The Top 5 Misconceptions of IoT Network and Device Security

portnox™

Introduction

The Internet of Things Promise

The Internet of Things (IoT) describes an interconnected system of standalone devices, which communicate and transfer data within the existing internet infrastructure, providing greater insight and control over elements in our increasingly connected lives. With an estimated 30 billion[1] connected devices to be deployed across the globe by 2020, the promise of a global Internet of Things is fast approaching, posing a whole new level of threats to connected organizations.

[1]Source: IDC, May 2016

The Rise of IoT devices used in Organizations

With time IoT devices will become more intuitive and efficient than we ever thought possible and by 2020 it is predicted that there will be 7.3 billion devices installed in organizations[2]. This also means more opportunities for hackers to find new ways of using IoT devices for malicious purposes against corporate networks. Cyber attacks are not new to IoT devices, but as they become more deeply interwoven into our lives and societies, it is becoming increasingly necessary to step up and take cyber defense seriously.

The Rise of IoT Device-Based Attacks

To a potential attacker, a device presents an interesting target for several reasons. First, many of the devices will have an inherent value by the simple nature of their function. A connected security camera, for example, could provide valuable information about the security posture of a given location when compromised.

Hackers are already using IoT devices for their malicious purposes in multiple types of attacks on networks and servers. DSL, DDoS and bot attacks in 2016 have proven that there is no shortage of opportunities that hackers are willing to exploit.

[2]Source: Gartner, November 2015

The Lack of IoT Device Regulation

IoT device vulnerabilities are unlikely to disappear anytime soon. Researchers James Scott and Drew Spaniel point out in their report, "Rise of the Machines: The Dyn Attack Was Just a Practice Run", that IoT related security vulnerabilities represent a classification of threats that we are just beginning to understand.

Scott & Spaniel are adamant that the lack of regulation on IoT device manufacturing has little to do with the vulnerability of the devices and more to do with economic trends:

> *Regulation on IoT devices by the USA will influence global trends and economies in the IoT space, because every stakeholder operates in the United States, works directly with United States manufacturers, or relies on the United States economy.*
>
> *Nonetheless, IoT regulation will have a limited impact on reducing IoT DDoS attacks as the United States government only has limited direct influence on IoT manufacturers and because the United States is not even in the top 10 countries from which malicious IoT traffic originates.*

Attack 1

Manipulation of Connected Cars

Security experts Chris Valasek and Charlie Miller grabbed headlines with their research on the vulnerability of connected cars when they hacked into a Jeep Cherokee using a laptop plugged into the vehicle's diagnostic port. This allowed the team to manipulate the cars headlights, steering, and braking.

Attack 2

Compromising Medical Devices

In April 2014, Scott Erven and his team of security researchers released the results of a two-year study on the vulnerability of medical devices. The study revealed major security flaws that could pose serious threats to the health and safety of patients. They found that they could remotely manipulate devices, including those that controlled dosage levels for drug infusion pumps and connected defibrillators.

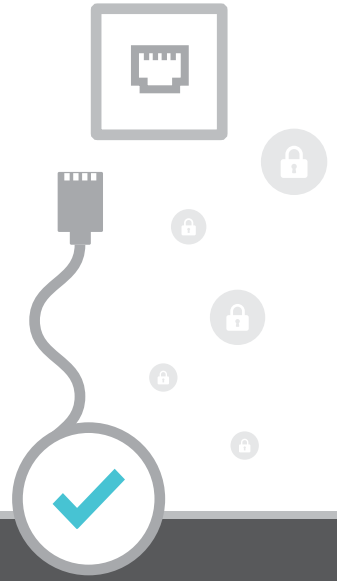
Top 5 Misconceptions of IoT Network and Device Security

01

Misconception 1:

Why would I care about the type of device that connects to the network? Someone has already approved it!

IoT devices seem to get all-access passes to corporate networks due to the assumption that they can bring no harm to your network.



FACT:

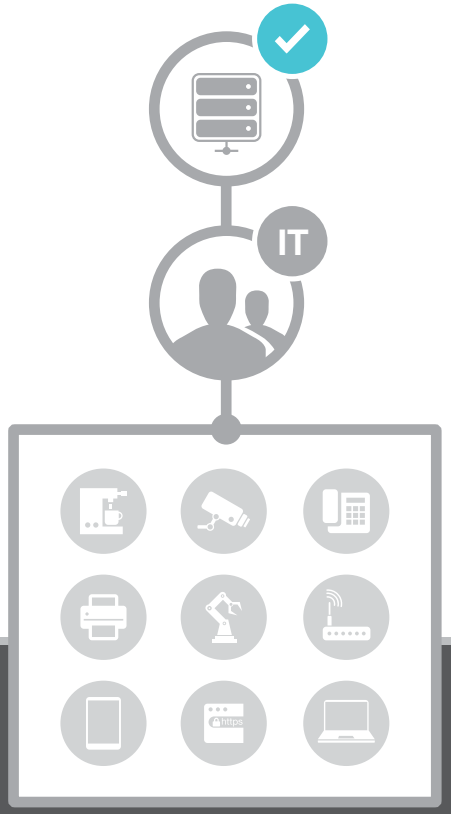
What users fail to comprehend is that IoT devices are possibly the weakest point in the corporate network. When an IP connects to an internet forum that's okay, but when that IP is an IP security camera, it probably means that, that IP security camera is compromised.

02

Misconception 2:

Only IT teams connect IoT devices to the corporate network

The notion that ONLY IT teams connect IoT devices to the organizational network doesn't reflect our reality.



FACT:

In reality, there are many instances where an employee can connect their own device to the corporate network without it being cleared by IT. For instance, a doctor might bring a medical device to help him better diagnose his patients, he just plugs the device into the hospital network and uses it. Since IT never checked its security settings, the hospital network becomes susceptible to malicious activity, such as the theft of patients' medical records.

03

Misconception 3:

If it's a hardware device – it's secure!

On-prem appliances provide security teams with a false sense that they are safer than other software-based solutions.

FACT:

The truth of the matter is that once appliances leave the vendor, regular firmware patch updates are required. Appliances that have not been vigilantly updated with the latest firmware patch expose corporate networks to security risks.

04

Misconception 4:

It's ok to connect your point of sales (POS), PC and IP Security camera on the same network segment

What can potentially go wrong? It's convenient and easy to define. There shouldn't be any issues from a security stand point. Right? Wrong!

FACT:

Since IoT devices are your weakest link, putting them on the same network segment as other devices, you not only put them at risk, you also make the hacker's job much easier.

The DYN Attack (2016)

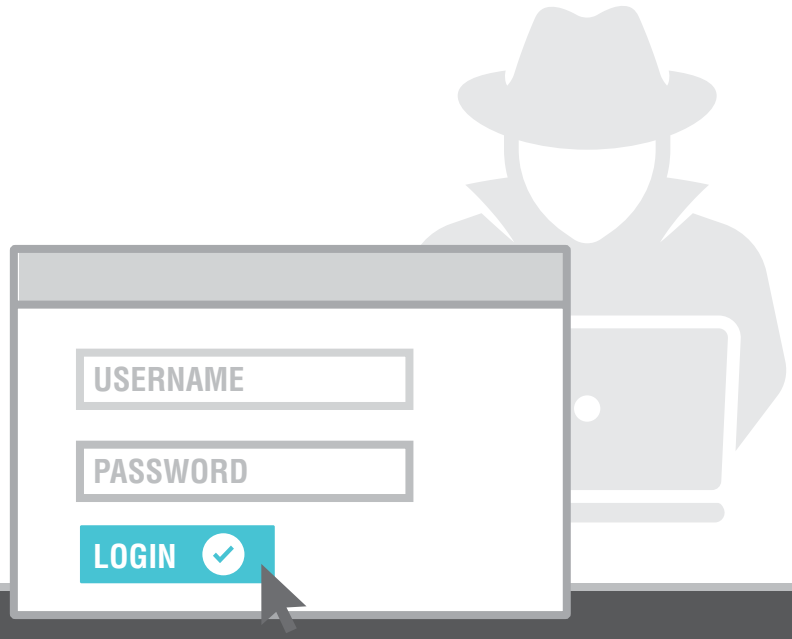
Multiple targeted DDoS attacks caused internet platforms and services, operated by DNS provider Dyn, to be unavailable. The attack was executed through a botnet consisting of a large number of internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai virus. With an estimated throughput of 1.2 terabytes per second, the attack is, according to experts, the largest DDoS attack ever on record.

05

Misconception 5:

If it's up and running, it's good to go!

Another common misconception is that if a device is working on default configuration, then that is enough. For example, setting up an IP camera on the network without first changing the default password.



FACT:

This default configuration poses a significant threat by exposing the device to attacks from other unsecured devices. Failing to change the default settings on an IoT device can allow a hacker to remotely execute malicious code, spy on users, break devices, or recruit them into a DDoS botnet through a known backdoor. Most users do not bother to change factory default usernames and passwords, making the hackers' lives much easier.

Building a Secure Foundation for IoT

While the trend of IoT devices may be a game changer in many respects, from a security perspective the game changes little. At its most basic level, security for the Internet of Things depends on our ability to see devices in the corporate network and control them.

All the above misconceptions can be easily remedied with Portnox next generation Network Access Control, Visibility and Management solutions that enables security teams to:

- **See** – 100% real-time actionable visibility. See all of your IoT devices with a centralized and agentless approach that is infrastructure vendor agnostic.
- **Control** – Segment your network and automatically sort IoT devices according to type or group. Mitigate risks by limiting access, placing in quarantine or blocking an infected device to immediately remediate security issues.
- **Automate** – delivering unique automatic actions, enabling security teams to reduce time and cost associated with manual responses.

About Portnox

Portnox protects the network from vulnerabilities that result from IoT and the use of authorized and unauthorized devices, giving full visibility into devices within the network as the foundation. On top of that, Portnox offerings deliver control, prevention, enforcement and management of activities for any user, any device, any network, anywhere.

Contact Us

Americas: usinfo@portnox.com | 1.855.476.7866 • **Europe:** dotell@portnox.com | (44) 1273.256325

www.portnox.com

portnox™