Cyber & Supply Chain Threats to the GC

Shared Services Canada - High Performance Computing

Oct 16, 2013

Carey Frey, Director Strategic Relationships Office
Communications Security Establishment Canada

Canada

CSEC: What We Do

- CSEC: Canada's national cryptologic agency
- Our Mandate
  - Foreign Signals Intelligence
  - IT Security
  - Support to Lawful Access
- 'B' Mandate
  - To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada

CSEC: IT Security Program

- We help prevent, detect and defend against IT security threats and vulnerabilities
- CSEC provides unique technical expertise, capabilities and classified information that we use to complement commercial security technologies available to IT security practitioners
- We use our own methods and operations to detect and defend against threats that are not in the public domain

Effects of Market Forces on Technology

- Market forces favour commercial and personal technologies over requirements for security features
- Our society is almost totally dependent on software and hardware commercial technology providers from global markets
- New products and new versions of products are rapidly produced
- No regulatory framework exists for hardware/software safety and security
- Traditional government policies and processes impose security requirements after products and systems have been developed
- Few incentives for commercial technology developers to invest in security

Technology Vulnerabilities

- "People write software sloppily. Nobody checks it for mistakes before it gets sold"
  - Peiter Zatko (Mudge), WhiteHouse Cyber-Security Summit (2000)

- Unintentional vulnerabilities or weaknesses
  - Design flaws
  - Implementation errors

- **Cyber Threat** – a threat actor, using the Internet, takes advantage of a known vulnerability in a product for the purpose of exploiting a network and the information the network carries

- Intentional vulnerabilities or weaknesses
  - Predetermined deliverables can be implanted in a product with or without knowledge of company.

- **Supply Chain Threat** – a product can be easily tampered with in the supply chain to later facilitate a cyber-intrusion against that product in order to exploit a network and the information the network carries

The Evolving Cyber-Threat

- Today, malicious cyber activities are directed against Canada and our closest allies on a daily basis

- Threat actors range in sophistication from malfeasant hackers to organized crime groups, to terrorists to nation states

- Canadians trust the GC to defend Canada's cyber sovereignty and protect and advance our national security and economic interests

An Issue of National Security

- **Risks from vulnerable technologies**
  - Covert and persistent access by cyber threat actors in Canadian data centre / cloud infrastructures threatens the sovereignty of GC information and the continuity of government operations
  - Cyber threat actors are effective at exploiting enterprise technologies and management systems used to administer and operate data centre / cloud infrastructures

- **Risks from the supply chain**
  - Increases opportunities for threat actors to circumvent GC cyber security measures
  - More difficult for the GC to detect and remediate

GC Procurements

- CSEC is working in partnership with GC departments to eliminate or significantly reduce risks to the GC from cyber threats & global supply chain vulnerabilities

- CSEC will provide follow-up briefings on supply chain risk mitigation to interested suppliers for GC consolidated initiatives
  - Companies must be willing to sign a CSEC non-disclosure agreement to receive this information

- Security requirements for cyber-protection, cyber-defence and supply chain risk mitigation must be met by suppliers in order to successfully bid on GC consolidated initiatives
  - As the IT Security authority for the GC, CSEC will seek long-term partnerships with successful suppliers
  - CSEC will assist Treasury Board Secretariat of Canada (TBSC) and Public Works and Government Services Canada (PWGSC) in the pedigree analysis of supply chain information provided by respondents
- Examples of these requirements can be found on CSEC's website under Technology Supply Chain Guidance