DIY Insider Threat Detection

(technical) perspectives and considerations within ICS environments

Dieter Sarrazyn
@dietersar
Insider ??
Insiders ...
Insiders ...

"an insider is a person that has been *legitimately empowered* with the *right to access, represent, or decide* about one or more *assets* of the organizations environment"

“Countering insider threats” - Dagstuhl Seminar Proceedings, 2008

http://drops.dagstuhl.de/opus/volltexte/2008/1793
Insiders ...

• (compromised) Employees
• (compromised) Contractors/Vendors
• Cleaning crew
• Visitors
Insiders ...

“Sleepers” can be triggered by ...

• Social unrest
  • Strikes / people being laid off
• Compassion / alternate beliefs
• External uncontrollable events

“trusted” people can quickly become untrusted
Some scenario’s

What are the potential "goals" of the insider threat actor?
Scenario’s

disgruntled employees abusing (ex-)rights

Energy
An oil-exploration company hired a temporary consultant to assist in setting up a Supervisory Control and Data Acquisition (SCADA) system that enabled communication with offshore platforms and detection of pipeline leaks. When his contract was about to expire, he requested permanent employment. The request was rejected and his contract ended. For two months following termination, he planted malicious programs on the organization's systems that temporarily disabled the SCADA system.

Water
An electrical supervisor developed applications for a SCADA system used by the water industry. After termination, he installed a malicious program on one of the organization's critical systems, damaging the SCADA system.

Scenario’s

Stuff being dropped onto the network

Contractor/visitor laptops
Scenario’s

Backdoor(ed) connections

- DSL often with WiFi enabled
- Bridging to the internal network possible
- (proprietary) remote access
Considerations – things that you can do yourself

Detecting, preventing and/or deterring insider threats
Considerations

Do you know your network?

Visible <> invisible network

http://www.smartceo.com/kci-technologies-know-who-owns-your-network/
Considerations
“visible” network
Considerations

“invisible” network
Considerations
network

Baseline your environment

• Asset / inventory management
• Bridge systems
• Remote access
• SIS connections

http://www.smartceo.com/kci-technologies-know-who-owns-your-network/
Considerations

network

• Volume/usage monitoring
  • (big) usage of gmail, dropbox ...
  • Large print jobs
  • A lot of DNS requests ...

• Authentication

• Segmentation/zoning

• Use honeypots within your ICS network(s)
Considerations

network – rogue device/AP detection

Passive device ... No introduction of (new) bridges...

https://www.flickr.com/photos/teknyka/6592496831/
Considerations

network – distributed rogue device/AP detection

ARP/AP probe zone 1
Get ARP DB for zone 1
Get approved AP’s

ARP/AP probe zone 2
Get ARP DB for zone 2
Get approved AP’s
Rogue AP/device discovered
Considerations
System

- system security baselines
- media sanitization techniques
- “true” restricted desktop
Considerations

Users

Do You Know Your People? Really?

- Work schedule
- Badge#: 2345
- Serial#: 1234567
- 703-555-1212
- Patterns of activity
- jdoe@ic.fbi.gov
- IP Addr: 1.1.1.1
- Works for Business Development

https://www.slideshare.net/SelectedPresentations/ht-t17
Considerations

Users

• Behavior related
  • Logon / logoff hours
  • Websites visited
  • (internal) servers accessed
  • Physical locations visited

• HR related
  • Background checks during hiring
  • Identify “key personnel”
  • Governance accreditation
  • “missed” promotion
  • Radicalization
Considerations

users – (Privileged) access

• (ab)use of admin credentials
• (ab)use of (privileged) service accounts
• Revoke (logical) access if role(s) change
Considerations

Physical
Considerations

Physical

• Verify physical access of everybody
  • Revoke physical access if role(s) change

• Know who is where at what time

• 4 eyes principle

• Motion detection
Considerations

Physical

• Verify physical connections to DSL or other internet lines

• Perform regular physical walkthroughs

• Rack alarms
Considerations
Logging & Monitoring

ARP/AP probe
System logs
Honeypot info
Other logs
Considerations
ICS Vendor management

---

LITTLE BOBBY

I HAVE THREE ANONYMOUS SOURCES THAT SAY MY PRODUCT IS BETTER THAN OUR COMPETITORS!

MAC GUFFIN

FAKE NEWS.

--AND TWO SECURITY TESTING VENDORS SAID SO TOO!!!

MAC GUFFIN

HACK FQOE

BUG OUT

RANDOMWARE

PROMOTED CONTENT.

by Robert M. Lee and Jeff Haas

---

Jun 2018

DIY Insider Threat Detection
Considerations

Training / awareness
Summary
Summary

• DIY insider threat detection/protection is doable ...

• However you need
  • (skilled) People
  • Knowledge/experience
  • Time
  • Management support
  • Equipment & tools
  • Still some Budget
  • To get your IT to know/understand OT
Summary
DIY insider threat detection & prevention

Dieter Sarrazyn
dieter@secudea.be
@dietersar
https://be.linkedin.com/in/dietersarrazyn