How Perimeter Cybersecurity Leaves You Exposed

Scott A. Mossbrooks, Senior Director of Sales
Topics

• What are hackers after?
• Cybersecurity Truths and Myths
• Issues being seen with utility’s cyber security
• Reported compromised utilities
• Why system monitoring is very important?
• IT Test
Why Am I here?

Because N-Dimension had done:
- Network Monitoring and Reporting
- Vulnerability and Pen testing
- NERC CIP Gap Analysis
- Cyber awareness training
- Cyber security, Defense-in-Depth and UTM
- Disaster recovery plans
- Work very closely with:
  - NERC
  - DOE/DOD
  - APPA
  - NRECA
What Are Hackers After?

- Financial information
  - Customer’s/Employee’s social security numbers
  - Customer’s/Employee’s credit card numbers
  - Customer’s/Employee’s checking account numbers
- Control (terrorism, chaos)
- Bored, having fun
How Are the Breaches Occurring?

CAUSES

- Phishing/Hacking/Malware: 31%
- Employee Action/Mistake: 24%
- External Theft: 17%
- Vendor: 14%
- Internal Theft: 8%
- Lost or Improper Disposal: 6%
Myth: Our utility is secured because our (SCADA, AMI, etc.) vendor uses encrypted or encoded data

Truth: While it is true that your data (SCADA, AMI, etc.) is secure, the communication paths are wide open for hackers and malware. Never assume that your fiber, cellular, etc. provider uses advanced cybersecurity. Most only protect data over their networks, not the network itself.
Issues (Myths and Truths)

Myth: Our utility is secured because our (SCADA, AMI, etc.) vendor uses encrypted or encoded data.

Truth: While it is true that your data (SCADA, AMI, etc.) is secure, the communication paths are wide open for hackers and malware. Never assume that your fiber, cellular, etc. provider uses advanced cybersecurity techniques to protect your data. Most only protect data over their networks, not the network itself.

FIX: Secure Your Communication Paths
Myth: Our utility uses firewalls, so we are protected from hackers.

Truth: While firewalls are helpful, many are not configured properly or are not maintained with patches and updates. With today’s sophisticated hackers, Unified Threat Management (UTM) devices with Intrusion Detection software (IDS), Monitoring and Alerting is needed. When using in a Substation, Network Control and proper environment hardening is needed. Think Defense in Depth.
Myth: Our utility is secured because our (SCADA, AMI, etc.) vendor uses encrypted or encoded data

Truth: While it is true that your data (SCADA, AMI, etc.) is secure, the communication paths are wide open for hackers and malware. Never assume that your fiber, cellular, etc. provider uses advanced cybersecurity. Most only protect data over their networks, not the network itself.

FIX: Bi-directional Firewalls and Monitoring
Myth: Our employees are our greatest asset.

Truth: Actually employees represent the greatest risk to your utility’s security (cyber and physical). Use of thumb drives, downloading movies at work, Facebook at work, on-line gaming, not locking computers, social engineering and more make your employees the weakest link.

However, employers share the blame by not updating and reviewing cyber policies annually. Also for not doing cyber awareness classes or webinars.
Myth: Our employees are our greatest asset.

Truth: Actually employees represent the greatest risk to your utility’s security (cyber and physical). Use of thumb drives, downloading movies at work, Facebook at work, online gaming, not locking computers, social engineering and more make your employees the weakest link.

However, employers share the blame by not updating and reviewing cyber policies annually. Also for not doing cyber awareness classes or webinars.

FIX: Train, train, train and test your employees.
**Myth:** If we do not know we are not protected, we cannot be held responsible.

**Truth:** Really? The ostrich with head in sand defense? A utility is responsible for any data that is stolen from their utility or any damages hackers cause. Yes, there is cyber insurance but most utilities do not have it. So the best thing to do is to be proactive, install UTM devices, monitoring and do annual testing of your cyber defense system.
Myth: If we do not know we are not protected, we cannot be held responsible.

Truth: Really? The ostrich with head in sand defense? A utility is responsible for any data that is stolen from their utility or any damages hackers cause. Yes, there is cyber insurance but most utilities do not have it. So the best thing to do is to be proactive, install UTM devices, monitoring, and do annual testing of your cyber defense system.

FIX:
Educate and train your senior management and directors
Newly Reported Compromised Utilities

• In 2017, a city released the Ransomware when one of the utility employees clicked on what appeared to be a legitimate email. Luckily the files that were locked were not major important ones but clean up still took two weeks.

• In 2017, a Co-op released Ransomware when one of the employees clicked on a phishing email and the files that were locked all but paralyzed the utility. It took a few days to get utility operating properly again and over 2 months by a third party to clean everything that was damaged, including firewalls. This Co-op was waiting for board approval to add our monitoring and more cyber defenses when it happened.

• In 2017, A large governing body over municipal power had one of their VPs log into his email from a hotel. The hotel internet had malware on it and the malware sent bogus emails to everyone in his address book causing confusion.
• A Rural Electric Cooperative (Co-op) who uses an IP based phone system. A hacker programmed the IP based phone system that every time a Co-op customer call the customer service lines, the phone system would call a 1-900 number and the Co-op customer would be charge for the call.

• A Rural Electric Cooperative (Co-op) who had just installed a new HVAC system at their Co-op. This Co-op has a sharp IT group and they noticed new outbound communications to an unknown IP address soon after the HVAC system was installed. They traced the activity back to the HVAC system and the IP address to Russia.
A Midwest utility that uses an AMI service recently discovered their AMI server had a hacker actively in it. This was discovered by their 3rd party monitoring service and it was not an easy fix. The utility thought the 3rd party AMI vendor was managing and protecting the server.

The 3rd party AMI vendor thought the utilities 3rd party IT vendor was servicing and protecting the AMI server. The 3rd party IT vendor didn’t know they were supposed to be doing this. To make matters worse, the utility had no clue where the server was physically located. It took this utility 6 weeks to hire another vendor to find the server on the network, figure out who was minding it and get it fixed. The utility reported that while the system had been hacked and it it connected to their finance system, there was no customer data compromised.

As of last week, there was additional hacker activity discovered in this server and it was again traced back to China. The 3rd party monitoring vendor is working with the utility and 3rd party IT vendor to fix the issue, check firewall rules and change how the AMI vendor access the server remotely.
Today...

What You’re Doing Well:
• Firewalls
• Malware protection
• Anti-Virus protection
• Spam or email filters

Why Cyberattacks Are Still A Risk
• Firewall Log Analysis
• Time to do everything
• Staff to do everything
• Monitoring of your Network devices
• Cybersecurity alerts, bulletins, community data
• Expertise and someone to help if you are breached
• Professional Remediation Service
What We Have Learned

1) Many small-midsize utilities don’t know what they don’t know about cybersecurity – it’s complex
   - Internal threats
   - External threats
2) Limited security resources and expertise
3) Annual security scans provide limited value
4) Existing cybersecurity information not actionable
5) Board members and utility management are concerned about risk exposure

N-DIMENSION FULFILLS A CRITICAL GAP
Knowing Is the “Key” – From Start to End

Why is Cyber Security Monitoring Required?

- Hackers are increasingly targeting utilities
- Firewalls are not enough
- Cyber Security is complex - requires deep expertise and vigilance
- Compliance Requirements – NERC CIP, PCI, ISO, etc.
- Multi-layered cyber security strategy is best practices

- Complex Nature of Cyber Security Incidents and Lack of Understanding Thereof in Power & Energy Companies
- False Sense of Cyber Security
- Being the Basic Component of Cybersecurity Risk Management Plan, Best Practices and Information Security Life Cycle

Source: NIST SP800-61r2 (Computer Security Incident Handling Guide)
Where To Begin?

Start with Cyber Security Monitoring (N-Sentinel Monitoring)

• Monitoring is a great first step to cyber security. It watches your networks (IT, OT) for malware, viruses and hacking attacks. It will alert to issues being seen, keeps a log of the issues and allows cyber experts to identify and fix weakness in your defense. It is intended to be used with cyber security already in place.

• This will help utilities, either directly or indirectly, in establishing many of the ICS Recommended Best Practices, meeting NERC and PCI compliances.
• Comprehensive continuous cybersecurity monitoring service for utilities
• Monitoring of both internal and external traffic
• Utility cyber community intelligence
• Actionable threat data and reports
• Advanced threat alerts
• Hybrid service delivery combines cloud-based cybersecurity technology backed by cybersecurity experts
• Easy, fast deployment and hands-off management
Network Monitoring Points

1. Behind firewall
2. Between Utility’s IT and OT network
3. Between SCADA (or other OT applications) and OT network

- Web Portal
- Reports
- Alerts

- N-Dimension Security Analysts
- Network Operations Center
- Community-based Utility Contextual Analysis

- Internet
- Web DMZ
- Corporate Network
- Operations Network
- Substations
- AMI
- OMS
- Distribution Devices
How Cyber Threats Often Gain Access

1. Attacks that pass through firewall
2. Third Party Access
3. Internal Breaches
4. Communications
5. System Vulnerabilities

Vendors  Cloud  Grid Network  ISO

Corporate Applications

Engineering Applications

AMI Head-End Server

SCADA Operations Servers

SCADA Host

SCADA Operations Personnel

Smart Meters Collectors
## Examples of Activity N-Sentinel Detects

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>• Port Scans</td>
</tr>
<tr>
<td><strong>Malware/Trojans</strong></td>
<td>• CNC Channels, Exploit Kits, Black Energy</td>
</tr>
<tr>
<td><strong>Exploit Attempts</strong></td>
<td>• Heartbleed, Shellshock</td>
</tr>
<tr>
<td><strong>DOS/DDOS</strong></td>
<td>• NTP Amplification Attacks</td>
</tr>
<tr>
<td><strong>Policy Issues</strong></td>
<td>• Cleartext Passwords, Cleartext Credit Card Numbers</td>
</tr>
<tr>
<td><strong>Malicious Files</strong></td>
<td>• dll, pdfs, images</td>
</tr>
</tbody>
</table>
From Data Overload To Actionable Data

1. Cumulative N-Sentinel Cyber Alerts for 3 Utilities

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>82,309</td>
<td>2,398,009</td>
</tr>
<tr>
<td>2</td>
<td>4,871,216</td>
<td>6,642,130</td>
</tr>
<tr>
<td>3</td>
<td>1,422,703</td>
<td>1,673,264</td>
</tr>
<tr>
<td>Total:</td>
<td>6,387,228</td>
<td>10,713,403</td>
</tr>
</tbody>
</table>

2. Cloud-based Threat Intelligence and Analysis

3. Clear identification of critical threats needing action

Priority 1: Malware-CNC Win.Trojan.AllAple Variant, illegal botnet
Priority 1: Non-secured data two-way activity with Internet, from substation cameras.
Priority 1: Malware-CNC Win.Trojan.AllAple Variant, man-in-the-middle
Priority 1: Heartbleed Attempts
Sample Email Alert

Event Criticality Priority Level – P1 being most critical.

Event Category

Sensor ID
Server-other TLSv1 large heartbeat response - possible ssl HEARTBLEED attempt

Overview:
A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

Impact:
Vulnerability is remotely exploitable. If exploited, allows unauthorized disclosure of information.

Technical Information:
A vulnerability was found in OpenSSL versions 1.0.1 through 1.0.1f. These versions contain a flaw in its implementation of the TLS/DTLS heartbeat functionality of function tls1_process_heartbeat/tls1_process_heartbeat in the library ss/tls1_lib.c. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time. The sensitive information that may be retrieved using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- cookie (identification processes and content that can be leveraged to bypass explicit mitigations)

Recommendations:

1) Ensure that systems affected by the vulnerability and upgrade it as soon as possible to OpenSSL 1.0.1g

2) Implement network intrusion detection signatures to identify repeated attempts to leverage the vulnerability. An attacker will likely send hundreds of attempts because the vulnerability only exposes up to 64KB of data from a random section of memory.

3) Perform historical review of VPN logs to identify instances where the IP address of a session changed repeatedly between two IP addresses. It is common for an IP address to legitimately change during a session, but it is fairly uncommon for the IP address to repeatedly change back and forth between IP addresses that are in different network blocks, geographic locations, from different service providers, or rapidly within a short time period.

References:
US-CERT:
https://www.us-cert.gov/ncas/alerts/TA14-098A
CVE Details DB:
CVE Mitro:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
OSVDB:
http://www.osvdb.org/show/osvdb/105485
Ad Aware Pro Security Activation

lavasoftsecure@gmail.com <lavasoftsecure@gmail.com>2:09 PM (20 hours ago)to me (10/21/2016)
Hi Scott Mossbrook,

You have purchased Ad-Aware Pro Security software by paying us $48.00 from your (Order id : UD953G24) on (Date : 09/06/2015). The reason for this e mail is that you did not activate this your purchased program last year. So as per new promotion we are re activating new license keys without any additional cost. One of our technicians will help you generate new license keys.
For activation assistance kindly reply with your phone number.

Thank You,
Roger Smith,
Supervisor LAVASOFT
(logo here)
Hi Scott Mossbrook,

You have purchased Ad-Aware Pro Security software by paying us $48.00 from your (Order id : UD953G24) on (Date : 09/06/2015). The reason for this e mail is that you did not activate this your purchased program last year. So as per new promotion we are re activating new license keys without any additional cost. One of our technicians will help you generate new license keys.
For activation assistance kindly reply with your phone number.

Thank You,

Roger Smith,
Supervisor LAVASOFT

(logo here)
Email from a friend:

COBBY12345@aol.com

Summary of Email: In Greece on a fishing trip, our group was robbed and I need help getting home.

My Response: WTF?

Next email: Thank you for offering to help. I need $20,000 wire transfer to the bank below asap so I can get home. This group has offered to assist us.

My next step: I double checked the email to see if my friend had been hacked or someone was spoofing his email. My friend’s email is COBBY12345@aol.com

So what did I conclude?
What to do with Spam of Phish

If it is from a known emailer or friend:

• Call them and ask them about the email
• If it is a work email, have your IT expert check it for you. They might even check personal ones for you if they have time.
• Ignore the email. Responding to it can make matters worse if their computer is already compromised or infected.

If it is from an unknown emailer:

• If it is a work email, have your IT expert check it for you. They might even check personal ones for you if they have time.
• Ignore the email. Responding to it can make matters worse if their computer is already compromised or infected.
Scott Mossbrooks

Senior Sales Director

scott.mossbrooks@n-dimension.com

660-355-1802 – office/cell