Miles Anderson

November 29, 2023

Port of Antwerp Case Study - Cyber-Physical Breaches

Cyber-physical threats refer to an attack that uses a combination of cyber technology and physical action to impede the options of a physical space. Between the years 2011-2013, one of the earliest cases of a cyber-physical breach occurred at the Port of Antwerp. Through organized plotting, illegal activities, and hacking devices, the scheme on the Port of Antwerp went unnoticed until 2013, and the culprits succeeded with little to no consequence.

Contributing Factors

There are several factors that made the Port of Antwerp a vulnerable target to the cyber-physical breach. Firstly, the Port of Antwerp is a shipping port. Shipping ports are hotspots for crime such as the smuggling of narcotics, illegal immigration, and piracy (Kirkpatrick, n.d.). However, the Port of Antwerp is much different from the average shipping port. Specifically, the Port of Antwerp is in the top 20 largest shipping ports worldwide, containing water systems that lead into the heart of Europe (Kirkpatrick, n.d.). I rank this as the number 1 contributing factor because vulnerability to crime in this port is much more likely due to the massive size of the port making it more difficult to notice discrepancies within cargo or inside the workplace. Cyber attacks in particular require a keen eye to detect early, and the size of this port makes challenging

to detect the slight errors that indicate the beginning of a cyber attack. To mitigate the risks caused by the size of the shipping port, more personnel and cyber technology will be needed in order to keep track of all containers and stop crime before it occurs. I believe the second biggest contributor to the cyber-physical attack is the PIN numbers of the cargo containers. Once the criminal gang gained access to the PIN, they were able to manipulate all data about the containers and run their crime syndicate through the port. To mitigate this, a container's drop off location and date should not be affected by its PIN. There should be multiple other codes linked to the container's information, as well as two-factor authentication in order to make changes to aspects such as drop off date, time, and location.

"Pwnie"

"Pwnie," pronounced "phony," refers to a hacker device that uses keylogger technology and is used to record information such as login credentials, bypass network defenses, and transmit data to control systems (Kirkpatrick, n.d.). In the Port of Antwerp breach, pwnies, along with other surveillance devices, were used to conduct the attack. Once deployed, the criminal gang running the scheme gained complete access to cargo containers by pulling their PIN numbers, and were able to smuggle drugs, manipulate the pickup date and location of the containers, and send their own drivers to revive the smuggled goods (Kirkpatrick, n.d.). Although the pwnies are physical objects, they were not noticed inside the workplace whatsoever. This is because the pwnies are disguised as regular surge protectors and internet routers (Kirkpatrick, n.d.). Hidden in plain sight, authorized workers had no idea there was malicious technology inside of their workplace. The Port of Antwerp being such a large and detrimental shipping port likely made these pwnies even harder to notice. In order to mitigate

against a pwnie, workplaces should keep count of exactly how many surge protectors, internet routers, and similar devices present in their workplace. Devices should be labeled, and a daily count of these devices should be taken at least once each day. This way, devices placed without authorization can quickly be discovered and discarded. This may be a timely and tedious task, but it would be the most effective way to avoid a foreign device such as a pwnie from infiltrating the workplace.

Cyber Security in Associated Organizations

The fact that an enterprise's cyber security resources alone may not be enough to defend against cyber attacks is indubitably true. In reality, all companies and organizations associated with an enterprise must have secure cyber defenses as well. If an associated organization is compromised to a cyber attack, it is likely that information from other companies will be stolen and used in harmful ways. To mitigate such instances, companies should be careful what information they share with one another. Confidential information in particular should be shared under high discretion. Additionally, enterprises should not associate with other organizations who do not have adequate cyber security defenses. Before exchanging any information, companies need to verify exactly what type of protections they have in place in order to defend against cyber threats.

Cybersecurity and Physical Security

One of the main factors that made the cyber-physical breach on the Port of Antwerp possible is the physical break in. The criminal gang planned and successfully conducted a

physical break in on the Port of Antwerp, planting their pwnies and other surveillance devices to gain access to the PIN numbers and control of containers (Kirkpatrick, n.d.). One of the reasons cyber attacks are so dangerous is that they can be done anonymously and from a distance. The criminal gang took a big risk of breaking into the port in person, and potentially could have compromised their entire operation. If the proper security measures were in place, it's possible that this scheme could have been thwarted in its tracks during the time of the break in. As a cyber security professional, avoiding situations such as these are the reason why I would care for and prioritize physical security so much. In order to mitigate physical risks, proper personnel and technology need to be used on a 24 hour basis every day. Well trained security guards should be in place, rotating in and out on their shifts at all times. Panic buttons, which are buttons that can be quickly pressed to alert authorities in the case of an emergency, should be abundantly available around the workplace. As far as other technology goes, surveillance cameras are essential. They need to be high quality and placed correctly throughout the workplace to ensure there are no blind spots. The correct cyber defenses should be in place so the surveillance feed can not be tampered with or shut down by an outside source. Motion detecting cameras should also be used to alert authorities of unauthorized activity in the case of a physical guard not being present.

Conclusion

Cyber-physical threats can be extremely destructive, even more so than your average cyber attack. It is important to balance cyber security and physical security in order to mitigate cyber-physical threats. The scheme occurring at the Port of Antwerp started in 2011 and wasn't discovered until 2013 (Kirkpatrick, n.d.). It is impressive, concerning, and somewhat scary that

this threat was present for so long while going under so many people's noses. It is essential for workplaces to be thoroughly searched for any foreign objects and unauthorized changes within the network to catch signs of tampering early on. Cyber security professionals will continue to use the cyber-physical breach that occurred on the Port of Antwerp as an example, and will learn from the mistakes made there to create more secure workplaces in our society today.

References

Kirkpatrick, Charles. *Port of Antwerp Case Study - Early Example of Cyber/Physical Threat.* (n.d.). https://docs.google.com/document/d/1aTbWd_H_HEfFTixruiTwmJVERE5_HEkcNIZmYi6pchI/edit#heading=h.s44548ln3mw.