Common Threats, Risks, and Mitigation Methods to ICS's

Joshua Lane

2/24/2019

The most common threats or the ones that are noticed and reported the most are incidents with malware and virus outbreaks (3). That would make viruses and malware the biggest threats to industrial cyber systems. According to Kaspersky, 53% of the incidents reported in interviews with multiple companies were due to viruses and malware which was usually downloaded to the system through spear phishing attacks (8). The second biggest threat to industrial cyber systems is a targeted attack more commonly known as "Advanced Persistent Threats (APT's)" which affected over a third of the companies interviewed (8). Despite humans being the weakest link in the cyber security chain and causing most cybersecurity breaches, these companies were not concerned enough with the risk their own employees pose to their infrastructures. Human error was only the sixth biggest concern, under such things as threats from third parties in second, and ransomware in fourth (8). Internal threats are the most impactful because of the lack of security on the inside of industrial cyber systems.

The risks to industrial cyber systems include but are not limited to "loss of life, long lasting impact on the environment, … fines from regulators, customers, or partners who have been put at risk, loss of product or service…," and company closure (3). Each of these may apply to one or more types of industrial companies. The average annual business financial loss due to an ICS cybersecurity breach is $347,603 which includes direct and indirect financial consequences (9). That amount of money going towards something else in these companies would allow for many more companies to thrive, ultimately boosting the economy.

Mitigating some of these risks can be addressed through planning cyber systems out to be more secure. Constantly keeping operating systems up to date is an area where quite a few companies were lacking (14). Older versions of operating systems often have easily exploitable vulnerabilities which can be determined quickly by any hacker or virus/malware. There is also a critical need to educate staff about common cybersecurity threats and risks through training (14). With educated staff, statistically a third of those incidents would most likely not have happened in the first place. The difference in the costs, both financial and other, would be astronomical with that large of a percentage of incidents removed. The lack of knowledge about what these kind of mitigation methods can do, and the financial costs have deterred a lot of smaller companies from effectively seeking out training programs (15). When the weakest link is simply unprepared, it creates a huge gap in internal security, and this is a problem that needs to be addressed because of the impact ICS cybersecurity breaches can have.

References

Business Advantage. (2017). *The State of Industrial Cybersecurity 2017* [PDF File]. Retrieved from https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf