Physical Cybersecurity: Securing IoT in Your Enterprise

Abstract: The Internet of Things is creating new business opportunities and opening new risks. There are more devices creating and transmitting data than there are people connected to the internet. But these devices can be used in unintended and dangerous ways. In this world of the Internet of Insecure Things, it is easy to overlook which devices are connected and which are transmitting information without your knowledge. You need to understand what devices are connected and how this connection could affect your intellectual property, customer data, and company's reputation.

Businesses are going through a revolutionary shift in their processes; connecting devices, sensors, actuators and data to enter the world of the Internet of Things (IoT). IoT is poised to supercharge the economy, enabling new business models and applications, and has become an integral part of today's workplace. This transformation and explosive growth is not without risk. IoT devices open a new threat vector that is putting intellectual property, customer data and your company's reputation in jeopardy.

Enterprise IoT

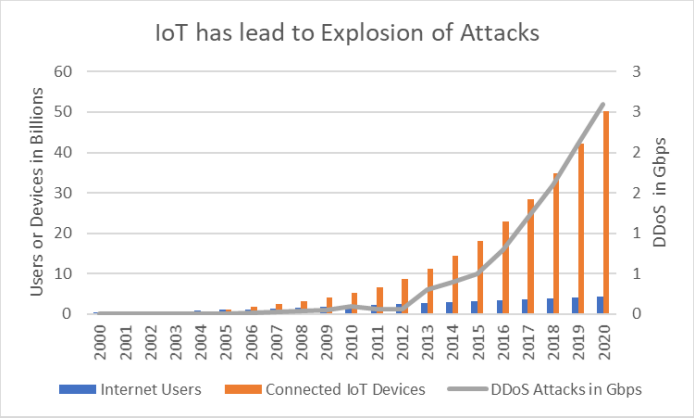
It's expected by the end of 2017, IoT will be adding nearly $2 trillion to the world economy in goods, services and business efficiency[1]. From omni-channel retail shopping to enhanced manufacturing flow and improved customer satisfaction in banking and healthcare, IoT devices are a part of every industry and location. By utilizing these new connected technologies, businesses can get more done with less effort and connect with their customers on a whole new level. And since most of the IoT devices require little to no set up, there are no barriers to businesses using IoT when upgrading or implementing their systems. Simply plug and play.

Risk of IoT

IoT devices and services enable us to interact with our environment in new ways, but with this convenience comes risks. Connected devices are opening new threat vectors by putting company data, personal identifiable information and intellectual property in jeopardy.

In addition, IoT devices themselves are open to compromise. In October of 2016 Dyn, a Domain Name System (DNS), was attacked by multiple distributed denial-of-service attacks (DDoS attacks), causing major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.

Ping bots on compromised IoT devices orchestrated the attack. Dyn estimated the attack involved over 100,000 malicious endpoints with an attack strength of 1.2 TB. With 8.4 billion devices (and growing), brute force attacks carried out by IoT devices can pose a massive risk to companies' services and sensitive data, even if only 1% of devices are susceptible.



[1] http://www.gartner.com/newsroom/id/3598917

Your company could also be at risk from compromised IoT devices.

Let's consider Target's recent point of sale terminal breach. It began after an HVAC contractor's credentials were compromised[2]. Once the first credential passes that barrier, a hacker will work their way horizontally and vertically until they're able to acquire valuable company assets.

IoT device security is notoriously poor, in part because manufacturers can't be relied upon to build them securely. These devices are already inside the firewall — the virtual barrier around the enterprise's network — and blocking the attacks can be an overwhelming challenge.

To defend against these devices, we need a paradigm shift in how we think about protecting the logical assets of a company. You can no longer just looking at protecting your cyber assets with traditional security applications like firewalls, IDS, and DLP. You must broaden your view to include the physical realm and become aware of all connected devices entering your enterprise, any of which may lead to data theft.

Different industries are using the exploding IoT market in diverse ways and each has their own inherent risks.

Banking

Retail banks have been using an early form of an IoT device for decades: the automated teller machine (ATM). Since their widespread deployment, ATMs have been making banks far more efficient by removing the need for long wait times to see a human teller. With the widespread use of online banking, retail banks are again looking at IoT technologies to enhance the user experience and make their branches more efficient. Banking will continue to evolve as the Internet and the IoT continue to affect our daily lives.

But with the adoption of IoT in retail branches, banks need to be aware of the additional security implications. Not only do they need to watch for card skimmers at ATMs, but they also need to be aware of how the newly adopted devices expose their customer's information on the network.

Retail

Retailers are investing in IoT technologies, such as automated inventory verification and sensors on shelves, to create a seamless customer experience across all platforms. By addressing supply chain performance, with real-time visibility enabled by automation and IoT technology based analytics, retailers are enabling superior customer experiences and location-based marketing efforts.

For retailers, the immediate hurdle to overcome is how to manage, analyze and act on the reams of data pouring in from all connected devices without exposing their customers, or leaving their supply chain open to hacker infiltration. Many attacks have

[2] http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

targeted retailers, including Target, Home Depot, Kmart, etc. IoT devices are one more threat vector that hackers can use to target retail companies.

Healthcare

The use of IoT in healthcare will radically shift how medical professionals gather information and interact with their patients, from remote monitoring with smart sensors to medical device integration. It has the potential to not only keep patients safe and healthy, but also improve how hospitals manage inventory of vital equipment and medicine, as well as delivery of physician care.

Healthcare IoT isn't without its obstacles. The number of connected devices and the tremendous amount of data they collect can be a challenge for hospital IT staff to manage and secure, especially if the data is being exchanged directly between IoT devices.

Manufacturing

Manufacturers across all areas —automotive, chemical, durable goods, electronics, etc. — have invested heavily in IoT looking to see benefits in efficiency and cost reduction. Manufacturers are currently using IoT to track assets in their factories, consolidate their control rooms, and increase their analytics functionality through predictive maintenance.

To do this, manufacturers are connecting legacy systems to the IoT network wherein they'll share data and control. These smart sensors and smart robots can then act with little supervision during the manufacturing process.

But by connecting these devices, companies are exposing themselves and their systems. Hackers can enter the networks through unsecure IoT devices, allowing the theft of intellectual property and exposing industrial control systems to interruption. These systems are timed to run in a certain order at a certain time, and any interruption can result in a disruption on the line leading to significant loss of product and revenue.

Transportation

IoT is dramatically accelerating the pace of innovation in the transportation industry. Soon our automobiles will be smart devices on wheels. Already, automobiles built after 2010 include numerous connected systems, providing drivers with the ability to listen to satellite radio, use smartphone apps, navigate roadways, request roadside assistance and diagnose problems remotely. Tesla models can even be upgraded wirelessly.

As transportation becomes more connected through IoT, a coordinated system designed to get everyone safely to their destination on time will emerge. However, this dependence on technology and connectivity opens vehicles to potential hackers. The hacking of a Jeep Grand Cherokee[3] demonstrate that the risks of hacking are very real, especially as more and more vehicles become part of IoT. It's one thing for a computer to crash, and another when it's your car.

[3] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Physical Cybersecurity Attack Lifecycle

Initial Compromise

Hackers want access to private company information and data to gain access through holes in network security. Brute force methods—such as a dictionary attack—take time and sophisticated tools to carry out. A much easier method is using social engineering, such as a phishing attack, or just walking in through the front door.

Gaining physical access is often considered a top priority for a hacker when trying to breach a defense-in-depth solution. Security professionals recognize that protecting computers and networks from physical access can be extremely challenging.

Consider the breach at Sony[4], where compromise was through physical access. That access likely happened because someone on the inside helped. Physical cybersecurity breaches, including those stemming from inside jobs, are difficult to contain and successfully recover due to evidence tampering or simple removal.

Once the hackers enter your building, there are any number of things they can do, like installing an infected USB drive, connecting key loggers, setting up rogue listening devices, or firing up rouge access points. Then, they'll infiltrate, all by detecting a user's access credentials.

Establish Foothold

Establishing a foothold ensures the hacker has complete access and control over the initial victim's computer. After testing the stolen credentials, the hacker will confirm they can gain access from outside the network. They then begin mapping out the network and security, much like compiling a treasure map. While a hacker may be looking for a specific set of data, they will take the opportunity to map the entire network and sell the additional results.

Escalate Privileges

To take over the network, the hacker will need to obtain more control and dive deeper into the system. One method is through privilege escalation in which the attacker uses any error or flaw in the system, either vertically or horizontally, to obtain extra privileges not

[4] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12

intended for the infected user. Specifically, they will be looking for credentials or privileges that will allow Admin access for precise parts of the networks or servers.

There are two directions a hacker can take for escalating privilege: Vertical and horizontal. Vertical privilege escalation, also known as privilege elevation, is where a lower privilege user gains access to functions or content reserved for higher privilege users or applications. Horizontal privilege escalation occurs when a normal user accesses functions or content reserved for other normal users.

Move Laterally

Hackers usually do not land in the exact spot of their target. Thus, they need to move laterally to find the key pieces to complete their mission. Once the attacker has an established connection to the internal network, they seek to compromise additional systems and user accounts. Because the attacker is often impersonating an authorized user, evidence of their existence can be hard to see. In this phase, they will move from the entry point to their final goal.

Data Theft

Now that the hacker has access to your complete network, they will exfiltrate any of the data that could be of value, such as company intellectual property, customer information, or sensitive data that could damage your company's reputation.

Legacy Systems Inefficiency

IoT devices are entering the enterprise and extending attack surfaces to attack paths unavailable in the past. We already know that gaining physical access is often a top priority when attacking a defense-in-depth solution. Access Control systems and connected cameras can see what someone is doing in real-time, but can't distinguish what radio frequencies are operating just outside a company's windows, or what IoT devices may be connecting to the network without authorization.

IoT devices and sensors are based on common hardware and software stacks running open source operating systems and network stacks. Manufacturers leave services running to make it easier to upgrade and "future proof" their products. This can also make a hacker's job extraordinarily simple as they can use the same tools and defaults set by the manufacturer to gain access and exploit IoT devices.

Buildings, automobiles, refrigerators, light switches and other hardware last a long time, decades even. They typically require little maintenance, and are rarely replaced until repair bills exceed value, or until they fail. IoT software and hardware is disposable, usually without provisions for upgrading. In fact, it's a common expectation among customers and manufacturers that IoT components will be replaced after 5 years. This expectation leads to functional devices that are exposed to unpatched vulnerabilities over time.

Modern devices are increasingly being connected daily to multiple networks beyond corporate control. Compromised devices effect every network they are credentialed for, not just where the breach originated. A single breach has an exponential ripple effect on customers, employees and shareholders when protected information is compromised.

IoT connectedness expands the threat surface, creating exponential complexities while magnifying the probability that a single failure turns into a cascade. Traditional threats may affect a single system, or set of systems, but the advent of IoT connectedness changes the calculus of a cascade failure. This means *all* connected cars are crashed, not just one. Once inside a network, traditional cybersecurity devices are not effective against IoT breaches. Cybersecurity needs to begin at the physical perimeter of a network.

Mitigate IoT device threats

Physical security is important to cybersecurity. We need to maintain a physical perimeter to mitigate the exposure risk of IoT in the enterprise space.

Here are some steps you can take to protect your enterprise from the new attack vectors created by the Internet of Things.

1. **Asset inventory** – Identify, track and profile your IoT endpoints.
2. **Separate out the trusted and untrusted** – Deploy Wi-Fi networks that are separate and specifically for employee devices and guest use.
3. **Perform Trust evaluation** of new IoT devices before deployment.
4. **Keep an eye out for unknown IoT devices** in your environment with sensors that monitor the radio frequencies.
5. **Use a risk driven strategy for IoT projects**, asset and function based. Best defense is to implement a pervasive and mature cybersecurity policy based on latest industry security standards and practices. Understanding both strategic risk and operational risk.

You need to build a secure environment based on your risk tolerance and be aware of third party products and services coming into your company.

IoT compromises can start out innocuous, but can quickly escalate into a serious threat. You need 360º defense in-depth awareness of your space. Detect all devices that come into the premises. Prevent unauthorized devices before they can breach a secure zone. Monitor with zone-based defense by flagging known and unknown devices.

Inpixon Indoor Positioning Analytics can help you create situational awareness in a security dome. Keep an eye on all the IoT devices in your premises. Your security dome safeguards intellectual property, customer information, and ensures your company's reputation protected. Let's make sure security isn't an afterthought.

Visit us today! www.inpixon.com/IPA