CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2015 Colloquium
October 08 to 09, 2015
Lima – PERU

D2-03_01

Implementing Cyber Security in Five Steps

Germán Fernández
Belden
Spain
german.fernandez@belden.com

SUMMARY

The adoption of TCP/IP based technologies for Substation Automation networks and for WAN communications between substations opens a new range of cyber security threats. A good Cyber Security policy maintains the reliability and safety of Substation and Grid Operations.

Cyber Security has become a common term used to refer to protection barriers against threats coming from Cyber Space. But Cyber Security is much more than this simple concept. Cyber Security is a collection of measures adopted to prevent unauthorized use, malicious use, denial of use, or modification of information, facts, data, or resources. This means that we are not just talking about intentional attacks coming from outside our network. We need to establish preventive measures for internal attacks and unintentional modification of information or any threat that could lead to a Denial of Service of our communication network. In this collection of measures we can include devices, configurations, internal security policies and training. Recovery strategies after attacks are also critical to protect uptime.

The concept of Defence in Depth can be implemented by establishing policies and countermeasures at four different levels, Network, Host, Application and Data. It means each layer of protection is designed to address a specific type of threat. If one security measure is bypassed or fails, the next layer steps in to defend the system. In this paper we are going to cover some best practices to protect the network layer inside the substation.

We need to see Cyber Security as a rolling process and not as something static. Surrounding conditions may change, and we need to adapt our systems and policies to these changes. We will define five levels or steps of Cyber Security countermeasures with concrete recommendations to secure our network.

KEYWORDS

Cyber Security, Defence in Depth, Cyber Threats, Vulnerabilities, Substation Networks, Substation Ethernet Switches, Deep Packet Inspection, Firewalls

INTRODUCTION

Many factors have led to the new range of security challenges faced by electrical substations today. The adoption of new technologies – such as transmission control protocol/internet protocol (TCP/IP)-based technologies for both substation automation networks and wide area network (WAN) communications between substations – has opened these networks up to more cyber threats. A good cyber security policy, however, is a simple first step to maintaining the reliability and the safety of substation and grid operations.

Cyber security is often used to describe protection against online attacks, but a more holistic view of cyber security involves a collection of measures adopted to prevent unauthorized use, malicious use, denial of use, or modification of information, facts, data or resources. Cyber security not only refers to intentional attacks from outside the network, but also internal issues and unintentional modifications of information.

With both internal and external threat sources in mind, it is important to establish preventative processes for any issue that could lead to network downtime. These measures could include devices, configurations, internal security policies, and employee and contractor training. And since it's not realistic to assume all threats can be prevented 100 percent of the time, recovery strategies after issues occur are also critical to protect network uptime.

Historically, substation control networks were based on local connections and proprietary applications. Systems were designed for safety, reliability and ease of use, and security was not traditionally a concern of network managers or installers. But this approach is no longer valid.
Today's communications networks are characterized by the use of:

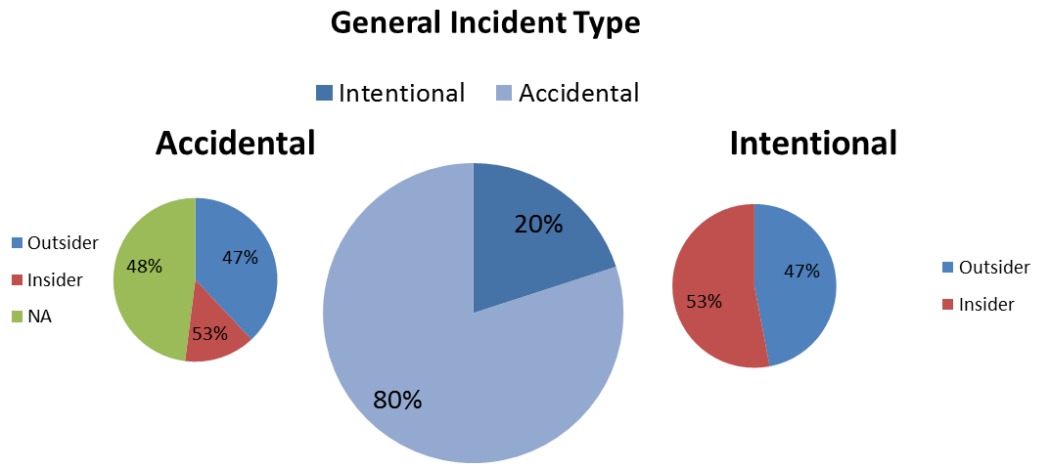
- Commercial off-the-shelf technology
- Ethernet and TCP/IP-based communications protocols
- Open standards, IEC60870-5-104 and IEC61850
- Integration of legacy industrial protocols (DNP3) and Modbus TCP
- Remote connections (multiple devices and mobility)
- Interconnection with company IT systems
- Use of public networks

The complexity of power grids has increased over the years. As they have become interconnected with systems across countries, it has made failures and mistakes more likely – and their potential impact greater in scope and cost.

ANALYSIS OF CYBER THREATS

Most network security incidents are accidental instead of intentional. According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) vulnerability analysis2, authentication flaws were the most abundant vulnerability type identified in 2013.

This liability is of particular concern because an attacker with a minimal skill level could potentially gain administrator level access to devices that are accessible over the Internet. Other common vulnerabilities identified in the analysis include factory hard-coded credentials and weak authentication keys.



Types of Incidents - Data Source: Eric Byres (Tofino Security)

Unintentional threats, such as equipment failures and employee carelessness, and deliberate threats, like cyber hackers and viruses, have different types of consequences. They impact information systems, network infrastructure management and power system assets differently. Due to the critical role the communications network plays in the operation and protection of the high voltage and medium voltage grids, a DoS attack may lead to service disruption and financial losses, as a result of repairs and equipment replacement.

There mentioned threats have different types of consequences for our Information Systems and the Network Infrastructure Management. All these consequences may have different impact in the Power System assets. Due to the critical role that plays the communications network in the Operation and Protection of the HV and MV Grids a Denial of Service may lead to a disaster in terms of Service Disruption (penalties, compensations,…) and Financial Losses due to repairs and Equipment replacement.

Cyber security is an iterative process – not static. As surrounding conditions or threat sources change, systems and policies may need to be updated to address those changes.

To understand this process, it's important to differentiate between risks, vulnerabilities and threats.

While a **risk** is the likelihood that something bad will happen that causes harm to an information asset (or the loss of the asset), a **vulnerability** is a weakness that could be used to endanger or cause harm to an information asset. A **threat** is anything (manmade or an act of nature) that has the potential to cause harm.

- **Preventive Security** controls are intended to prevent an incident from occurring. This means to reduce the number and type of Vulnerabilities and Risks.
- **Network Design Security** minimizes the Vulnerabilities and isolates them so if an attack occurs, it will not affect other parts of the network.
- **Active Security**, before and during the event, active measures and devices that will block traffic or operations not allowed nor expected in our network.
- **Detective Security** controls are intended to identify and characterize an incident in progress or after it by evaluating activity registers and logs.
- **Corrective Security** controls are intended to limit the extent of any damage caused by an incident. Need to build in protocols for retrofitting Preventive Security and the Network Design measures once Vulnerability is detected.

NETWORK BEST PRACTICES

Preventive Security - Physical

- Physical Perimeter Protection
- Access Register
- Secure Cabinets
- No External Drives/Ports in PC's in the Operational Network (e.g. USB)
- Avoid Labels with Information about the passwords and users or MAC/IP address/masks

Preventive Security – Logical

- Disable Console Ports after commissioning
- Passwords Policy (avoid weak passwords, force to change default password, personal user and password for outsourced services)
- Use of Radius, Tacacs+, LDAP, 802.1x servers for user validation and instruction filtering
- Limit Information in the Hello Banner via web interface, telnet or console port
- Limit Validation Attempts and inform of Validation failures
- Set up Users Profiles with different permissions
- Limit Traffic per Port (ingress and egress traffic)
- Disable Unused Ports (ports not used can be electrically disconnected)
- Block Unused Ports TCP/UDP Port of not used Services
- Use Secure Protocols: Block Telnet, HTTP, allow HTTPS and SSH. Use SFTP instead of FTP
- Configuration Files Backup Policy
- Port Security (IP Address)
- Define a set of SNMP Traps to be sent in case abnormal situation
- Configuration File Encryption

Network Design Security

- Redundancy Mechanisms (Device, protocols and media level)
- Establish Physical Conduits (limit the number of connections between zones)
- MAC Filtering (address and range of addresses) (limiting the type of devices to be connected)
- MAB: MAC Authorization Bypass for non 802.1x devices
- Only SNMPv3 because it is encrypted
- Use of MMS(less common) and only one management system
- Establish Logs Register-Alarms-Actions processes and policy with remote servers
- FW - Segmentation DMZ
- IP Subnets
- VLAN's Segmentation 802.1Q and QinQ
- Establish Logical Conduits to limit the traffic between zones
- Use of NAT 1:1 and 1:N to hide the local address map
- Include Tunnelling in the design for remote connections to avoid MiM(Man in the Middle)

Active Security

- Use of ACL's
- Layer 3 Firewall (IP Filtering, Stateful Inspection, Application)
- Include IP and MAC addresses in the same Firewall rules
- Dynamic ARP Inspection
- Encryption (SSH/SSL 128bit Encryption)
- VPN Tunnelling with dynamic encryption
- Port Destination Filtering (TCP/UDP)
- DPI (Deep Packet Inspection) Protocol Specific (Layer 7 Firewalls)
- Active use of Antivirus SW (Spyware, Malware, Trojans…)

Corrective Security

- Device Replacement Policy (SLA, Spares…)
- Configurations Parameter Backup effective policy
- FW Updates policy (measure the impact in the complete system)
- Define how to incorporate new countermeasures to new and existing systems

Detective Security

- Log File Analysis. Specific SW tools to analyse in conjunction the log files from all the network devices in the substation to check for attack patterns..
- Monitoring (IDS, traps from the NMS…)
- Periodical check of predefined configuration files with existing configuration files at the devices. (specific sw tool and database for file management)
- Pairing of MAC and IP addresses and check for any change in the pairs. (to avoid IP spoofing)

CONCLUSION

Substation cyber security requires vigilance against both accidental and intentional threats. An entire network can be protected by segmenting the network into smaller virtual local areas networks VLANs) with limited access points.

Following a Defense in Depth model allows for building in multiple layers of security protocols, so any system failure or breach results in limited damage, which can be controlled or managed more efficiently. Meanwhile, the large portion of the system remains protected and up-and-running

True Security Requires Vigilance

Precise knowledge of the network topology, protocols and type of traffic is absolutely essential for a reliable design of security policies and countermeasures. The network administrator must know how and where components are connected in order to allow the necessary conduits and establish the security zones.

Even electrical substation networks evolve over time, and documentation can easily become outdated. A good set of preventive countermeasures will force any new device connected to the network to be validated by an administrator and trigger a documentation process review.

Throughout a network's operational lifetime, it is necessary to carry out repetitive, but essential, maintenance tasks. For example, the threat of cyber-attacks means that responsible network administrators should change device passwords regularly, implement upgrades to fix bugs and maintain regular antivirus updates. An active Corrective Security plan is also needed to maintain the robustness of a network.

A few security generic measures that utility operators can implement include:

- Prioritize. Make sure your mission-critical systems are secure first.
- Create a culture of security. Keep teams informed and educated on security best practices.
- Update your existing risk assessments regularly, including both physical and virtual checks.
- Do not apply a one-size-fits-all solution across the entire IT and SCADA system. The threats, risks and goals of these systems are different, so the solutions should be as well.