Case Study

City of Raleigh

Public Utilities Department seeks insight into their security risks and measures

Damon Small - Technical Director

nccgroup

SITUATION

As a part of the critical infrastructure to provide water and waste services, the team responsible for the industrial control system (ICS) and supervisory control and data acquisition (SCADA) system wanted to understand their operational technology (OT) risk maturity level. Given the importance of providing stable utilities to the community, the City of Raleigh needed to remain fully functional while the assessment took place.

Challenges:

- Lack of visibility into the environment
- Ensure client remains fully operational during the time of engagement with no outages
- Increasing government regulations due to OT vulnerability in the industry
- Facilitate communication between client and third-party support vendor regarding information security

TASK

The City of Raleigh engaged NCC Group to conduct a Cyber Security Review (CSR) of their OT system. They wanted to understand how the OT systems were interacting with the IT systems and if NCC Group could detect interruptions between the two. During the engagement, the client became concerned about a critical radio frequency (RF)-based system which we worked to address as a specific portion of the assessment. It was later determined that Managed Detection and Response (MDR), and Security Improvement and Remediation (SIR) services would be ideal solutions to continually monitor and improve their OT and IT environments.

ACTION

Twenty-three detailed documents were received from the client that needed to be analyzed for accuracy. It was also essential to ensure the documents received were conducive to performing the review.

Action items:

- Coordinated with the third-party vendor to ensure the understanding of the environment was factually correct.
- Used twenty-three detailed technical documents to analyze past network data.
- Presented a series of workshops to discuss how control systems work and identify threat actors the company should be aware of.
- Gathered documentation to examine the client's technology infrastructure.

RESULTS

- Passive, packet capture (PCAP)-enabled vulnerability assessment methods allowed NCC Group to analyze OT devices without introducing the risk of service interruption.
- Counseled client on the importance of using mitigating controls to protect unsupported software.
- Created an understanding of the client's system, documentation, and established processes to keep information updated.
- Helped the client prioritize key business drivers for the next fiscal year.

AT A GLANCE

CHALLENGES

- Increase in industry vulnerability
- Lack of visibility
- Remain fully operational
- Work with a third-party vendor
- Government review processes

RESULTS

- Analyzed data while remaining fully operational
- Updated and protected unsupported software
- Secured documentation processes
- Prioritized budget

SERVICES RENDERED

- CSR
- MDR
- SIR

> "Just as we were beginning our engagement with NCC Group, the Colonial Pipeline attack happened, so we saw our review as being very timely. Our primary goal was to prevent these sorts of incidents from happening to our utilities. I feel better after working with NCC Group because we are better protected and are more equipped to safeguard our community from potential threats."
>
> - Client Security Manager

uscons-info@nccgroup.com www.nccgroup.com