Securing the internet of things

In the era of mission-critical IoT, federal network security begins with visibility

Niels Jensen
Senior Vice President of Americas Sales, ForeScout Technologies

FEDERAL AGENCIES INCREASINGLY depend on a wide array of connected devices – including sensors, controllers, motors and even weapons systems – to support their missions. The Census Bureau relies on connected handhelds for the decennial population count, the Department of Veterans Affairs relies on networked hospital equipment, federal buildings rely on ID card readers, and so on.

Those devices have limitless potential to improve operational efficiencies and safety in the delivery of government services. But in this era of connected "things," agencies must evolve their cybersecurity strategies to account for this fundamental change in their network infrastructures.

The scale of the problem

Securing what are typically referred to as internet of things (IoT) devices is challenging because most were not designed with security in mind. They often cannot support features such as password protection or encryption. Yet the biggest security challenge is detecting the devices in the first place.

IoT devices cannot be readily identified by traditional cybersecurity tools because they generally do not support an agent – a small piece of software on PCs and mobile devices that allows them to be scanned for malware and vulnerabilities.

How big is the problem? In its early phases, the Department of Homeland Security's Continuous Diagnostics and Mitigation program detected 75 percent more devices on federal civilian networks than were previously known. Discovering that networks are 75 percent larger than expected represents a massive visibility gap. Unknown, unmanaged infrastructure on this scale creates huge risks for agencies.

Closing the visibility gap

Administrators need tools that allow them to automatically and agentlessly detect, profile and enforce policy-based controls on connecting devices. With a consolidated view across the network, agencies can automatically detect legacy systems as well as new IoT devices, classify everything according to function and criticality, and assess the security posture of the devices. The government's two major cybersecurity programs – CDM and the Defense Department's Comply to Connect – are premised on real-time diagnostics, remediation and risk reduction. The first and most foundational step of those two programs is complete asset visibility.

In addition to improving security, such visibility can create major efficiencies. It allows managers to reassign anyone tasked with asset inventory (who today walks around with a pen and clipboard) to higher-order tasks. Combined with automation and orchestration between security tools, it allows agencies to comply

davooda/Shutterstock/GCN Staff

As daunting a security challenge as IoT is, the government **must address it smarter and faster** than it has any cybersecurity challenge before it.

with mandates in near-real time. Meeting requirements such as those in the Federal Information Security Management Act, Command Cyber Readiness Inspections, Binding Operational Directives and even the Federal IT Acquisition Reform Act will soon no longer take the form of a "snapshot" or audit. It will represent a continuous state.

Connected devices enhance agencies' missions in innumerable and essential ways. Yet they also create a vastly larger threat surface and introduce complexity into agencies' IT networks. DOD and civilian agencies must remain committed to "cyber basics" while pursuing newer technologies, such as agentless asset discovery, to adapt to fast-changing IT landscapes. They must make securing IoT devices part of their risk mitigation strategies and demand the same of contractors and suppliers.

As daunting a security challenge as IoT is, the government must address it smarter and faster than it has any cybersecurity challenge before it. Its citizen customers are counting on it. ■

Niels Jensen *is senior vice president of Americas sales at ForeScout Technologies.*