TRANSIT CYBERSECURITY: BRIDGING THE GAP

Faith Group's Cybersecurity Expert Chris Kadlick provides insight into security, cyber hacks, and how they can be prevented.

Password Tips

Use Password Phrases, with letters (upper and lower case), numbers, and special characters. Doing this, you don't have to remember a lot. Here are some examples.

2021Lindsey@)@! – 15 characters (special characters, female name, numbers), and if I read the online password chart correctly, this would take 2 trillion years to crack.

3##HappyDays4$$ - 17 characters (easy to remember, pick a number, use shift twice on the same number, capitalize the first letter of 2 simple words, pick another number and then shift twice again.

Chris Kadlick, CISSP
Sr. IT Security Consultant

Why is the Transit Market so vulnerable to cybersecurity hacks as opposed to other markets?

CK: Often Transit systems have run on legacy mechanical and electrical systems that at one time may have been manually operated and now have some type of automation to remove the 'people' component from flipping a switch or turning a valve. This is a slimmed version of the actual process, but the goal is automation, speed, cost savings, functionality, and process and manufacturing improvements, to name a few. There are many benefits to automating the Industrial Control System (ICS), but unfortunately there are some challenges with the technology being used to handle this, with the lack of cybersecurity being the most prevalent factor.

If ICS or Critical Infrastructure Markets follow secure cybersecurity best practices, conduct proper audits and assessments, conduct routine scans for vulnerabilities, and mitigate those issues when discovered, have a proper patch management program in place, and do all the "right" things they still have a probability for compromise, but the key is to make it so difficult that the adversaries move on to easier targets.

How are Cybersecurity hacks unique to the Transit Market?

CK: Transit Market hacking by cybercriminals is not unique and is in fact quite common. "According to the X-Force Threat Intelligence Index 2020, IBM X-Force Incident Response and Intelligence Services (IRIS) reported that the transportation sector was the third-most attacked in 2019."[1]

The industry, in general, uses archaic systems either in a Supervisory Control and Data Acquisition (SCADA) or ICS and now Industrial Internet of Things (IoT). These types of systems are typically not included, not capable, or too sensitive sometimes to be included in the patch management programs for organizations to keep updated and, therefore, serve as easy (relatively speaking) targets to go after.

It is not just these underlying systems that pose the largest risk as these systems do not generally contain user populations. It is the upper network connected layers where the infiltration happens, and then these lower layers become the soft spot.

Attackers could potentially cause serious damage to systems and people if the right controls are not in place. Often ICS's will have secondary controls in place when logical controls fail.

[1] https://securityintelligence.com/posts/securing-travel-transportation-operations/

So any company that uses internet access is open to be attacked?

CK: Yes, any and all are vulnerable, but it is not so simple to say just because you have an Internet connection, you are going to be hacked. Also, the transport mechanism is not the vulnerability but rather certain security configuration layers need to be in place to create the total overall security solution. A threat and vulnerability assessment (TVA) should be performed to identify and remedy any of these risks.

How damaging can a cyber attack really be?

CK: A good hacker can pretty much destroy everything for most businesses. Very large companies could survive major attacks, but the small and medium-sized are truly very vulnerable. If a hacker wanted to destroy a company they would compromise your network, gain entry, and not do ANYTHING for months until they know they have presence beyond your disaster recovery and backup period. At that point they will start the attack, and this way if you try to recover, guess who is STILL going to be there? The Hacker! Also, keep in mind Hackers or Advanced Persistent Threats are often well funded and very determined.

To date, there has only been one confirmed cybersecurity hack related death. This happened September 2020 at a German hospital after they succumbed to a ransomware attack. And other ICS hacks in the past that could have potentially caused the death of others, as I stated earlier this is often not the main goal.

What options do Owners have to prevent attacks?

CK: The first step would be performing a Threat and Vulnerability Assessment (TVA), which is an assessment of an organization's cybersecurity posture to detect and categorize and prioritize known vulnerabilities and threats using a variety of tools with an end goal of building a targeted plan for the mitigations of those threats and vulnerabilities. Password management, updating operating systems, firewall protections, event monitoring/alerting, Intrusion Prevention System / Intrusion Detection Systems, information security & remote access policies (VPN access controls), dual factor authentication, and inventory management, are some of the controls that should be implemented to help prevent an attack like this from happening.

Since Covid-19, Cybersecurity attacks are up 400%. In one day, 80,000 attacks are accounted for.

We also partner with Penetration Testing firms to provide a holistic view into your network reliability. Penetration Testing acts out actual attacks on your system to find deficiencies and identify pain points. Testing is an excellent way to have your network 'hacked' by cybersecurity professionals without suffering the consequences from a breach of your network and allows your organization to have, common, intermediate, or advanced threats and vulnerabilities repaired and remediated, depending on the agreed upon contract with the penetration engagement company before succumbing to the same from an adversary.

Say a company had a firm come in and perform a Threat and Vulnerability Assessment (TVA), is that good for say, the next 5 years?

CK: No, performing a TVA every 5 years would be ludicrous. I would suggest performing a TVA no less than every 2.5 years, and that is bare minimum! Technology changes so fast. Most should have penetration testing done every 1-1.5 years as well for medium sized organizations and up. Smaller companies are targets like everyone else, but on a much smaller scale. They are usually subject to malware or ransomware and not necessarily "cyber attacks" like the one the water treatment plant experienced.

The Cost of a Breach

These are some of the worst Transit cybersecurity breaches to-date.

In late 2016, riders of San Francisco's Muni transit system rode for free for a weekend, after a ransomware attack against the San Francisco Municipal Transportation Agency (SFMTA). The attackers used a variant of the HDDCryptor malware to infect 2,112 computers, encrypting their data and preventing them from operating normally – holding them to ransom for 100 bitcoin ($73,086)

In August 2020 Southeastern Pennsylvania Transportation Authority was hacked and it took down its real-time bus and rail information for two full weeks.

In 2017 Sacramento Regional Transit (SaRT) suffered a ransomware attack that crippled its website and destroyed data. Researchers have also previously proven hackers could take over the brakes and controls of vehicles.