Changing Cybersecurity Threats in the Context of the Internet of Things: Don't Blink or You'll Miss It

10 July 2017

In this hoganlovells.com interview, Washington, D.C.-based Hogan Lovells senior associate Paul Otto talks about security issues created by the exponential growth of the Internet of Things (IoT).

Can you start by giving us an overview of cybersecurity threats in the context of the IoT?

Otto: To start, it's helpful to understand the broader landscape and the threats involved in the IoT space. First, the number of connected devices has been proliferating at an extraordinary pace and is expected to eclipse the total U.S. population this year. That growth is explosive and exponential.

Consequently, there has been a corresponding uptick in the number of IoT-focused attacks. The number of vulnerabilities affecting software and hardware has risen at a similar speed. All of that combines to create a dynamic, difficult, and evolving landscape for cyber threats.

It is important for organizations' risk management and incident response processes to include consideration of the threats, actors, and motivations, as well as the nature of cyberattacks that may occur for internet-connected devices.

Are there any patterns developing in terms those responsible for threats?

Otto: There has been a range of attackers and threat actors, motivated by a variety of rationales. They have sought to compromise devices, to repurpose them for their own gain, or any number of other motivations. They may be targeting the confidentiality or integrity of data or the device or the availability of the product or service. Those attacks have begun to proliferate in the IoT space.

In addition, over the last year there has been an uptick in ransomware attacks, which are typically financially motivated and target data by locking it away. Those attacks may have a significant impact on IoT as numerous devices and corresponding services are taken down.

Against that backdrop and based on numerous industry reports, it remains the case that external actors are the primary threat and the source of the majority of attacks. This is an important distinction, because IoT-connected devices less frequently have the full benefit of enterprise network protection, as would an organization's servers and systems.

And what about the threats themselves? Any general or industry-specific patterns?

Otto: The U.S. Government Accountability Office (GAO) recently outlined a number of types of cyberattacks that could affect IoT devices, and it's important to understand the types of attacks that may occur.

Typically, attackers begin with the controlling software — like a hack against software within devices or the app that that is the interface — and the resulting damage impacts functionality or can take the device offline completely.

IoT devices also are exposed to other types of attack, with potentially more devastating results. One common attack is denial of service, which seeks to compromise integrity of IoT devices to knock systems or services offline. That could compromise thousands — or even millions — of devices.

As for specific sectors, a recent development is a significant increase in the number of attacks focused on medical devices. It could be security researchers or more malicious third parties seeking to cause the device to cease functionality or cause the device to function differently. Of course in the case of a medical device, that may create a risk to patient safety. A frequent example we see is third parties purchasing devices on the secondhand market then seeking to identify vulnerabilities. They may inform a company in advance — then demonstrate the vulnerability. It takes time to walk through the patch-up process, meanwhile the researcher may be seeking to publish or profit from the results.

Does anything else complicate matters? How are manufacturers seeking to counter these attacks?

Otto: There are commonalities to these vulnerabilities and attacks in the IoT space. The sheer volume of devices and apps, achieved by the falling cost of adding connectivity, creates its own problems.

Conversely, devices are increasingly designed to minimize power consumption, which may be in tension with more advanced security protection. And the ability to patch vulnerabilities swiftly may become more difficult with the proliferation of these devices.

The shorter timescale of software development typically, with support provided by major vendors, even for some of the most complex software is in tension with a potentially much long deployment lifespan for devices.

Finally, the connection with and use of cloud infrastructure creates a much larger space for these attackers to operate in. Everyone involved in the IoT is well advised to consider secure cloud capabilities as much as secure device capabilities.

About Paul Otto

Paul Otto is a senior associate at Hogan Lovells who understands the regulatory environment surrounding cybersecurity risk management and incident response. Leveraging his technical background and capabilities in computer science and engineering, he brings insight to clients as a compliance counselor who understands hardware, software, and technological innovation.

Contacts

Paul Otto

Partner

> Read the full article online