portnox™

IoT Security Vulnerabilities: Hype or the Real Deal?

Jan 26,2017

IoT is already impacting the way we communicate and do business. This trend is expected to continue according to Business Insider – their forecast for IoT devices connected to the web lies currently at 34 billion by 2020. IoT is expected to enable business growth by lowering operations cost, increasing productivity and opening new markets with new offerings and developments. But at what risk? Hackers are already using IoT devices for their malicious purposes in multiple types of attacks on networks and servers. DSL and bot attacks in 2016 have proven that there is no shortage of opportunities hackers are willing to exploit.

It's difficult to protect your network against threats that you cannot see. IoT devices entail a hidden aspect of networking, and can connect as a gateway into your infrastructure. This means that once an infected device is attached to your network, it automatically creates a security breach, making IoT device management and network security management even more difficult.

The variety of IoT devices and their widespread adoption make it difficult to distill them into one ecosystem. The numerous networks available for connecting these devices- wired,wireless, cellular and internet – only add another layer of complexity to an already complex system. Strengthening the security measures on premises is no longer enough.

Advanced persistent threats (APTs) are particularly successful when establishing continuous remote access to the network for accessing data, as the distance reduces the risk of detection.

IoT Vulnerabilities call for a Holistic Security Approach

The security vulnerabilities we are all exposed to because of the growth of IoT devices are varied and intricate . IoT devices entail innovative developments, introducing new firmware and operating system technologies into the market at an astounding pace. These innovations bring with them new risks and security weak links, at an unprecedented rate, that businesses cannot afford to underestimate.

A need for controlling access of devices into the network, as well as full visibility of the actions devices and users take once they have entered the network, has emerged. Traditional security solutions such as firewalls and antiviruses simply don't do the trick for IoT devices. Hardware patches on the fly are time consuming and deemed irrelevant. A holistic approach to network security is required.

With BOYD and BOYN driving the fast growing quantities of IoT devices, threats can come from anywhere at any time. It's almost impossible to stop employees from connecting IoT devices to the corporate network (for business and for pleasure), as the convenience of such use far outweighs their awareness to network security. That is why Network Access Control (NAC) is making a comeback as a critical component of business infrastructure. Securing your corporate networks form IoT devices needs to take a preventative form as opposed to reactive. A layered approach to network security, with policies to deal with access as well as segmentation of the network, is called for.

NAC is the best solution for IoT Security

Next Gen NAC can control and manage any attempted access and monitor activities on corporate networks whether they are spread on various servers or located on the cloud. NAC on the cloud provides security teams with real-time visibility of what exactly is going on in their networks without the encumbrance of heavy installments and complex configurations.

NAC speaks to each device separately, authenticates it – no matter what type of device it is – and blocks an untrusted device or user trying to enter the network, while alerting the security team of the attempted breach.

The new security paradigm requires managing, monitoring and securing an interconnected and broad set of applications, networks and devices, some of which we

cannot even yet foresee. CISOs and Network Security Administrators should be prepared for emerging devices in an ever changing ecosystem. The increased complexities and IoT vulnerabilities should not be overlooked. NAC is the best all-round solution that can simplify the daunting security task and help mitigate the risks.

So are IoT security vulnerabilities the real deal? Absolutely! No hype, only genuine need for businesses to protect themselves. Is protection really possible? Absolutely. It always has been, by going back to the basics of protecting the network in a layered approach using Next Gen Network Access Control.

Get Your Free IoT Security Risk Assessment With Portnox

Ofer Amitai

CEO

Categories

IoT

Network Security

Our Technology

Threat Detection and Response

Network Access Management