Cyber Security Maturity Model

Facts About Intrusions

WHO IS BEHIND DATA

- 48% were caused by insiders
- 11% implicated business partners

WHAT COMMONALITIES EXIST?

- 85% of attacks were not considered highly difficult
- 61% were discovered by a third party
- 86% of victims had evidence of the breach in their log files
- 96% of breaches were avoidable through simple or intermediate controls
2008-2011 Is The Cyber Tipping Point

- ESTONIA
- GEORGIA
- KOREAN DDOS ATTACK
- DOD THUMB DRIVE BAN
- DEFENSE INDUSTRY (DIB)
- WIKILEAKS
- OPERATION AURORA
- STUXNET
- NASDAQ
- SONY
- IMF
- RSA
- ..........DIGITAL TERRORIST

Characterizing Advanced Persistent Threats

- Characterizing Malware
  - **Stealth level** – From openly known to highly covert using cloaking tactics
  - **Known vs. Unknown** – Targets known, unpatched vulnerabilities to true zero-day, unknown vulnerabilities
  - **Broad vs. Targeted** – Broad attacks trigger for all victims that falls into trap while targeted attacks single out particular “victims of interest”
  - **1-time vs. Persistent** – One-hit wonders vs. sustained, self-updating code meant to establish long-term hold of system
### Lessons Learned From APTs

- **Persistent, pervasive, aggressive, and purpose driven**
  - There is no single silver bullet
  - Effective response is not trivial, so stop acting like it is

- **APT rely on multiple attack vectors**
  - Requires comprehensive security controls framework

- **Persistence with long-term campaigns**
  - Lengthy campaigns are easier to detect in the long run, but the trick is detecting early in the campaign lifecycle
  - Requires end-to-end situational awareness

- **Increasingly rely on zero-day attacks**
  - Attackers will sometimes be successful at least initially
  - Must monitor for outbound connections and illegitimate cross-platform activity

- **Regularly exploit weak identity controls**
  - Must deploy strong internal and external identity layers, including mandatory enterprise identity services

- **They know a lot about us**
  - But, they don’t know everything
  - Dynamic Defense is best chance to break attack chain

### The CIO / CISO Nightmare

<table>
<thead>
<tr>
<th>UNPROTECTED TECHNOLOGIES</th>
<th>Virtualization</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud Computing</td>
<td>Web 2.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY ARCHITECTURE</th>
<th>Extensive point products</th>
<th>Limited APT Defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Silo’ed security design</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LACK OF COLLABORATION</th>
<th>Inconsistent security management, policies and control</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>POOR SECURITY VISIBILITY</th>
<th>Gaps in security monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lack of real-time awareness</td>
</tr>
</tbody>
</table>
Top DoD Issues

1. Insider Threat
2. Advanced Persistent Threat
3. Supply Chain Risk Management
4. SCADA Vulnerabilities
5. Mobility
6. Identity Management
7. Cloud Security
8. Resiliency

Cyber Security Maturity Model*
Cyber Warfare Strategy

NATION STATE Resilience
ADVANCED PERSISTANT THREAT
CONVENTIONAL THREAT

Most Organizations

Agility / Speed of Action

E
Reactive & Manual
People based following doctrine and doing their best to "put out fires"

D
Tools-Based
Applying tools and technologies piecemeal to assist people in reacting faster

C
Integrated Picture
Loosely integrated with focus on interoperability and standards based data exchange for IA situational awareness

B
Dynamic Defense
Predictive and agile, the enterprise instantiates policy, illuminates events, and helps the operators find, fix, and target for response

A
Resilient Enterprise
Predictive & mission focused, isolates and contains damage, secure supply chains and protect key critical infrastructures to operate through cyber attack

*Cyber Security Strategies, LLC
Security Reference Architecture
Key Design Principles to Increase Maturity

- Industry Standards (NIST, Federal Enterprise Architecture)
- Defense-in-Depth - Multiple Layered Security Approach
- System-Wide Intelligence and Collaboration
- Interoperability
- Modularity
- Resource Constraints
- Business vs. Security Trade-off
- Regulatory Controls

Cyber Economics and Cyber Maturity

- Single interoperable management infrastructure
- Cloud Computing
- Security into hardware (memory and power savings with hardened security)

*Cyber Security Strategies, LLC
Cyber Economics and Cyber Maturity: Best Practices

1. IT Consolidation
2. Virtualization
3. Cloud Computing and Mobility
4. Interoperable Net Defense
5. Enterprise Procurements
6. Security into Hardware
7. Unified/trusted Supply Chains
8. Coordinated Research
9. Smarter Users and Highly Skilled Operators
10. Automation of Manual Processes (inspections/training/exercise)

*Cyber Security Strategies, LLC*

Governance: the CIO vs Cyber Czar
Are We Ready?

Who is in charge?

What is the plan?

Clear Roles and Responsibilities?

Is Government Shifting Resources to Face the Threat?

Is Industry Shifting Resources?  (do they have the business case)

Does Public And Private Sectors agree on the Strategy, the Technical Architecture, Compliance Requirements, and Commitment from Users to Safeguard the Internet?

Summary

1. Cyberspace is fundamentally a civilian space, one where we must all share responsibility within a participatory framework and where rules of behavior are clear, practical, and enforceable
2. Attacks manifest as “lengthy campaigns” vice “single events”
3. Security isn’t trivial, and we must stop acting like it is!
4. In addition to technology controls, we must also ensure effective controls for people, facilities, management, operations, etc.
5. Assume attackers will be successful at least some of the time
6. Cyber Security Maturity with clear attainable investment goals critical
7. Simply put, the top 20% of threats, the APT, pose all the risk
8. Risk Management Framework must be exercised and requires comprehensive security architecture and accountability at all levels