Promoting a Culture of Cybersecurity among Critical National Information Infrastructure

ITU Workshop, Doha, Qatar
February 18-21, 2008
By R.Azrina R. Othman
CyberSecurity Malaysia
Agenda

• Background of Cyber Security Issues
• Introduction to the National Cyber Security Policy
• Awareness level
• Knowledge Sharing Platform
• Cyber Security Exercise
• Way Forward
Cyber Threats are Real, Cyber Attacks Are Happening!

Cyberspace must be part of everyone’s life, says PM

Federal Prosecutor: Cybercrime Is Funding Organized Crime

Bebas tapi bertanggungjawab

Invest in cyber security, says expert

Cyber Wars

Chinese hackers cyber-attacking British government networks

by Staff Writers

London (AP) Sept 6, 2007

Chinese computer hackers are infiltrating British government networks, giving them access to secret information, according to media reports on Thursday.

The reports in The Times and The Independent newspapers come a day after US President George W. Bush said he may bring up the issue of suspected Chinese cyber-attacks on the US defence department in a meeting with China’s President Hu Jintao.

UTM hit by virus attacks

More than 6,000 computers infected

DPP branches attacked by Chinese computer virus

By Rich Chang

STAFF REPORTER

Monday, Jul 23, 2007, Page 3
Recent Incident Of Cyber War Against A Nation

Cyber Attack on Estonia

- Occurred in May 2007
- Estonia was under cyber attacks for 3 weeks
- Attack targeted government, banking, media and police websites
- Paralyzed internet communication.
- Attacks from 128 sources outside Estonia
- US and European countries aided Estonia in overcoming the cyber attacks

Impact:
Huge economic losses incurred as online based transactions were disrupted
Cyber Attacks on Malaysia?

WHAT IF OUR CRITICAL INFRASTRUCTURE ARE UNDER ATTACK?

ARE WE READY?

HOW DO WE DEAL WITH IT?
Agenda

• Background of Cyber Security Issues
• Introduction to the National Cyber Security Policy
• Awareness level
• Knowledge Platform
• Cyber Exercise
• Way Forward
Introduction to The National Cyber Security Policy

In 2006, National Cyber Security Policy (NCSP) was initiated by the Ministry of Science Technology and Innovation, to harness national effort to enhance the security of Malaysia’s Critical National Information Infrastructure (CNII)
Objective of the National Cyber Security Policy

1. To address the risks to the CNII
2. To ensure that critical infrastructure are protected to a level that commensurate the risks faced
3. To develop and establish a comprehensive program and a series of frameworks
Malaysia’s Critical National Information Infrastructure will be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social well being and wealth creation.

**NATIONAL CYBER SECURITY POLICY THRUST**

- **PT 1 EFFECTIVE GOVERNANCE**
  - Framework for high level decision making body

- **PT 2 LEGISLATIVE & REGULATORY FRAMEWORK**
  - Framework adopted as baseline for addressing legal issues

- **PT 3 CYBER SECURITY TECHNOLOGY FRAMEWORK**
  - Framework as baseline for formulating Infosec requirement

- **PT 4 CULTURE OF SECURITY & CAPACITY BUILDING**
  - Addressing the Human element

- **PT 5 RESEARCH & DEVELOPMENT TOWARDS SELF RELIANCE**
  - Need coordinator to develop roadmap for research

- **PT 6 COMPLIANCE & ENFORCEMENT**
  - Identify baseline standards & risk assessment framework

- **PT 7 CYBER SECURITY EMERGENCY READINESS**
  - Have proper emergency response mechanism in place

- **PT 8 INTERNATIONAL COOPERATION**
  - Identify & coordinate international platform

**CRITICAL NATIONAL INFORMATION INFRASTRUCTURE**

- Banking & Finance
- Emergency Services
- Water
- Government
- Energy
- Health
- Defense & Security
- Food & Agriculture
- Transportation
- Information & Communication
NCSP’s Policy Thrust 4: Culture of Security & Capacity Building

- Develop, foster and maintain a national culture of security
- Standardise and coordinate cyber security awareness and education programmes across all elements of the CNII
- Establish an effective mechanism for cyber security knowledge dissemination at the national level
- Identify minimum requirements and qualifications for information security professionals
Agenda

- Background of Cyber Security Issues
- Introduction to the National Cyber Security Policy
- Awareness level
- Knowledge Platform
- Cyber Exercise
- Way Forward
Survey 2007 among CNII Organisations - By Sector

The Conference was targeted at participants from GLCs and CNII organisation, the largest number of turnout is from government linked companies.  

Total of about 100 respondents

Type of Critical Infrastructure sector/organisation respondent belong to

- Government: 37%
- IT and Telecommunication: 18%
- Banking & Finance: 11%
- Others: 34%

Note: CNII - Critical National Information Infrastructure
Does your organisation conduct cyber security awareness programme for all staff?

60% of respondents has conducted some form of cyber security awareness programme for staffs.

% of organisations that have conducted security awareness programmes for staff

- Yes: 60%
- No: 40%
Survey 2007 among CNII Organisations
- Guidelines for Evaluation of IT Products

Do you know that there is a standard guideline (ISO/IEC 15408 Common Criteria for IT Security Evaluation) that can be used to request, develop and evaluate secure IT products?

One third of the respondents are aware that there is such standard guideline to evaluate IT products.

Organisations are aware of standards for security evaluation of IT products

- Yes: 37%
- No: 33%
- Not Sure: 24%
- Planning to have: 6%
Agenda

• Background of Cyber Security Issues
• Introduction to the National Cyber Security Policy
• Awareness level
• Knowledge Sharing Platform
• Cyber Exercise
• Way Forward
Outreach Program

CYBER SECURITY AND INTERNET SAFETY AWARENESS CAMPAIGN

Content Partners
- MIMOS
- Microsoft
- ChildNet
- enisa
- MOSTI
- International CERT Communities
- Other industry partners

Content Localization & Packaging
- Publication
- Video clips
- Web
- Poster
- Road shows
- Safety Guide

Content Channels
- MOSTI
- KTAK
- MOHE
- MOE
- KPWKM
- MOL
- MDEC

Target Audience
- Children / students
- Parents/home users
- Organizations

Content Localization & Packaging

Outreach Program

Let’s Make The Internet A Safer Place
www.esecurity.org.my

Copyright © 2007 CyberSecurity Malaysia
Slide no: 16
Competency Development Programs

- Promote various platforms for engagement sessions
  - Seminars, forums & roundtable (e.g. Infosec.my conducted quarterly)
  - Demos and talks to specific critical sectors
  - Focus group mailing lists discussions

- Encourage hands-on participation
  - Hands-on Workshops
  - Cyber Exercises
  - Expert Lab

- Promote Information Security Professional Certifications
Portal for Critical National Information Infrastructure (CNII)

- The CNII Portal is a security resource portal designed specifically to meet the needs of security practitioners (management & technical) within Critical National Information Infrastructure organisation.

- Platform to share guidelines and best practice among CNII, across sector

- Provide latest news on information security and security advisories
Customized contents for Management & Technical security practitioners
Security Outlook page for Managers, CIO, CISO.

Information Guiding Principles page.
Securing Our Cyberspace

Technical Information page for System Administrators, Developer.

Tips page.

Malware Information
Anti Virus Database
Host Database
Safe Email Practices
Home User PC Security: Know the Threats and Countermeasures
Time Synchronization Based on Operating Systems
Agenda

• Background of Cyber Security Issues
• Introduction to the National Cyber Security Policy
• Awareness level
• Knowledge Sharing Platform
• Cyber Exercise
• Way Forward
Malaysian Incident Handling
Drill @MyDrill 2007

- Conducted on 22\textsuperscript{nd} Nov 2007 by CyberSecurity Malaysia
- Participated by a total of 6 teams
  - 3 ISPs
  - 1 Antivirus Vendor
  - 1 Domain Registrar
  - CyberSecurity Malaysia

High level Objectives

- Prepare for potential cyber-security activity related to the Global event such as Beijing 2008 Olympic Games
- Provide different levels of exercise to suit the needs of the various local teams
- Provide an exercise that can be effectively coordinated by the volunteer exercise control group (EXCON)
- Meet the other high-level objectives within the short timeframe available for the drill.
Drill Scenario Background

**Domain Registrar scenario**
- Inject 1 – Domain Registrar received report that there’s a C&C hosted outside Malaysia using a local domain mylovelybot.my. Request to take down domain.
- Inject 2 - Received report of DDoS targeting udp/random port number attacking their DNS.

**Anti-virus vendor scenario**
- Inject 1 – Antivirus Vendor received report from MyCERT involving thousands of PCs from Malaysia infected by a new malware.
- Removal & Advisories.

**Public Relations scenario**
- Inject 1 – Input from MyCERT and to produce press release on attack.
- Press Release.

**ISP scenario**
- Inject 1 - Report from home user informing of slowness in accessing Beijing Olympic website.
- Inject 2 - Website no longer accessible, further investigation shows > than 10,000 IP originating from Malaysia accessing the website, suspected botnet infected.
- Inject 3 - ISP received malware analysis report from AV vendor (malware infecting their user’s PC – bot) containing several critical information i.e. C&C host domain (mylovelybot.my)

**Crafted Port 80 attack**

**ISP infected customer**

**Legion of Anarchy**

**beijing2008.com.my (203.168.7.245)**

**mylovelybot.my**

**Securi**
F-Secure Malware Information Pages: Trojan Downloader:W32/MyDrill.A

Summary
MyDrill.A is detection for files used as part of a Malaysian Cyber Security Drill that took place during 2007.

MyDrill.A are harmless test files. Detection was added for the purpose of the drill.

Detailed Description
On execution this trojan will download a second trojan file from:

http://102.190[REMOVED]/gagie/2mainware.html

It is saved as C:\mainware.html and then later renamed and executed as C:\mainware.exe. The second trojan is also detected as Trojan-Downloader:W32/MyDrill.A.
Way Forward

• Innovate and generate materials relevant for the target audience

• Expand partnership with key stakeholders to reach out to target users.

• Device suitable platforms for information sharing among ICT & Information Security practitioners

• Assess effectiveness
Postal Address:
CyberSecurity Malaysia (formerly known as NISER),
Level 7, SAPURA @ MINES,
7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan,
Malaysia.

Office Hours:
Monday - Friday 08:30 - 17:30 MYT
(Note: Not operational every Saturday and Sunday)

Phone:
+603 - 8992 6888

Fax:
+603 - 8945 3250

Email:
info[at]cybersecurity.org.my

Map:
Click here to download CyberSecurity Malaysia location map.
Awareness Posters

(schools, public & organisations)
Awareness Videos

Email & Spam

Safe Chatting

Safe Internet Banking

Cyber Stalking