Mobile Security - Securing the Government of Canada

JUNE 2016 | EXECUTIVE SERIES | ITSE.80.001

Mobile devices such as smart phones and tablets have spread rapidly across the Government of Canada (GC), and while they boost productivity and efficiency, they can increase the risk of a compromise of GC information and networks. The increase in risk is due to the fact that employees take the devices outside of the office and connect them to unknown and possibly untrusted networks. A compromise of GC information or networks can result in issues such as: downgrades in system performance, outages, lost productivity, costly recovery efforts, and damage to the GC reputation.

Capabilities exist which can allow threat actors to:

- Identify, target, and deliver malware through a mobile device to GC networks;
- Access and use the network connections of the device (cellular, Wi-Fi, Bluetooth) for nefarious purposes;
- Use the device to infiltrate other GC networks;
- Access the device in order to retrieve stored GC information; and
- Use the phone as a mobile listening device.

Mobile Risk Management

A number of threats posed to GC networks through the mobile enterprise can be attributed to the fact that mobile device operating systems are typically less evolved than traditional desktop or laptop operating systems. Consequently, the strength and granularity of control inherent in a mobile device's operating system may not provide an appropriate amount of protection against cyber-threat actors.

Security controls for the mobile enterprise should be determined by a department's threat-risk profile. CSE's *IT Security Risk Management: A Lifecycle Approach* defines an IT security risk management process whereby a pre-defined set of baseline security controls can be tailored to meet the specific security needs of a department.

In order to secure GC information and networks, security controls need to be implemented and verified for the complete information system, from the mobile device through to the departmental network services that support business processes and information access.

GC networks are accessed through mobile devices every day.

Securing the Mobile Enterprise

Mobile devices use commercial cellular or Wi-Fi networks for internet access. Since the GC does not have control over the security of these networks, they are considered susceptible to additional threats. To help mitigate the risks of using untrusted networks, departments should secure their communications channel by enforcing VPN connections to GC networks and systems and ensuring only trusted Wi-Fi access points are used.

Mobile Device Management (MDM) technologies can be used for added security. MDM software can secure, monitor, manage, and support mobile devices within a network by controlling configuration settings and application use, securing data, and integrating communication services.

Protecting the GC from compromises can be significantly enhanced through departmental control of devices and by keeping them free of malware. Departments should implement strong mobile device policies as unrestricted personal use of devices can have a significant negative impact on a department's security posture.

Securing the Mobile Device

Securing mobile devices is a key component to protecting the GC, its information, and its networks. It is the department's responsibility to assess the level of risk associated with using mobile devices and choose the most appropriate practices to enhance the departmental security posture. As a general baseline, departments should strive to implement the following best practices:

- ✓ Ensure operating systems and applications have the latest patches and updates applied;
- ✓ Install up-to-date anti-virus and spyware protection;
- ✓ Update passwords often, especially before and after travel;
- ✓ Restrict administrative privileges;
- ✓ Ensure appropriate security settings on devices and applications. CSE can provide tailored advice and guidance based on a department's needs;
- ✓ Verify that mobile devices are unable to access the internet at the same time as accessing the department's internal network;
- ✓ Ensure proper security settings for VPN access; and
- ✓ Maximize monitoring capabilities for devices that are associated with international travel to look for unusual or unauthorized activity.

CSE's Mobility Suite

To help departments mitigate the mobility threat, CSE has put together a suite of Mobility Security publications that when applied can help GC departments significantly reduce their threat surface in regards to mobile devices. Visit our Wireless and Mobility webpage to download:

- Mobile Technologies in International Travel;
- Mobile Device Management Solutions;
- Security Requirements for Wireless Area Networks;
- Risk Management for iPads;
- Wireless Network Security; and
- Mobile Devices and Wireless Signals.

If you would like to learn more, sign-up for CSE's Wireless Security course (#350).

In 2015, Symantec discovered 430 million new and unique pieces of malware. A 36% increase from 2014.

2016 Symantec Internet Security Report

If you would like to read more about Mobile Security, visit our Wireless and Mobility webpage.

Questions?

Contact ITS Client Services
itsclientservices@cse-cst.gc.ca
613-991-7654

Mobility and CSE's Top 10 Security Actions

CSE's Top 10 Security Actions provide a prioritized list of security measures that can be applied not only to GC networks, but also to mobile devices. The Top 10 Security Actions are IT security considerations that are important to address when deploying mobile devices that connect to GC networks and systems.