

www.segu-info.com.ar agradece especialmente a FAM por la realización de este documento.

BlackBerry - Informe de análisis de riesgo (I)

Servicio BlackBerry

El sistema BlackBerry contempla desde su definición una serie de aspectos de seguridad orientados a garantizar la confidencialidad y la integridad de la información, tanto la que circula por los canales de comunicación, como la que es almacenada y procesada por los dispositivos móviles utilizados.

La tecnología BlackBerry permite mucho más que la sincronización del correo personal con el dispositivo móvil. Permite establecer accesos a Internet y a la Intranet y en consecuencia a las aplicaciones corporativas que ahí se ejecuten.

Esto convierte al dispositivo móvil en una práctica y poderosa herramienta de trabajo, pero también genera un riesgo similar a los que generan otras tecnologías inalámbricas o móviles. Esto significa que se está llevando la red de comunicaciones de la empresa hasta donde se encuentre el dispositivo móvil.

Los sistemas de dispositivos móviles actuales tienen capacidades avanzadas convirtiéndolos en una estación de trabajo más dentro de las redes corporativas. Los sistemas operativos y el software, tanto en la infraestructura central como en los dispositivos y los protocolos de comunicación tienen vulnerabilidades que son pasibles de explotación.

Del análisis de riesgo realizado se desprende que se deberán tener en cuenta en el diseño del sistema a implementar todas las medidas de seguridad que el sistema ofrece y definir la configuración más adecuada para la Empresa y las contramedidas a aplicar para vulnerabilidades conocidas así como las recomendaciones de seguridad desarrolladas por el proveedor.

Por lo expresado se deberá tener en cuenta lo siguiente:

- Se deberá analizar y definir el estándar de seguridad en función de las opciones de seguridad que brinda el sistema. Para ello se debe relevar todas las opciones de seguridad configurables, definir la política de seguridad y administración de la misma.
- Se deberá definir la metodología de actualización y mantenimiento de las versiones del software tanto del BBES como del dispositivo móvil.
- Establecer los puntos de control de la infraestructura y uso de la misma
- Procedimientos funcionales para el alta y habilitación de equipos y usuarios a utilizar el sistema. En tal sentido se considera necesario definir el marco normativo y efectuar el análisis de riesgo operativo correspondiente.
- Definición de procedimientos de emergencia ante pérdida o robo de un dispositivo móvil y la contratación de seguros de los dispositivos móviles
- Definición de recomendaciones de seguridad en la utilización de estos dispositivos y el riesgo asociado al uso de información confidencial en los mismos.

Se adjunta el análisis de riesgo en el que se basa el presente informe.

BlackBerry Enterprise Service

TABLA DE AMENAZAS					
Sistema de Información	Componente	Fuente de Amenaza	Acciones de Amenaza	Motivación	Capacidades
BlackBerry ES	BBES	Hacker	Intrusión Denegación de servicio Código Malicioso Acceso no autorizado	Sabotaje Diversión Popularidad	Técnicas de hacking Conocimientos específicos de la plataforma BBES
		Usuarios Internos	Intrusión Denegación de servicio Codigo Malicioso Acceso no autorizado	Curiosidad Disconformidad Inteligencia	Técnicas de hacking Conocimientos específicos de la plataforma BBES
BlackBerry Dispositivos	Hardware	Robo/Perdida	Perdida de Información confidencial Perdida de activo Usurpación de identidad	Descuido Robo Ingeniería social	Ladron Técnicas de Ingeniería social
	Software	Hacker	Ejecución de código malicioso Desbordamiento de memoria Denegación de servicio	Sabotaje Diversión Popularidad	Técnicas de hacking Conocimientos técnicos del dispositivo
	Comunicaciones	Hacker	Escucha de comunicaciones	Ingeniería social Robo de información	Conocimiento de redes inalámbricas

TABLA DE VULNERABILIDADES				
Sistema de Información	Componente	Vulnerabilidad	Fuente de Amenaza	Acciones de la amenaza
BlackBerry ES	BBES	Blackberry Enterprise Server Router SRP Packet Denial of Service	Paquetes malformados de SRP (protocolo de la encaminamiento del servidor) al router. Podría explotarse solamente por un atacante que este en condiciones de personificar la infraestructura del Blackberry o tiene posiblemente acceso a la red interna.	Denegación de servicio
		RIM BlackBerry Enterprise Server Attachment Service does not properly handle PNG image files	Mensaje con anexos de imágenes PNG	Código malicioso contenido en el archivo PNG puede comprometer el servidor
		Research in Motion (RIM) BlackBerry Attachment Service does not properly handle TIFF image files	Mensaje con anexos de imágenes Tiff	Denegación de servicio del Blackberry Attachment Service
		BlackBerry Enterprise Server fails to properly handle Microsoft Word attachments	Un archivo MS Word anexo, mal formado.	Código malicioso contenido en el archivo Word puede comprometer el servidor
		RIM analysis of buffer overrun in decompression algorithm	Un error de código en el algoritmo de descompresión	Posible ejecución remota de código
BlackBerry Dispositivos	Software	BBProxy	Troyano	Acceso indebido a la red interna
		URL	Al procesar URL excesivamente largas	Denegación de servicio
	Comunicaciones	Sniffing	Intercepción de comunicaciones inalámbricas	Confidencialidad de la información
	Hardware	Perdida/Robo	Descuido/Robo	Perdida de información confidencial o privada Perdida del activo físico
Componentes NO BlackBerry	Microsoft Windows Server	Los componentes deben ser asegurados siguiendo las recomendaciones del proveedor BlackBerry y los estándares internos. Estos componentes no serán evaluados en el presente análisis de riesgo.		Posibilidad de pérdida de integridad de la infraestructura y posibilidad de comprometer la red de datos
	IBM Lotus Domino			
	IBM Sametime server			

Tabla de Controles					
Sistema de Información	Componente	Vulnerabilidad	Probabilidad Ocurrencia	Control	Referencia
BlackBerry ES	BBES	Blackberry Enterprise Server Router SRP Packet Denial of Service	BAJA	Instalar BlackBerry Enterprise Server 4.0 Service Pack 4 o Posterior	http://www.kb.cert.org/vuls/id/392920
		RIM BlackBerry Enterprise Server Attachment Service does not properly handle PNG image files	MEDIA	Install BlackBerry Enterprise Server 4.0 Service Pack 3	http://www.kb.cert.org/vuls/id/646976
		Research in Motion (RIM) BlackBerry Attachment Service does not properly handle TIFF image files	MEDIA	Instalar Service Pack 3, después install software version 4.0 Service Pack 3 Hotfix 4.	http://www.kb.cert.org/vuls/id/570768
		BlackBerry Enterprise Server fails to properly handle Microsoft Word attachments	ALTA	For BlackBerry Enterprise Server 4.0, install Service Pack 3, then install version 4.0 Service Pack 3 Hotfix 4	http://www.kb.cert.org/vuls/id/520718
		RIM analysis of buffer overrun in decompression algorithm	BAJA	BlackBerry Enterprise Server software version 4.0 Service Pack 1 - Download BlackBerry Enterprise Server software version 4.0 Service Pack 1 Hotfix 1 OR BlackBerry Enterprise Server software version 4.0 Service Pack 1 Hotfix 3	http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB04075&sliceId=SAL_Public&dialogID=1072073&stateId=1%200%201092075

BlackBerry Dispositivos	Software	BBProxy	MEDIA	Aislar los servidores de BB y de correo asociados en la DMZ, siguiendo las recomendaciones del proveedor.	http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/1181821/828044/1181292/Placing_the BlackBerry Enterprise Solution in a Segmented Network.pdf?nodeid=1265885&vernum=0
		URL	MEDIA	Instalar BlackBerry Device Software 4.2 Service Pack 1 (4.2.1).	http://browsers.about.com/b/a/000054.htm
	Comunicaciones	Sniffing	ALTA	Encriptación punto a punto del canal de comunicación	Documentación técnica del proveedor
	Hardware	Perdida/Robo	ALTA	Cifrado de datos local Procedimientos de acción remota para bloqueo y eliminación de información Seguros	Recomendaciones del fabricante
Componentes NO BlackBerry	Microsoft Windows Server	Vulnerabilidades conocidas		Aplicación de estándares del proveedor de cada plataforma y del proveedor de BB	Placing BB Enterprise Solution in a segmented network - "Protecting non-blackBerry components"
	IBM Lotus Domino				
	IBM Sametime server				

Análisis de riesgo					RIESGO	
Sistema de Información	Componente	Vulnerabilidad	Probabilidad Ocurrencia	Impacto	Bruto	Controlado
BlackBerry ES	BBES	Blackberry Enterprise Server Router SRP Packet Denial of Service	BAJA	ALTO	MEDIO	BAJO
		RIM BlackBerry Enterprise Server Attachment Service does not properly handle PNG image files	MEDIA	MEDIO	MEDIO	BAJO
		Research in Motion (RIM) BlackBerry Attachment Service does not properly handle TIFF image files	MEDIA	MEDIO	MEDIO	BAJO
		BlackBerry Enterprise Server fails to properly handle Microsoft Word attachments	ALTA	ALTO	ALTO	BAJO
		RIM analysis of buffer overrun in decompression algorithm	BAJA	ALTO	MEDIO	BAJO
BlackBerry Dispositivos	Software	BBProxy	MEDIA	ALTO	ALTO	BAJO
		URL	MEDIA	BAJO	BAJO	BAJO
	Comunicaciones	Sniffing	ALTA	ALTO	ALTO	BAJO
	Hardware	Perdida/Robo	ALTA	ALTO	ALTO	MEDIO
Componentes NO BlackBerry	Microsoft Windows Server	Vulnerabilidades conocidas		ALTO	ALTO	BAJO
	IBM Lotus Domino					
	IBM Sametime server					

BlackBerry (BB) – Informe de riesgo (II)

La tecnología BB extiende las fronteras tecnológicas y de control a las palmas de nuestras manos. Es por ello que toda la arquitectura fue pensando en la seguridad de la información y de las empresas que la adopten. En el informe de riesgos realizado anteriormente se evaluaron todas las amenazas y vulnerabilidades reportadas definiendo las contramedidas correspondientes a cada caso.

En principio, parece estar todo controlado por la tecnología. La arquitectura BB esta diseñada para facilitar el acceso en forma segura a la red interna para obtener los servicios de correo, mensajería, Internet, etc. No obstante, la información almacenada en los dispositivos (agendas, contactos, archivos, etc.), están siendo transportados en forma permanente fuera del ámbito de control de las organizaciones.

Ahora bien, la tecnología no puede controlar todo. Los seres humanos estamos continuamente expuestos a amenazas y riesgos que no son factibles de mitigar con la tecnología.

El mayor riesgo en el caso de los dispositivos móviles es la utilización de los dispositivos por parte de terceros no autorizados exponiendo la información que con tanto esmero se protegió desde la arquitectura tecnológica.

El valor intrínseco de estos dispositivos lo convierten en un atractivo para ser objeto de robo o hurto, pero también quienes quieran obtener información sensible pueden hacerlo obteniendo un dispositivo móvil como el BB.

Estadísticas de la Cámara de Informática y Comunicaciones señalan que en promedio se robaron alrededor de 25.000 celulares por mes en los últimos 18 meses. Los robos aumentaron sustancialmente desde la devaluación del peso, que triplicó el precio de los equipos. (*fuentes: www.segu-info.com.ar*)

Una de las herramientas que brinda la tecnología BlackBerry es el acceso controlado por contraseña. Esta obliga al propietario a habilitar el equipo cada vez que se necesita acceder a los servicios provistos por la organización y a la información almacenada en él. El tiempo de inactividad del dispositivo es contabilizado a fin de poder establecer un bloqueo automático para que no pueda ser accedido por terceros.

Las opciones de configuración de BB permiten establecer políticas detalladas logrando el nivel de seguridad adecuado para las organizaciones. No obstante ello, el mayor riesgo es aquel que no puede ser controlado. En este caso el riesgo que no podemos controlar esta dado por:

- Robo o hurto del dispositivo
- Extravío
- Descuido temporal
- Acceso indebido por conocidos relacionados

La forma de reducir estos riesgos es llevar al máximo posible el tiempo de bloqueo automático de estos dispositivos por ejemplo a 15 minutos. Se asume para ello que si el dispositivo esta diseñado para estar en las manos de los usuarios, si por 15 minutos este no realizó actividad alguna, es por que el mismo no esta en uso y en consecuencia, este puede no estar debidamente custodiado por su propietario.

Como se mencionara anteriormente, las motivaciones que potencian estos riesgos son el valor propio del dispositivo y en muchos casos, la suposición del valor de la información que estos contienen. Este último es propio de aquellos que planifican la obtención de información sensible con el objetivo de cometer algún tipo de ataque, basado en ingeniería social.

El Gartner Group recomienda en su artículo "How to Ensure That PDAs and Smartphones Don't Compromise Business Security" publicado el 28/8/2006, que deben establecerse políticas claras en la utilización de los dispositivos móviles que incluyen mecanismos de autenticación fuertes y encriptación de los datos almacenados en ellos.

En el siguiente cuadro se indican las contramedidas a aplicar en dispositivos móviles con tecnología inalámbrica en función de la movilidad del usuario y el valor de la información en riesgo.

	Valor de la información en riesgo			
		Bajo	Medio	Alto
Movilidad del empleado	Baja	Proteger descubrimiento de activos	Proteger descubrimiento de activos, Antivirus, protección por contraseña	Proteger descubrimiento de activos, Antivirus, Protección por contraseña, Eliminación remota de información en el dispositivo, Encriptación
	Media	Proteger descubrimiento de activos, Antivirus, protección por contraseña	Proteger descubrimiento de activos, Antivirus, protección por contraseña, Eliminación remota de información en el dispositivo, sincronización	Proteger descubrimiento de activos, Antivirus, protección por contraseña, Eliminación remota de información en el dispositivo, aplicación de parches de software, Encriptación
	Alta	Proteger descubrimiento de activos, Antivirus, protección por contraseña, Eliminación remota de información en el dispositivo	Proteger descubrimiento de activos, Antivirus, protección por contraseña, Eliminación remota de información en el dispositivo, aplicación de parches de software	Proteger descubrimiento de activos, Antivirus, protección por contraseña, Eliminación remota de información en el dispositivo, aplicación de parches de software, Encriptación

Fuente: Forrester - Analyst reports - Managing and Securing Mobile Devices
(<http://www.csoonline.com/analyst/report2794.html>)

Las políticas de seguridad del dispositivo BlackBerry deben contemplar:

- Bloqueo automático en un tiempo por inactividad de 15 minutos
- Acceso por contraseña
- Procedimiento de eliminación remota de información ante pérdida o robo/hurto del dispositivo
- Encriptación de información almacenada
- Control de acceso por los canales de comunicación inalámbricos o de sincronización (bluetooth o USB) y encriptación.

Estas políticas suelen ser "antipáticas" desde punto de vista del usuario, y considerando que generalmente se trata de ejecutivos, gerentes o directores, se hace más difícil su implementación.

Es por ello que los aspectos relacionados con las tecnologías móviles deben estar incluidos en las políticas y normas de seguridad de la información y contar con el respaldo de la alta gerencia.

Es muy común que las empresas implementen tecnologías como BlackBerry como una novedad y comiencen otorgándoles dispositivos a directores y ejecutivos "claves" de la organización, pero con el tiempo se va incrementando su utilización debido a que se transforma una poderosa herramienta para otros empleados de la empresa. Este crecimiento suele ser descontrolado corriendo el riesgo de perder de vista que tipo de información se esta manejando en estos dispositivos.

Es necesario hacer tomar conciencia a los usuarios de estos dispositivos de manera adecuada al momento de su entrega, mostrándoles el riesgo que implica su utilización.

Por ultimo, deben existir procedimientos precisos y claros para actuar en caso de denuncia de pérdida, robo o hurto de los dispositivos, que permitan el bloqueo y la eliminación de los datos contenidos en ellos.