Ethan Massingill

Professor Davis

CSCI 570-01

4/8/2023

Research Facility

My facility considered a general research facility with a back outside area including a Wind Turbine. It does allow the public into the lobby with two public terminals and public wifi, however the rest of the facility itself needs to be secured other than authorized personal. For the public area special consideration will need to be considered to not allow the terminals or wifi to interact with other aspects of the network, and not allowing full access to the terminals themselves. Each personal should have an RFID badge with them that are used to access the secure areas with this in mind RFID skimming might be an attack vector that needs to be handled. Some of the risks to consider for this environment will be how to handle the outside area and keeping it secured physically. Due to the sensitive nature of the research other areas of consideration will be the device and user access along with implementing data loss prevention techniques. Likewise, the room housing the security and networking environment will need to be secured physically except for authorized employee access. Finally, because of the network needing internet access a DMZ should be considered for the sensitive servers and a forward-facing firewall for out of network traffic along with securing the network room itself, along with the ports. There are also several IoT devices such as fire monitors and LED lights that need to be secured properly.

I would generally want to start for securing this network with the physical side first. This building is a two building with an outside area. First thing would be to secure the outside area, where the wind turbine, power meter, and outside wifi, are connected. I would start with putting up a high physical fence with anticlimb collar, specifically a roller barrier placed at the top, and anticlimb paint which has been shown to stop attacks. For example a study published in 2020 by Sandia National Lab found that by applying the anticlimb paint was more effective than a barrier without it, with the subjects specifically stating that “the barrier was too slippery” ( Salazar) and that even with more people attempting to work together to climb over “…the coated barriers were much more difficult to defeat than the uncoated versions even with added help”( Salazar). Next would be to install the outside, power over ethernet, cameras to overlook the front entrance and wind turbine. These cameras would need to have motion recognition, and object detection especially near the wind turbine area. This would help not only detect a penetration and help deter attack, but also help in the recovery effort if something was to happen. This usage of smart tracking motion cameras has been used most recently and famously in the War in Ukraine where security camera footage helped piece together crimes committed against citizens in Bucha and identify the units responsible, specifically tracking their movements. (Al-hlou, et al). Because of the outside access point, I would need to turn off the SSID broadcast so that only the allowed devices can see the signal and it is not visible to the public, likewise I would need to lower the range so it does not leave the fenced area. The access point itself would need to use WPA2-Enterprise encryption, which complies with IEEE 802.11i standards. This would be one of the strongest modes of encryption available according to Chad Brooks an IT expert writing for business.com (Brooks). There would also be an RFID card reader located at the back entrance to the building with a mantrap to this outside area that would need to be physically secured, likewise the RFID and mantrap can be turned off and locked outside of operating hours. The power meter device would need to be physically encased in locked storage while still receiving the signal since it is wireless. For the wind turbine the power cables and data cables would need to be behind a physical lock and secured, along with the ladder for maintenance locked and secured correctly. For all the physical securing this is one of the most vital aspects even in the world of Cyber Security according to the New Jersey Office of Homeland Security which underlined the importance of this aspect stating.

“If an adversary has physical access to a space or network, all information systems and information are considered “fair game” and are vulnerable to compromise and theft. Systems and devices may be left behind and unattended outside the view of security cameras; screens may still be unlocked with access to files, network shares, and other resources; and sensitive or confidential data may still be open in plain view on the screen and can be captured, stolen, modified, and/or deleted.” (NJCCIC)

For the first-floor security I would need to make sure the reception area, and its devices, are only accessible through the employee door which has another RFID card reader to lock that door. Here, however, a mantrap would be implemented to only allow one authorized person through at a time while providing a screening area for the security team. Tim O’Leary describes how he installed mantraps to deal with a unique aspect for NATO facilities stating “One interesting project was setting up mantraps for strategic NATO facilities that were sealed from radio frequency (RF) waves. They were designed to be attack- and explosion-resistant and impervious to passing cryptographic RF snooping.” (O’Leary). This would allow my facility to monitor staff entering and exiting so that unauthorized personal will be unable to get passed the second set of door locks. For two public terminals along with the public wifi are on separate vlans compared to the rest of the network, however I would need to make sure to implement a captive portal, and client isolation so that someone cannot communicate with other clients on the wifi. This would help prevent lateral attacks from happening through the wifi and the spread of potential malware from this vector. For the public terminals specifically, they are meant to only allow users to view the research centers website, and videos. I would need to lock down the system access using Access Control List on these terminals, this would be done under a Role-based access for these terminals in the lobby. The importance of this feature will secure the terminals from interference and tampering and is widely used in the cyber security space and can even improve the network performance (7Security). For example, if someone tried to bypass the allowed areas it would give them a warning message that they do not have permission to access that part. I would need to make sure all the USB ports are turned off so that even if someone attaches an USB it does nothing. Physical locks are placed on the equipment itself to prevent theft and vandalism.

The lab itself contains a few company devices such as terminals and a printer. The terminals here have DLP policies on them along with employee authorized Role-Based access control. An example of how this would be used is it would give the Technician Bob only access to the areas on the terminals he is approved for, and only able to retrieve, look at, and touch data that fits within his allowed scope. This method has been proven to stop data leaks and other security issues, such as rapid elevation, using the principle of least privilege also known as Zero Trust. This policy was not used in the recent SolarWinds supply chain hack which allowed rapid unrestricted access once the network was breached. (Khare).

Inside the Lab employee area there is a separate server room where one of the terminals is dedicated to IT and houses the IDS monitoring software to watch the network and the traffic it contains for abnormalities. This terminal is located inside of the network room so that it is behind another RFID locked door secure from the other employees. The IDS system itself is one of the keystone aspects of protecting the entire network. Here also it monitors the DLP metrics that have been set up. Having this centralized collection area for network monitoring. For example, if another employee tries to extract a large amount of data at once that triggers the DLP anomaly alert it would log the event and allow a response from the security team. (7Security). On this terminal also would need to handle device logging, as all the authorized mac address devices are using the COPE method, which while could be more expensive it provides a higher security value to the facility. (Macpherson) Likewise housed in here are the network routers, switches, firewalls, and servers. These are all also physically locked behind closets along with a tripwire guarding the area. The firewall DMZ is configured to specifically guard the RADIUS/IOT server along with the database. The RADIUS server is used to verify that the badges have access to the specific areas which they are scanned. Ports on every device of this room are assigned port access security with only one mac addresses associated with the proper port. For example, if Carol scans a badge but does not have access to the IT area the RADIUS server will deny her access through the RFID lock. That way the port shuts down if someone connects an unauthorized device. For example, if Bob tries to plug in his laptop to the same ethernet cable to access the network it would disconnect this port and trigger an alert.

As far as the entire network it uses a firewall to access and process incoming and outgoing traffic towards and from the internet. Here is where NATTING takes place. Likewise, to secure the devices on the network further a centralized, such as Paessler PRTG Network Monitor, must be used. This will provide the proper SEIM which will help monitor and protect the full network. For example, if malware somehow infects one of the terminals the SEIM would trigger an alert and a playbook ran depending on the type of attack. This would provide the on-premises monitoring tool needed for the facility. (Brame) Access to the controls for the higher privileges will only be granted to the IT employees. The fire detectors and LED lights would need to be secured physically and in the correct places likewise, and a proper placement for the motion sensing light, with a anticlimb collar, inside the fenced in area to help deter intruders.

This is, of course, only a start of the security implementation. One of the key aspects that will also need to be completed would be proper security education and staff to monitor, guard, and respond to threats. Education itself for emerging threats and how to prevent them is key to every network and facility, especially one which involves industrial equipment such as the Wind Turbine. This would involve training sessions, audits, and staying up to ate on the threats. In fact according to mimecast a recent study showed that “human error (is) playing a part in so many security breaches – more than 90%...” (Mimecast). An example of this would include phishing simulation or having a pen-testing red team come in to test the network. With education in mind this is one of the most important aspects of securing the network.

Work Cited

Al-hlou, Yousur, et al. “Caught on Camera, Traced by Phone: The Russian Military Unit That Killed Dozens in Bucha.” *The New York Times*, The New York Times, 22 Dec. 2022, www.nytimes.com/2022/12/22/video/russia-ukraine-bucha-massacre-takeaways.html.

Brame, Daniel. “Paessler PRTG Network Monitor Review.” *Infrastructure Management* , PC Magazine, 31 July 2020, www.pcmag.com/reviews/paessler-prtg-network-monitor.

Brooks, Chad. “Wireless Security: How to Deploy WPA2-Enterprise.” *Wireless Security In The Enterprise: Deploying WPA2-Enterprise*, Buisness.com, 6 Mar. 2023, www.business.com/articles/deploying-wpa2-enterprise-encryption/.

“The Importance of Physical Security and Its Implications on Cybersecurity.” *Garden State Cyber Threat Highlight*, NJCCIC, 14 Jan. 2021, www.cyber.nj.gov/alerts-advisories/the-importance-of-physical-security-and-its-implications-on-cybersecurity.

Khare, Shweta. “How Just-in-Time Privilege Elevation Prevents Data Breaches and Lateral Movement.” *Help Net Security*, Help Net, 1 Sept. 2022, www.helpnetsecurity.com/2022/09/01/how-just-in-time-privilege-elevation-prevents-data-breaches-and-lateral-movement/.

Macpherson, Shawn. “What Are the Benefits of a COPE Mobile-Device Strategy?” *The Checker*, DEVTRA Inc, 20 June 2019, www.thechecker.net/stories/blog/what-are-the-benefits-of-a-corporate-owned-personally-enabled-cope-mobile-device-strategy.

Mimecast. “Cybersecurity Training for Employees.” *Mimecast*, Mimecast, www.mimecast.com/content/cyber-security-awareness-training-for-employees/.

O'Leary, Tim. “Mantraps: One Door at a Time | Locksmith Ledger.” *Mantraps: One Door at a Time*, Locksmith Ledger International, 4 Jan. 2023, www.locksmithledger.com/electronics-access-control/article/21288760/mantraps-one-door-at-a-time.

“The Purpose of Intrusion Detection & Prevention Systems.” *Information Security Blog - 7Security*, Seven Security Group, 10 June 2021, www.7sec.com/blog/the-purpose-of-intrusion-detection-and-prevention-systems/.

Salazar, Jeremy. “Summary Report for the Anti-Climb Coating Test Project: Simulated Attack and Skid-Resistance Tests.” *Summary Report for the Anti-Climb Coating Test Project: Simulated Attack and Skid-Resistance Tests (Technical Report) | OSTI.GOV*, USDOE National Nuclear Security Administration (NNSA), 1 June 2020, www.osti.gov/biblio/1763556.