ASSET INVENTORY AND CLASSIFICATION

Revision 1

2/19/2023

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

Table of Contents

1 EXECUTIVE SUMMARY

An asset inventory report is an essential part of maintaining electrical grids in locations across the nation. The company CEDAR (also known as the Cool Electrical Distribution and Redistribution is one of these locations that resides in the north side of Chicago. CEDAR houses its own management, has full time staff, houses various assets, and operates the power grid/power distribution in the Chicagoland area. This report provides CEDAR with a summary and analysis of their assets based on the information provided by the CEDAR team. In this report, the company's network infrastructure, physical infrastructure, data, and security will be reviewed. Hardware assets are put into a spreadsheet for each location that CEDAR has which is attached with this report. There are a handful of security risks that have been identified because of inventorying CEDAR's assets. Almost all of them are because of outdated hardware and software that is being used at each of CEDAR's locations. This hardware is considered end of life and is no longer supported by their manufacturers leaving them prone to be hacked into. They will need to be addressed in the future.

2 OAKBROOK PGCC

The Oakbrook center houses the main control center for the electrical grid. This grid is responsible for all the primary electric outputs for the citizens within the Chicagoland area. Enclosed within that system, Oakbrook will be used as the main power grid controller center. This building is considered a huge asset as it is the main control grid for CEDAR.

2.1 Non-Technical Physical Assets

When it comes to the physical assets of Oakbrook's location, the building itself serves as a physical asset. The building houses a total of 24 rooms with the presence of a warehouse, conference room, offices, cubicle spaces, telecommunication room, and various rooms for amenities such as restrooms and break rooms. The location itself does not house any physical security nor does it have any access controls. This poses a huge security risk and would need to be addressed.

2.2 Hardware Assets

Oakbrook's main control center houses a single firewall for traffic filtering, 60 workstations for staff to use running Windows XP Pro. These workstations will be running the proprietary HMI that serve as a control panel for the electrical grid for the grid operators. There are 2 servers located housing Oracle Solaris 10 servers used for the SCADA system. In the Oakbrook location there are 60 workstations running Microsoft XP Pro, support for which ended on April 8, 2014. This poses a huge security risk.

Given that all the software is outdated, there is an immediate need for upgrades.

2.3 Routers

The Oakbrook center has three layer three routers. R2 in this center is responsible for creating a point-to-point link from Oakbrook to the Waukegan backup center as well as an internet connection. This power grid control center also has an additional router to connect R2 to the admin and user network deeper into the main PGCC network and SCADA peripheral interfaces. The last router is for creating a WAN link from the SCADA interface to the CEDAR electrical power grid.

2.4 Firewalls

According to the provided documentation from CEDAR, there is one firewall present at the Oakbrook site. We will have to do a security assessment and vulnerability testing on this firewall and evaluate if we must upgrade it.

2.5 Servers

In the Oakbrook location, the PGCC uses two servers. These servers are the main form of control for the power grid. The following servers are used:

1. A Solaris 10 server which will be used to cover the core operations of the Supervisory Control and Data Acquisition (SCADA) system. Also, it will be used for direct communication with

other power grid components via MTU (Main Terminal Units). Through MTU, communication will be established with RTU (Remote Terminal units) and PLC (Programmable Logic Controllers) which are used to control the grid.

2. A windows 2008 server which uses MS SQL 2005. This server hosts the main application that grid operators will use. Also, it communicates with the previously mentioned Solaris 10 server. This server is responsible for archiving all data, notify operators, and transmitting any interventions to the Solaris server to issue on the grid. Housed within the Windows server is also all of the personal identifiable information of all the customers.
    1. The Windows 2008 server functions as the "Historian" for power load and consumption data and is utilized for billing and reconciliation purposes by both energy providers and customers.

2.6 Workstations

The Oakbrook location has 60 workstations. These workstations are in the office area of the Oakbrook building. All the workstations use Microsoft XP Pro which is outdated. Therefore, an immediate upgrade to these workstations is needed.

3 WAUKEGAN PGCC

The Waukegan center houses the backup control center for the electrical grid. In case of a shutdown in the main location at Oakbrook, Waukegan will be used as backup and provide full functionality. The Waukegan location serves as another huge asset which has two networks: Admin and User network and the Backup PGCC network.

3.1 Non-Technical Physical Assets

The Waukegan location has one building. This building, as mentioned before, will be used as a backup PGCC and a backup computer room. In total, the building has 17 rooms. The most important rooms being the computer room, Telecommunication Room, and Radio, Satellite, SCADA Control Room. Other rooms in this building are the Break Room and Locker Room, Electrical Grid Map Room, Cubicle Area/Support Staff, Office Space, and a couple of bathrooms and offices.

3.2 Routers

There are three routers at the Waukegan site:

1. The first router is an edge router and has two external links, one link to Lombard site (providing Internet to Waukegan) and another link to Oakbrook site. This router is also connected to the Admin and User network.
2. The second router is also an edge router and has a link connected to the CEDAR Electrical Power Grid. This router is also connected to the SCADA Peripheral Interfaces.
3. The third router is an internal router which is connected to the Admin and User network and the Backup PGCC network.

3.3 Firewalls

According to the provided documentation from CEDAR, there are no firewalls present on the Waukegan site. Implementations of firewalls will be necessary for the security of the GCC.

3.4 Servers

In Waukegan, the PGCC uses two backup servers. These servers are primarily used in the event of an outage over at the Oakbrook location. The servers are the exact same as the ones in Oakbrook and are the following:

1. A backup Solaris 10 server which will be used to cover the core operations of the Supervisory Control And Data Acquisition (SCADA) system. Also, it will be used for direct communication with other power grid components via MTU (Main Terminal Units). Through MTU, communication will be established with RTU (Remote Terminal units) and PLC (Programmable Logic Controllers) which are used to control the grid.
2. A backup Windows 2008 server which uses MS SQL 2005. This server hosts the main application that grid operators will use. Also, it communicates with the previously mentioned

Solaris 10 server. This server is responsible for archiving all data, notify operators, and transmitting any interventions to the Solaris server to issue on the grid. Given this server is a backup of the one found in Oakbrook, the Windows server also contains all of the personal identifiable information of all the customers.

3. The Windows 2008 server functions as the "Historian" for power load and consumption data and is utilized for billing and reconciliation purposes by both energy providers and customers. The historian sends frequent logs from the SCADA system to MISO.

3.5 Workstations and Printers

The Waukegan location has 20 workstations. These workstations are in the office area of the Waukegan building. These workstations are outdated, running on Microsoft XP Pro, which its support ended on April 8, 2014. Therefore, immediate upgrades need to be made to these workstations.

There are two router printers located in the Waukegan office space which are accessed by employees through their workstations.

4 LOMBARD

The Lombard location houses CEDAR's customer service center and repair dispatch team. Furthermore, the Internet connection comes through the Lombard location then it goes to the Oakbrook and Waukegan locations. The Lombard location is responsible for payment processing for customers. This is done with a T1 connection to JP Credit Card Clearing.

4.1 Non-Technical Physical Assets

The Lombard location has one building. In total, the building has 140 rooms. One room is a data center and two are bathrooms, the rest are offices for staff.

4.2 Routers

The Lombard location has one router which has connection to the Internet and also to links to Oakbrook and Waukegan. We will have to evaluate the security provided by this router and potentially upgrade it. There is also a T1 connection present from one of the routers to JP Credit Card Clearing for credit card payment.

4.3 Firewalls

According to the provided documentation from CEDAR, there is one firewall present at the Lombard site. We will have to do a security assessment and vulnerability testing on this firewall and evaluate if we must upgrade it.

4.4 Servers

Given Lombard houses CEDAR's support team and data center, it houses a total of five servers. These servers include a Linux server, Microsoft 2003 server, and three 2008 Microsoft Servers. These last three servers house the CRM system for payment processing.

4.5 Repair Dispatch Team

The Lombard location has 100 repair dispatch trucks and there is a laptop in each one of these trucks (100 mobile laptops) for service technicians to use. These mobile laptops are running Windows XP Pro which have been outdated for some time and an immediate upgrade needs to be done.

4.6 Workstations

The Lombard location has 150 workstations. These workstations are in the office area of the Lombard building. From the provided documentation, these workstations are outdated because they are running Microsoft XP Pro. Immediate upgrades need to be made on these workstations to remain secure.

5 CONCLUSION

This report presents an analysis of the asset inventory for the Chicago power distribution company CEDAR. We have highlighted the physical and network infrastructure, spoken on the security present at each location, and have taken into account the data of all three of CEDAR's locations. During our inventory audit, it was discovered that most of the hardware and software being used is outdated and poses a significant security risk, and therefore, we recommend upgrading them as soon as possible. Overall, this report provides CEDAR with an understanding of their assets for all three locations, their strengths, weaknesses, and areas that require immediate attention.