Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information (https://www.cse-cst.gc.ca/en/node/1297/html/25231)

IT Security Bulletin for the Government of Canada

ITSB-89 Version 3

November 2014

1 Purpose

This list supersedes ITSB-89, the Top 35 Mitigation Measures, and is based on CSE's analysis of the cyber threat activity trends that impact Government of Canada (GC) Internet-connected networks.

2 Impact

The Top 35 has been condensed to a Top 10 for ease of use and to focus departmental efforts. Implementation of the Top 10 will result in eliminating the vast majority of cyber threats currently seen active in GC networks. As always, a departmental risk management process should be followed in the design and deployment of new networks.

3 The Top 10

Rank	Action	Description of Implementation
1	Use Shared Services Canada (SSC) Internet gateways	Reduce the number of discrete external connections to a departmental network by using the consolidated Internet gateways provided by SSC. Users will benefit from the protection provided by higher level cyber defences deployed at the enterprise level that monitors for, and can respond to, unauthorized entry, data exfiltration or other malicious activity.
2	Patch operating systems (OSs) and applications	Implement a timely patch maintenance policy for OSs and third-party applications to reduce departmental exposure to threats that could exploit known vulnerabilities. Use supported, up-to-date, and tested versions of applications. Moreover, the deployment of an unsupported OS or application, where updates are no longer available, will result in a significant risk of exposure to exploitation. Departmental tested and approved security patches need to be applied in a timely manner, ideally via an automatic patch management system.
3	Enforce the management of administrative privileges	Minimize the number of users with administrative privileges and revalidate frequently the requirement for users to have a privileged account. Change administrative account passwords according to an established schedule or sooner, as required. Use two factor authentication (2FA) for accessing sensitive applications or for remote network access. Perform administrative functions on a dedicated workstation that does not have Internet or open e-mail access.
4	Harden Operating Systems (OSs)	To prevent compromise of assets and infrastructures that are connected to the Internet, disable all non-essential ports and services, and remove unnecessary accounts. Both an enterprise-level auditing and anti-virus solution are key elements of any secure configuration. CSE has published ITSB-110, Microsoft Windows 7 Enterprise Edition Hardening Configuration Guidance, to support the deployment of this OS. Special consideration needs to be given to network architecture choices, security procedures. Further security controls should be applied to the OS when mitigating these risks; consult CSE's ITSG-33, IT Security Risk Management: A Lifecycle Approach, for more information on selecting and applying security

		controls.
5	Segment and separate information	Information stores should be categorized, taking into consideration information protection needs due to sensitivity or privacy. Networks should be zoned by segmenting infrastructure services into logical groupings that have the same communication security policies and information protection requirements. This logical design approach is used to control and restrict access and data communication flows. Further, monitor and enforce controls to maintain zone protection and integrity.
6	Provide tailored awareness and training	Initiate regular awareness activities on current user-related vulnerabilities and proper user behaviours. IT security awareness programs and activities should be frequently reviewed, maintained and accessible to all users with access to departmental systems. Although system safeguards are expected to curtail suspected malicious activity on the networks, the human element will continue to provide an element of exposure. Current examples of spear phishing or the improper handling of removable media demonstrate the continued need to focus in this area. In addition, regular threat reporting to management on attempted or actual compromises will help to reinforce the behaviour changes required. Management involvement in information protection decisions is essential in choosing appropriate security controls.
7	Manage devices at the enterprise level	Use GC furnished equipment (GFE) within a device management framework and provide control over configuration change management. If a bring-your-own-device (BYOD) scheme is to be considered for a network with low expectations of confidentiality and integrity, a strict control policy must still be implemented as one element of the risk mitigation strategy.
8	Apply protection at the host level	Deploy a Host-based Intrusion Prevention System (HIPS) solution to protect systems against both known and unknown malicious activity. HIPS can also take active measures by stopping an application or closing ports in the event of an intrusion. Monitoring HIPS alerts and logging information will provide early indications of intrusions.
9	Isolate web-facing applications	Use virtualization to create an environment where web-facing applications can run in isolation. Internet browsers and e-mail clients are examples of applications that are susceptible to exploits that execute malware. Security exploits specific to such applications can be confined to this sandbox. Any malware that infects the virtualized environment cannot get out of the sandbox; therefore, the malware cannot infect the host or enterprise.
10	Implement application whitelisting	Explicitly identify authorized applications and application components, and deny all others by default to reduce the risk of executing zero-day malware. Application whitelisting technologies can control which applications are permitted to be installed or executed on a host. The whitelist can be defined by a selection of several file and folder attributes (e.g., file path, filename, file size, digital signature or publisher, or cryptographic hash). Application whitelisting policies should be defined and deployed across the organization using group policy management.

4 Conclusion

Other lists such as the Australian Signals Directorate (ASD) Strategies to Mitigate Targeted Cyber Intrusions and the SANS 20 Critical Security Control Solutions are excellent considerations for generic networks. However, the relative ordering of items within those lists is not always applicable in a GC context. The Top 10 list above was established with an analysis of current threats that impact GC Internet-connected networks. CSE intends to assess the recommended mitigation measures on a continuous basis and produce an update annually.

Download a visual overview of the Top 10.

5 Contacts and Assistance

ITS Client Services
Telephone: 613-991-7654
E-mail: itsclientservices@cse-cst.gc.ca