THE STATE OF IIoT SECURITY

SUMMARY

Without a doubt, the Internet of Things (IoT) and Industrial Internet of Things (IIoT) are two of the most popular topics regarding global digitization and optimization of industry operations and personal tasks. Most publicity around these subjects discusses the immense potential IoT and IIoT can bring to the public and businesses around the world. However, great opportunities are usually followed by significant threats. No exceptions here, as security and cybersecurity are undoubtedly the main challenges to be overcome to realize the full global potential of IIoT.

Before we go into more detail, let us be clear that IIoT is a subcategory of a broader term - IoT, so they share many similar concepts regarding security, however in this article we will focus more on the cybersecurity of Industrial Internet of Things, as it is the market where Teltonika Networks has the most focus at the moment. You can find out more about IIoT and its technologies, challenges, and benefits in another Industry Insights article by clicking here.

IIOT SECURITY THREATS ARE REAL

The numbers associated with cybersecurity and cybercrime markets are astounding; according to Bromium Inc. cybercrime economy has grown to $1.5 trillion dollars annually. On the other side, the spending for cybercrime prevention will result to cybersecurity market reaching $300 billion by 2024 as estimated by Global Market Insights in 2019. These numbers sound so extraordinarily that we must break down the potential loss areas for businesses. So, according to Accenture, the main components of a cybercrime related loss consist of business operations time lost due to malware attacks and loss of information which accounts to 43 percent of total losses. Now, let us take a better look at some of the most impactful cyberattacks on IIoT deployments.

STUXNET

One of the most famous IIoT cyber-attacks happened in 2007 when an Iranian engineer planted the Stuxnet virus at an Iranian nuclear research facility in Natanz. Stuxnet is a malicious computer worm, designed to spread itself throughout the whole computer network and to look for specific programmable logic controllers (PLCs). Then it introduces infected rootkit onto the PLCs, making them act in a harmful manner while reporting to system operators that all operations are normal. Without major international scandal, Stuxnet has caused at least a thousand of nuclear enrichment centrifuges to spin so fast they ruined themselves and infected over 200 000 computers in the process.

INDUSTROYER

On December 17th in 2016 a cyberattack on Ukraine's power grid has caused massive power outages, leaving almost 3 million inhabitants of its capital Kyiv without electricity for an hour. As later documented by ESET – this was a premeditated and purposeful attack to test the capabilities of malware known as Industroyer. It has exploited legacy industrial protocols which were created without much attention to cybersecurity because they were never designed to be used in a system which is connected to the Internet.

MIRAI

Another famous network security breach is known as The Mirai – a botnet created by Paras Jha, an undergraduate student from New Jersey. The concept behind Mirai is brilliant: it searches the global web for devices with open Telnet ports and attempts to take over control by using 61 standard username/password combinations. Once the device is accessed, it is added to the virtual army of Mirai botnet which acts as a centrally controlled collection of connected devices. Later, these devices can be utilized to launch DDoS attacks during which the target server is bombarded with web traffic until it's overwhelmed.

These three attacks are very different, but they teach an important lesson – even the smallest detail or least significant piece of equipment in IIoT deployment is a potential security risk. Even more, all of these attacks were preventable – Stuxnet and Industroyer both exploited lack of virtual and physical network segmentation whereas Mirai would have been much less effective with more attentive password management by the users of devices and device manufacturers.

WHAT CAN BE DONE TO STAY SAFE?

There is no single device, protocol, functionality, or topology to negate all cybersecurity threats in an IIoT environment. The most critical first step is to recognize the paramount shift in the way we use and control all infrastructure, as we merge legacy devices with state-of-the-art connectivity gateways and big data cloud platforms. System architects must continuously track and evaluate their system security and have contingency plans if something goes wrong. IIoT movement will result in billions of connected devices around the globe, and all of them can be a potential security risk. Let's take a look at a few steps to minimize significant cybersecurity threats.

DEVICE CONNECTIVITY LAYER SEGMENTATION

Traditionally, internal firewalls are used to protect networks and IIoT environments. However, the number of connected IIoT devices is rapidly increasing. Such devices are also going beyond traditional network topology, communicating not only internally but also having direct channel to the Internet cloud platforms, meaning that protection at a single point such as core switch is not enough. Some IIoT infrastructure developments would require investments of astronomical proportions if all the IIoT connection points were covered with separate firewalls.

Moreover, policy management and configuration across hundreds, possibly thousands of firewalls create an almost unmanageable situation. This issue was highlighted by The Target breach in 2013 when a group of hackers compromised point of sale (POS) systems of the retailer using vulnerabilities in their HVAC systems since they shared the same network. One way to solve this is device layer micro-segmentation which with the help of VLANs and ACLs ensures that particular type of IIoT equipment will not have access to the portions of the network which is not required for their operation. The great thing about this is that segmentation is done in software and operates at the device connectivity layer, meaning that if the device moves, the policy goes with it with no need to reconfigure.

EASY PASSWORD MANAGEMENT

Password management is an obvious first step when ensuring network security. However, the Mirai botnet has highlighted that even today, there are millions of connected devices with standard or easy to crack passwords just waiting to be hacked. All equipment, which is connected to the Internet must have strong and periodically changed admin passwords to prevent unauthorized access. To address this, Teltonika Networking devices are programmed to demand a change of the standard password during initial setup and an active password attempt counter blocking login attempts after fifth incorrect combination. Besides, Teltonika Remote Management System provides convenient password generator tool which allows to generate random or defined passwords and enforce all the routers and gateways monitored with RMS with the new credentials. You can check a separate article about the security of Teltonika Remote Management System (RMS) here.

ADVANCED FIRMWARE SECURITY FUNCTIONS

Many professional IIoT deployments are done with tools that are not up to the task. The conflict between procurement departments, operational technology (OT) and IT departments result in choosing incorrect, usually less expensive devices. Later, cost savings can result in damages larger than the savings. Such situations can easily be addressed by using professional connectivity hardware, such as gateways and routers which have advanced security features embedded in their firmware. These traditionally include multiple supported VPN services for encrypted communication, robust firewalls, and active DDoS prevention mechanisms. Teltonika Networks specialize in products that are designed for IIoT mission-critical communication; you can browse our portfolio of secure and reliable routers & gateways here.

FINAL THOUGHTS

The future of IIoT is both bright and scary at the same time. One thing is apparent; nothing will stop increasing digitization and interconnection of devices, infrastructures, and platforms. IIoT Security is a task that cannot be solved with a single product, function or technology. It is a constant process of minimizing risks and as technologies evolve so do cybersecurity threats. Security of hardware, firmware, and software is one of the key focus areas for Teltonika Networks product development. Our gateways and routers are used in the most sensitive connectivity infrastructures across the globe. If you want to find out how we can address your IIoT security challenges – contact us.