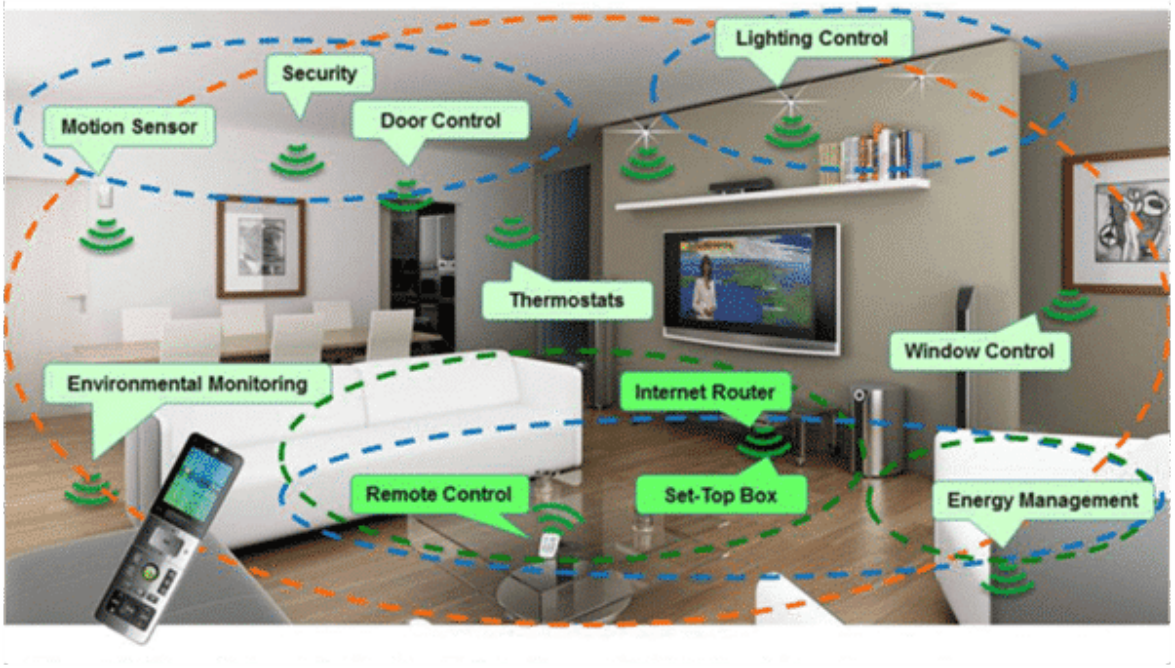

Protecting Your Digital Life In The Age Of IoT

Unless specifically demonstrated otherwise, you should assume that every electronic device in your home is capable of ratting on you in one form or another. Here are some steps that can protect you. TN Editor

The Internet of Things (IoT) device universe is expanding. This statement echoes for the fifth year in a row—only the numbers change as they grow bigger. Indeed, as the universe of IoT devices grows, so do the dangers they bring. With Gartner's predicted 20 billion IoT devices by 2020 and 25 billion by 2021 comes not only lack of certification for IoT security (ISO/IEC 27030 is still in draft version and there are no clear dates when it can be released) but also real dangers right now from interconnected, insecurely designed, and not properly updated and maintained IoT.

Such constant expansion clearly demonstrates the attitude of those who participate in the IoT market. New models are introduced with shiny new functionality, but secure design, and extensive quality assurance and testing remain low on the priority list.

17 entry points to a connected home

Each new component added to the network poses a new possible risk and widens the attack surface for each household. This attack area for households is already large. On average, there are 17 devices connected to the internet for a single household, including computers, phones, gaming consoles, smart TVs, watches, cameras, NAS devices, printers, and thermostats.

This means every household has 17 devices on average that are:

- Collecting your private data
- Sending your private data for further analysis to the cloud
- Serving as a possible entry point to the network
- Disrupting internet services by participating in DDoS (distributed denial of service) attacks

Our data shows that almost 43 percent of devices are using an operating system (OS) that is no longer supported. This does not mean immediate danger and exploitability because of differentiating OS lifecycles, but it does suggest a huge number of interconnected devices out there that are possibly no longer maintained by vendors, though they still exist in the local network as part of a device base. Even if we approximate that no more than a quarter of these devices are really vulnerable, that's an impressive 10 percent of the overall device universe left to be exploited, posing real danger.

The risks posed by rogue devices

The most dangerous scenarios point toward devices that are unsupported, discontinued, or no longer maintained. They might still be storing sensitive user data after they are left connected to the internet with their ports forwarded.

Remote access attempts executed by malicious outsiders or host discovery scanners and unauthorized attempts to access the open port make up more than 65 percent of overall suspicious and malicious activities registered daily. Based on CUJO AI data attempts to check open ports or scan for possible vulnerabilities, this kind of activity

happens at least 10 times a day per household. Apart from the direct danger to sensitive user data, no longer used and forgotten devices can serve as a trampoline or proxy inside the local network.

Other typical scenarios include leaving default credentials when connecting the device to the network. Given that IoT device configuration is often too complex or there's no way to change the default built-in credentials, this is usually left "for later" and never done at all. The same considerations come with vulnerability patching and firmware updates.

IoT devices were often overlooked as minuscule, unimportant details of the overall network. This view has changed completely after the initial Mirai botnet attack. Hundreds of thousands of low calculating power devices can be coordinated together to unleash a huge, volumetric DDoS attack.

And there are several considerations when talking about IoT device security and protection:

- How to protect them on the perimeter?
- How to protect devices inside the network?
- How to distinguish legitimate device behavior from malicious?
- How to protect the device that is no longer maintained by the vendor itself?

What can be done to secure the home?

With the evolution of a chaotic IoT device market, new problems arise. How do you deal with the massive amount of discontinued and possibly no longer used devices still connected to the network and partially alive in zombie mode?

Cloud services used by such devices can be no longer available, patches are no longer released, and the manufacturer has shifted to a different type of product. And this problem will become more and more relevant with the practically unregulated expansion of the IoT device market. Parts of the internet become an interconnected landfill.

How to minimize the impact?

- Monitor your household by identifying what devices are in your network. Review them occasionally to dismiss ones that are no longer used, thus decreasing the attack surface for your home network.
- Change the default credentials, especially for IoT devices. Secure them with strong passwords according to the latest recommendations.
- Deploy protection to the edge of the home network to disallow malicious outsiders access to your inner network while at the same time disallowing your devices from participating in illegal activities or communicating with malicious nodes.
- Utilize security solutions driven by artificial intelligence that are capable of proactive protection for deterministic IoT devices by analyzing their behavior and determining typical vs anomalous behavior.

Read full story here…