CEDAR DESIGN CONSIDERATIONS

3/2/2023

Group 15: Bilal, Gent, Met, Thomas, Oluwatosin

Table of Contents

1 REPORT OVERVIEW

Creating a design consideration report is important given that it outlines the factors that need to be considered when designing and implementing a secure network and security infrastructure needed by CEDAR. This report provides a comprehensive overview of the factors that need to be considered to give CEDAR the systems it needs to safely continue operation and to fulfill all its business requirements. This includes server related considerations, meeting compliance, disaster recovery planning, and having the right access controls.

2 OUR DESIGN CONSIDERATIONS

After much research, we have highlighted a handful of design considerations that are important to review in building CEDAR and the infrastructure that it needs to remain operational. The Power Grid Control Center application setup is present at both our Oakbrook and Waukegan locations with Waukegan acting as our backup that has identical infrastructure and can immediately take over function in a matter of milliseconds should the Oakbrook location ever go down for whatever reason. Knowing this, it is important to note that whatever hardware, software, structure, or system that we have present in CEDAR's Oakbrook location must also be designed for the Waukegan location to have it fully equipped to take up the task.

2.1 Retaining the Solaris Server

A Solaris 10 server constitutes the core of the Supervisory Control and Data Acquisition system (SCADA), which directly communicates with the power grid components. The only issue with using a Solaris 10 server is that it already reached its end of life on January 1, 2021, which means that the standard support, updates, and patches have been stopped; The extended support however was extended till 2024 but the longevity and long-term efficiency of the SCADA system is crucial to the operation at CEDAR. CEDAR, have expressed its desire to keep its system in the Solaris 10 server environment. We intend to respect their decision, and our design suggestion would be to use a Solaris 10 container. Oracle Solaris 10 containers is a software that allows customers like CEDAR to move their application environment that uses Oracle Solaris on newer hardware. This means that a Solaris 10 environment can get new patches while running in Solaris Zones.

2.2 Windows and SQL Server

Another important part of our system that needs to be considered is the windows 2008 server that hosts the main application used by the grid operator and is also used to store all the power load, and consumption information used for customer billing. This server reached its end of life and extended support on January 14, 2020, which makes any updates and patches unavailable. Our proposed design for this is to upgrade to the latest windows server, which is the windows 2022 server, this server's mainstream end of life is not until October 13, 2026, with its end of extended support not until October 14, 2031, which gives us ample amount of time to decide to either migrate or upgrade to whatever the newest server at that time is, CEDAR has no objection to upgrading the window servers. The new server provides our network design with the option of multi-layer security, firmware protection, secure connectivity, and virtualization-based security. This upgrade also ensures that the grid can be easily accessed by operators, and customer information about energy consumption can be properly collected and collated.

There is also the Microsoft SQL 2005 server that is housed on the Windows 2008 server. This server reached its end of life on the 12th of April 2016; This means that using an outdated server might lead to further issues for the system application. The proposed solution for this is to update the SQL server to the most recent option, which is the Microsoft SQL 2022 server. Since we would be updating the Windows server it makes sense to also update the SQL server so that we do not run into compatibility and potential security vulnerabilities issues as that version of the SQL server is no longer eligible for technical support or security updates and patches. The newer SQL server is more compatible with our upgraded Windows server. It also has enhanced security with it being the most secure database over the last 10 years, provides business continuity through Azure, and has seamless data analytics amongst many other things.

2.3 Operating System and Workstations

In addition to what is needed for the grid management system, it is also important to consider upgrading the workstations that the grid operators would be using to access the grid application. CEDAR's workstation for accessing the grid is currently running Windows XP Pro. This along with CEDARs hardware has unfortunately reached end of life since the 8th of April 2024, which means that newly discovered bugs or security holes can neither be fixed nor patched making it open to vulnerabilities and exploits. It would also be incompatible with newer software. Our team considered upgrading it to the newest operating system that Windows has to offer which is windows 11 OS. We aim is to provide the grid operators with a workstation that has the most up-to-date, secure, and functional environment to carry out the operations that their job requires. Using Windows 11 will communicate very well with the upgraded Windows server.

2.4 Customer Relationship Management System

CEDAR has a custom customer relationship management system that is hosted on the three Windows servers in the Lombard location. Our design involves replacing the custom CRM system with Microsoft Dynamics 365 because a lot of hardware components that we would be upgrading to are also Microsoft products and it would make compatibility seamless. Dynamics 365 is a suite of solutions that helps to manage engagement with customers. It offers different products like Dynamic 365 sales, Dynamic 365 customer service and field service, Dynamic 365 customer insights, Dynamic 365 fraud protection, and others that can be important to the operation at CEDAR. With this upgrade, we can fulfill the accounting and customer billing, and customer service functions that the previous CRM was designed for.

2.5 SCADA

Considering that we have a SCADA system that is core to the operation at CEDAR, we must take extra measures to protect it as we cannot take any chances with malware attacks; Most technological devices or systems are susceptible to malware like viruses, worms, and trojans, and there is certain malware that specifically targets SCADA systems like Stuxnet, Havex, and Black Energy amongst other various SCADA targeting malwares. With this knowledge, we must be taking proactive steps to keep our SCADA system safe from possible attacks; We plan to implement security tools like SIEM, NGAV, IDS, and IPS systems.

All security measure is to ensure that signature-based detection, behavioral-based detection, machine learning, and AI-based detection is present in our multi-layer security solution, thereby limiting the possibility of attacks by malware and other malicious actors on our SCADA system.

2.6 Technical Access Controls

CEDAR has a lot of technical components that can be exploited by malicious actors so we must implement measures to control who can get access to any of our technical assets. There would be strict security measures to ensure that only authorized personnel can access, modify or carry out any operation on any CEDAR's technical asset; the initial operational structure provided by CEDAR already has firewalls that provide some level of security. In addition to that we would have NGAV, patch management, EDR, IDS and IPS systems, and SIEM on all systems and technical assets (our workstations, servers, routers, etc.). There also would be the implementation of different types of access control like role-based, mandatory, discretionary, rule-based, and time-based access control to ensure that all systems have multilayer security. The implementation of our design not only provides security, but also enforces detailed access log information, detailed audits, and report analysis, threat response, and ensures that the principle of least privilege access is strictly enforced at CEDAR. It was also mentioned that remote access to the grid is not necessary and that creating backdoors must be avoided. Having these controls ensure that the grid is secure from external threats, such as cyberattacks or unauthorized access. Restricting remote access, also reduces the potential attack surface, which can be a major vulnerability for any system.

2.7 Physical Access Controls

Physical security is just as important as cybersecurity. That is why physical access controls are necessary because CEDAR houses important assets in all three locations that we need to protect. There would be strict control measures to ensure that only authorized personnel can access the buildings, this would include locks, keys, access cards or employee cards, and biometric authentication; There would also be some perimeter security, surveillance systems, and security personnel must be present at all times. In addition to all this, we would also include having a thermostat to control the temperature and humidity of the rooms with SCADA as SCADA systems must be maintained under controlled temperatures.

2.8 Leaving PLUNC

CEDARs executives have cited trust issues over PLUNC and have opted to leave PLUNC altogether as part of their next phase. This would mean that CEDARs network would have to be rebuilt from the ground up. This adds a layer of complexity when redesigning CEDARs infrastructure and we have to analyze the business and technical requirements for the new network infrastructure as well as propose an implementation plan. This allows us to create a much more secure and efficient network that better caters to the needs of CEDARs business requirements.

2.9 Maintenance

The maintenance of all the components designed to make CEDAR functional is important to the overall health of CEDAR. This includes components like SCADA systems, servers, workstations, and customer service systems. Our design for CEDAR's infrastructure includes but is not limited to a quarterly maintenance check on the environment for at least 2 years after its implementation. We can always do a routine check, when necessary. It is also important that the end-of-life dates of our newly upgraded hardware and software are known so that they can be constantly upgraded at the appropriate time. With the kind of service that CEDAR provides, having a system down because of failure to update might have severe consequences on the entire operation at CEDAR. The CRM must be constantly monitored, and its reports must be regularly reviewed; Updates like security updates, patches, and bug fixes from the vendors and creators of the infrastructure systems must be followed up on and applied to CEDAR's system on a need-to-do basis. The dispatch trucks and their workstations must be constantly serviced and maintained to stay in top condition for customer service functions. Our design objective is to ensure that after designing and implementing, CEDAR as an organization can maintain and sustain the environment that they are provided with.

2.10 Compliance

CEDAR as an electric distribution company has some regulations and compliance that it needs to adhere to; Taking into consideration all the operations at CEDAR we have structured our design to be and remain compliant with every regulation that it needs to stay in business. As an electrical company that also, CEDAR is required to be compliant with the North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), Energy Policy Act of 2005, and Critical Infrastructure Protection (CIP). Other compliance that might be required includes Occupational Safety Health Administration (OSHA), Payment Card Industry Data Security Standard (PCI DSS), the Illinois Personal Information Protection Act (PIPA), and other state-level regulations that applied to CEDAR's operations. Aside from the electric distribution compliance (reliability and stability) that CEDAR must adhere to, it is also important that CEDAR is complying with standards to protect the privacy and security of its client data.

2.11 Disaster Recovery Plan

Having a thorough disaster recovery plan is essential for CEDAR given that they deal with critical infrastructure and that they have a lot of confidential data housed within its locations. CEDAR must be prepared to respond to a breach to get its operations running up again. Organizations that do not have a disaster recovery plan will often not succeed in reverting to their former business models and have the success that did they did prior. A detailed and efficient disaster recovery plan should include functional data backups for critical data with redundancy. These backups should be stored remotely to ensure security. Another part of the plan that is crucial is training employees and formulating guidebooks to direct employees during a disaster. This can help CEDARs team get back onto their feet and respond faster to any threats.

2.12 Logging

Logging should be implemented in CEDAR as well. These logs should be used for data aggregation and analysis. These logs capture all of the activity generated by all devices in the network therefore increasing security. It is an efficient way to also automate auditing. In the event of an attack, all the activities performed by an attacker will be logged and fixing the method of attack can be remediated. If hackers attempt to breach the network by scanning open ports or sniffing traffic data, that activity will be logged and reported to the appropriate team so that they may be able to respond to the issue. Logging will be limited to the administrative staff minimizing access to those who don't need it.

3 CONCLUSION

All of our design considerations consist of either implementing things that were not formerly present in the infrastructure and upgrading the components that already exist. They highlight the critical factors that need to be considered when revamping CEDARs infrastructure. Our team has identified a handful of important considerations. These include the use of a Solaris 10 container for the SCADA system, upgrading to the latest Windows and SQL server versions available, upgrading employee workstations to the latest hardware available, implementing technical and physical access controls, maintenance, compliance, disaster recovery planning, and finally logging. By implementing these design considerations, CEDAR will have a much more secure and efficient network that meets its business requirements, ensures that it is meeting compliance, and is well-prepared for any potential disaster.

REFERENCES

"14 Major SCADA Attacks and What You Can Learn from Them." *14 Major SCADA Hacks*, 23 Dec. 2021, www.dpstele.com/blog/major-scada-hacks.php#:~:text=14%20Major%20SCADA%20Attacks%20and%20What%20You%20Can,...%208%20German%20Steel%20Mill%20...%20More%20items.

"ASHRAE Recommended Data Center Temperature & Humidity." *AVTECH*, 9 Feb. 2022, avtech.com/articles/23418/ashrae-recommended-data-center-temperature-humidity/.

"One Flaw Too Many: Vulnerabilities in SCADA Systems." *Security News*, Trend Micro, 16 Dec. 2019, www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems#:~:text=It%20should%20be%20noted%20that%20SCADA%20system%20vulnerabilities,perform%20denial%20of%20service%20%28DoS%29%2C%20or%20steal%20information.

"Principle of Least Privilege Benefits." *Imprivata*, 31 Mar. 2022, www.imprivata.com/blog/what-are-the-benefits-of-the-least-privileged-principle#:~:text=Follow%20these%20best%20practices%20for%20the%20principle%20of,be%20modified%20or%20removed%20as%20needed.%20More%20items.

"Standards ." *NERC*, www.nerc.com/pa/Stand/Pages/default.aspx.

Corporation, Microsoft. "What Is CRM?" *Microsoft Dynamics 365*, dynamics.microsoft.com/en-us/crm/what-is-crm/.

"What Is Access Control?: Microsoft Security." *What Is Access Control? | Microsoft Security*, www.microsoft.com/en-us/security/business/security-101/what-is-access-control.

Compliance Corner, www.misoenergy.org/stakeholder-engagement/compliance-corner/#:~:text=Compliance%20Corner.

Farrelly, Jessica. "Types of Compliance Small Businesses Should Know About." *Electric*, 11 May 2022, www.electric.ai/blog/types-of-compliance.

Genea. "What Is Physical Access Control? - Modern Security Systems." *Genea*, 1 Feb. 2023, www.getgenea.com/blog/what-is-physical-access-control/.

Lutkevich, Ben. "What Is Access Control?" *Security*, TechTarget, 7 July 2022, www.techtarget.com/searchsecurity/definition/access-control#:~:text=The%20goal%20of%20access%20control%20is%20to%20minimize,to%20protect%20confidential%20information%2C%20such%20as%20customer%20data.

Nicaise, Vincent. "Stuxnet Computer Worm: What Legacy Today?" *Stormshield*, 18 Jan. 2023, www.stormshield.com/news/stuxnet-what-lessons-can-be-learned-twelve-years-on/.

Wangsness, Cole. “What Is a SCADA System and How Does It Work?” *OnLogic Blog*, 20 Sept. 2022, www.onlogic.com/company/io-hub/what-is-a-scada-system-and-how-does-it-work/.