Communications Security Establishment
Centre de la sécurité des télécommunications

CYBERJOURNAL

EDITION 5 – WINTER 2014

IN THIS EDITION

Web 2.0 Security Risks

Security Questions

Data Diodes in a Cross-Domain Solution

The Importance of a Departmental TA

Two-Factor Authentication

GTEC 2013 Re-cap

Cloud Computing

ITS Learning Centre News

About This Newsletter

Subscribe

Contact Us

THE CHANGING NATURE OF HOW WE WORK

The ever changing nature of technology demands that cyber security be an iterative process which continues to evolve. These days, not only is the technology we use rapidly evolving, the way we perform our daily tasks and use technology is also changing. With the introduction of cloud computing, Web 2.0 technologies and wireless devices, the workplace has expanded into an environment of increased participation and collaboration that reaches beyond conventional barriers.

Consequently, information security must reach beyond IT departments. More than ever, security is everyone's concern. In the face of today's cyber threats, employee vigilance will continue to be a critical success factor in preserving the confidentiality, integrity and availability of our information assets.

In this edition of Cyber Journal we explore some of the technologies, such as cloud computing and Web 2.0, that are altering how and where we perform our duties. As cyber-threat actors are becoming more sophisticated, we also discuss the importance of IT security threat and risk assessments to Government of Canada (GC) departments and agencies. CSE has a variety of online publications to help GC departments leverage best practices in the development of a comprehensive departmental security plan.

Originally signed by

Toni Moffa
Chef adjointe, Sécurité des TI

www.cse-cst.gc.ca

February 2014

Canada

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

WEB 2.0 SECURITY RISKS

The GC Workplace 2.0 strategy is changing the way we work. Workplace 2.0 aims to update the tools and technologies that public servants can access to better connect, collaborate and communicate across the GC. For example, public servants are now using various Web 2.0 tools, such as GCPedia and GCForums, to share expertise and knowledge internally while collaboratively authoring documents.

Web 2.0 has changed the internet into a dynamic and interactive environment by allowing users to increase participation, collaboration and information sharing across the world. However, these same technologies can introduce security risks.

Threats to GC information assets resulting from the introduction of these tools include:

- Information leakage;
- Information integrity;
- Unauthorized access;
- Malicious code;
- Impersonation; and
- Fraud.

GCPEDIA
PEOPLE & KNOWLEDGE
GENS & SAVOIR

Organizations can take the following steps to protect against these threats:

1. **Data Protection** - Label all documents and data with appropriate security and protection classifications and follow proper use and storage handling procedures;
2. **Secure Development** - Train developers to follow a secure software development lifecycle to help ensure that they create applications and websites without including known and avoidable vulnerabilities;
3. **Secure Communications** - Make sure to use Web 2.0 websites that support secure login using Transport Layer Security/Secure Sockets Layer (TLS/SSL);
4. **Monitoring and Auditing** - Use Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems to detect virus outbreaks, network anomalies and intrusions; and
5. **Awareness and Training** - Provide mandatory user security awareness training for known Web 2.0 threats.

Departments seeking guidance should consult the Guideline for External Use of Web 2.0 released by the Treasury Board Secretariat (TBS) Chief Information Officer Branch (CIOB).

FEBRUARY 10 - 14, 2014 IS SECURITY AWARENESS WEEK

Security Awareness Week is an annual event during which departments are invited to promote good security practices and share them government wide. It is an excellent opportunity to increase employee awareness and promote departmental security services.

To learn more or obtain products to promote security awareness week visit:

www.tbs-sct.gc.ca/sim-gsi/sc-cs/awareness-sensibilisation-eng.asp

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

DID YOU KNOW? CONSIDERATIONS FOR "SECURITY QUESTIONS"

Web-based services and applications that rely on passwords often use "Security Questions" as the primary means to recover account access when a password is forgotten. By correctly answering a security question, the user regains access to their account.

If these questions are not carefully chosen, they can be less secure than the original password. For many, the answers to these questions can be easily found online. To make matters worse, unlike passwords, the answers are not usually required to be case sensitive, contain special characters, or have a minimum length.

A threat actor can easily force a lock-out of an account or simply click on the "Forgot Password" link, and then answer the security question in an attempt to gain access.

Users need to consider these security questions carefully, and choose one that does not have an easy-to-find answer (e.g., a pet's name) or a limited number of answers (e.g., colour of first car). The key is to strike a balance between unique answers and memorable ones that serve their intended purpose.

HAVE A COMSEC QUESTION?

Departmental Security Officers, Departmental COMSEC Authorities and COMSEC Custodians can access essential information for protecting their COMSEC material through the following channels:

COMSEC Client Services
comsecclientservices@cse-cst.gc.ca
(613) 991-8495

Crypto Material Assistance Centre (CMAC)
cmac-camc@cse-cst.gc.ca
(613) 991-8600

COMSEC User Portal (CUP)
https://comsecportal.cse-cst.gc.ca

USING DATA DIODES IN A CROSS-DOMAIN SOLUTION

GC departments and agencies looking to transfer or exchange data electronically between two different security domains should always use an approved Cross-Domain Solution (CDS). An approved CDS can provide the additional security controls required to mitigate the risks of connecting networks which are at different security levels.

Part of the solution can include the use of data diodes to physically restrict network communications to only one direction. This is typically accomplished through the use of a fiber optic hardware device that has a transmitter on one end, a receiver on the other end, and all other functionality physically disabled. Therefore, the implementation of a data diode prevents the transmission of data in the wrong direction, and satisfies an important security control requirement of a one-way CDS.

It is important to note that data diodes do not apply any filtering to the data. Data filtering is another critical security requirement for the transfer of data between different security domains. Data filtering analyzes individual data formats including complex formats, such as Microsoft Office and PDF files, to identify inappropriate content that contravenes departmental data-transfer policies.

CSE can provide advice and guidance on the use of data diodes and meeting the challenges of securely implementing a CDS. For general questions related to CDS requirements, contact CSE IT Security Client Services itsclientservices@cse-cst.gc.ca.

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

THE IMPORTANCE OF PERFORMING A DEPARTMENTAL THREAT ASSESSMENT

GC departments and agencies are responsible for ensuring the integrity, availability and confidentiality of the data they create, process and hold. In today's highly inter-connected world, accessing data via IT systems from anywhere is easier than ever. This is also true of those who may have malicious intentions. Determining which security controls, among thousands, to implement while balancing usability, business operations and cost has become extremely complex.

The only way to make the right decisions is by understanding what threats are of highest risk in the context of the organization's business. This knowledge will enable the organization to select security controls in a meaningful and responsible manner. The first step is to conduct a departmental threat assessment (TA).

The threat assessment provides a basis for selecting and adjusting security controls to mitigate the most relevant threats; the risk assessment provides the basis for implementing these security controls in a balanced fashion based on the risk appetite of each organization. To implement a balanced set of security controls, departments need to clearly define and express, through a departmental TA, the types of threats against which they plan to protect their information systems.

Departments need to perform their TAs collaboratively with all relevant stakeholders. TAs make it possible for decision makers to distinguish between threats that a department can afford to accept, and those against which they must protect. A departmental TA forms a "baseline" assessment that sets the threat context for that department, upon which specific IT projects can build their unique security requirements and select appropriate security controls.

Successful departmental TAs should be:

- Conducted by broad departmental representatives, information owners and IT security practitioners along with guidance from lead GC security agencies, as well as participation of the Departmental Security Officer, IT security coordinator, program and service delivery managers, corporate security representatives, and key IT operations personnel;
- Enablers of clear business decisions on the value, criticality and sensitivity of information to inform protection needs;
- Conducted with the intent of identifying all relevant threats to departmental business activities and their supporting IT environments;
- Able to clearly identify threats, such that departments can determine which threats it wishes to explicitly protect its information systems against, and those it will accept;
- Based on reliable threat data pulled from multiple sources such as existing TRAs, privacy impact assessment reports, incident reports, and those requested from lead security agencies; and
- Effectively promulgated within departmental IT security communities and consistently used by IT projects.

To learn more, visit our IT Publications web-site and download ITSG-33: IT Security Risk Management: A Lifecycle Approach or past editions of the Cyber Journal.

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

ONE-FACTOR VS. TWO-FACTOR AUTHENTICATION

In IT systems, authentication is about identifying an individual to ensure the user is who he or she claims to be. Traditionally, this is accomplished using a combination of a username and a password, which is often referred to as one-factor (or secret password) authentication.

While the password associated with a username is supposed to be secret, users often:

- Do not keep their passwords secret;
- Select passwords that are too simple; or
- Use common words in their passwords.

Password dictionaries are commonly available on the internet to help threat actors gain unauthorized access to network environments. Additionally, short complex passwords can easily be cracked using a brute-force attack during which a computer program uses every possible combination of characters until the password is found.

By solely using one-factor authentication, a threat actor only needs to learn a single 'secret' to gain access to the network. This risk can be reduced by adding a second factor to the authentication process. As an example, system access would require a valid username and both a correct password (1st factor) and a hardware token (2nd factor).

Two-factor authentication is used to reduce the threat to network assets by significantly increasing the effort it takes to gain access to a network. Two-factor authentication is Mitigation Measure #6 in the CSEC Top 35 Mitigation Measures (ITSB-89A) and additional information can be found in User Authentication Guidance for IT Systems (ITSG-31).

CSE AT GTEC 2013

In October 2013, CSE actively participated in Canada's Government Technology Exhibition and Conference (GTEC). Over the course of the event, CSE employees manned our booth, answering questions about how to "boost your cyber immune system". The focus was on CSE's IT Security Services including the Top 4 Mitigation Measures which, if implemented, will stop the vast majority of cyber intrusions the GC is facing. Additionally, attendees learned about best practices for IT Security while travelling, using social media, or using mobile devices through a set of interactive tablet applications.

CSE also gave two presentations during the conference:

John Forster, Chief of CSE, presented the role Cyber Security plays in the GC. Covering the most pressing cyber threats, Mr. Forster outlined the steps that GC departments can take to protect their IT infrastructure now and in the future.

Scott Jones, DG of Cyber Defence, presented a step-by-step look at an intrusion 'in-progress', outlining the actions that could have been taken to prevent the intrusion from happening.

On behalf of CSE, we would like to thank everyone who stopped by our booth to ask questions or attended one of our presentations. We hope to see everyone again at GTEC 2014!

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

SECURITY IMPLICATIONS OF CLOUD COMPUTING

In private industry, businesses have been embracing the use of cloud computing for years. Cloud applications such as data storage, HR management, e-mail and file sharing are all seeing an increase in demand. This increase can be attributed to the cloud's ability to enable collaboration while reducing costs.

Public cloud computing is the provision or sharing of computer applications, infrastructure and services over the internet by a third party service provider. The service provider invests heavily in infrastructure and software applications, and then sells its services to many businesses, sharing its resources among many clients. Sharing resources helps to reduce costs for businesses by allowing them to spend less of their revenue on infrastructure and more on profit-generating projects.

However, public cloud usage can introduce some important security implications such as:

- Legal considerations;
- Privacy and protection of personal information;
- Multiple tenancy and data leakage;
- Availability;
- Access control; and
- Insecure Application Programming Interfaces (APIs).

An integrated risk management approach, as outlined in ITSG-33, must address all the different types of risk, and include a stipulation of service provider requirements, clear governance, and effective operational controls. Prior to using cloud services, organizations should ensure a formal Service Level Agreement (SLA) is put in place that considers the following points:

- ✓ Provisions for IT support services;
- ✓ Restrictions on geographical location;
- ✓ Restrictions on activity monitoring;
- ✓ Exit clauses;
- ✓ Business continuity services and security incident handling;
- ✓ Retention and preservation of digital evidence;
- ✓ Secure data deletion;
- ✓ Security assurance, regulatory compliance and audits;
- ✓ Security management, certification and accreditation and vulnerability advisory services;
- ✓ Notification and reports; and
- ✓ A clear understanding of cloud provider ownership and third party relationships.

DID YOU KNOW? TECHNOLOGY SUPPLY CHAIN GUIDANCE

CSE's Technology Supply Chain Guidance publication contains guidelines for developing contracting clauses for "managed" telecommunications equipment and services. This publication can help you formulate a comprehensive contract when a contractor is given responsibility for managing a GC network.

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

ITS LEARNING CENTRE NEWS

New EMSEC Course

The ITS Learning Centre (ITSLC) will soon be offering an Emission Security (EMSEC) course in the COMSEC Program of Study. This course is designed to give a basic introduction on emission security principles and how these principles can prevent the exploitation of compromising emanations.

Departmental COMSEC Authority (DCA) Course

The online DCA course was developed by the ITSLC for employees who have the responsibility of implementing the requirements of a departmental COMSEC program. The launch of this new online initiative is slated for the fall of 2014 and will be available via the Canada School of Public Service.

Participant Surveys

To ensure participants are applying the skills and knowledge received during their training in the workplace, ITSLC will randomly select and contact participants within two to three months of course completion to conduct a brief survey. As the ITSLC endeavours to provide comprehensive and viable training solutions, all comments and feedback received will assist us in assessing the relevance of our course offerings and their effectiveness in the workplace.

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: ITS Learning Centre

DOWNLOAD OUR LATEST CATALOGUE:

ITSLC Catalogue

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 CSE 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 CSE 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 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 Centre:

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.