Dave McCurdy
EIA President
& Executive Director
Internet Security Alliance

ANSI Annual Conference
October 1, 2003
The Internet Security Alliance is a collaborative effort between Carnegie Mellon University’s Software Engineering Institute (SEI) and its CERT Coordination Center (CERT/CC) and the Electronic Industries Alliance (EIA), a federation of trade associations with over 2,500 members.
Sponsors
Growth in Incidents Reported to the CERT/CC

- 1988: 6
- 1989: 132
- 1990: 252
- 1991: 406
- 1992: 773
- 1993: 1,334
- 1994: 2,340
- 1995: 2,412
- 1996: 2,573
- 1997: 2,134
- 1998: 3,734
- 1999: 9,859
- 2000: 21,756
- 2001: 55,100
- 2002: 110,000
Attack Sophistication v. Intruder Technical Knowledge

Intruder Knowledge

- High
- Low

Attacker Sophistication

- Low
- High


Tools
- DDOS attacks
- www attacks
- automated probes/scans
- GUI
- network mgmt. diagnostics
- denial of service
- packet spoofing
- sniffers
- sweepers
- back doors
- disabling audits
- burglaries
- exploiting known vulnerabilities
- hijacking sessions
- password cracking
- self-replicating code
- password guessing

“stealth” / advanced scanning techniques
Financial Impacts of Attacks

• Klez virus:
  - Clean-up and lost productivity: $9 billion
• Code Red: 1 million computers affected
  – Clean-up and lost productivity: $2.6 billion
• Love Bug: 50 variants, 40 million computers affected
  – Clean-up and lost productivity: $8.8 billion
• Nimda
  – Clean-up and lost productivity: $1.2 billion
• Slammer
  – Clean-up and lost productivity: $1 billion +
  – Blaster & So Big combined clean-up and lost productivity estimate $2 billion
“Installing a network security device is not a substitute for a constant focus and keeping our defenses up to date... There is no special technology that can make an enterprise completely secure.”

– National Plan to Secure Cyberspace, 2/14/03
Step 1 Invest in Cyber Security

- US Government increasing spending 64% for cyber security.

*****

For business there is a 21% ROI for early incorporation of security
- CSO Magazine 12/02
Step 2. Adopt and Implement Best Practices

- Cited in US National Draft Strategy to Protect Cyber Space (September 2002)


- Endorsed US India Business Council (April 2003)
Common Sense Guide
Top Ten Practice Topics

• Practice #1: General Management
• Practice #2: Policy
• Practice #3: Risk Management
• Practice #4: Security Architecture & Design
• Practice #5: User Issues
• Practice #6: System & Network Management
• Practice #7: Authentication & Authorization
• Practice #8: Monitor & Audit
• Practice #9: Physical Security
• Practice #10: Continuity Planning & Disaster Recovery
Step 3. Risk Mitigation/Cyber Insurance

“Until recently, traditional property insurance may have provided some coverage for virus-related exposures, but as of January 2002, the majority of insurers eliminated it as well.”

CSO Magazine

“The insurance industry has a pivotal role to play, particularly by developing cyber insurance policies.”

Paul B. Kurtz, Senior Director for National Security

Are you covered? Should you be covered?
- Many policies no longer cover cyber
ISAlliance Cyber-Insurance Program

- Free cyber check-up provided by AIG for members
- Market incentive for increased security practices
- 10% discount for ISAlliance members
- Additional 5% discount for implementing ISAlliance Best Practices (July 2002)
- Discounts more than offset sponsorship dues
- Audit program to be announced soon
Step 4 Join ISAlliance

Join and participate in a cybersecurity information sharing organization
Benefits

- Share critical information across industries and across national borders
- Provide secure setting to work on common problems
- Provide economic incentive programs
- Develop model industry programs
- Give policy makers an alternative to regulatory models
CERT Knowledgebase

Examples

Figure 3: Special Communications index page

Welcome to the CERT Communications database, a resource for technical staff for the latest information on current internet or special concern vulnerabilities that are preventive information for the distribution of special communications.

New NCs by Author:
The first entry was received via e-mail in March 1994 and produced over time. The latest for our audience is presented and for ease of distributing this information, the CERT Communications Distributed Database is the Special Communications index page.

Other Documents:

You can search or browse the database using three key fields:的地, field, and type. The search is customized database access to the database. You can also customize database access to the database for your needs, such as the search on the left side of the Communications Distributed Database. The search is available from our website, and is published for customizable features.

If you have questions or comments about this database, please contact us at CERT Coordination Center.
Benefits of Information Sharing Organizations

• May lessen the likelihood of attack

“Organizations that share information about computer break ins are less attractive targets for malicious attackers.” – NYT 2003

• Participants in information sharing have the ability to better prepare for attacks
Benefits of Information Sharing
Organizations/Examples

• SNMP vulnerability
  – CERT notified Alliance members Oct. 2001
  – Publicly disclosed Feb. 2002

• Slammer worm
  – CERT notified Alliance members May 2002
  – Worm exploited Jan. 2003