Managing Cyber Security Across the Enterprise

Asif Effendi
September 3, 2015
austinssi
Managing Cyber Security Across the Enterprise

Highlights:

- Oil and Gas Threat Landscape
- Challenges in Securing Control Systems
- Cyber Security Strategies
- Conclusion
# Threat Landscape

### # of Reported Incidents (ICS-CERT)

- **2008**: 0
- **2009**: 50
- **2010**: 100
- **2011**: 150
- **2012**: 200
- **2013**: 250
- **2014**: 300

Managing Cyber Security Across the Enterprise

@NTXISSA #NTXISSACSC3
Increase in sophistication of cyber attacks

Increase in Sophistication of Attacks Against Infrastructure

- Yes: 76%
- No: 5%
- Unsure: 19%

Major reasons for industrial network malfunction incidents:
- SecurityIncidents.net

Malware attacks 35%

Downtime of the industrial process due to malware incidents:
- SecurityIncidents.net

Advanced Persistent Threats (APT)
- Deep Threat, Dusk, Entropic, Equifax, Sony, Tesla

Generic Malware
- Many EDS attacks are unsophisticated but their impact is severe:
  - Worms, Trojans,
  - Blockers, Password theft, remote access, vandalism.
Largest sector of cyber incidents is Energy industry

Distribution of Cyber Incidents (ICS-CERT)

- Critical Manufacturing, 17%
- Communications, 5%
- Commercial Facilities, 2%
- Water, 4%
- Transportation, 5%
- Postal & Shipping, 1%
- Nuclear, 3%
- Info Tech, 4%
- Government, 2%
- Energy, 53%
Challenges in Securing Systems

Difference in security attribute between ICS and Enterprise systems

1. AVAILABILITY
2. INTEGRITY
3. CONFIDENTIALITY

1. CONFIDENTIALITY
2. INTEGRITY
3. AVAILABILITY

Courtesy: Kaspersky Lab
Differences/similarities in security controls considerations between ICS and Enterprise systems

<table>
<thead>
<tr>
<th></th>
<th>ICS</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life Span</td>
<td>15 – 20 years</td>
<td>3 – 5 years</td>
</tr>
<tr>
<td>COTS Related Vulnerabilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Third Party Access to Systems</td>
<td>Frequent</td>
<td>Limited</td>
</tr>
<tr>
<td>Security Considerations in Implementation</td>
<td>Limited</td>
<td>Yes</td>
</tr>
<tr>
<td>Wireless Access to Systems</td>
<td>Significant</td>
<td>Limited</td>
</tr>
</tbody>
</table>
Defense in Depth in securing ICS

ICS Specific Policies, Standards, Procedures, Awareness

Physical Security

Perimeter Security

Internal Network Security

Host Security

Application

Data Security

Security policies, standards, procedures, education, backup and restoration, business continuity, disaster recovery

Guards, Locks, Access Controls

Firewalls
DMZ
ACL Configured Routers
VPN
IDS
IPS

Security Zones
Network Segments
Network Based IDS
Internal DMZ
Internal Firewalls

Access Control
Authentication
Password Management
Application Vulnerability Management
Secure Software Development Methodology

Patch Management
Intrusion Prevention
Virus Protection
Host Based Firewall
Server Hardening
Port Controls
Access Controls
Continuous Monitoring Auditing

Endpoint Security
Secure Communications
Access Controls
Authentication
Cyber Security Strategies

Risk Based Approach and Management to Securing ICS

Managing Cyber Security Across the Enterprise
Managing Cyber Security Across the Enterprise

Cyber Security Strategies

Network Segmentation

ZONE 1
- Backup Control Center
- Remote Business Peers
- External Communications Infrastructures

ZONE 2
- Corp PSX
- Business Workstations
- Email Server
- FTP Server
- Wireless Access Points

ZONE 3
- External Business Comm. Server
- WWW Server
- DB/Historian
- Security Server
- Authentication Server

ZONE 4
- Control System LAN
- Engineering Workstation
- HMI Computers
- Configuration Server
- Database Server
- Historian
- Applications Server
- Data Acquisition Server
- CS PSX
- CS MODEM Pool
- Control System Field Device Communications Infrastructure
- Field Comm Bus
- Field Locations

(Reference: Defense in Depth Strategies, Idaho National Laboratory, Department of Homeland Security Based on ISA 62443)
Rapid integration of “Commercial Off the Shelf (COTS) in ICS environment comes with vulnerabilities and risks

Industrial control systems are not easy to secure

Hacker knowledge base is growing rapidly, resulting in more sophisticated attacks

Risk has to be managed although it can not be eliminated. Risk based “Defense in Depth” mitigates cyber risks at multiple layers in an organization
The Collin College Engineering Department

Collin College Student Chapter of the North Texas ISSA

North Texas ISSA (Information Systems Security Association)

Thank you