

Trinity Salva

Professor Kirkpatrick

November 23rd, 2025

CYSE 200T

Port of Antwerp Cyber-Physical Case Analysis

The Port of Antwerp attack happened because criminals used hacking, phishing emails, and weak physical security to steal containers from the port. This paper explains what caused the attack, what a “pwnie” device is, how companies can protect their supply chains, and why physical security is important.

Question 1: Contributing Factors

What caused the attack to succeed?

The Port of Antwerp attack happened for many different reasons. One reason was that the port relied a lot on computers to track containers, but the security on those computers was not strong enough (Kirk, 2015). Criminals first used spear-phishing emails to trick workers into clicking fake links. This let the attackers into the system because employees did not realize the emails were dangerous.

Another problem was the PIN number system the port used. Each container had a PIN, and if someone had the PIN, they could pick up the container. When the criminals stole these PINs, they could pick up containers without being stopped.

The port also didn't have good monitoring on its networks, so the attackers stayed inside the system for almost two years without getting caught. The port was huge, with thousands of people coming in and out every day, which made it easier for criminals to move around without being noticed (Kirk, 2015).

Criminals also used tools they bought from the dark web, showing how easy it is today for people to buy hacking programs (Symantec, 2014).

To stop attacks like this, companies should train staff about phishing, use better passwords and multi-factor authentication, watch their networks closely, and separate important systems from less important ones.

Question 2: A Pwnie & How to Mitigate

What is a pwnie device and how can organizations defend against it?

In this attack, criminals used a device called a "pwnie." A "pwnie" is a small device that looks like a normal object, such as a power strip or router, but it secretly steals information. The criminals in this case placed pwnies in the port offices. These devices recorded what workers typed on their computers, including usernames and passwords, and then sent the information back to the criminals (Kirk, 2015).

To stop this type of attack, companies should protect their buildings better. Only trusted employees should be able to enter sensitive areas. Workers should check equipment often to make sure nothing strange has been plugged in. Companies should also use stronger passwords, multi-factor authentication, and software that warns them when an unknown device is connected.

Another important defense is teaching employees what these devices look like. Many people don't realize that a pwnie can be hidden inside something normal, so training can help workers spot suspicious objects early. Companies can also make rules that employees must report anything unusual they see. Even small things like a cable that wasn't there before could be a clue that someone is trying to break in. Good communication and awareness can stop attacks before they happen.

Question 3: Protecting the Supply Chain

How can companies better protect their supply chain?

The Port of Antwerp attack showed that even if one company has good security, another company it works with might not. Ports work with many partners, like trucking companies and shipping companies. If one partner has weak security, attackers can use that weakness to break into the whole system (Fortinet, 2014).

To protect the supply chain, companies should check the cybersecurity of the partners they work with. They should make sure partners follow rules like the NIST Cybersecurity Framework. Important information like PIN numbers should always be encrypted. Companies should also share information about threats so everyone knows what to watch out for. Working together helps everyone stay safer.

Another way to protect the supply chain is to limit how much access each partner gets. For example, a trucking company should only be able to see the information it needs, not everything in the system. This is called "least privilege," and it helps keep hackers from moving around too

easily if they break into one partner's network. Companies can also set up monitoring tools that watch for strange behavior, like someone logging in at weird times or trying to access files they normally wouldn't use. If a problem is detected early, companies can shut down access before the attackers steal anything. Finally, having a shared emergency plan helps all partners know what to do, who to call, and how to respond if something goes wrong.

Question 4: Physical Security Mitigation Strategies

Why does physical security matter and what actions help reduce risk?

Cybersecurity is not only about digital tools, it also involves protecting buildings and equipment. In the Antwerp case, the criminals entered the offices and planted pwnies. If the port had stronger physical security, the criminals might not have gotten inside (Kirk, 2015).

To improve physical security, companies should use ID badges or fingerprints to let people into sensitive rooms. They should use cameras and alarms, lock their networking equipment in secure cabinets, and require visitors to sign in and be escorted. Checking equipment often can help find any device that shouldn't be there. These steps make it much harder for attackers to sneak in without being noticed.

Conclusion

The Port of Antwerp cyber attack shows how dangerous it can be when cybersecurity and physical security are weak at the same time. Criminals used phishing, weak PIN systems, and secret devices like pwnies to steal containers for almost two years. To prevent attacks like this, companies must improve their cybersecurity training, protect their physical buildings, and make sure their supply-chain partners follow good security rules. Understanding this attack helps us learn how to better protect important places like ports in the future.

References (APA)

Fortinet. (2014). *How European drug traffickers used cyberattacks to steal from container*

shipping. Fortinet Blog. <https://www.fortinet.com/blog>

Kirk, C. (2015). *Cybercrime at the Port of Antwerp*. [Case study provided in class].

Symantec. (2014). *Industrial cybercrime and the rise of targeted attacks*. Symantec Security Response.