IoT: Internet of Things or Internet of Threats?

When we talk about interconnection, we usually think in terms of computers, tablets and smartphones. The Internet of Things (IoT) describes a world where just about anything can be connected and communicate in a "smart mode" by combining simple data to produce usable intelligence. With the IoT, the physical world is becoming one big information system with the ultimate goal of improving quality of life and empowering new business models.

However, this also means that more personal information and business data will reside in the cloud and be exchanged between thousands of devices that may have exploitable vulnerabilities. One weak link in the security chain could provide hackers with nearly limitless doorways that could be unlocked and lead to sensitive information.

Currently, more things are connected to the Internet than people. According to Gartner, there are approximately 6.4 billion connected devices in use worldwide in 2016, and that number is slated to reach 20.8 billion by 2020[1]. In this quickly evolving world, all the things that connect to the Internet are exponentially expanding that attack surface for hackers. An HP study shows that 70 percent of IoT devices contain serious vulnerabilities[2]. There is undeniable evidence that our dependence on interconnected technology is defeating our ability to secure it.

Security executive agree. Radware conducted a survey of more than 200 C-level security executives from the U.S. and United Kingdom with the goal of understanding their greatest challenges, threats and opportunities when it comes to information security. In Radware's *Security and the C-Suite: Threats and Opportunities*, respondents clearly identified the Internet of Things as one of their top security concerns. Thirty-three percent of executives in the U.S and 29% in the U.K. cited it as an "extremely likely" target in the next three to five years.

1 http://www.gartner.com/newsroom/id/3165317
2 http://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.V6NU_ywm7IW

Two sides to the IoT security coin.

The Internet of Things includes a vast and ever-growing array of networked devices—including smart meters used by utilities, medical devices for monitoring patients' conditions and delivering care, as well as sensors that do everything from supporting public safety to automating manufacturing processes. When it comes to security and the IoT, executives face a two-part dilemma.

The first is mitigating the risk of vulnerabilities created or compounded by networked devices. Organizations must consider the possibility of a huge increase in unknown vulnerabilities at the device level, as most lack antivirus or advanced endpoint and threat detection capabilities. While sensors and other IoT devices can fuel exponential improvements in speed, accuracy and efficiency of information collection, they also can make a business vulnerable to intrusions and attacks. Even a company's network carrier can be affected if attackers use IoT devices to generate massive spikes in network traffic.

The other side of the IoT security dilemma is being protected from devices—that is, addressing the risk of the "things" themselves becoming vehicles for an attack. For example, in the past utility customers may have worried that a meter reader would forget to close a back gate, leaving the house unsecure. These days, they want assurance that they're not letting a nefarious robot into their homes—putting data privacy and personal safety in jeopardy. On a broader scale, hackers could potentially take control of thousands of smart meters, wreaking havoc on the electrical grid.

Healthcare is another area where vulnerabilities could be devastating. Imagine a patient receiving an email threatening to alter his or her pacemaker's performance unless a ransom payment is made. It may sound far-fetched, but healthcare has become a frequent target. Already, numerous attacks have blocked hospitals' and other providers' access to their own data. Networked medical devices provide another potential avenue for such schemes.

'Fingerprinting' devices

With the advent of billions of non-traditional IT devices, accurate device identification will simultaneously become more important and more difficult. The primary tool that has long been used for device and user identification—namely, IP addresses—is rapidly declining in its security value.

Dynamic IP addresses, global Network Address Translation (NAT) and anonymous proxies are just a few of the tools out there that are making the connection of IP address and device or user very hazy.

One potential solution is device fingerprinting—a rapidly growing technology that employs various tools and methodologies to gather IP-agnostic information about the source, including running a JavaScript on the client side. The device fingerprint uniquely identifies a web tool entity by combining dozens of attributes of a user's device to identify and then track activities, generating a behavioral and reputational profile of the user.

Mitigating the threat of ‘things’.

Regardless of an organization’s interests around the IoT, the time has arrived to start taking proactive steps to ensure security. In the end, the full vision of the IoT may or may not come to pass, or it may take longer than some predict. What is undeniable is that connectivity is exploding. While most people may be unaware of how the IoT functions, they will expect it to be secure. Similarly, they will be largely clueless to the potential impact they (and their new gadgets) have on the threat landscape, and thus cannot be relied upon to maintain security capabilities on these devices. As a result, the burden of protecting organizations from the possible wave of new, larger threats falls to the security operations teams.

Learn More at DDoS Warriors

To know more about today’s attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.