten auf dem Endgerät verschlüsselt, sobald das Gerät gesperrt wird. Als weiterer optionaler Schlüssel kann der „Grand Master Key“ erstellt werden, der den

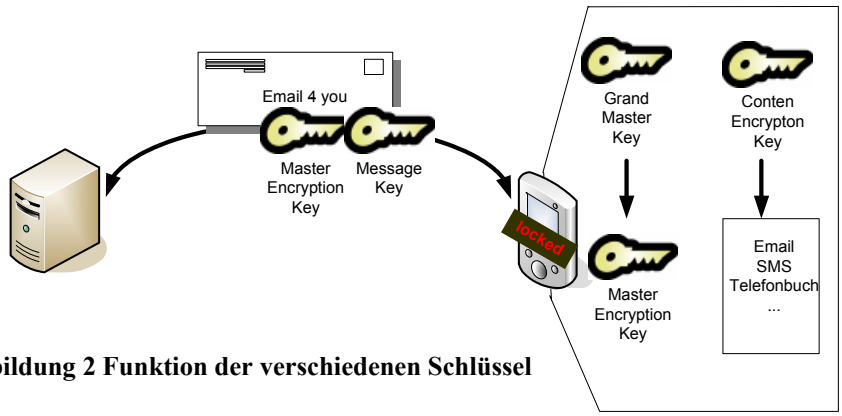



**Abbildung 2 Funktion der verschiedenen Schlüssel**

[4] *Dieser Virus befällt sowohl Windows als auch Windows Mobile Geräte und ist aufgrund dieser Fähigkeiten „crossover“ benannt worden. http://www.zdnet.de/news/security/0,39023046,39141458,00.htm*
[5] *Java 2 Micro Edition, http://java.sun.com/javame/index.jsp*
[6] *Eine Selbstdarstellung / Einschätzung der Sicherheit der RIM-Lösung hat Jim Balsille, RIM CEO, auf einer IEEE-Konferenz gegeben. Die Präsentation zum Vortrag ist im Internet verfügbar: http://www.ewh.ieee.org/r7/toronto/chapters/power/rim.ppt*

„Master Encryption Key“ auf dem Endgerät verschlüsselt, sobald das Gerät gesperrt wird.

Der „Master Encryption Key“ ist für jedes Endgerät eindeutig und ist sowohl dem Endgerät als auch dem BES bekannt. Dieser Schlüssel ist der für die sichere Datenübertragung wichtigste Schlüssel, er kann entweder vom Benutzer erneuert werden, bzw. wird bei entsprechender Policy automatisch in einem definierbaren Intervall erneuert. Alle Nachrichten werden mit dem „Master Encryption Key“ vor der Übertragung verschlüsselt. Ein zusätzlicher Schlüssel, der SRP[7]-Authentifizierungskey, dient nicht der Verschlüsselung von Daten sondern ausschließlich der Authentifizierung der Endgeräte gegenüber dem BES.

Damit Nachrichten aus der Übertragungs-Queue weiterhin entschlüsselbar bleiben, werden die so genannten „previous keys“ (die „alten“ Master Keys) für eine gewisse Dauer gespeichert (maximal 7 Tage, da dies die maximale Queue-Dauer einer Nachricht im BES ist). Die „Master Encryption Keys“ aller BlackBerry Endgeräte werden vom BES zentral in der Konfigurationsdatenbank (siehe Abbildung 3) im Klartext gespeichert.

Die eingesetzten Kryptokomponenten auf den RIM-Endgeräten sind FIPS 140-2[8] Level 1 zertifiziert[9] (bei der Nachrichtenverschlüsselung kommen 3DES und AES zum Einsatz, beides Verfahren, die heute als „sicher“ gelten[10]), dies bedeutet, dass die Komponenten freigegeben sind für die Übermittlung sensitiver, aber nicht klassifizierter Informationen in US Regierungsbehörden[11]. Eine entsprechende Zertifizierung bestätigt die Benutzung anerkannter Kryptomethoden in sicherer Form und wird von unabhängigen Testlaboren untersucht. Diese Zertifizierung beschränkt sich auf die Implementation & Auswahl der Kryptooalgorithmen und beinhaltet in der zertifizierten Stufe (Level 1) nicht die physische Sicherheit – die RIM-Endgeräte gelten nicht als „tamperproof“, d.h. es existieren keine besonderen Schutzvorkehrungen, die das „physische“ Auseinandernehmen verhindern, um an die Speicherbausteine mit den Daten zu gelangen[12]. Die „Content Protection“ (Verschlüsselung der Daten auf dem Endgerät) ist optional (und erst ab Version 4.0 überhaupt möglich) und wird häufig aufgrund von (je nach Endgerät-Leistungsfähigkeit durchaus spürbaren) Performance-Einbussen nicht aktiviert. Die Content-Protection verschlüsselt die Daten auf dem Endgerät sobald das Gerät ausgeschaltet oder gesperrt ist und stellt eine der wichtigsten Schutzmassnahmen bei Verlust des Gerätes dar. Ist die Content-Protection nicht aktiviert liegen die Daten auf dem Endgerät im Klartext vor, ist zusätzlich noch kein Zugangspasswort eingerichtet (was häufig aus Bequemlichkeit und der Anforderung „always on“ erfolgt), so kann jeder unautorisiert auf die Daten zugreifen[13]. Sowohl die „Content Protection“ als auch das Zugangskennwort (inklusive „Qualitätsanforderungen“ an das Passwort) lassen sich zentral über die Policy des BES steuern; allerdings werden diese zusätzlichen „Hürden“ und „Performance-Einbussen“ von Anwendern teilweise so stark abgelehnt, dass Administratoren sich gezwungen sehen, diese Schutzmassnahmen zu deaktivieren.

---

*[7] SRP: Server Router Protocol. Ein RIM-proprietäres Protokoll, welches die Grundlage des Push-Dienstes bildet und i.d.R. über TCP-Port 3101 eine Verbindung vom BES zum RIM-Netzwerk herstellt (in Europe: srp.eu.rim.com*

*[8] Der FIPS 140 Standard dokumentiert Anforderungen an kryptographische Systeme: und deren physische Sicherheit, dabei gibt es 4 Level (Level 1 bis Level 4), inkrementellen Anforderungen an die Sicherheit: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*

*[9] Die Zertifikate können online eingesehen werden: http://csrc.nist.gov/cryptval/140-1/140crt/140crt500.pdf und http://csrc.nist.gov/cryptval/140-1/140crt/140crt593.pdf*

*[10] Die maßgebliche Forschungsarbeit zum Thema „Schlüssellänge“ wurde von Arjen Lenstra im Jahr 2000 unter dem Titel „Selecting Cryptographic Key Sizes“ veröffentlicht: http://www.win.tue.nl/~klenstra/key.pdf*

*[11] Der Begriff „sensitive but not classified“ ist ein in den USA und Canada definierte Bezeichnung für Informationen, die nicht offiziell „klassifiziert“ wurden, aber trotzdem nicht öffentlich sind.*

*[12] @Stake, eine namhafte Firma in der IT-Security Branche, hat in einer Untersuchung auch die physische Sicherheit der Endgeräte evaluiert und bescheinigt den untersuchten Geräten eine gewisse Resistenz gegen physische Angriffe: http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/645094/An_@stake_Security_Assessment.pdf?nodeid=644990&vernum=0. Allerdings ist diese Untersuchung von RIM beauftragt worden.*

*[13] Ein solcher realer Fall von fahrlässigem Umgang wird in einem Artikel beschrieben, der viele Aspekte mobiler Security am Beispiel eines auf ebay verkauften BlackBerry aufzeigt: http://www.wired.com/news/business/0,1367,60052,00.html*

RIM versichert, dass auch in den RIM-Netzen keine Möglichkeiten bestehen, die Nachrichten zu entschlüsseln, auch nicht im Kontext des „lawful intercept[14]“.

## 3.3 Der BlackBerry Enterprise Server (BES)

Der BES besteht aus einer Vielzahl ineinander greifender Dienste; die Struktur und die Kommunikationsbeziehungen des BES sind in Abbildung 3 dargestellt. Da der BES mehrere Datenbanken benutzt und mit den Mail-Servern kommuniziert, existieren mehrere Accounts für den BES auf diesen Systemen mit sehr weit reichenden Privilegien:

| | **Logon Locally** | **Logon as Service** | **Local Administrator** | **Exchange Read-Only Administrator** | **Exchange Mail-Store Administrator** |
|---|---|---|---|---|---|
| **Service Account** | √ | √ | √ | √ | √ |
| **Server Management Account** | √ | √ | √ | √ | √ |
| **User Admin Account** | X | √ | √ | √ | X |

[14] *Eine Archtitektur für „lawful intercept“ ist in RFC 3924 beschrieben: http://www.rfc-editor.org/rfc/rfc3924.txt. Als „lawful intercept“ werden Abhöraktionen bezeichnet, die im Einklang mit der nationalen Gesetzgebung stehen. In Deutschland gilt z.B. die Telekommuniaktions-Überwachungsverordnung (TKÜV): http://bundesrecht.juris.de/bundesrecht/tk_v_2005/gesamt.pdf.*

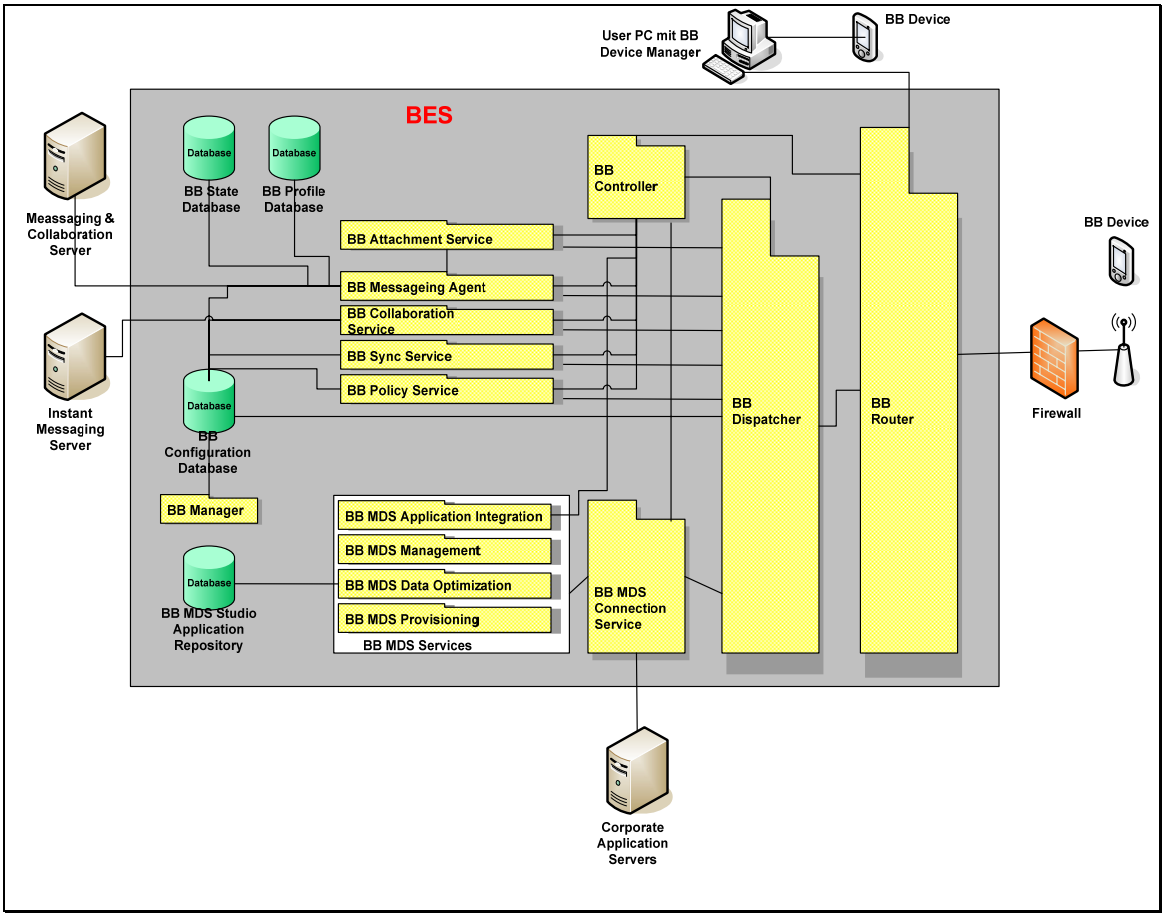



**Abbildung 3 Dienste des BES**

Diejenigen BES-Komponenten, die nicht direkt mit dem Email-Server kommunizieren, greifen über die „Configuration-Database“, eine MS-SQL-Datenbank, auf die Konfigurationseinstellungen zu. Diese Datenbank beinhaltet unter Anderem folgende Informationen:

- Die eindeutigen (sprich: Geräte-spezifischen) SRP Authentifizierungsschlüssel und SRP User-IDs, welche für die Authentifizierung der Endgeräte am BES benutzt werden. Dies ist das wichtigste geteilte Geheimnis zwischen BES und Endgerät – und steht im Klartext in dieser Datenbank.
- Die eindeutigen (sprich: Geräte-spezifischen) öffentlichen und privaten Schlüssel, die der BES für die Umsetzung der Policy auf den Endgeräten benutzt.
- Die PIN jedes Endgerätes.
- Kopie der Master Encryption Keys für jedes Endgerät
- User Listen

Da diese Datenbank eine MS-SQL-Server Datenbank ist und in dieser Datenbank die sicherheitsrelevantesten Informationen stehen, sollte dieser Server intensiv gehärtet werden[15]. Insbesondere muss der „sa“-Account mit einem starken Passwort geschützt werden und die eingehenden SQL-Verbindungen sollten auf BES beschränkt werden.

[15] *Microsoft hat unter http://msdn.microsoft.com/library/en-us/dnnetsec/html/THCMCh18.asp?frame=false eine gute Anleitung zur Härtung des MS-SQL-Server publiziert.*

Neben der „Configuration Database“ ist der Attachment-Service unter Sicherheitsaspekten ein weiterer kritischer Dienst. Die Aufgabe des Attachment-Service besteht in der Bereitstellung von Email-Attachments bestimmter Formate. Wenn Emails mit Anhang für einen BlackBerry-Benutzer empfangen werden, so wird zunächst nur die Email auf des Endgerät übertragen – erst auf Veranlassung durch den Benutzer wird der Anhang verarbeitet und übertragen. Untersuchungen der Gruppe „Phenoelit“ haben ergeben, dass dazu auf bekannte C-Bibliotheken zurückgegriffen werden, die teilweise fehlerbehaftet sind[16]. Diese fehlerhaften Bibliotheken ermöglichen die Ausführung von beliebigem Code auf dem Attachment-Service-Server[17]. Der Attachment-Service sollte deswegen vom Rest des BES getrennt werden und insbesondere keine Verbindung zur Configuration-Database aufbauen können, da sonst durch einen erfolgreichen Angriff auf den Attachment-Service sämtliche Daten in der Configuration-Database gegenüber dem Angreifer exponiert werden können. Um einen solchen Angriff zu starten, ist „lediglich“ der Versand einer Email mit präpariertem Anhang an einen BlackBerry-Benutzer notwendig.

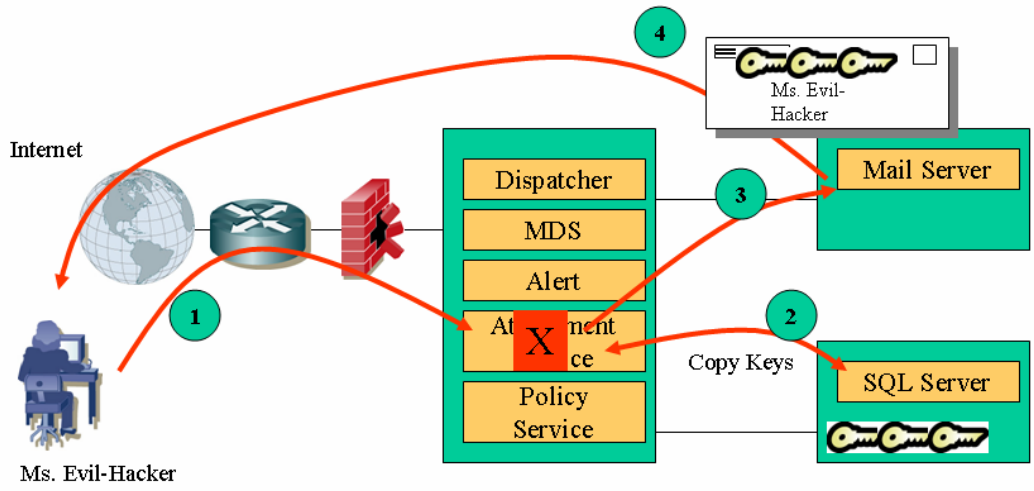



**Abbildung 4 Erfolgreicher Angriff auf den Attachment-Service**

Der in Abbildung 4 dargestellte Angriff kann durch die Auslagerung des Attachment-Service verhindert werden, da der Attachment-Service nicht mit Configuration-Database kommunizieren muss (siehe Abbildung 5).

[16] *Der Vortrag zu den Untersuchungen von Phenoelit wurde auf der Blackhat Europe 2006 gehalten: http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-fx.pdf*
[17] *RIM hat die betroffenen Bibliotheken mittlerweile durch aktuelle Versionen ersetzt; ist der BES auf dem aktuellen Patchlevel, so ist dieser Angriff nicht mehr möglich.*

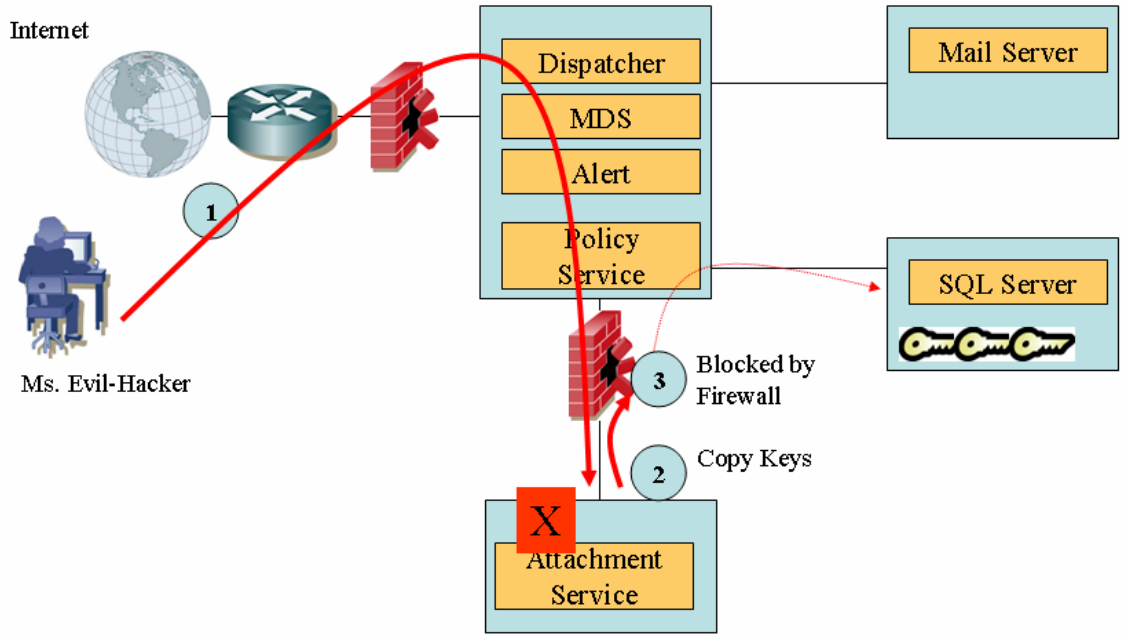



**Abbildung 5 Durch eine Änderung der Architektur schlägt der Angriff fehl.**

## 4 ORGANISATORISCHE ASPEKTE

Neben den technischen Aspekten sind organisatorische Aspekte für einen sicheren Betrieb einer BlackBerry-Infrastruktur zwingend zu berücksichtigen. Diese Aspekte können unterteilt werden in die Kategorien „Richtlinien“ und „Prozesse“ und sind in ihrer Bedeutung und Anwendung nicht auf BlackBerries beschränkt, sondern allgemein auf den Bereich „Mobile Computing“ erweiterbar. Die wichtigsten organisatorischen Aspekte sollen betrachtet werden.

Um sinnvolle Richtlinien und Prozesse zu etablieren ist es hilfreich eine Kategorisierung der Geräte, der Anwendungen und Daten und der Benutzer vorzunehmen. Dabei sollte die Art der Anwendung die Auswahl der Endgeräte bestimmen und nicht umgekehrt.

Die Art der Anwendung der Geräte bestimmt in der Regel, welche Daten auf dem Gerät gespeichert werden. Dafür kann eine Kategorisierung mit Hilfe von Fragestellungen durchgeführt werden:

- Wird das Gerät als PIM eingesetzt?
- Wird das Gerät für Unternehmensanwendungen (SAP, etc.) eingesetzt?
  - Von wo erfolgt der Zugriff? Aus dem Internet? Aus dem unternehmenseigenen WLAN?
- Wird das Gerät als mobiler Datenträger benutzt?
- Wird das Gerät als Telefon genutzt?
- Wird das Gerät für den Internetzugang genutzt?
- Ist abzusehen, dass auch private Daten auf den Endgeräten gespeichert oder verarbeitet werden (z.B. private Termine im Kalender, private Emails oder auch private Bilder, mp3-Dateien etc.)?
- Muss davon ausgegangen werden, dass Benutzer ihre eigene Software auf den Endgeräten installieren werden (Spiele, Photoalbum, etc.)?

Die Kategorisierung der Endgeräte basiert auf ihren technischen Möglichkeiten. Diese Kategorisierung ist nicht unabhängig von der Kategorisierung der Anwendung, da die Anwendung, wie schon erwähnt, die Auswahl der Endgeräte bestimmt. Die relevanten Fragestellungen in diesem Kontext sind:

- Welche Schnittstellen zur Datenübertragung besitzt das Gerät?
- Welches Betriebssystem ist auf dem Gerät installiert?
- Kann Software nachinstalliert werden? Auch vom Endbenutzer?
- Kann eine Speicherkarte installiert werden?
- Kann von einer Speicherkarte Software gestartet werden, die nicht installiert werden muss?
- Kann eine Password-Policy erzwungen werden?
- Kann Hardware (z.B. eine WLAN-Karte) nachinstalliert werden?

Die nächste Kategorisierung versucht den Benutzer zu beschreiben. Dies ist sicherlich die schwierigste Kategorisierung, aber trotzdem hilfreich um ein besseres Verständnis für den Gesamtkomplex „Mobile Computing“ zu gewinnen. Die Fragestellungen sind dabei, im Gegensatz zu den beiden vorhergehenden Kategorien, „weicher“ Natur:

- Welcher Unternehmenshierarchie gehört der Benutzer an?
- Welches technische Verständnis hat der Benutzer?
- Welches Sicherheitsbewusstsein hat der Benutzer?
- Wie mobil ist der Benutzer? Wo muss das Gerät welche Funktionalitäten bieten?
- Welchen Verfügbarkeitsanspruch hat der einzelne Nutzer?
- Steht der Benutzer dem „Mobile Computing“ persönlich aufgeschlossen gegenüber, oder betrachtet er dies eher als zusätzliche Belastung?

Aus den vorhergehenden Kategorien können die Antworten zu den grundlegendsten Fragen abgeleitet werden:

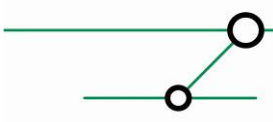
- Welche Daten werden mit dem Endgerät verarbeitet?
- Wie sind diese Daten klassifiziert? Welche Konsequenzen ergeben sich aus der Klassifizierung?
- Wie werden diese Daten übertragen?
- Wo werden diese Daten gespeichert?
- Welche Anforderungen aus der Klassifizierung ergeben sich für die Übertragung und Speicherung der Daten?

Diese Kategorisierung bildet die Grundlage der Definition von Richtlinien und Prozessen und kann auch als Basis für die Entwicklung eines Trainingsprogramms für die Mitarbeiter dienen.

## 4.1 Richtlinien

Ohne definierte, umsetzbare und überprüfbare Richtlinien gibt es keine Handhabe um zum Beispiel die Benutzung von Passwörtern oder Verschlüsselung zu erzwingen. Diese Richtlinien müssen sich als Dokument in die globale Security-Policy eines Unternehmens eingliedern und unterliegen denselben Verfahren zur Veröffentlichung und Revision wie alle anderen schon vorhandenen Richtlinien auch. Dabei ist das Ziel dieser Richtlinien einen zum Unternehmens-PC mindestens äquivalenten Sicherheitsstandard auf den mobilen Endgeräten, unter Berücksichtigung der besonderen Merkmale und des Einsatzzwecks, zu etablieren; die Unterschiede liegen in den Besonderheiten des Einsatzes, der Mobilität und der Möglichkeiten der Endgeräte, so dass die „PC-Sicherheitsrichtlinie“ nicht 1:1 übertragen werden kann. Der zu etablierende Sicherheitsstandard muss mindestens äquivalent sein, die dafür vorgeschriebenen Ansätze können aber erheblich von den PC-Ansätzen differieren. Dies wird z.B. insbesondere an der Passwort-Policy deutlich: Eine komplexes Passwort (z.B. ms91Hu$8W!&) lässt sich auf einer vollwertigen PC-Tastatur leicht eingeben, das gleiche Passwort auf einem BlackBerry, MDA oder Smartphone (ggf. noch über eine Softtastatur) einzugeben ist den meisten Benutzer





nicht zumutbar. Aufgabe einer Richtlinie ist es, diesen scheinbaren Widerspruch aufzulösen. Ein möglicher Ansatz besteht aus der Gestattung einfacherer Passwörter (z.B. 5 Zeichen alphanumerisch, als Beispiel 12te3), die sich gut eingeben lassen, gekoppelt mit der technischen Maßnahme, dass nach einigen wenigen aufeinander folgenden Fehleingaben des Passwortes sämtliche Daten auf dem Gerät gelöscht werden.

Wie viel „Sicherheit“ notwendig ist basiert auf der Fragestellung nach der Art und dem Umfang der verarbeiteten und übertragenen Daten. Die Klassifizierung der Daten ist unabhängig vom verarbeiteten Endgerät – eine „vertraulich“ eingestufte Datei behält diese Einstufung unabhängig davon, ob sie auf einem Unternehmens-PC oder auf einem mobilen Endgerät gespeichert wird. Die Datenklassifizierungsrichtlinie definiert die verschiedenen Klassifizierungen, gibt vor, wie Daten zu klassifizieren sind und schreibt vor, welche Schutzmassnahmen auf Daten der einzelnen Klassifizierungen anzuwenden sind. Ein einfaches komprimiertes Beispiel einer solchen Richtlinie ist in folgender Tabelle zusammengefasst:

| **Klasse** | **Beschreibung** | **Beispiel** | **Richtlinie für Speicherung** | **Richtlinie für Übertragung** | **Richtlinie für Löschung** |
|---|---|---|---|---|---|
| Öffentlich | Diese Daten können ohne jeden Schaden veröffentlicht werden | Zur Veröffentlich-ung bestimmte Publikationen | Keine | Keine | Keine |
| Intern | Externer Zugriff sollte nicht möglich sein. | Arbeitsan-weisungen, Angebote | Daten SOLLTEN gelabelt werden. Klassifi-zierung SOLLTE auf Medien sichtbar sein. | Die Informationen SOLLTEN bei der Übertragung über öffentliche Netze verschlüsselt werden. | Keine |
| Vertraulich | Daten dieser Klasse sind innerhalb des Unternehmens vertraulich und vor Zugriff geschützt. | Kundendaten Projektdaten | Die Informationen MÜSSEN gelabelt werden. Dokumente MÜSSEN gesichert aufbewahrt werden. | Die Informationen MÜSSEN bei der Übertragung über öffentliche Netze verschlüsselt werden. | Alle Träger (Disketten, Papier etc.) dieser Informationen MÜSSEN physisch vernichtet werden |

Ein besonderer Aspekt in Bezug auf mobile Endgeräte ist die Kürze der Produktzyklen – ein PC oder Laptop hat einen durchschnittlichen Lebenszyklus von 3 – 4 Jahren wohingegen ein 3 Jahre altes Mobiltelefon oder ein 3 Jahre alter BlackBerry technisch komplett veraltet ist. Ersatzteile sind in der Regel nicht mehr erhältlich, aktuelle Betriebssystemversionen lassen sich meistens nicht mehr einspielen und als Statussymbol hat dieses Gerät auch keinen Wert mehr. Dies führt häufig dazu, dass Anwender mit dem „alten“ Gerät unachtsam umgehen, es gerne „verlieren“ oder aber privat modernere Geräte anschaffen, die dann im Unternehmen eingesetzt werden sollen. Insbesondere die privaten Geräte stellen aber ein ernstzunehmendes Problem dar, da die Umsetzung einer Unternehmensrichtlinie auf einem privaten Endgerät nicht erzwungen werden kann und das Helpdesk die Vielfalt an verschiedenen (privaten) Geräten

nicht unterstützen kann, was vom Anwender mit seinem privaten Endgerät aber erwartet wird. Deswegen ist das explizite Verbot privater Endgeräte, und dazu zählen auch Beschaffungsprogramme, bei denen der Mitarbeiter an den Anschaffungskosten und/oder Betriebskosten beteiligt wird, ein zentraler Bestandteil einer erfolgreichen Richtlinie.

Welche weiteren Richtlinien sind in Bezug auf mobile Endgeräte sinnvoll? Auch wenn der Inhalt der Richtlinie von Unternehmen zu Unternehmen unterschiedlich ist, sind die aufzugreifenden Aspekte auf wesentliche Punkte zu verallgemeinern:

- Richtlinie zum Umgang mit mobilen Endgeräten: Diese Richtlinie beschreibt die Sorgfaltspflicht des Mitarbeiters. Wohin darf/darf nicht/muss er das Gerät mitnehmen? Welche Datensicherungsmaßnahmen sind zu ergreifen? Was ist explizit verboten (Installation von Software, Hardware, etc.)? Wer muss bei Verlust informiert werden?
- Richtlinie zum Virenschutz auf mobilen Endgeräten: Da diese Endgeräte häufig außerhalb des Sicherheitskontexts des Unternehmens benutzt werden, gilt es dabei besondere Vorkehrungen zu treffen, einerseits um das Gerät und die dort gespeicherten Daten selbst zu schützen, andererseits um das Unternehmensnetzwerk vor Einschleppen von Viren über mobile Endgeräte zu schützen.
- Richtlinie zum Internetzugang mit mobilen Endgeräten: Falls die mobilen Endgeräte auch für den Zugang zum Internet (z.B. per Hotspot am Flughafen) genutzt werden, dann stehen diese Endgeräte nicht durch die Unternehmensinfrastruktur geschützt (zentrale Firewall, Proxy-Server mit URL-Filter und Antiviren-Software) sondern direkt im Internet. Dadurch wird das Endgerät den Bedrohungen aus dem Internet uneingeschränkt exponiert und der Benutzer ist zu größtmöglicher Sorgfalt und Vorsicht anzuhalten. Diese Richtlinie kann die Benutzung des Internet, außer zum Aufbau einer VPN-Verbindung ins Unternehmen, auch explizit verbieten (über die VPN-Verbindung ist dann ggf. auch wieder ein Internetzugang geschützt durch den Proxy-Server möglich).
- Passwort-Richtlinie für mobile Endgeräte: Wie im Eingang zu diesem Kapitel bereits erwähnt, kann es durchaus sinnvoll sein, für mobile Endgeräte eine andere Passwort-Richtlinie zu definieren als für Unternehmens-PCs. Wird keine spezielle Passwort-Richtlinie erstellt, so gilt wahrscheinlich die allgemeine Passwort-Richtlinie.

## 4.2 Prozesse

Richtlinien sind ein wichtiger Bestandteil der Organisationssicherheit; aber ohne definierte, dokumentierte und überprüfbare Prozesse, die klare Handlungsanweisungen und Abläufe beschreiben, fehlt den beteiligten Personen der Handlungsrahmen innerhalb dessen sie sich bewegen. Ähnlich wie bei den Richtlinien, sollten sich die Prozesse im Themenbereich „Mobile Computing“ bzw. „Mobile Security“ an den bestehenden Prozessen orientieren, aber auch bei den Prozessen existieren einige wichtige Besonderheiten, auf die kurz eingegangen werden soll. Welche zusätzlichen Prozesse müssen definiert werden?

- Prozess zur Erstinbetriebnahme/Erstausgabe eines neuen mobilen Endgeräts: Bevor das Endgerät an den Benutzer ausgegeben wird, muss die Security-Policy auf dem Gerät umgesetzt (dies kann ggf. die Installation von Software, Einbindung ins Management-System und Installation einer „Policy“ beinhalten) und das Gerät mit der relevanten Software (VPN-Client, SAP-Client, etc) bzw. den relevanten Daten (Abteilungsadressbuch, etc) bestückt werden. Die Identitätsinformationen des Gerätes (Typ, Modell, Seriennummer, IMEI[18], ausgegebene SIM-Karte) sollten inventarisiert sein

[18] *Die „International Mobile Equipment Identifier“ ist eine weltweit eindeutige Gerätenummer eines Mobiltelefons, welche beim Einbuchen in ein Mobilfunknetz an den Netzbetreiber übermittelt wird. Sollte das Gerät gestohlen werden, kann es anhand dieser Nummer gesperrt werden, so dass das Gerät selbst mit einer anderen SIM-Karte nicht mehr benutzt werden kann. Allerdings kann die IMEI eines Geräts geändert werden, wenn sie in einem überschreibbaren Speicherbereich auf dem Endgerät steht.*

um dem Helpdesk einen individuellen Support zu ermöglichen, bzw. um das Gerät im Falle eines Verlustes sperren zu können.

- Prozess bei Verlust des Endgeräts: Verlust, entweder durch „Diebstahl“ (des Gerätes oder der Daten wegen) oder durch „Verlieren“, ist ein Risiko mit einer sehr hohen Eintrittswahrscheinlichkeit und potentiell hohem Schaden. Ein „Incident Response“ Prozess für den Verlustfall ist zwingend notwendig und sollte folgende Aspekte berücksichtigen:
  - Wie unterrichtet der Benutzer das Helpdesk über den Verlust?
  - Welche Maßnahmen leitet das Helpdesk ein?
    - Sperren des Endgeräts beim Netzbetreiber,
    - Sperren der SIM beim Netzbetreiber,
    - Sperren des Mail/Blackberry-Accounts für das Endgerät,
    - Remote-Kill des Endgeräts[19].
- Prozess beim Ausscheiden des Mitarbeiters: Dieser Prozess beschreibt die Schritte, die beim Ausscheiden des Mitarbeiters aus dem Unternehmen, stattfinden müssen, um die Vertraulichkeit und Verfügbarkeit der Daten auf dem mobilen Endgerät sicherzustellen. Dieser Prozess weist Ähnlichkeiten zum Verlustfall auf, unterscheidet sich jedoch in einem entscheidenden Detail: Der Motivation des Benutzers. Im Verlustfall hat der Benutzer ein eigenes Interesse (und wenn es „nur“ das Interesse an einem Geräteersatz ist) den Verlust zu melden, dieses Eigeninteresse hat er beim „Verlassen des Betriebs“ nicht (mehr). Diese geänderte Interessenlage muss im Prozessdesign in der Form berücksichtigt werden, dass die „Aktion“ nicht mehr vom Benutzer, sondern vom Unternehmen ausgehen muss. Die Frage über den Verbleib der Hardware (als „Abschiedsgeschenk“ beim ausscheidenden Mitarbeiter, im Gerätefundus des Unternehmens) sollte hier auch berücksichtigt werden.

Die grob skizzierten Prozesse müssen regelmäßig in Bezug auf die Funktionsfähigkeit (funktioniert der Prozess?) und Nachvollziehbarkeit (ist nachvollziehbar, wer welchen Teilschritt des Prozesses korrekt oder fehlerhaft abgearbeitet hat?) geprüft werden um rechtzeitig Korrekturen vornehmen zu können.

Mit freundlichen Grüßen,

Dror-John Röcher
CISSP, CCSP

ERNW GmbH
Dror-John Röcher
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 173 6745905
www.ernw.de

---

[19] *„Remote Kill“ bezeichnet eine Funktion, bei der mit Hilfe einer speziellen SMS vom Management-System aus sämtliche Daten auf dem Endgerät gelöscht werden. Auch wenn dieses „Feature“ häufig ein „Key Selling Point“ verschiedenster Security-Lösungen ist, so kann es doch trivial unterlaufen werden, indem die SIM vom Dieb/Finder aus dem Endgerät entfernt wird.*