Is Your Enterprise Data Secure From the Inside Out?

JEFF SCHILLING
Chief Security Officer
Jeff Schilling, CISM

Chief Security Officer | Armor

- Retired U.S. Army Colonel
- Former Chief of Current Operations of the DOD’s Global NetOps Center for JTF-GNO (Cyber Command)
- Former Chief of Current Operations U.S. Army’s Cyber Command
- Former Director, Incident Response, Dell SecureWorks
Agenda

- How has the threat changed?
- How has the security team approach changed?
- The military approach to protection, from the inside out
- Narrowing your focus
- How to think about protection from the inside out
How Has the Threat Change?
**C-LEVEL**
Commodity Threat
80%

**B-LEVEL**
Targeted Threat
19.99%

**A-LEVEL**
Advanced Targeted Threat
0.01%
The Kill Chain

1. RECONNAISSANCE
   - Open-source research, social network research, port scan, IP sweep, Google research

2. WEAPONIZATION
   - Combine the exploit tool with the method

3. DISTRIBUTION & STRATEGY
   - Phishing email, website drive-by, SQL inject script

4. EXPLOITATION
   - Infected Word doc or PDF opened; Java script exploited in browser; command line SQL inject

5. PERSIST/LATERAL MOVEMENT
   - Registry key changed; privilege escalation; look for open connections

6. COMMAND & CONTROL
   - Malware or compromised system reaches out for instructions

7. ACTION ON TARGET
   - Search the target; Destroy or disrupt; Package and prepare data for exfil
Surface Area of Attacks

- Servers/ Applications
- Access/ Networks
- Humans/ User terminals
How Has the Security Team’s Approach Changed?
Security spending doubled in past 4 years

Many of these organizations were “compliant” on various security frameworks

Major shortage in security talent and getting worse
Spend Cycle

$100 BILLION

To date, organizations globally are spending $100 billion annually on cybersecurity tools and services — and still losing the war.

$170 BILLION

That figure is projected to jump to $170 billion by 2020.

History has proven that spending doesn’t equal safe outcomes.

The Jelly Doughnut Approach

Most people secure from the outside in, focusing first on perimeter security and then internal data segmentation, if they can get to it.
The Real Deal with Big Data and Artificial Intelligence

Threat actors are still able to evade the most sophisticated big data and artificial intelligence system.

In reality, businesses could be “cutting away” threat indicators that are important.
Narrowing the Focus
The 98%

- Active Directory
- Remote Access
- User Workstations
- Bring Your Own Device
- Vulnerable Public Websites
- Vulnerable Network Infrastructure
Finding the 2%

All about protecting the databases

Email

Share Point

File Shares

Business Application Databases
Protecting Endpoint vs. Protecting the Data

Endpoints vs Data
Interdicting the Kill Chain

1. **RECONNAISSANCE**
   - Open-source research, social network research, port scan, IP sweep, Google research

2. **WEAPONIZATION**
   - Combine the exploit tool with the method

3. **DISTRIBUTION & STRATEGY**
   - Phishing email, website drive-by, SQL inject script

4. **EXPLOITATION**
   - Infected Word doc or PDF opened; Java script exploited in browser; command line SQL inject

5. **PERSIST/LATERAL MOVEMENT**
   - Registry key changed; privilege escalation; look for open connections

6. **COMMAND & CONTROL**
   - Malware or compromised system reaches out for instructions

7. **ACTION ON TARGET**
   - Search the target; Destroy or disrupt; Package and prepare data for exfil

**Threat actors halted**
The Military Approach to Protecting Soldiers
Layered Defense, from the Inside Out
Protecting from the Inside Out
Defining Your Strategy

- Risk Reduction
- Reduce Attack Surface Area
- Drive up the Skill Level of Threat Actors Required to Exploit Your Environment

It’s not about the tools. It’s how you use them.
Step 1: Data Classification
Product portfolio based on workload risk levels supporting your multi-cloud strategy

<table>
<thead>
<tr>
<th>Data Classification Level</th>
<th>LOW SECURITY REQUIREMENT</th>
<th>MEDIUM SECURITY REQUIREMENT</th>
<th>HIGH SECURITY REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

**Typical Workloads**
- PUBLIC OR NON-SENSITIVE INFORMATION
- PRIVATE INFORMATION
- HIGHLY SENSITIVE INFORMATION

**Cloud-based Solutions**
- **LOW SECURITY REQUIREMENT**
  - Public clouds / DIY + Software security solutions
  - or
  - Private clouds / DIY + Managed security solutions

**Outsourcing Adoption Cycle**

---

CONFIDENTIAL DO NOT DISTRIBUTE | BETWEEN YOU AND THE THREAT
Step 2: Start at the Host Level
Building a Solid Security Foundation

• Hardened Operating System
• Anti-Malware or Application Whitelisting
• Monitoring Memory for Changes (APT detection)
• File Integrity Monitoring
• Patch Management
• Logging Enabled
Step 3: The Application Stack

- Patching
- Patching
- Patching
- Application Level Encryption for Databases
Step 4: Network Segmentation and Zero Trust Model
Bringing It All Together

It takes time for threat actors to work through the kill chain

1 2 3 4 5 6 7

Dwell Time
How long to remove a threat actor from the environment.

- Hypervisor Firewall
- Anti-Malware Protection
- OS File Integrity Monitoring
- Log Management & SIEM
- Vulnerability Scans
- Hardened Operating System
- Patch Management

MISSION
THREAT INTELLIGENCE
Reduce noise with Armor’s proprietary threat intelligence platform, talented team and layered edge defense

MISSION
SECURITY OPERATIONS
Reduce dwell time utilizing secure architecture and forged in battle techniques managed by Armor’s proactive relentless SOC

CONFIDENTIAL DO NOT DISTRIBUTE | BETWEEN YOU AND THE THREAT
In Conclusion

• Assume you user base is compromised
• Think about how you disrupt the threat actor’s kill chain
• Narrow the focus of what you truly can protect
• In the end, ”it’s the data, stupid”
Q&A
Thank You

JEFF SCHILLING  Chief Security Officer