ENTERPRISE integration

armis

"Partners in IOT Security"

IoT Security – The Age of the Unmanaged Device

By Nadir Izrael

The Internet of Things (IoT) is upon us. And the experts say it is going to be huge. Some say it will be bigger than the Internet in the 1990s, bigger than the PC, and even bigger than mobile. It will have a global impact on how we live and conduct business improving how we connect, collaborate, create, and deliver services from the digital workplace to healthcare to energy to manufacturing and even how we practice law.

At the core will be these new IoT devices such as smart devices, TVs, printers, VOIP phones, wireless peripherals, business collaboration systems, HVAC systems, lighting systems, security systems, jet engine components, oil rig drills, manufacturing systems, medical devices and more. Eight billion today, growing to 20+ billion by 2020, according to Gartner. We are way beyond BYOD.

Connectivity First. Security Second.
But there is a challenge. With the new IoT age, it is connectivity first – security second. This is true for manufacturers, consumers, and businesses alike. The focus is on getting the device, hooking it up, and establishing connectivity. Security takes a back seat. Whether this is an employee bringing in a device, or new connected devices being installed by operations or facilities, IT and security are too often not aware or involved to ask crucial architectural questions. In May 2017, McKinsey reported that security issues\represent the greatest obstacle to growth of the IoT – and its potential.

The Security Blind Spot
These new devices bring three challenges to businesses and security professionals:

No. 1 Designed to Connect. IoT devices are designed to connect. In many cases, they are actively seeking connections, whether you want them to or not. Which means attackers can search, find, and attempt to connect to these devices anytime. And you won't even know about it.

No. 2 They May Be Invisible. In many cases, IoT devices may not be connecting to the corporate wireless or wired network. This effectively renders them, and the connections they make, invisible to businesses. In such a situation, traditional network access control and networking solutions cannot see the device or the connection. And in this case, you truly cannot manage what you cannot see.

No. 3 They Are the New Attack Vector. With the Mirai attack in October of 2016, millions of IoT devices were easily and remotely compromised, creating the largest, and most coordinated IoT exploitation to date. It impacted companies globally, including Amazon.com, Airbnb, Netflix, and many others. The attack preyed on IP printers, cameras, DVRs, etc., and created a massive distributed denial of service (DDoS) attack. One of the critical take aways often missed in reporting on Mirai, was that hundreds of companies had devices in their environments compromised – and they never knew. And that latest (not)Petya ransomware attack now unmanaged devices like ATMs and Point of Sale machines. And June 2017 out of the UK reported that 92 percent of attacks against businesses were targeting IoT devices. These new devices are being preyed upon.

Real Situations – Real Consequences
The fact is that in our research, we have found that businesses do not see 40 perecent of the devices in their

environment. That number is way too high. Here is a short list of what we have discovered.

No. 1 Compromised Devices
- Tablet streaming video from the board room to an unknown outside location.
- Infected heart monitor providing incorrect patient data and trying to infect other medical devices.
- Security cameras and routers on the network that are compromised and part of a botnet.

No. 2 Unmanaged Devices
- Smart TV with exploitable vulnerability compromising devices that connect to it.
- Automotive plant assembly line with quality control sensors accessible wirelessly without notification.
- Printer with open hotspot that allows hackers to circumvent network access control.

No. 3 Uncontrolled Networks
- Outside network is bridged to corporate LAN via corporate desktop.
- Credentials being stolen due to corporate laptop connected to a rogue network.
- Open network exploited by malicious devices in order to attack corporate devices.

The Traditional Approaches and The Unmanaged Device
These new IoT devices are effectively unmanaged devices – as are many devices in your environment today. You can't manage them or secure them in the ways we have done with our servers, laptops, and mobile devices. This means they are defenseless in this new age. For those devices that do have user IDs or passwords, too many have default credentials that are never changed or simple easily-exploited log in's. Not to mention, the user interfaces are so seriously lacking to make security practical.

These are the challenges with the current approaches:
- **Endpoint Protection** – This won't work because most devices cannot host an agent. So it is a non-starter.
- **Firmware Updates** – Many IoT devices do not have a simple method for automated firmware updates.
- **Mobile Data Management (MDM)** – These devices might be smartphones or other mobile devices. However, as we have seen, MDM solutions are costly and require administration as well as compliance. And it doesn't address a large volume of devices brought in by visitors, contractors, delivery people, and others.
- **Network Solutions** – These typically only see the unmanaged or IoT device when it is connected to the network. Devices that are off the network with a wireless connection to a rogue or shadow network are invisible. They are unstoppable via current network access controls.
- **802.1x** – This will not address devices that cannot have certificates (e.g. a printer). Even if 802.1x solutions whitelist IoT devices, they do not address situations where a third-party device is masquerading as a privileged device. Or worse, they are blind to an infected or compromised device that still has access privileges.

Three Critical Needs
To be effective today, an IoT security solution needs to have three critical things to protect the business information.

Discover
This critical first step is not as simple as it seems. We talk to CISOs everyday who just want to know how many devices, managed and unmanaged, are in their environments. Visibility is the key first step, as you need to be able to identify and report on the devices coming in and out of your environment – even across local and remote offices. The sheer magnitude of IoT and Internet connected devices means IT cannot tag and manage all of them manually.

ENTERPRISE integration

armis

"Partners in IOT Security"

Profile
Seeing the devices is a first step, but not enough. Businesses need to be able to profile or fingerprint the device, whether it be a Smart TV, Amazon Echo, wireless printer, smart phone, NEST or closed-circuit security camera. You need to know how it is behaving, and if it is behaving properly. These new devices only have a few functions and need a certain number of connections. So, when they act outside of their normal or expected behavior, you need to be alerted.

Sanction
These new devices offer the promise of efficiency and productivity. So, you want to be able to let them into your workplace, but in a safe manner. Any IoT security solution should also let you remove any device in question from connecting to your networks or even your approved devices from connecting to unapproved networks. This should be able to be done manually or automatically.

From the advent of the PC, to the Internet, to mobile devices, to the cloud, history is a clear guide for us. With every technological advance and device, there are new security risks. Those new security risks are real, especially with the advent of these new IoT and unmanaged devices. Designed to connect in an ever-increasing wireless world, many of these devices are not built with security in mind.

Now is the time for businesses and security professionals to include IoT security as a part of their comprehensive cyber-security strategy. Compliance and internal audits are identifying IoT devices as a point of vulnerability. Businesses need to be able to see and control any IoT devices in their environment.

Chief Technology Officer Nadir Izrael has been in the cyber security space for 10 years. He guides the technology vision behind Armis to address the growing managed and unmanaged devices in today's enterprises. Previously senior software engineer at Google.