LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 11
Date: November 13, 2017

Manufacturing and Industrial Sectors Are Cybersecurity Targets

Industrial and Infrastructure Networks are Prime Targets for Attackers

- Operational technology networks are used with specialized Industrial Control Systems (ICS) to monitor and control physical processes, such as assembly lines, mixing tanks, and blast furnaces. These networks are ripe targets for adversaries, according to a new study from industrial cyber security company CyberX.
- A full story link to the report is in the references below.
- Many of these networks are exposed to the public internet and easy to crack using simple vulnerabilities like plain-text passwords.
- A lack of even basic protections like antivirus can enable attackers to quietly perform reconnaissance before sabotaging physical processes.
- Once attackers get into an OT network, it's relatively easy for them to move around and compromise industrial devices.
- Motives range from criminal intent to operational disruption and even threats to human and environmental safety.
- In the report, Omer Schneider, CEO and co-founder of CyberX states, "We don't want to be cyber Cassandras—and this isn't about creating FUD—but we think business leaders should have a realistic, data-driven view of the current risk and what can be done about it."
- CyberX analyzed production traffic from 375 OT networks worldwide across all sectors. It finds that a third of industrial sites are connected to the internet, making them accessible by hackers and malware exploiting vulnerabilities and misconfigurations.
- More than three out of four sites have obsolete Windows systems like Windows XP and 2000, leaving them vulnerable to destructive malware such as WannaCry/NotPetya, Trojans such as Black Energy, and new forms of ransomware.
- Nearly three in five sites have plain-text passwords traversing their control networks, which can be sniffed by attackers performing cyber reconnaissance and then used to compromise critical industrial devices. In addition, half of the sites don't have any AV protection.
- Almost half have at least one unknown or rogue device, and 20 percent have wireless access points, both of which can be used as entry points by attackers.
- In addition, 82 percent of industrial sites are running remote management protocols like RDP, VNC, and SSH. Once attackers have compromised an OT network, this makes it easier for them to learn how the equipment is configured and eventually manipulate it.

- To demonstrate these concerns, Thehill.com recently published an article titled, “Feds Warn About Cyberattacks on Energy, Industrial Firms” (article link in references below)
    - The Department of Homeland Security and the Federal Bureau of Investigation issued a joint statement on Friday, warning of an increased danger posed to infrastructure sectors by a malicious "multi-stage intrusion campaign," which the agencies warned had successfully compromised several of their security networks.
    - The analysis (from CERT) points to cyber-attack campaigns going on since at least May of 2017 that the agencies said have been targeting the aviation, energy, and nuclear industries.
    - The agencies did not name any specific networks that had been compromised by the attacks.
    - Hackers reportedly used emails and malicious websites in a phishing campaign to obtain the credentials necessary to access and sabotage the networks.
    - According to the report, the campaign’s first focus was on "staging targets," third-party and peripheral organizations tied to the primary targets, which hackers then use to house their malware for attacks.
    - The agencies said that the hackers were targeting the company-controlled sites of specific agencies to access information on equipment and organizational designs and "control-system capabilities" that could be used to further harm the organizations.
    - The new revelations of hacking attempts represent an escalation of initial threats identified by the agencies in an earlier report provided to Reuters in June, which identified a narrower set of nefarious activity targeting energy, nuclear, and manufacturing sectors.

Takeaways

- We don’t hear about network compromises or network breaches involving the industrial and manufacturing because they do not have a duty to disclose to the public
- Trust me when I tell you that they are being attacked and often, especially cleared contractors, for intellectual property.
- Many in these sectors argue that they don’t have anything of value. I hope this podcast has changed your mind.
- If you don’t know where to begin, I suggest NIST’s Cybersecurity Framework Manufacturing Profile to perform a level of self-assessment, then perform and external penetration test. Links to these are in the references below.
- After that, I strongly recommend a third party to perform a risk assessment based on the ISO 27001 risk based framework.

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC’s security services, he is also the practice lead for the organization’s incident response, forensics, and litigation support practice.

References:

https://cyberx-labs.com/en/home/

http://thehill.com/policy/cybersecurity/356540-feds-warn-about-cyber-attacks-on-energy-industrial-firms

https://www.us-cert.gov/ncas/alerts/TA17-293A

http://www.reuters.com/article/us-japan-mitsubishi-digital-realty/japans-mitsubishi-u-s-partner-to-invest-1-8-billion-in-data-centers-media-idUSKBN1CQ02T

http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

https://www.iso.org/isoiec-27001-information-security.html