WiNG

IoT Insecurity: A Clear And Present Danger For The Enterprise

OCTOBER 30, 2016 **PETER WAGNER**

The implications of an internet of insecure things were highlighted once again recently, when hackers leveraged tens of millions of IP addresses from a range of connected devices, including IP cameras, baby monitors, and home routers, to launch a massive Distributed Denial-of-Service attack on Dyn, a domain name systems service provider.

The attack, which temporarily slowed access to web services such as Twitter, Airbnb and media sites at companies such as CNN and the New York Times, is a stark reminder of why the Internet of Things is a big issue for enterprise security.

Billions of new devices are being connected to networks every year, and some of these, such as medical equipment and industrial control systems, are mission critical. They must be safeguarded. But it's equally important that the rest of the network be protected from this rising tide of "things". Even the most benign device can be an entry point into a corporate network, an enabler of lateral movement across it, or a means of extracting sensitive data from it.

Many of the devices being connected to networks have only rudimentary security and vulnerable operating systems (including a surprisingly large number with Windows XP!), and hackers are exploiting them to gain a foothold into companies' systems. Once inside, they can use their access to disrupt operations, steal money or exfiltrate sensitive data like intellectual property or financial information. Things like HVAC systems and retail point-of-sale terminals have already been involved in large-scale breaches, such as the one at Target.

So what can companies do to tackle this critical issue? The most effective solutions for mitigating IoT-related security risks will most likely have several characteristics.

Automation. This will rapidly become a requirement in order to deal with the large volume and variety of devices coming on to corporate networks. Various market forecasts suggest that by 2020,

anywhere from 50BN to 200BN things will be connected to the internet, so more traditional approaches will quickly be overwhelmed by this flood of devices and their myriad use cases.

Intelligence. The new security solutions will leverage machine-learning/artificial intelligence to uniquely identify devices, swiftly establish their "normal" behavior, and then spot deviations from these baselines.

Analytics. Enterprise security teams and network operators will need flexible, granular analysis capabilities to monitor network health, as well as track down potential threats fast.

Enforcement. Policy-based enforcement becomes a requirement at the scale IoT device populations will soon reach. This allows operators to protect their assets without having to manually configure and reconfigure underlying infrastructure.

Integration. New IoT-centric solutions must be integrated smoothly into existing security frameworks, and should leverage the capabilities of installed control points like switches, firewalls, and intrusion prevention/detection systems. Enterprises are looking for additional intelligence and control, but not a new shadow infrastructure to maintain.

Existing cybersecurity firms are developing IoT-focused offerings, and in some cases they will take the lead in helping companies to tackle this rapidly growing threat. But in other cases, the challenges will be distinctive enough that completely new approaches will be needed. Our recent Wing IoT Startup State of The Union study (http://wing.vc/blog/iot-startup-state-of-the-union-2016) found that relatively few young startups had been formed to date in the IoT security field. We expect to see more emerge here as the magnitude of the risks associated with IoT devices becomes clearer.

Failure to address these risks effectively could have serious consequences. IDC has forecast that by 2018 around two-thirds of enterprises will have been the victim of some kind of IoT-related security breach. As we noted above, hackers will use their access to steal data and money. But looking ahead, the development of smart cities and infrastructure mean that, in the absence of adequate security, cyber attackers could also take control of physical things such as power grids and building elevators, potentially putting lives at risk.

The Internet of Things is delivering huge benefits to the enterprise, both in terms of boosting efficiency and creating new revenue streams. But it's also taking us into a new era in which IoT-

related vulnerabilities are multiplying fast. Security can no longer be an afterthought. It’s time for fresh thinking about how smart devices can be protected—and about how we can be protected from them.

---

http://wing.vc/blog/iot-insecurity-a-clear-present-danger-for-the-enterprise
© 1990 — 2018 Wing, Menlo Park, CA