Central Reporting service

and

As the things are today!

Henk Bronk
Thursday, 25 September 2003
Agenda

2. Reporting Service
3. New services
4. Symposium
Cybercrime manual

Motives:

• To recognize cyber crime
• To prevent victims of cyber crime
• To structure the reporting of cyber crime
• National and international standardisation for recognition of the various types of cyber crime.
• The need of transparency of cyber crime
Target group

- Every organisation that becomes the victim of cyber crime or wishes to avoid becoming such a victim. (System Administrators, Management, Legal Advisors)
- CSIRTS
- Police and Law enforcement
Technical approach

- Principle of evidence
- General security measures
- Per type of cyber crime
  - Definition variety
  - Technical recognisability
  - Specific security measures
  - Data needed
  - Break into a computer
  - Disorder a computer
  - Destroy or change data
Legal approach

- **Categories of cyber crime**
  - Break into a computer
  - Disorder a computer
  - Destroy, change or disable data
  - Listen in

- **Analysis of specific articles regarding mentioned categories**
  - Criteria for punishableness
  - Explanation of the criteria

- **Linking prevailing legislation and/or regulations to the various types of cyber crime.**

- **Jurisdiction**

- **Data protection act**
Next steps,....

• Put into practice
• Helping the Police & Law enforcement with implementing the manual it in their organisation
• Discussing with intrest groups
• Business case “reporting it to the police”
• Starting point of EU-project
• Collecting input ...... From you !

→ Cybercrime@govcert.nl
Scope of the manual and Reporting Service (the link 😃)

- **Internet-related incidents.**
  Hard-/software and data saved in a computer are the target of the attack
  - Spamming
  - Hacking/cracking
  - Cross-site scripting
  - Port-scan
  - Worm and virus
  - Sniffing
  - Hoax
  - Open relay
  - Defacing
  - DoS attack
  - Spoofing
  - Trojan horse
  - Password guessing
Technique
Zendpunt

- Website
- E-mail
- SMS

Meldpunt

Reporting Service

Transmitting point

Thursday, 25 September 2003
Targets

• Collect incident reports from public and SMEs
• Produce statisticstical info about IT-security incidents
• Improve our service!
  – Information distribution
  – Internal Processes
  – Focus points (important topics, points of special interest, how-to’s)
New services

- SMS Alert
- E-mail Alert
- Reporting Service
- Monthly Newsletter
- Cybercrime manual

Future:
- Cert in a Box
- Benchmarking and Analyses

More and better info! Still improving, so......
Feedback, suggestions, more than Welcome!

Thursday, 25 September 2003
GOVCERT - International symposium on cyber security (August 21th and 22th 2003)

- **Principals:**
  - Ministry of Interior and Kingdom Affairs
  - The ministry of Economic Affairs

- **Speakers:**
  - leading speakers from Europe, the United States, Canada and the Asian Pacific in the field of Cyber Security presented their experiences and best practices of national and international cooperation
1st day theme

- Both elements of Cyber Security can only be obtained by cooperation of industry and government, both on a national and international level: “act local think global” is the approach we need.

- Main purpose
  Discuss the added value and best practices of National and international cooperation regarding Critical Information Infrastructure Protection (CIIP) and cyber crime.
Key findings 1st day

- The Society is getting more dependent on information structure, at the same time the Internet is increasing more rapidly than we can protect it.
- Appearance of threats is increasing, but also the number of vulnerabilities, and the sophistication of attacks.
- A blend of international cyber threats and physical threats makes coping more and more complex. All arrows are pointing in the wrong direction.
Conclusion

- A comprehensive approach is required.
- All parties involved, government, industry and society at large should be cooperating in this approach, each one based on their own position and responsibilities.
- Multidisciplinary working groups are suggested as the organizational structure to realize accepted outcomes. (This groups can act on a local or global level depending on the topic)
- For most issues a sensible approach is to start locally, on a national level, but to think globally
2nd day theme

- Cybercrime
  - Representatives of the European Commission, the US Department of Justice Criminal Division, the (Dutch) National Police Agency and law enforcement
  - An overview of how several cases, relating to cybercrime are dealt with and the initiatives that has been started on this subject
  - Data storage and date exchange, the prevention of and dealing with ICT-related security incidents and/or computer crime have become an essential part of security management and information protection
Conclusion

• Key words:
  – Awareness
  – Collaboration
  – Information sharing
Organize (1)

- **Multi disciplined (inter-) national working groups,**
  - Standardisation of detection tools
  - Legal issues, e.g. cyber crime (international)
  - Building case metrics/ make security measurable
  - Analyse structures for information sharing (e.g. ISACs)
  - Development of secure software & systems

- **Aiming at the collaboration between CERTs & other response teams,**
  - Emphasis on prevention;
  - Global daily situation reports;
  - Exercises (regional, international);
Organize (2)

- **Aiming at the collaboration between CERTs & other response teams,**
  - Emphasis on prevention;
  - Global daily situation reports;
  - Exercises (regional, international)
  - Detection technology (standard, open);
  - Sharing of event data;
  - Analysis of malicious code;
  - Develop methods to rank received info;
  - Develop multiple sources of info;
  - Help each other to create a national alerting service.
Overall conclusion

- “The time of raising awareness has passed, the time for collaboration has started!”

- The conditions for cyber security are taking form.
- At the same time the number and complexity of threats are increasing.
- Still, if we continue to cooperate and address each others responsibilities, we will be able to conclude that we are getting what we need:

  a secure cyberspace
Links

• Dutch National Alerting Service
  http://www.waarschuwingsdienst.nl

• Free SMS Alert (in Holland only!)
  http://www.waarschuwingsdienst.nl/render.html?cid=427

• Reporting service
  http://www.waarschuwingsdienst.nl/render.html?it=456

• Cybercrime Manual
  http://www.govcert.nl/render.html?it=218

• Email:
  - Feedback about Cybercrime manual <O> Cybercrime@govcert.nl
  - Contact (technical team) <O> cert@govcert.nl