Securing the Internet, Securing Our Way of Life

Stephen Trilling
The Internet is Pervasive

- The global economy is growing increasingly reliant on the Internet
- We need to consider the impact of cyber-attacks not only on individual businesses, but also their effect on the economy and, increasingly, our way of life
Cyber-Security Is Now a Boardroom and a Legislative Concern

- Estimated 2001 global cost from breaches: *Tens to hundreds of billions of dollars*
- 2001 projected US losses: *2.7% of US GDP*
Cyber-Threats of Today: Hacking and Denial of Service

- Hacking and Denial of Service attacks have already touched businesses and governments across the world
Cyber-threats of Today: Viruses and Worms

• The newest virus threats self-mutate, attack antivirus software, and can encrypt your files with strong encryption

• The latest computer worms use the Internet to update themselves on-the-fly

• # of distinct strains at the start of 2002: Nearly 59,000!
Blended Threats: A Deadly Combination

• Blended threats combine hacking, DoS, and worm-like propagation to rapidly compromise millions of machines and leverage them for insidious means

• These threats spread extremely rapidly: often without any human interaction!
Blended Threats: The Implications

- We’re no longer talking about thousands of machines launching an attack, but potentially tens of millions

Code Red Epidemiology
Nimda: 2.2M Systems Infected in 3 Days!

1. Infection of web servers via “Code Red-type” attack
Nimda: 2.2M Systems Infected in 3 Days!

2. Infection via email
Nimda: 2.2M Systems Infected in 3 Days!

3. Infection via Web browsing
Nimda: 2.2M Systems Infected in 3 Days!

4. Infection via shared drives
Nimda: 2.2M Systems Infected in 3 Days!

5. And infection to other files on each infected computer through traditional viral methods
Blended Threats: Potential Targets

• Today, online computers control numerous business and government functions, including:
  – Stock markets and trading
  – Transportation operations
  – Power generation and routing
  – Voice and data communications
  – Entire business supply chains
  – Military command and control systems

• Recent industry report – top two sectors hit by “severe” attacks:
  – Power and energy
  – Financial services
## Changing Attacker Demographics

<table>
<thead>
<tr>
<th>Classification</th>
<th>Attacker Description</th>
<th>Target</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Crime</td>
<td>Vandal, Script Kiddie, Packet Monkey</td>
<td>Email, Web Sites</td>
<td>Downtime, Defacement, Denial of Service</td>
</tr>
<tr>
<td>Computer Crime</td>
<td>‘Criminal’ Cracker, ‘Black Hat’</td>
<td>Assets</td>
<td>Monetary Gain</td>
</tr>
<tr>
<td>Information Warfare</td>
<td>Government Organization</td>
<td>Political Infrastructure</td>
<td>Political Power, Balance Change</td>
</tr>
<tr>
<td>Cyber Terrorist</td>
<td>Terrorists, Non-State Actors</td>
<td>Physical Infrastructure</td>
<td>Destruction</td>
</tr>
</tbody>
</table>
New Technologies Fuel the Fire

Projected by 2005:

<table>
<thead>
<tr>
<th>Broadband</th>
<th>Set-top Boxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration of one third of all US households</td>
<td>400M devices in use worldwide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Instant Messaging</th>
<th>Wireless</th>
</tr>
</thead>
<tbody>
<tr>
<td>300M users in the United States</td>
<td>2B Internet-enabled devices worldwide</td>
</tr>
</tbody>
</table>
A Good Security Process is a Closed Loop

1) Assessment
Inventory critical systems/assets and quantify their value

2) Planning
Develop policies, review processes and establish an incident response team

3) Implementation
Select and implement appropriate network security solutions

4) Monitoring
Monitor all deployed systems
Deploying Robust Security Solutions

- Organizations need a comprehensive, layered set of security solutions protecting clients, servers and gateways:
  - Application-level (layer 7) firewalls (perimeter/desktop)
  - Antivirus protection (gateway/desktop)
  - Vulnerability Assessment/Management
  - Intrusion Detection

- PLUS: Common management, alerting, logging and reporting
Symantec: A Total Security Solution

- Integrated security technologies across all platforms and tiers (Symantec Gateway Security appliance)
- Global 24x7 rapid response to emerging threats
- Comprehensive security management services
The Proactive Paradigm Shift

- Fingerprinting techniques are here to stay, but the industry MUST consider proactive security technologies as a front-line defense.

- Perhaps we need a conceptual shift (at least for critical environments): Specify what’s allowed and block everything else.
Conclusions

• Blended threats have truly global scope
• The tools to minimize these threats exist
• The responsibility to use them is ours