Protection of Critical Information Infrastructure in Korea

Kim, Woonyon

2005. 10

National Security Research Institute
Contents

- National Cyber Security Management System
- Critical Information Infrastructure (CII) Management System
- Case Study of the Critical Information Infrastructure Threats
- Conclusions
Establishment of National Cyber Security Management System

- Internet crisis of January 25, 2003 by the Slammer Worm
  - Paralysis of the internet banking services and shopping mall services

- A deepening information system dependency
  - National infrastructure control systems tend to be connected to the internet.
  
  ➨ We can predict a paralysis of critical infrastructures from an internet attack.

National Cyber Security Management System
Cyber Security Management System

- President
  - National Cyber Security Strategy Council
    - National Cyber Security Countermeasures Committee
  - Central administrative Agencies
    - Local Government
    - Government-invested Organization
    - Government-affiliated institutions
    - Research Institutes


Republic of Korea
### Relevant Laws and Regulations

<table>
<thead>
<tr>
<th>Relevant Laws and Regulations</th>
<th>Information Security Issues</th>
</tr>
</thead>
</table>
| **National Intelligence Service Act** *(Security Affairs Regulation)* | Functions of the National Intelligence Service  
- Security Activities for Documents, Materials, Facilities and Areas related to a National Security  
- Planning and Coordination of the Intelligence and Security Affairs |
| **National Cyber Security Management Regulation** | Provisions for a National Cyber Security Organizational Structure and Operation  
Apply to the Information and Communication Networks of the Ministries and Agencies of the Central and Local Government, as well as Public Agencies |
| **Framework Guideline on National Information and communication Security** | Basic Activities for an Information and Communication Security  
Management of an Information and Communication Security |
| **E-Government Act** | Provisions for the Protection Measures against a modification, disruption, disclosure or destruction of an Electronic document |
| **Information Infrastructure Protection Act** | Identify a Critical Information and Communication Infrastructure, and then establish and implement a Protection Plan  
Review and assess its Security Vulnerability every 2 years |
Roles of the National Intelligence Service

- Technical support for a critical information infrastructure which is defined by the Information and Communication Infrastructure Protection Act
- Supervising and coordinating all the national-level cyber security policies and management systems
- Planning and Coordinating the national information security operations
- National-wide comprehensive and systematic countermeasures against a cyber terror attack

Key roles are to protect critical information infrastructures.
CII Management System

Committee on the protection of information infrastructure

Ministries

CII Management Body

Critical Information Infrastructure

- Coordinating the protection policy and plan
- Improving the protection system
- Deliberation on the protection policy
- Reviewing the agenda

- Assignment or abolition of CII
- Establish a protection plan and the guidelines for CII
- Create standards for a Vulnerability analysis and assessment

- Implement a protection plan
- Analyze and assess security vulnerabilities (every 2 years)

Republic of Korea
Case for the National and Public Sectors

Reverse Connection

Top Secret

Attacker (Abroad)

National Organizations

Republic of Korea
Information sharing among the ARF members

Trends of Cyber Intrusions
- Globalization of the cyber attacks
- Various types of cyber intrusions from simple to sophisticated attacks
- Complicated attacks

Information sharing among the ARF member countries
- Information sharing of cyber threats
- Information sharing of incidents responses

Information Sharing among ARF Countries
Conclusions

Cyber Security Management System is the main system for protecting a national critical information infrastructure.

We need cooperation among the ARF member countries regarding cyber intrusion attempts.

Korea’s national cyber incidents response organization:

National Cyber Security Center

Tel: 82-2-557-0264

E-Mail: info@ncsc.go.kr
Thank you very much for your kind attention.