Managing Your E-mail from Over-flowing the Floodgates

Patricia Gilmore, CISSP

Treasurer, (ISC)²

INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM, INC.

Information Flow Under Attack

- **Five Worst Attacks*:**
  - **Code Red (2001)**
  - **Nimda (2001)**
  - **Melissa (1999) and LoveLetter (2002)**
  - **DDoS attacks (2000)**
  - **Remote Control Trojan Horse Backdoors (1998-2000)**

* *Information Security* magazine, November, 2002, reader's choices

The Coming Deluge …

- **Professionals Predict the Future**
  - **"Super" Worms and Polymorphic Code**
  - **Application-Level attacks**
  - **Massively Distributed Attacks Against Routing or DNS infrastructure**
  - **Kernel-Level Holes in OSes**
  - **IDS Evasion**
  - **Simultaneous Cyber and Physical Terrorist Attacks**

**Information Security* magazine survey of 220 readers reported November, 2002

Preparing for Inbound E-mail Attacks

- **Pro-active Measures You Can Take**
  - **Awareness and Training (Don't Open that Strange E-mail – it really DOESN'T Love You!)**
  - **External Facing OS hardening: Firewalls, DNS, E-mail and Web Servers**
  - **Keep 'Em Patched!**
  - **Up-to-date Anti-virus software everywhere (desktop, mail and file servers)**
  - **Stop it Upstream (Agreements with your ISP)**
  - **IDS and Incident Response Programs**

Securing Outbound E-mail

- **Requirements and Controls to Ensure E-mail <u>Confidentiality</u>**
  - **Protect Customer Privacy**
  - **Protect Company Proprietary Information**
  - **Message controls might include use of obfuscation and strong encryption**

Certified Professionals know how to make it work!

Securing Outbound E-mail

- **Requirements and Controls to Ensure E-mail Message Integrity**
  - **Protect against data tampering**
  - **Protect against falsified messages**
  - **Message integrity controls might include use of message authentication techniques, such as digital signatures**

Certified Professionals understand how to deploy such measures!

Securing Outbound E-mail

- **Requirements and Controls to Ensure E-mail Availability**
  - **Protect network bandwidth, and traffic flow against attacks**
  - **Employ HA systems, and Capacity management**
  - **Establish and test Business Resilience Plans, including actions to be taken if E-mail communications are disrupted**

Certified Professionals know how plan!

Conclusion

Sustaining The Flow of Your Company's E-mail means the difference between Business Survival and Failure!

(ISC)² — Securing Our Information Flow