Published on *The National Law Review* https://natlawreview.com

NIST Issues Internet of Things (IoT) Guidance

Article By:

Privacy & Security Practice Group at Mintz Levin

Smart machines connected to the internet have become ubiquitous in our daily lives. They make up the ***Internet of Things ("IoT")***, a vast web of interconnected iPhones and Fitbits, tablets and cameras, even baby monitors and implantable medical devices, and all are designed to improve and enrich our lives. The IoT is growing in scale and complexity every day, and so too are the dangers to consumers, businesses, and our country's technical infrastructure that the IoT creates.

After four years of research and collaboration with stakeholders, the ***National Institute of Standards and Technology ("NIST")*** recently released its final version of Special Publication 800-160 to provide much-needed guidance for securing IoT devices and systems throughout their entire life cycle. We offer this quick introduction and encourage you and your organization to get acquainted with the report.

What is all the fuss about?

The NIST released Special Publication 800-160 earlier than expected as a result of the highly publicized attack on Dyn Inc. last month. On October 21st, Dyn, whose domain name services facilitate traffic on the internet, experienced multiple Distributed Denial of Service ("DDoS") attacks caused by internet-enabled devices that had been infected with a form of malware allowing hackers to hijack great numbers of these devices simultaneously and flood Dyn's servers with bogus service requests. Dyn was ultimately able to mitigate the attacks but not before access to marquee websites such as Twitter, Spotify and the New York Times had been interrupted for hours at a time. This incident served as a glaring example of the susceptibility of the IoT and how it can be turned into a weapon capable of being deployed against the internet's critical infrastructure.

Not to mention some of the numbers! Researchers are predicting that the quantity of devices connected to the internet will rise from 6 billion presently to 20 billion by 2020, and some market analysts are forecasting global commerce related to the IoT market to be in the range of $1.7 trillion by that same year. With this magnitude of growth expected over the next few years it is even more crucial that we address the security risks linked to the IoT as early and as quickly as possible.

What does the NIST say about protecting the IoT?

Special Publication 800-160 emphasizes the vulnerability of devices that rely on post-manufacture

features such as firewalls, encryption and systems monitoring to ward off evolving and sophisticated cyber threats. Instead, the NIST encourages commercial and government technology developers to focus on simplifying design architecture and building out functional capability to counter threats, mitigate damage, and recover quickly from successful attacks.

The guidance highlights engineering-based solutions and includes a range of technical standards and security principles to consider over the full life cycle of a product or system, including the development phase, upgrades and maintenance, and during retirement. This life cycle approach is intended to ensure that the IoT remains secure and that intellectual property and consumer personal data are also protected.

Who else is taking this seriously?

There has been a recent flurry of activity from government to address threats to the IoT. The Department of Homeland Security also released a set of guidelines for securing smart devices that reinforces a “security-by-design” model, and Congress conducted a joint hearing of two House Energy and Commerce subcommittees to investigate the nature and impact of recent DDoS attacks on the internet. The president-elect has promised to do a comprehensive review of the country’s cyber profile and to develop enhanced defensive and offensive capabilities to address internet-based threats to our economy and national security.

Government is paying attention to the IoT as should industry stakeholders and consumers alike. Unfortunately manufacturers are focused on developing sleek and affordable devices and are unlikely to prioritize security features unless regulators and their customers demand that the products and systems they use are responsibly designed and safe to plug in to the IoT.

©1994-2025 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. All Rights Reserved.

National Law Review, Volume VI, Number 334

Source URL:https://natlawreview.com/article/nist-issues-internet-things-iot-guidance