Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CYBERJOURNAL

EDITION 2 – WINTER 2013

IN THIS EDITION

CYBER MITIGATION: THE ESSENTIAL STEPS

In this edition of Cyber Journal, we delve further into the topic of cyber mitigation and highlight some of the best ways to curtail the persistent nature of cyber threat methods with special feature articles on spear phishing (social engineering) and application whitelisting.

Trends are always emerging on the technology scene and as government stakeholders we must carefully consider both the merits and pitfalls of these trends. For example, our article on Mobile Device Management draws awareness to the associated security concerns of employees using mobile devices to connect into government networks and helps isolate the potential risks.

We trust that you will find this edition of Cyber Journal both informative and relevant.

Toni Moffa
Deputy Chief, IT Security

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBERJOURNAL

EDITION 2 – WINTER 2013

ESSENTIAL MITIGATION: STOP THEM IN THEIR TRACKS!

As a government IT security professional, you often hear of IT cyber intrusions. Stopping cyber threats from impacting your systems may seem like a daunting task. To increase the GC's network protection efforts, CSEC has used its unique threat knowledge to develop the *Top 35 Mitigation Measures.* The "Top 35" is a prioritized list of measures based on an analysis of incidents across the GC and CSEC's experience in operational cyber security.

The purpose of the Top 35 is to provide concise and proactive best practices to help mitigate against targeted cyber intrusions. The list also provides information about mitigation implementation costs and user acceptance to help organizations select the best set of measures for their requirements.

Implementing the top four measures as a package could prevent the vast majority of the intrusions that CSEC currently responds to. The top four mitigation measures are:

- Application whitelisting;
- Patching third party applications;
- Patching operating systems; and
- Minimizing administrative privileges.

Implementing these measures can be achieved gradually; starting with systems used by high-value and often targeted employees, and eventually extending the measures to all users.

High-value and often targeted employees might include:

- **Senior executives and their assistants;**
- **Help desk staff, system administrators;**
- **Users who have access to sensitive information;**
- **Users with remote access; and**
- **Users whose job role involves interacting with members of the public.**

As no single measure can prevent malicious cyber activity, CSEC strongly urges departments to first implement the top four measures as a package and then continue to improve their security posture by implementing the remaining measures as appropriate. To learn more or to download the entire list visit our IT publications web page: www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/index-eng.html

NEW RELEASES!

ITSB-89A: CSEC Top 35 Mitigation Measures

ITSB-94: Minimizing Administrative Privileges Explained

ITSB-95: Application Whitelisting Explained

ITSB-96: Assessing Security Vulnerabilities and Patches

ITSB-97: Cyber Case Study - Why The Top 4 Measures Are Essential

THE #1 MITIGATION MEASURE: APPLICATION WHITELISTING

What is application whitelisting?

It is an administrative practice used to prevent unauthorized or malicious programs from running.

What is a whitelist?

It's a list of applications that have been granted permission by the administrator to run.

How does it work?

When an application tries to execute, it is checked against the whitelist and, if found, the program is allowed to run.

Why should I do this?

Most intrusion detection systems have a list of undesirable applications; however, the ever increasing number of threats means that such a list can never be complete.

Where do I start?

High-value and often targeted employees as well as high-value enterprise services such as core application servers are a great first start.

Where can I get more information?

Application Whitelisting Explained, ITSB-95, is available on CSEC's IT publications website.

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBERJOURNAL

EDITION 2 – WINTER 2013

YOU'RE ON THE HOOK: SPEAR PHISHING

GC departments and their networks are frequently targeted by a wide variety of threat actors looking to steal GC information. Socially engineered e-mails are the most common technique used in malicious cyber intrusions. The e-mails aim to trick the recipient into downloading malicious software by clicking on a link or attachment.

Cyber intruders are technologically savvy, vulnerability conscious and aggressively agile; a successful intrusion can quickly lead to the loss of data integrity and confidentiality.

FACT: 42% of mailboxes targeted for attack are high-level executives, senior managers and people in R&D. That means 58% are going to people in other job functions such as sales, HR, media relations, assistants….-

Symantec, Internet Security Threat Report, 2011

Spear phishing has become very successful by using social engineering to tailor e-mails to individuals or groups based on their line of work, interest, or personal characteristics.

Spear phishing e-mails will be about a subject that is relevant to the recipient and will appear to be sent by a credible source. Socially engineered e-mails result in a more convincing message and entice the user into a false sense of security.

Before opening attachments or links within an e-mail ensure that:

1. You really know who is sending the e-mail and that the tone is consistent for that sender.
2. The content is really relevant to your work and not just related to your area of interest.
3. The web-address or attachment is relevant to the content of the e-mail.
4. You use extra caution if the e-mail is from a personal address (@yahoo.ca, @gmail.com) or a suspicious domain.

If you feel that you have received a suspicious e-mail, report the incident to your IT Service Desk.

SMART COMPUTING TIP

Microsoft has announced it will cease support to the Windows XP operating platform as of **April 8, 2014**. This means that departments will no longer have access to patches for known security vulnerabilities in Windows XP, significantly increasing the probability of a successful intrusion. Patching operating systems is one of the top four measures in CSEC's Top 35 Mitigation Measures. Upgrading operating systems across an entire department will take some time and CSEC strongly urges departments to plan ahead and upgrade your operating systems to a more recent version, preferably to Windows 7 or better.

**READ ONLINE:
Spotting Malicious E-mail Messages
(ITSB-100)**

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBERJOURNAL

EDITION 2 – WINTER 2013

TAKING CARE OF YOUR SECURE COMMUNICATIONS VOICE DEVICE

Today there are more than 20,000 COMSEC voice devices distributed throughout the GC. Each is used to protect the GC's most sensitive information. They are collectively managed within the National COMSEC Material Control System (NCMCS) and each one must be protected and safeguarded against unauthorized access from the time they are acquired to the time they are destroyed. These devices include desktop versions such as the STE/KSV-22, OMNI, SWT and vIPer, as well as small mobile devices such as the SGSM.

The one commonality among these secure voice devices is that they each require a cryptographic key to operate in a secure mode. It is not sufficient just to load your device with a key. In order to maintain the cryptographic health of your secure voice device, you must regularly update this key (known as a cryptographic rekey).

Your COMSEC Custodian should remind you when it is time to rekey your secure voice device and provide you with specific directions. To ensure your device is always operational and ready for use, CSEC recommends that you rekey your secure voice devices once every 3 months.

THE REKEY PROCESS

1. Download the SCIP ECU Rekey Handbook from: www.cse-cst.gc.ca/its-sti/publications/itsb-bsti/itsb46-annex-annexe-eng.html
2. Call: 613-949-5400 to update your Canadian keys.
3. Then, if you have a non-Canadian key loaded, call: 1-877-386-1820.

SECURE VOICE DEVICE BEST PRACTICES

- Learn how to use your device before you need to use it in an emergency.
- Physically secure the device or key when not in use.
- Return it to your COMSEC Custodian when you retire, change employment or vacate offices.
- Be aware of your surroundings. Your secure phone does not stop others from over hearing what you are saying.
- Report any equipment losses, thefts or unauthorized access immediately to your COMSEC Custodian.

DID YOU KNOW? RISK MANAGEMENT SECURITY PROFILES

To help security practitioners develop a baseline set of departmental security controls, IT Security Risk Management: A Lifecycle Approach (ITSG-33) includes several security control profiles. Specifically, ITSG-33 includes profiles that address the confidentiality, integrity and availability needs for the GC Protected A, Protected B and SECRET environments.

These suggested security control profiles constitute a starting point to aid in the development of tailored profiles which meet a departments specific business, technical and threat contexts, as well as risk tolerance. In addition, an Excel based profile tool has been created to help departments customize security profiles based on their risk management process.

To learn more about ITSG-33 security profiles and to access the online profile tool, visit our IT Security Guidance publications page: www.cse-cst.gc.ca/its-sti/publications/itsg-csti/index-eng.html

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

USING PORTABLE MEDIA FOR DATA TRANSFER

Information sharing across different security domains is an ongoing operational necessity within GC departments. In the case where departments do not yet have a full Cross Domain Solution (CDS) capability available, the most common solution is the use of portable media such as USB or CD-R to transfer data files manually. However, implementing such a solution introduces risks to both domains.

Before allowing portable media data transfer, there are some fundamental security issues which should be addressed.

Primary Risks and Threats

The primary risks are: the loss of sensitive data, introduction of malicious code and unauthorized data transfers.

- Data loss is the accidental or intentional transfer of sensitive or classified information through removable media to networks that are not authorized to protect that information.
- Portable media can be preloaded with malicious code to facilitate unauthorized access to information.
- Portable media can be lost or stolen.

Mitigation

To prevent data loss and the introduction of malicious code, all files should be scanned using a commercial virus scanner as well as format specific supplemental data filtering during a transfer.

Robust Media Security Policy

A robust portable media security policy will mitigate the associated risks and threats through the implementation of properly selected security controls.

Deploying a portable media data transfer solution should include addressing these security questions, as well as developing robust policies and procedures.

For more information contact IT Security Client Services itsclientservices@cse-cst.gc.ca.

SMART COMPUTING TIP

Adobe recently released Adobe Reader XI with improved security features. Since the introduction of Adobe Reader version 10, the application now includes a sandbox element which helps filter and protect against known threats. To carry out a successful intrusion, an adversary would first have to exploit a vulnerability in Adobe Reader, and then use another exploit to escape the sandbox, making it significantly more difficult for them to compromise a department's network. Many GC departments are running older Adobe versions which are not patched and do not use this sandboxing technology, exposing departments to a greater number of threats. Patching third party applications is one of the top four measures in CSEC's Top 35 Mitigation Measures. PDF files are a commonly used method of delivering malware via socially-engineered e-mails. Take stock of your Adobe version today and consider patching or upgrading to a more recent version to increase your security coverage and reduce your IT risk.

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

MOBILE DEVICE MANAGEMENT SOLUTIONS

Mobile devices have spread rapidly across the GC corporate enterprise and provide opportunities for government to boost productivity and efficiency. However, mobile devices can also increase the risk of compromising sensitive information. To help mitigate this threat, CSEC recommends departments deploy Mobile Device Management (MDM) solutions as part of their overall architecture.

MDM software can secure, monitor, manage and support mobile devices deployed within a network by controlling and protecting data and configuration settings. They have a wide range of capabilities including:

- Controlling security settings implemented inside the mobile device (basic solution);
- Extending and enforcing corporate security policies and controls to mobile devices (advanced solution); and
- Providing seamless integration with corporate systems and services.

It is important to note that MDM solutions cannot add controls and security features to mobile devices; other than those natively implemented on the device.

When considering whether to allow the connection of mobile devices into the GC corporate enterprise, managers must realize that MDM solutions are not the silver bullet to solving the security issues introduced by these platforms. They must consider both the capabilities of the MDM solution, and the inherent security controls implemented in the chosen device.

IT SECURITY TRAINING NEWS

The IT Security Learning Centre (ITSLC) offers educational opportunities to help maintain the highest level of cyber security for the Government of Canada. Since IT security requirements and best practices are continually evolving, the ITSLC regularly reviews its courses and programs of study for relevance, applicability, and effect. As a result, a new catalogue will soon be unveiled which will include some changes to the courses and programs of study.

Last fall, the ITSLC ventured into the e-learning arena with the launch of a new course titled, **Controlling Authority (CA)**. This course was provided in a blended learning solution of e-learning and a workshop. It focused on the delivery of comprehensive knowledge on the requirements to manage cryptographic keys on a network as well as the development of a Key Material Support Plan (KMSP). This is just the first of many courses that will be made available to the GC population in an e-learning format over the next few years.

THE LEARNING CENTRE ONLINE

For an updated look at our Programs of Study and other specialized courses or to register for any of our upcoming courses please visit our website at:

www.cse-cst.gc.ca/its-sti/training-formation/index-eng.html

its-education@cse-cst.gc.ca

CSEC's IT Security team is interested in knowing what security issues you face at your Department.

Please send us your questions, concerns or ideas for future articles: itsclientservices@cse-cst.gc.ca

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSEC IT Security commitment to share information, advice and guidance with the broader GC community to help Departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your department. In addition, the newsletter profiles key products and services offered by CSEC with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases, contact: itsclientservices@cse-cst.gc.ca.

CONTACT US

For general advice and security guidance support, contact:

✉ itsclientservices@cse-cst.gc.ca

☎ General Inquiries: (613) 991-7654

To report a cyber-incident contact the Cyber Threat Evaluation Centre:

✉ ctec@cse-cst.gc.ca

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ comsecclientservices@cse-cst.gc.ca

☎ General Inquiries: (613) 991-8495

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ cmac-camc@cse-cst.gc.ca

☎ General Inquiries: (613) 991-8600

For education and training services, contact the IT Security Learning:

✉ its-education@cse-cst.gc.ca

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.