CyberSecurity MALAYSIA

AN agency under MOSTI

INFORMATION SECURITY BEST PRACTICE:
SECURING BLACKBERRY

Registered office:
CyberSecurity Malaysia,
Level 7, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia
Phone: +603 - 8992 6888
Fax: +603 - 8945 3205
Web : http://www.cybersecurity.my

INTRODUCTION

"Despite the consumerisation of Information Technology (IT), BlackBerry is still ahead of the competition in satisfying the unique security requirements of highly regulated industries."

A majority of consumers will agree that BlackBerry® devices are not just applicable for corporate and business matters but also great in providing various types of entertainment! BlackBerry devices have become the new personal computer, storing as much data as a personal computer (PC) but providing greater flexibility and portability. With BlackBerry, you can call friends, access social media networks, do banking transaction and receive your individual as well as corporate emails anytime and anywhere. In addition, it is still the leader in offering email solution for corporate users (BlackBerry has a 'push' technology which helps to deliver emails to BlackBerry devices in seconds). In essence, BlackBerry has successfully captured its consumers' habits in doing 'everything' using their BlackBerry.

Due to these, BlackBerry devices are vulnerable to various security threats. As BlackBerry owner, whether you are a corporate BlackBerry user or using it for personal reasons, it is important that you secure your BlackBerry device. Let's look at some of the security threats that are targeting BlackBerry.

POSSIBLE SECURITY THREATS

According to the Juniper Networks Global Threat Center (GTC) report[1], common security threats targeting BlackBerry for 2011 are:

Malware

Malware (i.e. spyware, viruses, trojans, and worms) targeting BlackBerry, Nokia's Symbian and other mobile operating platforms continue to grow at a rapid rate. The same report indicates that variants of Zues Trojan were found on BlackBerry devices. Attacker can exploit the trojan to obtain user credentials of financial accounts to initiate online banking sessions.

Loss and Theft

A BlackBerry device is used to store a variety of information whether it is business or personal in nature. Thus, data lost due to misplaced or stolen BlackBerry will present a significant risk to organizations and consumers especially for those without security settings like passwords. Consumers and organizations will bear a specific impact as discussed below if the BlackBerry devices are lost or stolen.

1. **Data breach:** Customer's information contained in BlackBerry devices need to be protected appropriately. If the information is disclosed to unauthorized parties or manipulated by attacker, organizations may face legal action and reputational risk.
2. **Loss of intellectual property and trade secrets:** Business people may keep their trade secrets in their mobile devices. If the intellectual property falls into the wrong hands, it will create a devastating effect not just to the BlackBerry owner but to the owner's organization as well.
3. **Loss of personal information:** Contact details in BlackBerry devices that contain personal information of a person can be used for malicious purposes such as identity theft and fraud. Lately, it was found on the Internet that personal information such as these are sold to criminals.

[1]2012, Juniper Networks, Malicious Mobile Threats Report 2010/2011, http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

Data Communication Interception

The interception of communication is a threat to BlackBerry device that sends and receives data and connects to a network. Attacker may be able to intercept BlackBerry communications, including emails and voice calls, via specialized equipment or tool. Two examples of interception threat are Wi-Fi hacking and Man-In-The-Middle (MITM) attack. Through Wi-Fi hacking, attacker hijacks the online user's credentials to impersonate as a legitimate user, thus leads to financial loss and identity theft. In MITM attack, attacker intercepts BlackBerry communication and sees everything in clear text. This attack gives the attacker the access to sensitive information of an individual or corporate entity.

Exploitation and Misconduct

The exploitation and misconduct threat in BlackBerry involves inappropriate or suggestive use of BlackBerry device for personal amusement or monetary gain. As an example, an attacker may exploit the BlackBerry device and sent inappropriate or explicit pictures or videos residing in a BlackBerry to other users. As for monetary gain example, the camera features of BlackBerry devices enable grunted employees with malicious intent to transmit sensitive information to company's competitor and be paid for it.

Direct Attacks

A direct attack is an action performed by an attacker when malicious content is sent to BlackBerry devices via SMS, MMS and email causing damages to a BlackBerry system either to the components or the interface. For instance, browser-based threat is a threat that downloads malware without a user's knowledge when a user visits an infected website. The malware is programmed by an attacker to download all sensitive data including contacts, pictures in a BlackBerry device and sends them to the attacker.

BEST PRACTICES FOR SECURING BLACKBERRY

Now you have recognized security threats targeting your BlackBerry, you need to take actions to protect your BlackBerry and information in it. Thus, we recommend these best practises to assist you in securing your BlackBerry.

1. Enable passwords and pin codes

People can set their pin codes in a few places:

i. Lock the BlackBerry with a pin code. Pin code is the first mechanism that will defend the BlackBerry from unauthorised users. Pin code for BlackBerry is in numbers. Remember not to put your birth date since your close friends may aware of it. Use something that is unpredictable.

ii. Second mechanism, set passwords. If the unauthorised user can pass the pin code, password will be prompted. Below are some of the Do's and Don'ts of a strong password:

Dos	Don'ts
1. Use eight characters long (or more). 2. Ensure combination of uppercases, lowercases, symbols and numbers. 3. Choose easy to be remembered but hard to be guessed passwords. 4. Create different passwords for different applications. 5. Change your passwords regularly.	1. Avoid dictionary words in any language. 2. Never use passwords that are words spelled backwards, common spellings and abbreviations. 3. Avoid sequences or repeated characters such as '1234', '33333', 'abc123', or adjacent letters on the keyboard (qwerty). 4. Do not share passwords even with your trusted friends. 5. Never write down your passwords.

2. Set a time-out

Next, the third layer is time-out. Setting a time-out allows your BlackBerry to lock automatically after a specified duration. Say, the time-out is two minutes. When your BlackBerry is idle (idle means left untouched) for two minutes, it will lock itself automatically.

3. Enable wipe out if exceeds password and pin code failure

The fourth level will be BlackBerry wipe out. Number of attempts can be set from three to 10 (default is 10) for the wipe outs. The fewer the number, the less chance of password attempts. If the number of attempts exceeds, data will be wiped out and the device resets.

4. Prompt password when downloading or installing programmes

The next best practice is to set password for downloading or installing programmes. This can help protecting BlackBerry from being harmed by a malicious programme and preventing malicious codes from being injected in the BlackBerry.

5. Enable Content Protection BlackBerry Device Data

Please ensure you enable content protection to ensure that your data (such as emails, contacts, pictures) is not readable. Enable the content protection means that content is hidden in a special mechanism so that unauthorized person cannot see and manipulate the data. You can specify the level of your encryption, from strong, stronger to strongest.

6. Install antivirus, firewall and updates

Like computers, BlackBerry devices can be infected by malware. Install an antivirus in your BlackBerry from BlackBerry App World. Antivirus operates by tracing the uncommon behaviour of an application and deletes the infected programme. You need firewall to preserve your privacy from unwanted messages and lessen the exposure of social engineering attacks. Patches and updates are necessary because they fix the current vulnerability or security bug that is in the software. Firewall and latest updates for your BlackBerry device can also be downloaded from BlackBerry App World.

7. Only add people that you trust!

BlackBerry Messenger (BBM) allows users to interact among BlackBerry users without incurring any cost at all. The mistake made by users is when they publicly expose their pin numbers. Remember not to 'broadcast' your pin number. It might lead to leakage of data as an impact of social engineering. WhatsApp is an application that offers the same function like BBM but to a different target segment. You should only add users that you trust in BBM, WhatsApp or other application.

8. Enable BlackBerry Protect

Download BlackBerry® Protect™ from BlackBerry App World. BlackBerry Protect is an application designed to keep your information secure if your BlackBerry device goes missing or gets stolen. This BlackBerry offers automatic backup thus you can automatically back up your data daily, weekly or monthly. In addition, if your BlackBerry is turned off or not connected to the wireless network when a scheduled backup is due, BlackBerry Protect automatically backs up your data the next time that your device is turned on and connected.

Below are special actions that BlackBerry Protect can do to find your BlackBerry:

a. Map the current location of the device.
b. Make the BlackBerry device ring loudly even if it is in the silent mode.
c. Customised messages are shown at the home screen of the device even it is locked up.
d. Lock the device and optionally set a new password.
e. Permanently delete data from the device.

9. Logout after completing online transactions

You must logout after each transaction for any online application, including social network applications. This is to prevent users from being hacked by third parties through the social network pages. Plus, you do not want an anonymous person to withdraw your money without your consent!

10. Disable Bluetooth

Bluetooth device communications must be turned off when it is not used. Additionally, as a precaution, Bluetooth should be set to hidden or undiscoverable mode all times.

11. Delete pictures, videos and any potential data that can be manipulated

In the case if you want to repair your BlackBerry device, delete all data consisting of pictures and videos. You can make backup on your PC using the BlackBerry Manager application.

12. Connect Wi-Fi manually

Connecting Wi-Fi automatically to open networks can expose you to security holes. Attacks such as Man-In-The-Middle (MITM) attack or interception by third party can endanger users when the attacker tries to manipulate the data that is being intercepted. Turn off Wi-Fi if it is not being used. Your settings should enable you to choose Wi-Fi connection that you want to use.

13. Protect Global Positioning System (GPS) location

This is an issue of location based privacy. When applications have access to your GPS location information, they could potentially track your location or report your location back to a server. To prevent applications from using the GPS location on your BlackBerry device, perform any of the following actions:

a. Block specific third-party applications from using the GPS location information.
b. Block all third-party applications from using location-based services.
c. Turn off GPS technology on your BlackBerry device.

Be Smart, Alert!

B Block installations without passwords
E Enable time-out if exceed failure attempts

S Set passwords and pin codes
M Manually connect Bluetooth and Wi-Fi
A Add only people you trust
R Regular backups
T Turn off GPS location

A Always update firmware
L Log out after online transactions
E Encrypt data
R Remember passwords and never write them down
T Turn on BlackBerry Protect!

CyberSecurity Malaysia,
Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor Darul Ehsan,
Malaysia.

Tel: +603 - 8946 0999 Fax: +603 - 8946 0888
Email: info@cybersecurity.my
www.cybersecurity.my

People First,
Performance Now

Ministry of Science,
Technology and Innovation

Best Brand
Internet Security
2008 & 2009

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR4656

MS ISO/IEC 17025
TESTING
SAMM NO. 456
(MySEF LABORATORY)

Status Company