http://cyberparse.co.uk/2016/09/22/laser-printers-to-nuclear-plants-threatened-by-weak-iot-security/

Laser Printers to Nuclear Plants Threatened by Weak IoT Security

22/09/16

NEWS ANALYSIS: The biggest single problem for security of the Internet of Things is that for the most part there isn't any and most of the things that need securing can't be readily updated to include it.

SARATOGA, Calif. —It's probably impossible to accurately state how many "things" comprise the internet of things (IoT) in enterprises around the world.

Even best guesses are almost certainly wrong for the simple reason that until recently no one has even tried to count them.So let's agree that the number is significant, so large that some estimates place the total IoT traffic on carrier networks may be more than half of all traffic.Contrary to some popular conceptions that the IoT is made up of internet-enabled refrigerators and toasters, in reality the most connected to the IoT are so mission critical that they may be more important to your business than the workstations that you probably spend far more time and effort to secure. Depending on your business, they may be the numerical control machines in your manufacturing plant or perhaps even the automated forklifts that are being deployed in your warehouse. Or perhaps worse, the things that could be attacked might be the printers in your office. Or they might be something really big and scary—such as a nuclear power plant.

I spoke about these possibilities with James McNiel, CMO of network management and security company NetScout. McNiel was a keynote speaker at the NetEvents global press and analyst summit here. He said that one of the major problems that's currently below the security radar is ransomware being used not as a way to encrypt files, but instead as a way to prevent access to critical IoT devices.

“How much is it worth to a hospital to regain access to their blood gas analyzer so they can do surgery,” McNiel wondered.Unfortunately, the potential cost to the enterprise by attacks on its devices is significant. McNiel reminded me that the Stuxnet attack by the United States and Israel against the Iranian nuclear efforts was ultimately and IoT attack.

There, the Stuxnet worm drove the Iranian uranium centrifuges out of control while reporting normal operation to the operators.While Stuxnet was effective in delaying the Iran’s nuclear program, the code escaped into the wild, where it’s available to anyone who wants to modify it as an attack against any type of device controller.

There, the goal may not be to spin centrifuges out of control, but rather to implant software that sends a copy of all data handled by specific things to the party that launched the malware. Or it may be a ransomware attack that will make the thing unavailable until the ransom is paid.The amount of damage that can be done to an organization is hard to estimate, but there are examples. McNiel suggested that malware sent to a printer, for example, could result in a copy of every document being printed being sent to a competitor or to a nation-state trying to steal intellectual property.Or it could be used to infect an automated forklift or inventory barcode reader to tell someone else everything that’s in your warehouse, which items move the fastest, when there are peaks in demand and even where the items are shipped.And that’s just scratching the surface.The obvious question then is given that these devices are not secure and for the most part can’t be made secure, what do you do about it? For starters, when you buy new devices, specify that they must have some level of security, even if it’s just WPA2 encryption on WiFi.The next thing you need to do is protect your existing devices so that it’s harder to break into them. McNiel suggests that this can be accomplished by protecting the network segments the devices connect to. He said that it’s also important to monitor them.”You need to look for anomalies,” McNiel said. He said that there are other means to protect your devices, including deception, so that a hacker or the malware that’s inserted on your network can’t tell whether it’s found the real device, or a simulation, such as a honey pot, which is a simulated device, frequently running on a server, that appears to be an inviting target, but instead is designed to trap the intruder or the malware.When you find anomalies, you then

need to decide what’s causing it.

But if it’s malware and it’s not preventing access to the device, then the next step is to monitor the device for exfiltration of data.
If you find that, you can block the outgoing data and then examine the malware to see where it’s trying to transmit that data and what kind of data it want to send. With that information, you may be able to take further action such as blocking incoming connections from that site.But despite your best efforts, the bad guys will still get into your network. “You need to recognize when the device is legitimate and when it’s not,” McNiel said, adding that even with good security, your devices will be compromised.

That means it’s always necessary to monitor those devices closely, so you can take corrective action before it spreads or gets worse, he said.