NERC Lessons Learned:

"Risk of Internet Accessible Cyber Assets"

"Preparing Circuit Breakers for Operation in Cold Weather"

"Loss of Substation Data Circuits to SCADA"

"Firewall Failure After Time Limit Exceeded"

Donnie Bielak
Reliability Engineering

Published

- Title
  - Risk of Internet Accessible Cyber Assets
- Source of Lesson Learned
  - Western Electric Coordinating Council
- Date Published
  - July 24, 2018

Problem Statement

- Internet-connected capacitor bank was compromised by unauthorized internet users for seven months prior to discovery
- Access point installed with weak password by a previous SCADA manager and never turned over to new manager
- Information posted to Russian-based media site and was infected with ransomware
- Compromise discovered after device was unable to be accessed

Lesson Learned

- Device removed from service and performed forensic analysis to identify all malware
- Virus scan was also performed on all devices at the same site
- Logs reviewed on all of the devices to look for anomalous activity
- Other locations also scanned to determine whether they had similar installations or issues
- Cyber assets need to be properly installed and secured per policies and procedures

Published

- Title
  - Preparing Circuit Breakers for Operation in Cold Weather
- Source of Lesson Learned
  - Western Electric Coordinating Council
- Date Published
  - July 24, 2018

Problem Statement

- Two sequential B-phase faults occurred on a 500 kV line, apparently due to icing
- Three breakers failed, de-energizing an entire substation and tripping 1,150 MW nuclear plant off-line
- Breaker 1 opened properly for the first fault, but did not reclose correctly and was unable to respond to the second fault
- Breakers 2 and 3 failed to clear the fault quickly enough due to cold temperatures

Lesson Learned

- For Breaker 1, a defective motor contactor was discovered and replaced
- For Breakers 2 and 3, the manufacturer engineered a fix consisting of additional thermostatically-controlled cabinet heaters that prevent moisture from freezing inside the pneumatic control valve during cold weather conditions
- Breakers have several cold-temperature-related failure mechanisms
- Good practice to annually perform pre-cold weather checks for cold-sensitive components

Published

- Title
  - Loss of Substation Data Circuits to SCADA
- Source of Lesson Learned
  - Northeast Power Coordinating Council
- Date Published
  - August 7, 2018

Problem Statement

- During a scheduled transfer of its SCADA from the backup to the primary, all TelCo-provided remote substation data circuits lost
- After maintenance work had been completed, the company directed the TelCo to transfer all data circuits back to the primary
- The reconnection process failed resulting in a loss of operating and monitoring functionality for majority of substations
- Major network outage and multiple hardware failures within the TelCo's network
- All issues resolved in about 8 hours

Lesson Learned

- Schedule future SCADA data circuit transfers during daytime hours on business days
- Develop a script to disconnect and reconnect SCADA data circuits that splits the process into several blocks to mitigate risk of an outage to all of the TelCo-provided SCADA data circuits
- Collaboration with communication vendors who own and/or operate the circuits is essential

Published

- Title
  - Firewall Failure After Time Limit Exceeded
- Source of Lesson Learned
  - Midwest Reliability Organization
- Date Published
  - August 7, 2018

Problem Statement

- Firewall firmware security patch issued by the firewall vendor was applied to equipment, which unknown to all parties at the time, contained a process runtime limit of 213.5 days
- After reaching the 213.5 day limit of uptime, the entity experienced a loss of all SCADA-EMS RTU communications
- Network administrator attempted to failover to the backup firewall but both firewalls were experiencing the same firmware issue
- Two months prior to the event, the vendor had identified the runtime bug and notified their users via a “blog post”

Lesson Learned

- Rebooted the backup firewall and forced a failover to restore network traffic and RTU communications
- Entity scheduled proactive reboots of the control center firewalls and other affected firewalls
- Firewall firmware was upgraded to a new release
- Maintain network devices on a planned schedule in accordance with the latest vendor information, security bulletins, technical bulletins, and other recommended updates
- If available, entities should enroll in automated notification services for these updates

Links

- https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20180701_Risk_of_Internet_Accessible_Cyber_Assets.pdf
- https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20180702_Preparing_Circuit_Breakers_for_Operation_in_Cold_Weather.pdf
- https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20180801_Loss_of_Substation_Data_Circuits_to_SCADA.pdf
- https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20180802_Firewall_Failure_After_Time_Limit_Exceeded.pdf