2d Lt Marvin

CTC 7

In this “smart” technology revolution we are “marry[ing] the digital world with the physical action to better enable” the activity [1]. A clear case for this union is in the manufacturing industry. The manufacturing industry is embracing IoT devices in two main ways: digital supply networks and sensors. Digital supply networks use data from various points in the supply chain to inform the other points in how to make more optimal resource management decisions. There is risk though is that the data from one of these points have been altered by a malicious actor and leads to counterproductive decisions. This may not be causing physical damage, but it is hurting the company fiscally. With sensors there are risks because often sensors are not made by the company using them. Vendor vetting is crucial in the connected environment. You must make sure that the company selling the sensors is embedding security and access controls. If they aren’t then you are just increasing your attack surface exponentially.

This leads me to my vision for how the “smart” revolution is changing cyberwarfare. IoT devices augment the size of the battlefield in proportions that were unprecedented by the introduction of any other technology. In 2016 hackers were able to use millions of network connected devices to perform a Distributed Denial of Service (DDoS) attack that created a substantial outage for a European internet service provider [2]. In 2017 we saw the emergence of ransomware software that was able to worm its way onto corporate networks through connected devices at the periphery. These attacks are mainly external but as companies create larger networks of devices inside their domain hackers will look for inward attacks that could “potentially take control of manufacturing plants, transportation and logistics systems, and other operational centers.” In summary we can like cyberspace to the chain mail of a night. The more chain that these devices add the more likely there will be chinks in the armor.

Sources

1. Deloitte. (2018, February 27). Cybersecurity in the Age of Smart Manufacturing. Retrieved October 28, 2018, from <https://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/>
2. PwC. (2018, April 4). IoT risk and the smart factory: Building cyber resilience. Retrieved October 28, 2018, from <http://usblogs.pwc.com/industrialinsights/2018/04/04/iot-risk-and-the-smart-factory-building-resilience/>