The Fundamentals of Utility IT Security

Protecting Networks, Applications and Data

Center for Business Intelligence conference - Electronic Security for the Power Industry
Omni Ambassador East Hotel - Chicago, IL - October 28-29, 2002

The Current Situation…

- National defenses could be impacted by electricity outages or fluctuations
  - Electric Grid is part of the Critical Infrastructure
  - Electric Utilities have been regularly identified as targets for terrorist activity
- History: HIPAA and GLBA - who's next?
  - FERC SMD NOPR, Docket No. RM01-12-000
    ftp://ftp.nerc.com/pub/sys/all_updl/docs/ferc/NOPR/FERC-NOPR-RM-01-12-000.pdf
- The Energy Industry is in the media spotlight
- E-commerce and the Internet have changed the way Electric Utilities do business
- The demand for energy is increasing globally

The Fundamentals..

- Where to Begin
  - Get a Budget
  - Get Attention
  - Get Busy
- What to Secure
  - The Network
  - The Data
  - The Applications
  - The People
- Protection 101
  - Anti-Virus
  - Policy and Contracts
  - Data Classification
  - Encryption
  - Integrity Assurance, IDS, Proactive Scanning and Log Monitoring
  - Awareness Training
  - Divide and Conquer
- How to Stay Secure…
  - Get an Audit
  - Get Involved

Determine the Budget

- Security spending: size matters
  - Who is in charge of Security?
    - CSO, CISO, Security Director/Manager, Administrator…
  - Track all budgeted spending, ad-hoc requests and incident costs
- You get what you pay for…
  - Security isn't cheap (and quality isn't free either)
    - Beware of Quantity
    - Do the research to make timely and wise choices
- Don't wait for an incident to get money
- How much is too much?
  - You don't have to "outrun the bear" - *but*...
  - Watch out for security "snake-oil"
  - Scope for success
  - Consider spending more on security than coffee

Get Management Attention

- Require ownership of security issues
  - Upper Management must understand that they are ultimately responsible for the security of the company
- Require sign-off for risk acceptance
  - Encourages education of the risk, before sign-off/ownership
  - Job-security for everyone involved
- Keep them informed (but keep it simple and consistent)
  - Report [sanitized] incident information in real-time
  - Report prevented/well-contained incidents
    - Viruses, Worm, Trojans
    - IDS, Tripwire, Log monitoring, tip-off
  - Report all patches/updates installed, related to Security
  - Schedule monthly or quarterly meetings for updates and open dialogue/discussion

Get Busy…

- Get a dedicated Security Staff
  - Again, size matters..
  - One person should be in charge
  - Get people with integrity (not cheap); no reformed hackers
  - Certifications vs. Experience
  - Don't over-task your staff; flexibility is vital
- Find out *what* you need to secure
  - Assess your environment: identify and classify *everything*
  - Create many maps, diagrams, spreadsheets, documents, etc..
  - Prioritize - whatever keeps you off the front page of the newspapers is first on the list…
  - Look for the "low hanging fruit" or "quick-hits" to show progress
  - Research what it really takes to secure your unique environment

Securing the Network

- **Switches (No hubs!)**
  - Strong passwords
  - Secure and Restrict Access
  - Auditing
- **Routers**
  - Strict ACLs
  - Formal ACL change process
  - Strong passwords
  - Secure and Restrict Access
  - Auditing
  - No non-essential services
- **Firewalls**
  - Use them everywhere
  - Formal rule change process
  - Strong passwords
  - Secure and Restrict Access
  - Auditing
  - Watch out for “Swiss cheese” effect
- **DMZs**
  - Use them wherever there is a firewall
  - Employee access
  - Vendor support access
  - Vendor/Business Partner access
  - Control/Dispatch Centers
  - Excellent choke point for IDS, etc..
- **VPNs**
  - Employee access
  - Site to Site
  - Split tunneling
  - Hard to manage, if over-deployed
- **Wireless**
  - Just **don’t do it**… *yet*
  - Getting there, but still emerging tech
- **Microwave**
  - It may seem obscure, but obfuscation is not security - it has been hacked too

Securing the Data

- Data Classification!
- Account security
  - Client access/credentials
    - In storage
    - On the wire
- Trusted front-ends
  - Single layer of defense
  - False sense of security
  - Back-end data not secure
- Duplication
  - Only when necessary
- Database Security
  - Account permissions
    - Restricted to this use
    - Unique account for task
    - Principle of least privilege
  - Auditing
  - Access across a firewall
  - Database scanning tools
- Validation and Integrity
  - Don’t accept just any data
- Test Databases

Securing the Applications

- In-house or out-sourced?
  - The grass is always greener…
  - Whom do you trust?
  - Control over the code
- SDLC (Software Development Life Cycle)
  - If you code in-house, live by it
  - Request that your vendors provide SDLC documentation
- Play nice with Firewalls
  - Write applications that take advantage of the latest application level firewalls
  - Connection pooling
- Account security
  - Credential Storage
    - Encrypted, please
    - No flat files!
  - Credential location
    - Easy to modify for both client and server
    - Don't expose passwords to the interface; use a hashing algorithm
    - Create APIs to allow for the future (Biometrics, PKI, etc…)
- Separation of Duties
- Watch out for complex solutions

Securing the People

- Upper management
  - Tightest security
  - Helps you be visibly beneficial
- IT staff
  - Slow change in corporate culture
- Project staff
  - Become part of the PLC (Project Life Cycle)
- Development staff
  - Publish secure coding standards
  - Separation of duties
- Dispatchers/Control
  - First line of defense
- Help Desk staff
  - Typically, the weakest
- Contractors
  - Background checks

Protection 101

- Anti-Virus
- Policy & Contracts
- Encryption
- Data Classification
- IDS, Proactive Scanning and Log Monitoring
- Awareness Training
- Divide and Conquer

Policy and Contracts

Policy

- Write a policy for *everything*
- Develop a fast approval pathway
- Publish on an Intranet for reference
- Use a common look and feel for documents
- Standards & Guidelines

Contracts

- Get Security involved at the RFP
- Create clear and detailed SOWs
- SLAs for everything
  - Quality of Service metrics
  - Don't forget Backups
- Maintenance & Support Contracts
  - **Include vendor patching!**
  - Get a C-level on the hook
  - Backups and Data destruction

Anti-Virus

- Anti-Virus should be on **every single device** that could even *potentially* be a node on your network.
- Develop a **rapid deployment** mechanisms for virus pattern updates to all devices.
- Require A/V to logon to the domain/network
- Use multiple layers of defense
  - Different environments/platforms
  - Different Anti-Virus vendors

Encryption

- Management/Security **must** have the keys
- Create an infrastructure to manage keys
  - Get ready for PKI…
- Educate employees on when and how
- Make it easy to understand and use
- Only covers confidentiality (AIC)
- Performance assistance
  - IPSec off-load cards
  - SSL/VPN accelerators

Data Classification

- Create Data classification guidelines and standards that are easy to understand and use
- Publish on an Intranet for reference
- Classify all data, everywhere, all the time
- Make it part of the approval process
- Management sign-off

IDS, Proactive Scanning and Log Monitoring

- Integrity Analysis/Assurance
  - Tripwire, Cisco, AIDE, Intact, etc..
- Intrusion Detection Systems
  - ISS, Cisco, Dragon, Snort
  - HIDS, NIDS, MIDS
- Proactive Scanning
  - Regularly identify everything on the network
  - Only perform vulnerability scans on devices that can handle it
  - Scheduled vulnerability, port, and SNMP scans
- Log Monitoring
  - Event Logs
  - Syslog
  - SNMP

Awareness Training

- Mandatory training isn't well received
- Security can be boring, get someone with charisma and confidence
- Communicate the importance of security
- The most effective way to change culture
- Employee sign-off

Divide and Conquer

- Security Operations Center
  - 24/7 eyes and ears of Security
  - Threat and Vulnerability Analysis
  - Security Account and Device Provisioning
  - “War Room” - Incident Response coordination
- Security Review Board
  - Projects
  - Changes to Hardware, Software, Infrastructure…
  - Divestitures/decommissions
- Security Project Management Office
  - Security-related projects
  - Security Consultant participation in Business Projects

How to Stay Secure…

- **Get a Baseline Security Audit**
  - Whom do you choose?
  - How much do you spend?
  - What do you audit?
- **Get Involved in the "Industry"**
  - Information Security
  - Electric Power

Get a Baseline Security Audit

- Choose the right company…
  - Do your research
  - Industry knowledge is beneficial
  - A “Big-5” name doesn’t mean you are the best anymore
- Inform the Security and IT Staff
  - Let everyone know what is happening
  - Can significantly aid preparation efforts
- Prepare for the audit
  - Document every known risk; how and when you plan to fix
  - Identify gaps in knowledge of the security environment
  - Great reason to patch a few additional systems
- Schedule repeat audits
  - Keep the same company for consistency
  - Adhere to regular intervals

Get Involved in the "Industry"

- Industry seminars and user groups
  - Vendor user groups, Security and Energy Industry seminars
- Training and certification
  - Hackers never stop learning, why should your security staff?
  - Threat changes rapidly and requires current knowledge-base
  - CISSP, GSEC, etc…
- Participate in information sharing groups
  - InfraGard, ISSA, ES-ISAC , eUSA
- Read trade magazines and follow news
  - NIPC Watch, Energy Central Direct, CSO, CISO
- Challenge your vendors and partners
  - Pressure them for more secure products and partnerships
  - If they fail, don't be afraid to switch

Get Involved – Resources

- FERC – Federal Energy Regulatory Commission
  - http://www.ferc.fed.us/
- NERC – North American Electric Reliability Council
  - http://www.nerc.com/
- ES-ISAC – Energy Sector Information Sharing & Analysis Center
  - http://www.esisac.com/
- NIPC – National Infrastructure Protection Center
  - http://www.nipc.gov/
- CIAO – Critical Infrastructure Assurance Office
  - http://www.ciao.gov/
- CERT CC – CERT Coordination Center
  - http://www.cert.org/

Get Involved – More Resources

- InfraGard
  - http://www.infragard.net/
- ISSA – Information Systems Security Association
  - http://www.issa.org/
- SANS Institute – SysAdmin, Audit, Network & Security Institute
  - http://www.sans.org/
- Security Focus
  - http://www.securityfocus.com/
- Symantec Security Response
  - http://www.sarc.com/
- Internet Storm Center
  - http://www.incidents.org/
- X-Force Internet Intelligence Center
  - http://gtoc.iss.net/
  - http://www.iss.net/security_center/maillists/ *(subscribe to the Alerts)*
- Microsoft Security Center
  - http:/www.microsoft.com/technet/security/
  - http://register.microsoft.com/regsys/pic.asp *(subscribe to the Security Notifications)*

The End… Questions?

Contact Info:

Patrick Miller

patrick.miller@icctcorp.com

http://www.icctcorp.com

877.905.0209